

Enhancing transparency and compliance in alternative assets: a blockchain solution for fine art and real estate

Claudia Giannoni

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
of
University College London.

Institute of Finance and Technology
University College London

July 16, 2025

I, Claudia Giannoni, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

*To my husband, Budha,
without whom I would have never undertaken
this fantastic journey.*

*Your unwavering support and belief in me
carried me through every step. I owe this milestone to you.*

Abstract

The growth of alternative investment has been considerable in recent years, with alternative assets becoming a significant portion of investors' portfolios. Real estate and fine art represent a significant market share among alternative assets. Statistics show that transactions in the global art market amounted to 65.1 billion U.S. dollars in 2021 [1, 2]. Similarly, real estate is considered a valuable component of an investor's portfolio. Between 2016 and 2021, the global real estate investment management sector almost doubled, reaching approximately 5.16 trillion U.S. dollars in aggregate assets [3]. Unfortunately, fine art and real estate are attractive sectors for money laundering. The main reasons are the large monetary transactions involved, the potential for high-value assets, and the relative ease of disguising the true ownership and value of properties or artworks. A study identifying the most common methods of money laundering [4] confirms that antiquities, art, and real estate projects are particularly exposed to these criminal activities.

Blockchain (BC) is a digital technology that has gained traction in multiple industries. Although its popularity is mainly linked to cryptocurrencies such as Bitcoin and Ethereum, blockchain has multiple other applications. Thanks to blockchain, ownership and transaction history can be securely stored, increasing transparency and accountability. While existing blockchain solutions narrow the scope to specific business problems, this applied research takes a more holistic approach. Our purpose is to increase transparency and help combat money laundering in fine art and real estate to benefit society. The research explores the creation of the first blockchain registry for fine art and real estate. This blockchain ecosystem

dramatically enhances due diligence and increases transparency without compromising privacy and confidentiality. Starting with proof of concept of crucial features to increase accountability, we then design two hypotheses (for a permissioned and public blockchain). The system focuses on increasing data reliability through endorsement mechanisms and maintaining privacy while allowing increased transparency. This study was selected by UCL Innovation and Enterprise, which funded the development of an MVP (Minimum Viable Product).

Impact statement

The increased relevance of alternative assets in global investment portfolios has highlighted the importance of fine art and real estate as significant investment sectors. However, the inherent opacity of these markets makes them attractive targets for money laundering. My research, "Enhancing Transparency and Compliance in Alternative Assets: A Blockchain Solution for Fine Art and Real Estate", aims to address this problem by developing a blockchain-based framework to improve due diligence, enhance transparency, and mitigate financial crime risks in these industries.

This study makes a significant contribution to the advancement of transparency and regulatory compliance in the fine art and real estate industry. By developing a blockchain registry specifically designed for these sectors, the research addresses a critical literature gap and proposes a robust framework to improve due diligence processes. The novel blockchain solution presented in this thesis leverages public and permissioned blockchain structures, integrating endorsement mechanisms and zero-knowledge proofs (ZKPs) to ensure both transparency and privacy. The framework allows for secure provenance tracking, ownership verification, and transaction authentication, offering an innovative approach to combating financial crimes such as money laundering in fine art and real estate. This work has implications for financial institutions and regulatory bodies, as it provides a scalable model that streamlines compliance verification. The proposed system enhances the reliability of asset information while maintaining the confidentiality of stakeholders, creating a balanced and efficient approach to compliance, risk management and privacy.

Furthermore, by establishing a link between blockchain technology and regulatory practices, this study contributes to academic discourse on financial security and to the practical implementation of digital solutions in high value asset markets.

The impact of this research has been acknowledged in legal and financial circles. Selected aspects have been included in *Artificial Intelligence: Law and Regulation* (Kerrigan, C. ed., 2022, Edward Elgar Publishing, emphasizing its relevance to AI governance and regulatory frameworks. It was also presented at the *Sustainable and Impact Investments International Conference* in November 2023 and selected for publication in *Palgrave Studies in Impact Finance*, demonstrating its influence in shaping contemporary discussions on financial regulation and innovation. Beyond academic and theoretical contributions, the proposed blockchain solution was selected by UCL Innovation and Enterprise, which provided funding to develop a Minimum Viable Product (MVP), strengthening the feasibility and industry relevance of the designed framework.

This novel blockchain-based registry has the potential to improve transparency, reduce the risk of illicit transactions, and improve operational efficiency in asset verification. It also fosters investor confidence while ensuring privacy through permissioned blockchain networks and ZKPs. Positioned at the intersection of finance, law, and technology, this thesis offers a transformative approach to preventing financial crime in alternative assets. Its recognition by leading academic and industry platforms underscores its practical utility. Further development will pave the way for greater asset transparency and regulatory compliance.

UCL Research Paper Declaration Form

UCL Research Paper Declaration Form: referencing the doctoral candidate's own published work(s)

1. For a research manuscript that has already been published

(a) What is the title of the manuscript? *Artificial intelligence: Law and regulation*

(b) Please include a link to or doi for the work: ISBN: 978 1 80037 171 2
<http://dx.doi.org/10.4337/9781800371729>

(c) Where was the work published? UK

(d) Who published the work? Kerrigan, C.

(e) When was the work published? 2022

(f) List the manuscript's authors in the order they appear on the publication:

Chapter 20, Real estate. Alastair Moore, Claudia Giannoni, Nick Kirby and Nick Doffman

(g) Was the work peer-reviewed? Yes

(h) Have you retained the copyright? No

(i) Was an earlier form of the manuscript uploaded to a preprint server (e.g. medRxiv)?
'No', please seek permission from the relevant publisher and check the box next to the below statement:

I acknowledge permission of the publisher named under 1d to include in this thesis portions of the publication named as included in 1c.

2. For a research manuscript prepared for publication but that has not yet been published

(a) What is the current title of the manuscript?

1. Unlocking transparency: harnessing blockchain for anti-money laundering in alternative assets. The case of fine art and real estate
2. Blockchain technologies and art: opportunities and open challenges
3. Designing a threshold-based framework for automated money-laundering prevention in the fine arts market

(b) Has the manuscript been uploaded to a preprint server e.g. medRxiv' ?

Yes

1. SSRN-id4662355
2. SSRN-id4439318

3. N/A

(c) Where is the work intended to be published?

1. Palgrave Macmillan. Book series Palgrave Studies in Impact Finance.
2. Applied Sciences
3. BISE Business & Information System Engineering

(d) List the manuscript's authors in the intended authorship order:

1. Claudia Giannoni, Francesca Medda
2. Claudia Giannoni, Francesca Medda and Silvia Bartolucci
3. Claudia Giannoni and Johannes Sedlmeir

(e) Stage of publication:

1. Expected in 2025
2. Preparing for submission
3. Preparing for submission

3. For multi-authored work, please give a statement of contribution

1. Claudia Giannoni produced the work entirely, and Francesca Medda provided general guidance
2. Claudia Giannoni produced the work entirely, and Francesca Medda and Silvia Bartolucci provided general guidance
3. Claudia Giannoni conceptualized and structured the project, undertaking the majority of the work, while Johannes Sedlmeir was responsible for the technical verification.

4. In which chapter(s) of your thesis can this material be found?

1. and 2. In Chapter 3
3. in Chapter 5

e-Signatures confirming that the information above is accurate (this form should be co-signed by the supervisor/ senior author unless this is not appropriate, e.g. if the paper was a single-author work):

Candidate:  Date: 14/03/2025

Supervisor/Senior Author signature (where appropriate):

Date:

Acknowledgements

I am deeply grateful to my primary supervisor, Prof. Francesca Medda, for her invaluable guidance and unwavering support throughout my Ph.D. journey. I also thank my Ph.D. committee members, Dr. Hui Gong and Dr. Marios Samdanis, for taking an interest in my research, for their invaluable guidance, and constructive feedback. I express my deepest gratitude to UCL Innovation and Enterprise for providing funding to develop the Minimum Viable Product (MVP).

I sincerely thank my husband, Budha, for his constant support and encouragement, and the children for being a continuous source of happiness. Additionally, I express my sincere gratitude to all professionals whose assistance has been precious for my research. In particular, I thank Dr. Maria Grazia Vigliotti, for her invaluable guidance and patience. I also thank Helena Martin, Julie Seidel, Alvah Beander, Roeland Kollewijn, Ergina Xyodus, Harriet Hedden, and Dr. Nina Pearlman for the insight they provided into the fine art sector. Matt Meyer, Anne Rose and Raoul Lumb for their perspective on the legal sector, Alastair Moore Andrew Knight and the RICS Tech team for sharing their knowledge on real estate. The TechItalia team, particularly Pierpaolo Mucelli, for their feedback on the technical aspects of my blockchain solution, and Angus Scott for sharing his expertise on fine art and technology. The DAML community, particularly Wallace Kelly, Moritz Kiefer, for patiently answering all my questions, and Arya Bhattacharya for his support with MVP testing. Lastly, my heartfelt thanks to Prof. Dan Boneh for sharing his lectures on cryptography and zero-knowledge proofs (ZKPs).

Contents

1	Introduction	20
1.1	Context	20
1.2	Objectives and contribution	24
1.3	Structure of the thesis	27
1.4	Research methodology	31
1.4.1	Literature review	31
1.4.2	Design Science Research and Design Thinking Methodology	33
1.4.3	Interviews with industry experts	38
1.4.4	Case study selection criteria	41
2	Research background. Literature review	43
2.1	The fine art sector	44
2.1.1	Blockchain and new technologies in fine art	47
2.1.2	Money laundering in fine art	50
2.2	The real estate sector	53
2.2.1	Blockchain and new technologies in real estate	59
2.2.2	Money laundering in real estate	63
2.3	Recent changes and the role of technology	65
3	Research background. Blockchain technology	69
3.1	Blockchain across industries	69
3.2	Type of blockchains, governance and network	75
3.3	Data management	83

3.4	Blockchain potential for fine art and real estate	90
4	Case studies	95
4.1	Fine art: provenance and decentralized marketplace	97
4.1.1	Verisart. Provenance and authenticity	100
4.1.2	Maecenas. A Decentralised marketplace	111
4.2	Real estate: Due diligence and transaction process	118
4.2.1	Due diligence analysis	118
4.2.2	Interbank Spunta Project. (CordaR3)	129
4.3	The misuse of blockchain technology: Tornado Cash	133
4.4	Challenges of implementing blockchain in fine art and real estate . .	146
5	Proof of Concept: Fine art	154
5.1	Foundational elements of the Proof of Concept	154
5.2	Key features for a fine art decentralized registry	161
5.2.1	The network and data input	164
5.2.2	Proof of concept	169
6	Proof of Concept: Real estate	185
6.1	Foundational elements of the Proof of Concept	186
6.2	Key features for a real estate decentralized registry	189
6.2.1	Network and input data	190
6.2.2	Proof of concept	192
7	A proposal for a fine art and real estate blockchain registry	217
7.1	HP1. Solution to be deployed on a private blockchain	226
7.1.1	The network	227
7.1.2	The Minimum Viable Product (MVP)	229
7.2	HP2. Solution to be deployed on a public blockchain	245
7.2.1	A rigorous fine art due diligence	246
7.2.2	Identifying and investigating red flags	255
7.2.3	Soulution design. Blockchain registry and ZKPs	266

8	Conclusions	280
8.1	Answer to the research question	280
8.2	Challenges and limitations	289
8.3	Final considerations and further studies	291
	Appendices	294
A	Glossary and terminology	294
B	Acronyms	301
C	DAML code	302
D	Colophon	303
	Bibliography	304

List of Figures

1.1	Online and offline sales and share volume of art auctions globally in 2021. Source: Statista [5, 6].	21
1.2	Value of listed real estate market worldwide in 2024. Source: Statista [7].	22
1.3	Structure of this research	30
1.4	Positioning and presenting design science research for maximum impact, Gregor, S. and Hevner, A.R., 2013.	37
2.1	Online and offline sales and share volume of art auctions globally in 2021. Source: Statista [8].	45
4.1	Authentication attestations for an artwork.	106
4.2	Record and verification of attestation on the digital ledger (blockchain).	107
4.3	Application of confidence levels to individual attestations and certificates.	108
4.4	Creation of a link between a physical object and a digital certificate.	109
4.5	Digital certificate authentication system for an NFT.	110
4.6	Maecenas decentralised art gallery schematic process.	115
4.7	Description of the Dutch auction process in Maecenas.	116
4.8	Maecenas. Legal and compliance	117
4.9	Buyer journey. Phases Offer and contract	120
4.10	Buyer journey. Phases exchange, pre-completion, completion and registration	121

4.11	Seller journey	122
4.12	Causes of delay	127
4.13	14 Steps where smart contracts can improve due diligence	128
4.14	Tornado Cash, key steps	139
4.15	Tornado Cash, contract	140
4.16	Tornado Cash, deposit	141
4.17	Tornado Cash, withdraw	142
4.18	Tornado Cash, withdraw	143
4.19	Tornado Cash, fees	144
5.1	Blockchain Consortium. Level 1: Private. Participants can be museums and galleries, universities, main auction houses, asset managers, and private banks. Level 2: Public blockchain.	166
5.2	Input and validation	171
5.3	Creating asset and expert panel	173
5.4	Create Panel and invite professional, scrip results	183
5.5	Weighted score, scrip results	184
6.1	High-level description of the system. The figure shows how users have different access privileges. Through the user interface, users can retrieve documents from the ledger through a Remote Process Call (RPC)	192
6.2	The figure illustrates Step1, create and update an asset.	194
6.3	The figure illustrates the key steps to propose to sell the asset. Propose to sell and review the proposal.	198
6.4	The figure illustrates the key steps to propose to sell the asset. Accepting/rejecting an offer.	200
6.5	The figure illustrates the scoring system	204
6.6	Scrip results for smart contracts Asset	211
6.7	Scrip results for smart contract Asset Proposal	212
6.8	Scrip results for the smart contracts Sell Asset	212

6.9	Scrip results for the smart contracts Scoring	213
6.10	Parties set up in the DAML Sandbox	214
6.11	Smart contracts active in the Sandox for Solicitor 1	215
6.12	Details of the smart contract Asset	216
7.1	MVP. Workflow figure	232
7.2	MVP. Create asset. (Part. I)	234
7.3	MVP. Create asset (Part. II)	235
7.4	MVP. Asset created	236
7.5	MVP. Already voted	237
7.6	MVP.Score vote	238
7.7	MVP.Update Voters metadata	238
7.8	MVP.Get pending	239
7.9	MVP.Get total score	239
7.10	MVP.Get all assets	240
7.11	MVP. Create an offer	241
7.12	MVP. Revise an offer	242
7.13	MVP. Accept an offer	243
7.14	Artwork due diligence and verifications.	262
7.15	Client and transaction due diligence and verifications.	265
7.16	BC solution using ZK protocols	269
7.17	Artwork verifications in the blockchain	270
7.18	Client and transaction verifications	271
7.19	Transaction Score	274
7.20	Example of verification using ZKPs	279

List of Tables

1.1	Mapping of Research Chapters to DSR and Design Thinking Frameworks	37
1.2	Interviews with experts	40
4.1	Overview of case study boundaries and objectives	97
4.2	Summary of the main blockchain-based platforms in the art sector and main features.	100
4.3	Architectural Comparison: Blockchain vs Centralised Cloud-Based Systems	153
5.1	Key parameters for insurance companies	163
5.2	Most common fine art insurance related frauds	163
5.3	Artwork's data to be recorded to ledger	168
7.1	Integration of Primary and Secondary Data Across the Design Thinking Framework	220
7.2	Mapping of Expert Insights to Design Principles	225
7.3	Artwork due diligence	253
7.4	Client due diligence	253
7.5	Transaction due diligence	254
7.6	Artwork red flags	258
7.7	Client red flags	258
7.8	Transaction red flags	259
8.1	Comparative analysis Proposals (HP1, HP2)	288

8.2	Comparison of Public vs Semi-Private Blockchain Architectures . .	289

Chapter 1

Introduction

1.1 Context

Alternative assets increasingly represent a significant part of investors' portfolios, and over the past 25 years, they have evolved from a small part into a core holding. They can be defined as non-traditional investments not commonly found in financial markets, such as stocks, bonds, and cash [9]. There is no unanimous agreement on the definition of alternative assets, nor is there even any consensus on which individual asset types can be described [10]. In this study, we follow one of the most common interpretations [10, 11], which labels alternative assets (as most investors seem to do) to anything other than bonds and quoted equities. Although in 1996, alternative investments represented just 5% of global pension portfolios, in 2019, they represented more than 25% [12]. In 2020, private wealth investors allocated around 45% to nontraditional assets, institutions over 30%, and intermediaries below 30%. Among all investors, alternative assets represented more than 30% of portfolios worldwide [13].

Alternative assets are attractive to investors as they present real diversification benefits through their exposure to risks other than market risks. In other words, including assets across all classes effectively reduces the risk associated with holding an individual asset class [14, 15].

Fine art and real estate are well-regarded alternative asset classes. Fine art has

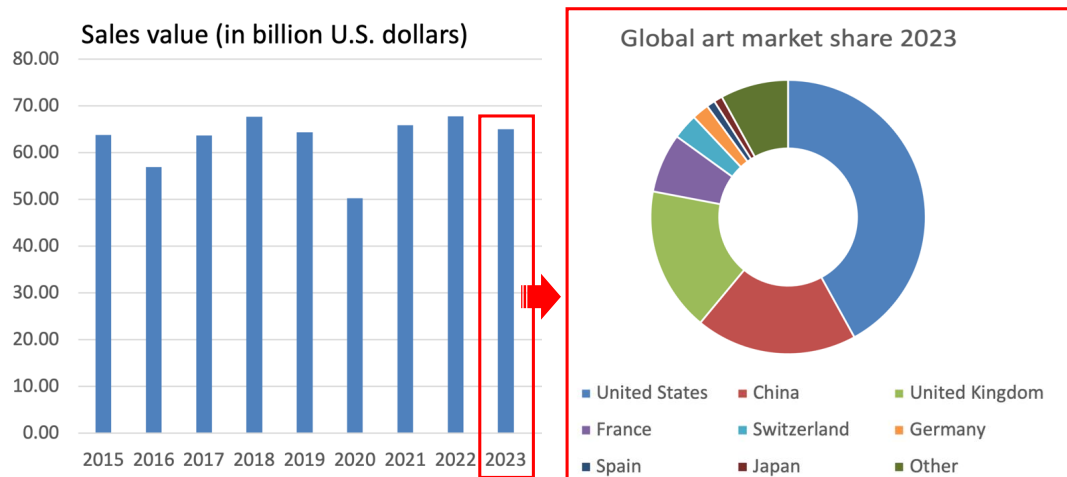


Figure 1.1: Online and offline sales and share volume of art auctions globally in 2021. Source: Statista [5, 6].

several attractive return characteristics for a long-term investor, including low correlations with other asset classes and the ability to retain its value in weak economic environments. Unlike stocks and bonds, art prices tend to correlate positively with inflation. The International Valuation Standard Council (IVSC) 2021 report states that global sales of art and antiques reached an estimated \$64.1 billion [16]. Fig. 1.1 (Left Panel) shows the global volume of transactions in the art market from 2015 to 2023. Although there was a sharp decline in 2020 due to the COVID-19 pandemic, overall, the total value of transactions in the global art market amounted to 65.9 billion US dollars in 2021, exceeding the sales recorded in 2019. Despite the sales volume in the art and antique market worldwide remained below pre-pandemic levels, it rose by 30% from 2020 to 2021 [6]. Fig. 1.1 (right panel) shows in more detail the distribution of the global art market share by country in 2023 [6, 5]. Three major art hubs, the US, the UK, and China, account for 78% of global sales, while the US is the largest market worldwide and accounts for \$27.3 billion (42%) of global sales by value.

Real estate is one of the world's largest industries and has always played a vital role in global economies. Institutional investors such as pension funds, insurance

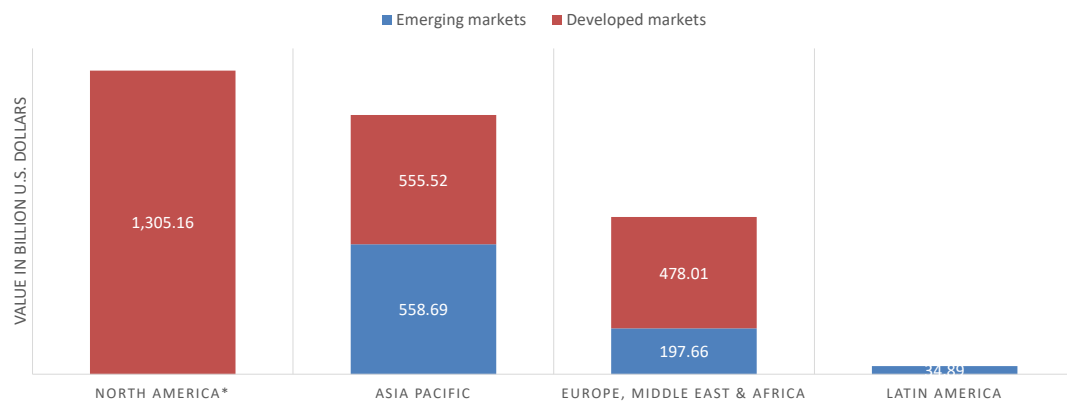


Figure 1.2: Value of listed real estate market worldwide in 2024. Source: Statista [7].

companies, and endowments allocate significant capital to this asset class [17]. Real estate is a valuable part of any well-diversified portfolio. Investors can access real estate directly (by buying land and buildings) or indirectly (using quoted, unquoted, and synthetic vehicles). In any form, incorporating real estate into an investment portfolio serves multiple primary objectives, such as achieving returns that exceed the risk-free rate and offering a protective measure against inflation. It introduces exposure to a different set of systematic risks and returns compared to stocks and bonds and can generate robust cash flows through lease and rental income [18]. The coronavirus (COVID-19) significantly affected the real estate sector, determining an overall decrease in real estate investment in the first half of 2020 [19]. However, Fig.1.2 shows that the aggregate market size of the listed commercial real estate market in Canada and the United States amounts to 1.3 trillion US dollars in 2024 and the value of the listed real estate market worldwide is greater than 3 trillion dollars [7].

As we can see from the data, fine art and real estate are attractive sectors to investors. Unfortunately, they are also often the target of money laundering activities. The main reasons lie in the large monetary transactions involved, the potential for high-value assets, and the relative ease of disguising the true ownership and value of properties or artworks. A study identifying the most common methods of money laundering [4] confirms that antiquities, art, and real estate projects are

particularly exposed to criminal activities. This is also because traditionally, real estate and art are classified as non-financial and therefore lack the regulation and rigid standardized controls for the financial sector [20]. To better understand the vulnerability of fine art and real estate to money laundering, we need to take a step back and first define this criminal activity. Money laundering can be described as “any act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets which are known or assumed to originate from a felony” [21]. Although there are many other definitions of money laundering, the one contained in the Swiss Criminal Code is very comprehensive and covers all activities aimed at obstructing the identification of illicitly acquired assets. These activities range from simply hiding assets to manipulating accounting records to the creation of false evidence [4]. Estimating the total amount of money laundered yearly or in a particular sector is extremely challenging. In the UK, the House of Commons briefing paper [22] acknowledges: “By its very nature, it is difficult to quantify what the scale of the problem is. The proceeds are hidden and often only come to light in the event of prosecutions”. Consequently, the negative economic effects of money laundering on economic development are difficult to quantify. However, the United Nations Office on Drug and Crime (UNODC) estimated that the amount of money laundered globally in one year is 2-5% of global GDP, or \$800 billion - \$2 trillion in current US dollars. The UNODC also state that due to the clandestine nature of money laundering, it is difficult to estimate the total amount of money that goes through the laundering cycle [23]. However, it is clear that this activity damages the financial sector institutions critical to economic growth and reduces productivity in the real sector of the economy by diverting resources and encouraging crime and corruption. This slows economic growth and can disrupt international trade and capital flows of the economy to the detriment of long-term economic development [24].

1.2 Objectives and contribution

There is abundant literature that investigates the fine art and real estate sectors, highlighting the key aspects of these industries. The contribution of this literature is extremely valuable for this research and is reviewed in Chapter 2. Authors have also analyzed why fine art and real estate are targets of money laundering, providing insight into how illicitly acquired gains can be disguised and reintroduced into the economy. This process exploits the opacity of these sectors, which is one of their major vulnerabilities.

Among the emerging technologies that are driving changes across industries, blockchain has the greatest potential to address this problem by increasing transparency. Substantial work has been done on blockchain technology. Its characteristics, governance mechanisms, and protocols are analyzed in detail from multiple perspectives. Without delving into technical details, as they fall outside the scope of this study, Chapter 3 explores key aspects of this technology to establish a foundational knowledge base for developing our solution. From the literature review, it emerges that blockchain technology could bring significant benefits to the fine art and real estate sectors, potentially increasing transparency and reducing intermediaries. Commercial actors such as Commerzbank, Deutsche Börsefintech 360X, and JPMorgan have started working on blockchain-based platforms, targeting tokenisation and trading of real estate and fine art assets. The proptech sector is entering a new phase [25] where great emphasis is placed on transparency and ESG (Environmental, Social and Governance) integrations. The fintech platform 360X, backed by Deutsche Börse and Commerzbank, has launched regulated secondary markets for tokenised assets such as real estate and fine art. Furthermore, a recent pilot project [26], involved the issuance of a digital real estate security on the Polygon blockchain under Germany's eWpG (German Electronic Securities Act) regulation, demonstrating how public blockchains can be used to enable compliant fractional ownership.

These examples show how the use of blockchain can improve transparency, efficiency, and regulatory alignment in traditionally opaque sectors. However, these

initiatives primarily focus on the creation of trading platforms and investment products. It is important to note that this research differs in its objective. This thesis proposes the design of a blockchain infrastructure for due diligence and provenance and prioritises legal accountability, governance, and institutional trust more than liquidity and market efficiency. Our purpose is to investigate blockchain as a regulatory and governance infrastructure, not a trading or investment tool. The innovation lies in designing a registry model that formalises due diligence, enhances auditability, and embeds institutional accountability through smart contracts. The emphasis is not on asset fractionalization or trading, but on using blockchain to improve transparency, compliance, and provenance verification in sectors highly vulnerable to money laundering. Our aim is to address the governance and compliance challenges at the core of real estate and fine art transactions, offering a framework that is regulatory in nature, not speculative. This positions the work as both academically original and practically distinct from existing commercial initiatives. To the best of our knowledge, little research has been conducted on the application of blockchain to these industries with the purpose of helping combat money laundering. We strongly believe that technology has the ultimate objective of benefiting society. Money laundering is connected to terrorist financing and other criminal activities that pose a threat to the economy and society as a whole. For this reason, we think exploring whether new technologies, particularly blockchain, can support governments and regulators to prevent money laundering in fine art and real estate is a topic worth investigating. It is important to highlight that money laundering activities prosper in opaque environments where multiple intermediaries, convoluted company structures, and untraceable sources of funds allow to hide illicit gains. Therefore, in our research, great emphasis is placed on the need to increase transparency. Fine art and real estate are targets of money laundering for their opacity and reduced surveillance compared to their industries, such as, for example, the financial sector.

This research proposes a blockchain-based framework that systematically mitigates money laundering risks in the fine art and real estate sectors by integrat-

ing structured due diligence processes, algorithmically verifiable compliance, and privacy-preserving transparency. By formalizing provenance and KYC checks in smart contracts, the solution ensures that identity, asset history, and risk indicators are not only recorded but also computationally enforceable. The proposed system introduces a dynamic transaction scoring mechanism that assesses risk based on multiple vectors, including asset origin, buyer profile, and red flags, to support real-time decision-making. Further, by utilising role-based access control (RBAC) and zero-knowledge proofs (ZKPs), the system allows key stakeholders such as regulators, auditors, and financial institutions to access essential compliance information without compromising user confidentiality. This architecture also supports cross-national cooperation by standardising due diligence workflows and enabling secure sharing of critical transaction metadata across jurisdictions. Overall, the framework shifts AML compliance from a reactive and document-heavy process to a proactive, automated, and auditable infrastructure, reducing the opacity that currently facilitates illicit financial activity in these sectors.

Compared to a centralised, cloud-based registry, where governance is enforced through administrative controls, blockchain technology enables a fundamentally different paradigm in which compliance and governance are embedded directly into code. In the blockchain architecture proposed in this thesis, no single party can tamper with or retroactively alter data, as control is distributed across the network. The registry leverages immutability, smart contract-based enforcement, and built-in auditability to ensure that key compliance actions, such as due diligence checks, provenance validation, and transaction monitoring, are performed systematically and verifiably. This design creates a secure, transparent environment that is particularly suitable for sectors prone to opacity and regulatory arbitrage. Regarding performance, it is important to note that this system is not intended for high-frequency trading. Fine art and real estate transactions are inherently high-value and low-frequency in nature. In this context, transaction throughput (TPS) is not a critical metric. Instead, trust, integrity, and compliance take precedence. The proposed registry accepts a latency of several seconds or even minutes, which

remains commercially acceptable given the transaction profiles involved. This trade-off ensures that the system remains robust, secure, and fit-for-purpose, without sacrificing the quality of verification, traceability, or legal enforceability that is essential for anti-money laundering efforts in these markets.

This study aims to fill the literature gap intending to (I) understand if and how blockchain technology can help increase transparency in fine art and real estate, and (II) design a blockchain-based solution to increase transparency, thus helping authorities and investors identify and mitigate risks of money laundering. The research focuses on the UK context and takes into consideration only physical assets, both in fine art and real estate. To accomplish our objectives, we need first to answer some granular questions. (Ia) What are the key features of the fine art and real estate industries, and what makes them vulnerable to money laundering? (Ib) What characteristics of blockchain technology make it a valuable tool to enhance transparency? (IIa) What are the key features that a blockchain solution should have to help increase transparency in fine art and real estate? (IIb) What factors should a proposed solution take into account to ensure its practical applicability in the fine art and real estate sectors, rather than remaining purely theoretical?

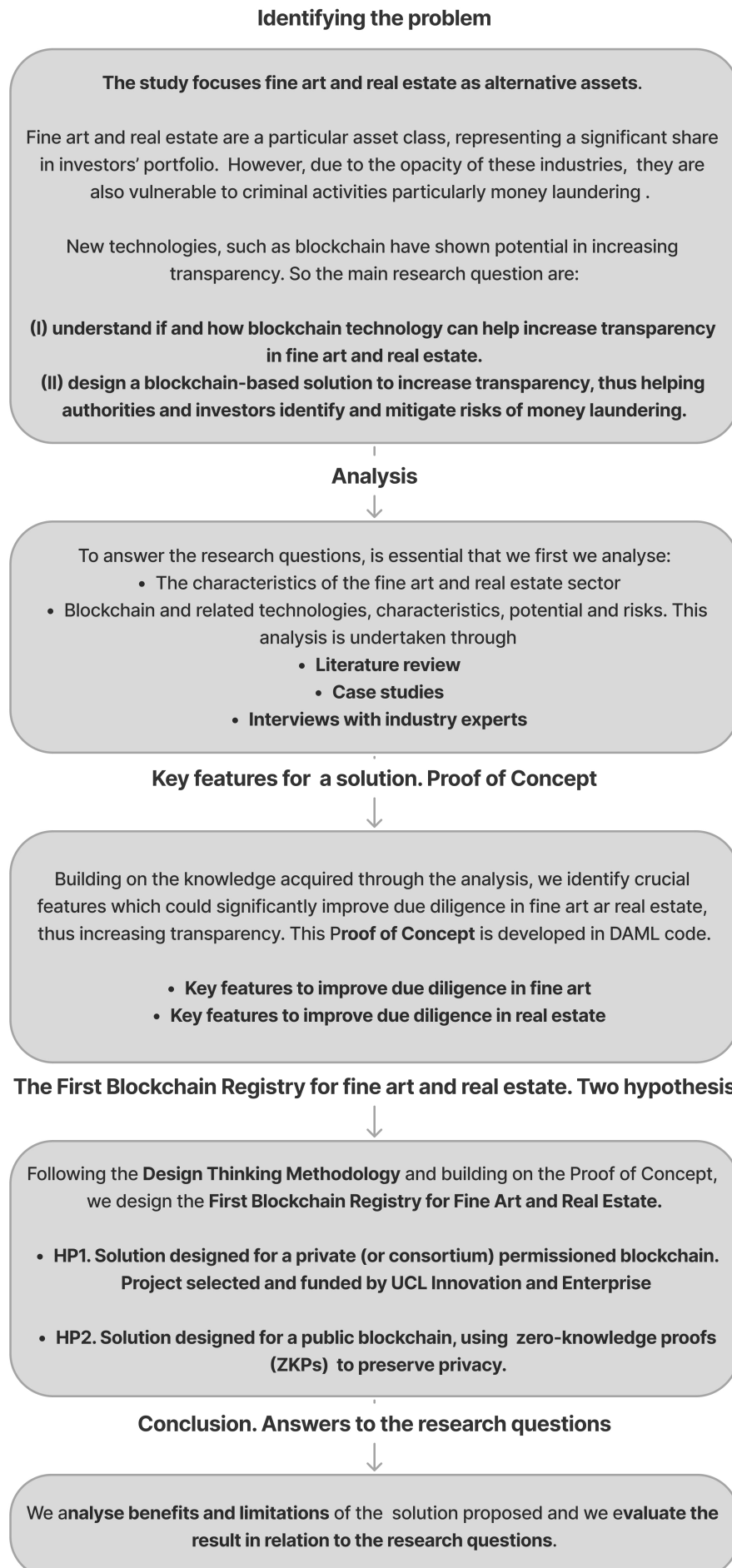
1.3 Structure of the thesis

This thesis departs from the traditional academic format to adopt a design-driven structure that reflects the iterative and integrative nature of the research. The structure is intentional and follows a progression aligned with the research objectives and hypotheses. Chapters 2 and 3 provide the contextual and theoretical foundation, offering a detailed analysis of the challenges in fine art and real estate transactions. The chapters provide the necessary insights into crucial characteristics of the fine art and real estate sectors, such as opacity, inefficiency, and money laundering vulnerabilities and key technical aspects of blockchain. Chapter 4 goes beyond a conventional survey by offering an in-depth technical analysis of existing

solutions in both sectors. Through the systematic examination of patents, technical documents, and system architectures, this chapter identifies not only adoption patterns but also uncovers underlying limitations and unresolved design challenges. This detailed investigation provides a robust technical foundation for assessing the strengths and weaknesses of current approaches and builds a clear rationale for evaluating blockchain as a governance and compliance infrastructure. These early chapters collectively establish the foundation of the research, combining a review of academic literature with empirical case studies to provide a comprehensive overview of crucial aspects of these sectors, challenges and current technological solutions.

Chapter 5 and 6 present the first original contribution by developing a concrete Proof of Concept (PoC) of key features, which are paramount to building a blockchain registry for fine art and real estate. The PoC showcase the flow of the most significant operations and how the smart contracts (developed in DAML) translate the workflow into actions. Chapter 7 builds on the PoC to propose the architecture for a blockchain registry for fine art and real estate. This registry is the first of its kind and represents a novelty in the academic and industry environment. Section 7.1 explores the registry architecture for a permissioned or consortium blockchain (solution funded by UCL Innovation and Enterprise), while Section 7.2 proposes an architecture for a public blockchain model incorporating zero-knowledge proofs to support privacy and cross-jurisdictional interoperability. Chapter 8 synthesises the findings, discusses governance implications, and situates the model within broader institutional and regulatory frameworks. While this structure may exhibit the pragmatism of an industry report, it is firmly grounded in academic rigor, integrating design science, regulatory analysis, and applied systems thinking to address a real-world governance challenge through a multidisciplinary lens. Furthermore, this research project incorporates an explicit effort to assess its academic relevance and knowledge contribution, following the guidelines proposed by Gregor and Hevner for positioning design science research for maximum impact [27]. The areas of investigation were selected based on their alignment with the Improvement category, which seeks to develop innovative solutions to existing,

well-recognised problems. This classification supports the research's relevance in both academic and applied contexts. As such, the proposed focus areas were also validated and considered strategically important by UCL Innovation and Enterprise, reinforcing the practical value and novelty of the work within a broader innovation agenda. The research structure is shown in Fig.1.3

**Figure 1.3:** Structure of this research

1.4 Research methodology

1.4.1 Literature review

The research aims to contribute to solving real-life problems by helping prevent money laundering activities, focusing on the fine art and real estate sectors. The literature review intends to provide context and background information for the research [28, 29]. To comprehensively capture relevant articles, we first screened the literature for key concepts to investigate crucial features of the technology and the sectors. We approached the research topic from multiple sides: (I) Technology, including blockchain, smart contracts, zero-knowledge proofs, cryptography, etc. (II) Law and regulations, including money laundering, anti-money laundering regulations, and cybercrime. (III) The domain of fine art, real estate, valuation, transaction processes in fine art and real estate, liquidity, etc. We then looked for pairwise conjunctions of these key concepts, such as “Money laundering AND fine art”, “Money laundering AND blockchain”, blockchain technology AND real estate and similar. This step allowed us to understand the state of the art regarding the use of technology in fine art and real estate, laws, and regulations already in place to combat money laundering activities, and identify research gaps. Thirdly, as from the previous steps of the research, influential and authoritative authors emerged, and we additionally investigated these authors’ most relevant publications. Fourth, we screened key well-established journals. Especially for technology-related topics, particularly for dynamic areas characterised by rapid and continuous changes, the search has been limited to the most recent years. Data extraction and analysis were performed according to the purpose and research. The first screening was conducted by reading the abstracts and making selections for full-text reading before making the final selection. However, to avoid missing out on important articles, this approach has been integrated with finding-focused searches. Once the initial articles had been collected, the texts were fully screened to ensure they met the inclusion criteria. This is a very iterative process, and multiple times articles have been added, running new searches following the multiple approaches described above. In addition, we conducted a backwards search. Data were abstracted in the

form of descriptive information grouped according to type of study, findings, conceptualisations of ideas, or theoretical perspective. Consistency is ensured as the analysis has been undertaken by the same individual. These are the main academic research databases used. Google Scholar, Scopus, Web of Science, PubMed, IEEE Xplore, Directory of Open Access Journals (DOAJ), JSTOR, SSRN, and Google Patents.

Given the interdisciplinary nature of this research and its focus on an emerging field, a broad range of sources was consulted. In addition to academic journal articles, the literature review draws on books, policy documents, and other relevant published materials to ensure a comprehensive understanding of the topic.

- *Reports.* Reports from well-established asset management companies, investment banks and consulting firms (Black Rock, Lombard Odier, KPMG, McKinsey, Bain and Company, Accenture and similar).
- *Expert perspective.* (I) Interviews with industry experts (auction houses, art curators and valuers, and professionals from the Royal Institute of Chartered Surveyors (RICS)) have been conducted online and in person. (II) Informal talks with UCL Art and Collection, a Swiss private bank Head of Systematic Research, a consulting firm Expert Partner (Data Science and Financial Services), a consulting firm Head of Sales and Business Development, ESG IQ (VI) RICS (Royal Institute of Chartered Surveyors) workshops in the RICSTech Partner program.
- *Statistics and data.* Statista.com
- *Blockchain related resources.* Stanford University's material. Prof. Dan Boneh, has very kindly provided invaluable resources regarding blockchain, cryptography and zero-knowledge protocols. The Science of Blockchain Conference 2023 (SBC'23) Arrillaga Alumni Center, Stanford University Aug 28 - 30, 2023, The 13th BIU Winter School on Cryptography, Stanford University.

1.4.2 Design Science Research and Design Thinking Methodology

This research is grounded in the principles of Design Science Research (DSR) [30, 31], and incorporates Stanford University's Design Thinking methodology [32] to address the complex and multidisciplinary challenges posed by opacity and inefficiency in real estate and fine art transactions. We combine Design Science Research (DSR) and Design Thinking (DT) to structure and develop a practical, yet academically grounded solution. These methodologies complement each other: DSR framework outlines phases such as problem definition, artefact design, demonstration, rigorous evaluation, and scholarly communication, while DT emphasizes iterative, human-centred phases (Empathize, Define, Ideate, Prototype, and Test).

The integration of Design Science Research (DSR) and Design Thinking (DT) within this thesis was both intentional and necessary, given the complex, multi-stakeholder nature of the problem space. DSR offers a rigorous academic framework for the development, demonstration, and evaluation of artefacts, ensuring that the research contributes meaningfully to the information systems knowledge base. It provides a clear structure through the relevance, design, and rigour cycles, enabling the alignment of theoretical analysis with practical system design. However, on its own, DSR does not fully capture the iterative, user-centred processes that are critical when designing systems intended for socially and institutionally embedded contexts, such as those found in the fine art and real estate sectors. This is where DT becomes valuable: it emphasises empathy, rapid ideation, prototyping, and iterative feedback, helping to ensure that the artefact is not only innovative or technically feasible but also meaningful and usable for real-world stakeholders. The use of DT complements DSR by grounding the design in lived experience and domain expertise, particularly through interviews and scenario-driven refinement. By combining the methodological structure of DSR with the human-centred ethos of DT, the research was able to deliver an artefact that is both academically rigorous and practically relevant. Table 1.1 matches the topics of this research with Design Science Research (DSR) and Design Thinking (DT) methodologies.

The thesis follows the DSR process by first identifying a pressing real-world problem: the lack of transparency and regulatory accountability in sectors prone to money laundering and information asymmetries. Initially emerging from disciplines like software engineering [33], DSR has evolved into a widely accepted approach in the information systems field [31]. Its strength lies in bridging technological innovation with behavioural science [30], making it particularly well-suited to addressing complex socio-technical challenges that include feasibility, usability, and regulatory acceptance. Central to DSR is the development of an artefact, whether a method, system, or process, that addresses a well-defined problem and is subject to iterative evaluation [34]. In this context, we develop a digital infrastructure for real-world asset registration and transfer, incorporating risk indicators and verifiable documentation to strengthen due diligence protocols. This artefact-driven approach situates our contribution firmly within the information systems domain. Our research DSR comprises three cycles. The relevance cycle defines the practical problem and establishes the design objectives [31]. As outlined in Chapter 2 the use of fine art and real estate for money laundering purposes presents significant regulatory and societal concerns. Despite growing interest in applying blockchain to this domain, there remains a lack of concrete, implementable models that consider legal and operational constraints. Our review of the literature confirms the existence of a research gap: although various studies speculate on the potential of blockchain in the fine art and real estate sector, they generally lack concrete implementation guidance that accounts for regulatory obligations and practical business conditions. This underscores the relevance of this research, which responds directly to the sector's exposure to money laundering risks. The design phase entails the construction of a technical framework to support auditable registration and ownership transfers, integrating trust anchors, visibility rules, and verifiability thresholds [35]. This framework is tested conceptually through risk scoring structures and transaction logic. Finally, the rigour cycle ensures theoretical and methodological soundness [30, 27], with validation derived from expert interviews assessing the

framework's applicability across sectors vulnerable to financial crime, including but not limited to fine art and real estate. Additionally, contributing to the knowledge base by developing a novel artefact that addresses real-world challenges can, in itself, constitute a meaningful research outcome [36, 37]. In this context, the thesis presents a synthesis of findings, drawing on insights from industry experts to explore both the potential and limitations of applying blockchain technology to the fine art and real estate sector. The work includes a proposed set of risk indicators that, if structured algorithmically, could support end-to-end verifiability of assets' transaction and ownership history, thereby addressing key concerns around provenance, transparency, and compliance. Furthermore, we took an additional step to evaluate the academic relevance and novelty of the study. The areas of focus have been identified following the design science research guidelines [27] to evaluate and position the knowledge contributions of the research project (Fig.1.4). The topics investigated mainly fall under the *Improvement* category as they aim to develop new solutions to known problems. For this reason, they have been considered relevant and worth investigating by UCL Innovation and Enterprise.

This research was selected by UCL Innovation and Enterprise and funding was granted to develop a Minimum Viable Product (MVP). The MVP represents the first step for creating a blockchain register for fine art and real estate. The MVP design and development follows Stanford University's Design Thinking methodology [32]. The design philosophy and practice were developed at Stanford University in 1957 and evolved into Design Thinking as an innovation management approach. This methodology provides a solution-based approach to solving problems. Design thinking is a non-linear process that has proven to be highly advantageous for addressing complex problems characterized by ambiguity or novelty. Facilitates comprehension of the human needs involved, reshaping the issue through a human-centered perspective, generating a multitude of ideas during brainstorming sessions, and embracing a practical approach to creating and evaluating prototypes. Design thinking is an iterative process characterized by five main phases: *Em-*

pathize, Define, Ideate, Prototype, and Test. The first step (*Empathize*) focuses on user-centric research to fully comprehend the problem. It also includes consulting subject matter experts to acquire comprehensive insights into the specific domain of concern. In the second step (*Define*), the information is analyzed and the core problem is identified. The process is human-centered, emphasizing the central role of individuals' perspectives and requirements. The third step (*Ideate*) can be seen as the ideation phase. Analyzing the information and achieving a deep understanding of the requirements constitutes a solid foundation for looking at innovative solutions to the problem statement. The fourth step (*Prototype*) is the development of a prototype or Minimum Viable Product to showcase the solution proposed. The fifth step (*test*) involves testing the prototype to verify functionality and resolve errors. Being an iterative process, the circle does not stop with the last step, and it can be repeated even in a non-chronological manner to incorporate feedback and improve the software. This methodology has proven effective, and multiple applications such as Airb&B, and UberEats have been developed following this approach. Design Thinking (DT) is not only a motor for innovation. It offers new models of processes and toolkits that help to improve, accelerate, and visualize creative processes, particularly in multidisciplinary research.

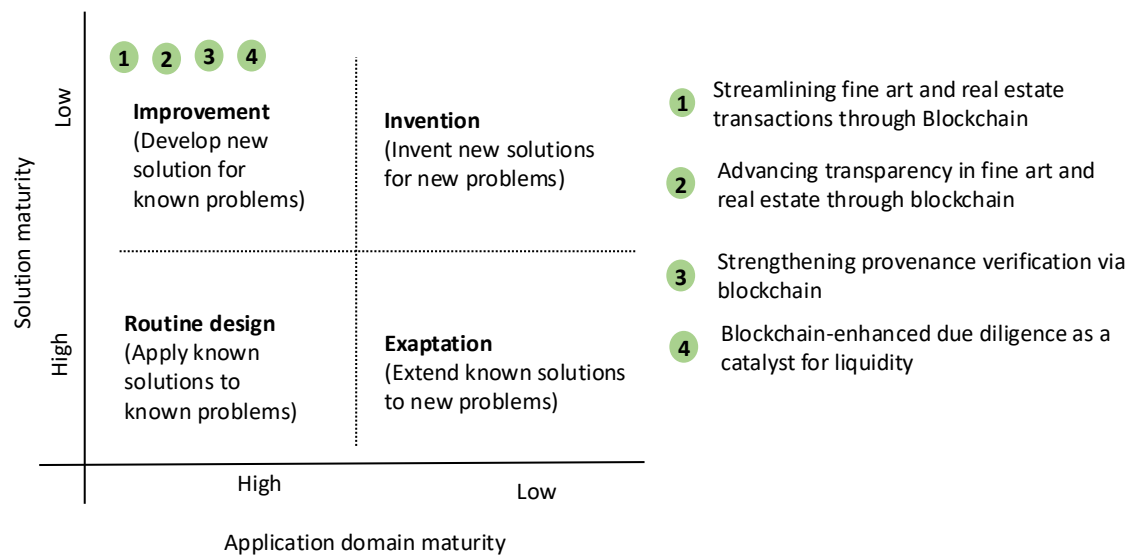


Figure 1.4: Positioning and presenting design science research for maximum impact, Gregor, S. and Hevner, A.R., 2013.

Topic	Design Science Research (DSR)	Design Thinking (DT)
Literature review and industry expert interviews	Relevance Cycle/ Rigour Cycle - Identifying problems (AML risk and opacity), finding research gap	Empathize – Reframing the challenge using insights from the industry
Sector and technology landscape, case studies	Relevance Cycle - Contextual understanding and requirement specification from domain stakeholders	Define – Clarifying problem spaces in each domain (risk, complexity, regulation)
Proof of Concept (Fine art and real estate)	Design Cycle - Synthesising legal, regulatory, and technical requirements for artefact creation.	Ideate - Drawing inspiration from practice and clarifying problems (risks, complexity, regulations)
Solution Semi-private Blockchain (HP1)	Design Cycle - MVP and evaluation via scenario testing	Prototype/Test - developing and testing smart contract logic reflecting stakeholder needs
Hypothesis Public Blockchain (HP2)	Design Cycle - abstraction of PoC2 to wider contexts and research contribution	Prototype/Test - Conceptual validation of extended architecture
Evaluate and implement a novel artefact	Rigour Cycle - Evaluating contribution to research and practical implementation	Test - Considers scalability, privacy, interoperability across sectors and jurisdictions

Table 1.1: Mapping of Research Chapters to DSR and Design Thinking Frameworks

1.4.3 Interviews with industry experts

To gain a deeper understanding of the core challenges facing the fine art sector, we conducted a series of interviews with industry professionals to integrate practical insights and business needs into our research. We chose to conduct interviews specifically with art market experts, as the fine art sector presents scarce regulatory literature regarding due diligence procedures. Real estate benefits from a more structured governance framework, particularly in the UK, where the conveyancing process is clearly defined and regulated by law. Conversely, the art market lacks a standardised approach to verifying provenance, ownership, and transactional integrity. While the real estate due diligence process is thoroughly examined in this thesis through the case study presented in Chapter 4 (*Due Diligence Analysis*), the fine art sector required a more exploratory and qualitative approach. Interviews with industry professionals allowed us to gather first-hand insight into the practical challenges and ambiguities encountered in art-related compliance and risk management, issues that are less formally documented than those in property transactions.

Participants were selected based on their expertise in key domains, provenance and valuation, technology, regulatory compliance, and risk management (Table 1.2). The fine art ecosystem intersects with multiple domains, ranging from valuation and collection management to legal compliance, financial risk, and technology integration. For this reason, expert selection followed a purpose-sampling strategy, targeting professionals with demonstrated expertise and practical engagement in areas relevant to the study. Art market professionals, including appraisers, curators, and gallery owners (e.g., Interviewees B, C, D, and E), provided insights into provenance verification, valuation practices, and the absence of standardised due diligence frameworks. Institutional voices from academia (Interviewees A and F) contributed a broader perspective on collection governance and museum-level documentation standards. To capture the legal dimension, we included lawyers and regulatory advisors (Interviewees I, L, and M), who helped articulate the legal grey areas in art transactions and their implications for anti-money laundering compli-

ance. Given the increasing attention from financial institutions toward alternative investments, experts from the banking and finance sector (Interviewees O and P) were included to represent the perspective of institutional investors and Ultra High Net-Worth Individuals (UHNIs), particularly on the need for greater transparency and standardisation in asset due diligence and risk evaluation. These financial experts also provided a strategic view on how risk metrics could align with ESG reporting and cross-border compliance. In addition, technology leaders and entrepreneurs (Interviewees G, H, and Q) provided critical information on the feasibility and market readiness of implementing digital solutions, such as blockchain infrastructure and zero-knowledge proofs, within a sector that is historically conservative and fragmented. By incorporating expert voices from these multiple fields, the study was able to evaluate key themes across valuation, risk, regulation, and technological adoption. This diversity was essential not only to inform the requirements for the proposed design solution but also to evaluate its practical viability across stakeholder groups involved in high-value transactions in fine art and comparable alternative asset markets. The interviews were conducted in person and via remote video conferencing, each lasting approximately 60 to 70 minutes. Given the different backgrounds of the interviewees, we followed a semistructured approach that allowed us to leverage the experts' diverse backgrounds and to capture nuances of personal perspectives and information that otherwise would be missed. The findings revealed three critical focus areas where expert input is essential for shaping technological solutions to real-life problems: provenance and artwork due diligence, transaction and client due diligence, KYC (know your client) procedures, and blockchain technology in the art industry.

Field of expertise	Years of exp.	Role	ID	Type
Art and communication	20+	Lecturer	A	In person
Art and antiques and valuation	20+	Art expert	B	Video call
Contemporary art and appraisal	20+	Certified appraiser	C	Video call
Contemporary art and art valuation	10+	Gallery owner	D	In person
Art and communication	10+	Curator	E	Video call
Art collection	10+	Head of art collections, university	F	In person
Data, technology	10+	Digital, data and technology lead	G	In person
Entrepreneur, investor	10+	Co-founder	H	In person
Technology, Data and Privacy Law	7	Partner	I	In person
International technology lawyer	7	Member of the management board	L	In person
Law and technology	7	Managing associate	M	In person
Art	17	Direction office, Gallery manager	N	Video call
Finance and technology	15+	Head of systematic research	O	In person
Finance and technology	15+	Global head of sustainability and non-financial risk solutions	P	In person
Art and technology	10+	CEO and founder	Q	In person

Table 1.2: Interviews with experts

1.4.4 Case study selection criteria

The case studies analysed in this thesis represent a cornerstone of the research, offering a structured and multidimensional lens through which to evaluate the current state of blockchain applications in fine art and real estate. Each case was examined in depth across multiple dimensions, including technical architecture, intended purpose, system functionalities, governance structures, and regulatory positioning. This granular analysis, informed by publicly available technical documentation, patents, and platform white papers, provided critical insights into the strengths and limitations of existing solutions. By studying how leading platforms address challenges such as trust, privacy, scalability, and compliance, the research was able to identify recurring technical gaps, such as issues with data provenance, role enforcement, or transparency, as well as best practices worth adapting. These empirical insights formed a practical knowledge base that directly shaped the design of the proposed system. The purpose of the research is to solve real-life problems. Therefore, rather than working from theory alone, we grounded the developed solution firmly in real-world experience.

Case studies have been selected according to these criteria: (I) *Relevance for the industry* (fine art and real estate), (II) *Relevance to understanding potential and risks of the technology*, (III) *Availability of technical material*, essential to perform a thorough analysis of the technology. Here are the selected case studies.

- **Fine art.** (I) *Verisart*. A blockchain application for the provenance and authenticity of artwork. (II) *Maecenas*, a blockchain application for tokenisation of artworks.
- **Real estate.** (III) *Real estate due diligence analysis*. A study of the transaction phases and the potential of blockchain applications to improve due diligence. (IV) *Interbank Spunta Project. (CordaR3)*. A blockchain solution to improve interbank operations and speed up transaction processing
- **Potential risks** (V) *Tornado Cash*. A study of potential risks posed by the misuse of blockchain technology.

For the fine art sector, the two case studies selected (Verisart and Maecenas) showcase different applications of blockchain technology in this industry. Verisart is more oriented toward creating a reliable provenance and tracking ownership, while Maecenas works on artwork tokenisation. For both case studies, white papers and patents are publicly available, allowing a detailed description of the technical solutions. Given the complexity of real estate transactions, we dedicate a case study to the due diligence process. This study is based on the material provided by the Law Society and the analysis of the Digital Street project of the HM Land Registry (HMLR) undertaken by the HMLR and the law firm Mishcon de Reya. The second selected case study for the real estate sector was Coadjute, an excellent application of blockchain technology to streamline the real estate transaction process. Unfortunately, technical material and patents were not available and it was not possible to analyze the technology. For this reason, this case study was excluded. However, from the available resources, we understood that Coadjute is powered by Corda, a secure form of blockchain known as distributed ledger technology (DLT), which enables Coadjute users across businesses that use different systems to participate in the transaction process. This application is particularly relevant to our research. For this reason, we selected the Interbank Spunta Project case study. The project uses R3's Corda blockchain to improve interbank operations and speed up transaction processing. This project is very interesting for exploring the use of blockchain in a financial context where privacy, confidentiality, and security are paramount. Finally, Tornado Cash was selected because it is crucial to highlight how the misuse of blockchain technology can pose significant risks and facilitate malicious activities. Tornado Cash is a smart contract mixer deployed on the Ethereum blockchain that seeks to anonymize user assets to protect their privacy. The Tornado Cash platform faced sanctions from the US Treasury Office of Foreign Assets Control (OFAC), as it was recurrently exploited to launder misappropriated funds. The complex technology behind the selected case studies has been analyzed, simplified, and explained to support an open discussion about the pros and cons of blockchain and what can be done to ensure blockchain is used to benefit society.

Chapter 2

Research background. Literature review

Through a literature review, this chapter examines the critical features of the fine art and real estate sector, and blockchain technology. This analysis is a crucial prerequisite to understanding whether and how the application of blockchain technology could benefit these industries and help combat money laundering. Before exploring the details, we make some considerations to provide a clearer rationale for the association of fine art and real estate and how a shared solution could benefit both.

Although fine art and real estate are separate asset classes, they have some common characteristics. For example, they may be relatively illiquid and involve relatively high purchase and sale costs compared to stocks and bonds. There are some similar risks associated with these alternative investments, such as the difficulty of evaluating their performance, determining the asset's current market value, and the complexity of establishing valid benchmarks. In addition, there might be a scarcity of historical risk and return data. [11]. In fine art, successful investment requires a high level of specialist knowledge beyond mere investment theory and practice. Low transparency in the market is a significant risk and fraud can be frequent. In real estate, risks can be seen in the low liquidity associated with physical assets. The time required to achieve a financial settlement can be long and investors might incur financial losses from being forced to hold property longer than expected or sell at a lower price. In addition, the market price can fluctuate during the inter-

val between the decision to sell and the execution of the sale. These characteristics make the transaction process, in fine art and real estate, particularly complex, and due diligence can be expensive and time-consuming. Finally, both sectors are often the target of money laundering activities because of their inherent opacity. In Chapter 4, we analyse some selected case studies and investigate some existing applications of blockchain technology to understand the state of the art and identify crucial challenges with current solutions.

2.1 The fine art sector

Due to the COVID-19 pandemic in 2020, countries worldwide implemented emergency measures to limit the spread of the virus, and auction houses, art dealers, and fairs had to cancel or reschedule in-person events. These closures hit the global art market hard, but at the same time, they drove companies and art professionals to enhance their online presence. Auction houses and dealers strengthened their digital departments and online sales of the art, and the antique market worldwide increased significantly in 2020 and increased even further in 2021, reaching a fifth of global art sales [38]. Fig. 2.1 shows the volume and value of the share online and offline in selected global countries in 2021. The UK, in particular, significantly increased its online sales and volume. A similar trend, although slightly less pronounced, can be observed in France and the United States [8, 39].

The art valuation field has significantly expanded with the art market's growth, as it is paramount for investors looking at artwork as an investment option to rely on accurate valuations. The IVSC identifies the following key criteria for estimating the value of an artwork: “authenticity, artist, school, signature and dating, genre, technique, dimensions, motif, innovation (hype), condition, market freshness, art and cultural-historical significance, quality, provenance, restitution freedom, rarity, period of creation, characteristic and performance” [16]. Among other factors, the art world considers the “biography” of artworks highly relevant as it is crucial to determining ownership and estimating value: since at least the 18th century, provenance has played an important role in prosperous European market centers, support-

ing the orientation of collectors and the valuation of art [40]. The authenticity of art objects and individual quality evaluations are critical to determining the aesthetic and artistic merit of works of visual art. Indeed, provenance signals whether an artwork has been part of a prestigious collection or exhibition, indicating authenticity and elevated aesthetic quality. Both of these factors have a significant influence on the economic value of the artwork.

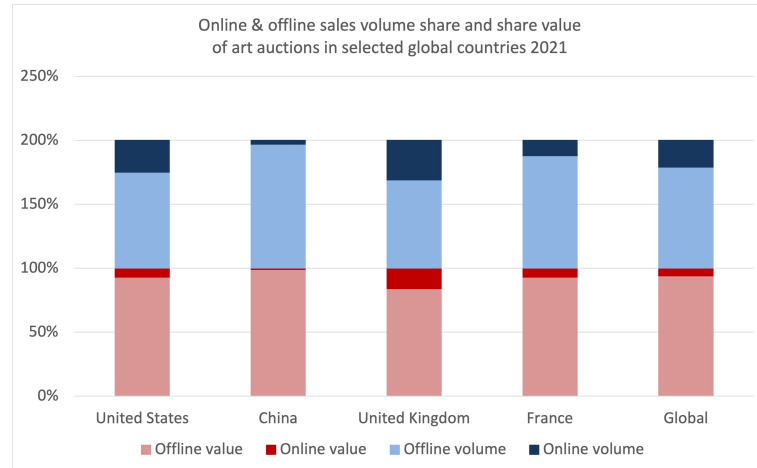


Figure 2.1: Online and offline sales and share volume of art auctions globally in 2021. Source: Statista [8].

Research on provenance is key to establishing ownership and it became relevant after World War II to return the looted artworks to legitimate owners. "Looking for Owners", for instance, describes the convoluted history of artworks, the great efforts, and the difficulties in tracing back the original owners and proceeding with the restitution [41]. Especially since the 1980s, the 'looted art and restitution' became an international issue, with 44 states committed to examining their collections of works of art that had been confiscated. This international agreement led to the development and professionalization of provenance research in museums, libraries, archives, research institutes, and private companies [40].

Provenance is also crucial to determine the authenticity of the artwork. During the 1990s, the British self-proclaimed physics professor John Drewe was the protagonist of a decade-long scam that rocked the international art market. His criminal scheme resulted in more than 200 forgeries on the art market between 1986 and 1995. John Drewe made his way into the upper echelons of renowned art institu-

tions, gained access to their archives, and plagued them with fabricated records of fictional exhibitions, restorations, and sales. According to his accomplice and the forger himself, John Myatt “about 120 of them are still in circulation at this time. All with impeccable provenances” [42]. Yan Walther, Chief of the Fine Arts Expert Institute (FAEI), said that more than 79% of the works of art examined by him were forged or not attributed to the correct artists and speculated that the percentage of forged works of art in circulation on the market could be as high as 50% [43].

Visibility and publicity can also contribute to increasing the value of artwork. Artists and creators in the creative industries often need to rely on powerful intermediaries to have access to a strong network to distribute and profit from their creations and to have visibility. Generally, artists have to go through a long journey to distribute their work to consumers with the consequence of adding high transaction costs. Ultimately, creators tend to capture only a small fraction of the value they create [44]. Competition can be particularly fierce, especially in the initial stage, when it is crucial for the artist to achieve a critical mass, triggering positive feedback. In general, the artist’s talent and innovation ability are important, but the speed at which they grow is crucial since the first artist to reach critical mass will take over the entire market.

The contemporary art market is driven by the “economy of attention” [45] with the consequence that the quantity of artworks sold is closely related to the investments of curators and investors. Market success depends on cultural success (and vice versa): the artist’s international visibility increases with the number of exhibitions in prestigious private and public collections and cultural institutions. As the circulation of works of art in the network of renowned public and private collections increases, an increasing number of new buyers will be, in turn, encouraged to include the artist in their collections, making the artist even more attractive to additional collectors and triggering self-reinforcing network effects [46]. Blockchain promises to increase the transparency of the art market, track ownership and provenance, and provide an infrastructure for tokenization of fractional artwork sales.

2.1.1 Blockchain and new technologies in fine art

The interest in blockchain technologies in the art sector increased around 2018. This technology looked particularly appealing for broadening the market's transparency, tracking ownership and provenance, and providing the infrastructure to tokenize fractional artwork sales. In July 2018, the Maecenas blockchain platform partnered with London gallery Dadiani Fine Art to offer fractional stakes in Andy Warhol's 14 Small Electric Chairs (1980) [47]. 31.5% of Warhol's work went up for sale in cryptocurrencies, including Bitcoin and Ethereum. The total dollar value of the cryptocurrency share in the work was \$5.6 million. In November, Christie's New York made art world history when it partnered with the Artory blockchain-secured registry. The auction house's \$318 million sale of the Barney A. Ebsworth collection, one of the most important sales of the year, recorded its transactions entirely on the blockchain [48].

Blockchain technology has core use cases in the arts concerning the creation of provenance and authenticity registries, digitally scarce tokens for new media and generative art, fractional equity and shared upside structures, and new forms of copyright registry. Provenance research is a time-consuming and costly part of gallery preparation for art fairs and a differentiating factor in the business model of art fairs. It is also central to museum practice as institutions revisit their own collections [49]. The characteristics of blockchain-based platforms naturally support proof of ownership, e.g., by querying the blockchain database where records of ownership and provenance have been immutably stored. Blockchain technology would have been key, for example, in well-known restitution cases such as that of Egon Schiele's Wally portrait (1912) [50] and Gustav Klimt's portrait of Adele Bloch-Bauer (c. 1907) [51, 52]. These cases show the potential power of an immutable and decentralized record. If the blockchain database becomes a registry of title, for example, of the legal ownership, then the legal ownership of the work becomes inseparable from the blockchain provenance. In this scenario, transferring the artwork's title creates a new record on the underlying blockchain.

Provenance describes the chain of ownership, while authentication concerns proving the correct authorship. Authentication of art occurs using various methods such as scientific analysis, experts' investigations, and endorsement through certificates of authenticity associated with the artwork. Scientific analysis and experts' knowledge provide the compendium to authenticate artworks, while blockchain allows combining data regarding authentication and provenance thanks to a chained record of ownership. It should be noted that the validity of the record depends on the accuracy and truthfulness of the data input on the blockchain. In the future, the issue of authentications, the keeping of the register by professional operators, the certificates of circulation of the works, and a whole series of documents and authorizations could be completely automatically managed by blockchain [49].

Non-fungible tokens (NFTs) appear to be of particular relevance for the creative industries. All information recorded on a blockchain can be considered a digital asset (or token), and the record of these assets is immutable and tamper-proof. Through smart contracts, parties can create new types of digital assets with custom-defined parameters and properties. The fungibility of a token is a token feature that shows whether assets can be completely exchanged throughout the trading process. A fungible token is equivalent to other tokens of the same type and can be divided into smaller units. An example fungible token is the Ethereum native currency ETH, where each ETH token is of identical value. On the other hand, non-fungible tokens have unique value and cannot be divided. These tokens have been used to represent unique assets such as collectables, certificates, deeds/rights, artwork, etc. On 11 March 2021, an exclusively digital piece of art "*Beeple collage, Everyday: The First 5000 Days*" [53] in the form of a non-fungible token (NFT) was sold for the equivalent of \$69 million [48]. The artist Beeple created a single NFT for the digital work that reflects the ownership rights to the digital art asset. This work of art can be viewed or accessed by anyone on the Internet; however, there is only a single owner. In a similar way, indeed, physical art is publicly acces-

sible in museums by non-owners. NFTs have paved the way for highly innovative approaches. For the first time, artists can monetize digital content, users or gamers can be owners of digital worlds, and rare collectables can be (re)produced digitally [54]. Buyers can re-sell their acquired creative content by transferring ownership of their NFTs on the blockchain. Even as the NFT changes ownership multiple times, prospective buyers can always check the historical ownerships on the blockchain to verify that the NFT originated from the authentic creator. In contrast, drawing up legal paperwork for the transfer of ownership and verifying content authenticity is not as easy in traditional (non-digital) channels. As a result, traditional secondary markets for creative content are dominated by a few established auction houses to facilitate resale, for example Christie's and Sotheby's leading the art market [44].

Blockchain, NFTs, and smart contracts have created alternative routes for content distribution that do not require complete reliance on traditional intermediaries, such as publishers, distributors, and auction houses [44]. In creative industries, blockchain can change how creators receive remuneration for their work. Artists can achieve more control together with more stake in the revenue generated from their creative work. They can rely less on or even bypass intermediaries and their associated costs, thus receiving a greater share of the revenue generated from their products. In addition, they can have more say on how their intellectual properties are priced, shared, and promoted. The demand for creative products (paintings, photos, songs) fluctuates over time, and smart contracts allow for transparent dynamic pricing. A correctly executed dynamic pricing mechanism benefits both sellers and buyers, as it can help price artwork more accurately and increase the transparency and accessibility of the product to buyers willing to pay little [44]. In contrast, in the traditional marketplace, the artist, the buyer, and the intermediaries may need to renegotiate to change prices according to fluctuation in demand. Furthermore, blockchain technology can help establish a reputation system. For example, the ledger will record if creators did not fulfil creative contracts on time or buyers/resellers failed to pay or to pay on time. One caveat on public blockchains

is pseudo-anonymity, i.e., participants can create new addresses to hide links with their past transaction records. Methods for clustering transactions (including looking at the span of someone's record) using an ID verification layer or a permissioned version of the blockchain may help identify and limit this behaviour. The reputation benefits of a long and good track record can also incentivize participants to maintain their identities [44].

Blockchain technology can be successfully applied by different cultural heritage organizations, from theatres to museums, from art galleries to monuments managed by public entities [55]. Moreover, technology has the potential to bring structural changes to such organizations [56]. Potential applications can be seen in the management of collections and collaboration between museums and other partners, such as other museums, collectors, universities, associations, and governments [49]. These collaborations raise the problem of tracking exchanges. Blockchain could allow the design of a system that combines this technology and IoT used to exchange cultural relics among museums and clarify the responsibilities of lenders, exhibitors, and carriers [57].

2.1.2 Money laundering in fine art

As mentioned above, the art sector is vulnerable to money laundering. Unfortunately, the lack of proper rules, monitoring, or even interest has led many launderers to look to this market to clean funds from criminal activities [20]. For money launderers, art and antiques have the advantage that their value is often uncertain and difficult to estimate. Ideally, they choose markets lacking transparency and purchase relatively unknown objects whose values are more difficult to estimate. They often purchase a few antiquities or artworks with legal funds and other items with illicit funds. This makes it more difficult for the police authorities to distinguish which assets have been purchased illegally. Furthermore, since it is not unusual to pay cash, illicitly obtained funds can be used to buy precious artworks from discreet private collectors who do not publicly advertise their items [4]. Because artwork's provenance is not always easy to verify, the money launderer can declare that the

object was bought years before from a public source such as a flea market. The general confidentiality surrounding the art world and the endemic unlawful activities (theft, robbery, and forgery) makes the situation worse [20]. International art lawyers [58] explain how such typical money laundering processes are based on the prevalent and notorious opacity of the professional art market and the secrecy of art transactions. Although institutions serving the financial sector are subject to stringent regulations, the art world is not as highly regulated at the national, local, and global levels. The situation is further exacerbated by the use of cryptocurrencies and the anonymity that blockchain platforms offer. While transactions may be recorded on the public ledger, the information can be of limited use to law enforcement without knowing the true identities of the transacting parties. This is because individuals can conceal their identity by using different public addresses, essentially allowing transactions to be conducted anonymously [59].

To summarise, these are some key reasons why the art sector is susceptible to criminal activities.

(I) *Prices can be manipulated* [60]. The valuation of artworks can be intentionally inflated to justify exaggerated insurance values or to secure substantial loans against the asset [60]. By artificially increasing the declared worth of an artwork, actors can facilitate the laundering of illicit funds through coordinated manipulation of price, quantity, and quality, often involving international transfers [61]. (II) *Anonymity and/or a lack of transparency*. While major auction houses operate within a framework of self-regulation and are expected to uphold ethical standards, they frequently accept cash payments and are not subject to the same strict reporting protocols as financial institutions. Additionally, although these entities and the trade associations they engage with act within legal parameters, there has historically been a reluctance to adopt rigorous preventive measures. This resistance stems from fears that tightening regulations could push more transactions into the black market [20]. (III) *Lack of provenance/history of ownership*. The longstanding norm of confidentiality in art transactions has led to widespread omissions in documenting prior ownership. Particularly in the post-World War II art trade, many

antiquities circulated in the market without clear origins. Thompson (2010) notes that the majority of such items sold over the past half-century lacked any verifiable provenance [62]. Unlike museums or professional dealers, private individuals often hold artworks with no supporting documentation, provenance trail, or record of sale—frequently accepted as normal under the assumption of family inheritance. This ambiguity creates opportunities for misuse and criminal exploitation [20]. (VI) *Commoditisation of art*. The increasing treatment of artworks as investment vehicles rather than cultural assets contributes to volatility in pricing. This commoditisation makes the sector susceptible to short-term speculative trades, which can be exploited to legitimise rapid financial gains through laundering strategies [61]. (V) *Portability of items*. Compared to other high-value goods, artworks are relatively easy to transport. This mobility, coupled with their discrete packaging and international appeal, facilitates cross-border movement of value in ways that are harder to trace than commodities like gold [60]. (VI) *Use of free ports*. Free ports function as international storage hubs for artworks and other valuable goods, often without requiring immediate customs declarations. Their confidential nature makes them attractive for individuals wishing to obscure ownership or the origin of funds. Notable examples include facilities in Switzerland, Luxembourg, Hong Kong, and Singapore. These zones enable long-term storage while deferring import duties, thus avoiding visibility in national registries. Although there have been regulatory attempts to require the declaration of cultural goods moving through free ports, enforcement remains limited [61, 60].

Besides these concerns, it is important to clarify the current regulatory obligations imposed on auction houses in the context of antimoney laundering (AML) compliance. While traditionally operating under a largely self-regulated model, auction houses within the UK and EU have, in recent years, become subject to formal AML requirements under the EU's Fifth Money Laundering Directive (5MLD) and the UK's Money Laundering Regulations (MLR 2017, as amended). These frameworks define Art Market Participants (AMPs) and require them to undertake

customer due diligence (CDD), enhanced due diligence (EDD) where applicable, risk-based assessments, and the reporting of suspicious activity to relevant authorities. However, implementation and enforcement remain uneven across jurisdictions and institutions. Moreover, private sales, thresholds below €10,000, and transactions routed through intermediaries can still allow for limited scrutiny, thereby preserving certain informational asymmetries. While reputable auction houses have adopted internal AML protocols, including client verification and provenance checks, these practices vary significantly and are not always subject to third-party auditing. As a result, despite the appearance of institutional compliance, the art market remains a space where opaque structures, cash-based transactions, and fragmented oversight continue to hinder comprehensive AML enforcement.

2.2 The real estate sector

This sector exhibits significant complexity. Real estate transactions are generally regulated by law, and processes are time-consuming and can be quite convoluted. The real estate industry is also known to resist change and to be seemingly allergic to adopting new technology. The real estate sector has a reputation for reluctance to modify established practices and a particular aversion to incorporating innovative technologies [63]. The characteristics of the market, heterogeneity, and immobility make it difficult to innovate. Real estate transactions face the challenge of information inefficiencies and, consequently, high transaction costs.

In the UK, the process of buying and selling properties is widely recognized as a highly stressful life event, often compared to significant milestones such as marriage, divorce, or having a child. The process is inherently outdated, complex, and fragmented. It is highly time-consuming and represents a considerable financial burden for buyers and sellers, given the annual incidence of more than a quarter of house sales falling through. The UK Government has acknowledged the need to enhance consumer understanding and transparency within the existing process, as such measures are critical to improving the overall experience. As a result, the government has committed to undertake a comprehensive process reform,

aligning it with the interests of buyers and sellers and mitigating the associated negative impacts. Based on a recent extensive investigation of the housing market, the UK government has determined that inadequate customer experience, significant time investment, inefficiencies, and a high transaction failure rate are the primary challenges property buyers and sellers face. These issues are primarily attributed to an inherent lack of transparency and the excessive fragmentation of the property market, which collectively contribute to many of the problems associated with buying and selling property. To address this problem, the UK Government launched a public consultation period from October 22, 2017, to December 17, 2017. The 2017 Conservative Party manifesto explicitly stated the Government's commitment to reform and modernize the home buying process to make it more efficient and cost-effective. The research [64] concluded that one of the critical areas of improvement is a 'better consumer experience'. According to the Ministry of Housing, Communities and Local Government, "...we are on the cusp of a digital revolution, which will allow us to replace the current largely paper-based approach to buying and selling." Moreover, there is a growing belief that technology could be transformative in this regard, offering the potential for significant improvements in the near future. According to the House of Commons Briefing Paper n. 06980, published on 27 February 2022[65] ('The Report'), the conveyancing process is complex, lengthy, fragmented, opaque and multi-staged. The Report recognized some key areas of concern, such as (a) the time taken to complete a transaction, (b) transaction failures, (c) consumer inexperience, (d) lack of transparency, (e) weak regulation of estate agents, and (f) lack of digitization which require urgent improvements.

The time taken to complete an investment is critical in determining the liquidity of real estate markets. Extended transaction timelines can impede timely entry and exit from the market, resulting in delays and potentially high opportunity costs for both buyers and sellers. In recent years, blockchain technology has gained traction in the real estate sector for its potential to introduce greater efficiency, transparency,

and reliability [63]. By automating key stages of the transaction process, blockchain systems offer the possibility of reducing the overall time required to complete a sale [66]. This is achieved through improved organisation, secure access management, and streamlined data distribution and verification. The integration of blockchain with smart contracts further enhances this capability by removing the need for multiple intermediaries. Trust between parties can be established through automated logic embedded in code, replacing manual enforcement with self-executing protocols. These digital contracts, stored on immutable and tamper-resistant ledgers, ensure that the terms of agreement are enforced consistently and transparently. As a result, Multiple intermediaries that in the current process contribute to increasing transaction costs might no longer be necessary [67].

Low liquidity is widely recognised by participants as a defining—and often problematic—characteristic of commercial property as an investment class [68]. In general terms, liquidity refers to an investor's ability to convert assets into cash (or vice versa) with minimal delay and minimal value loss [69]. However, this concept has been further refined by Crosby (2004) to encompass not just the speed of conversion but also the reliability with which an asset can be sold at or near its market value [68]. Liquidity in real estate is multi-dimensional, encompassing factors such as: (I) the rate of turnover/transactions and the time taken to transact, (II) the costs associated with transacting (both formal costs, buy or sell fees, and information costs), (III) the price of the asset and the prices of similar assets, and (IV) uncertainty regarding the return. Empirical studies, such as Devaney et al. (2015, 2016) [70, 71], have explored these dimensions in detail, particularly focusing on the time required to secure a buyer or seller, the duration until financial settlement, and the potential losses incurred when investors are compelled to hold real estate instead of more liquid alternatives like cash or equities. Much of the literature concentrates on how delays in property transactions can impede entry and exit timing, increasing risk exposure. This delay not only affects returns but also contributes to volatility, as investors become uncertain about when capital will be available. Bond (2004) [72] further notes that liquidity constraints have two compounding effects:

they prolong the period required to realise the market value of an asset, and they expose the seller to the risk of price movements during the sale process . Extended transaction times raise the likelihood of market fluctuations, thus introducing uncertainty into expected cash flows and undermining portfolio management strategies. Overall, liquidity in real estate seems to be "the relative ease with which an asset may be sold" [72]. From this standpoint, accelerating the transaction process is a crucial objective for improving market liquidity.

The first empirical study of time to transact for the UK commercial real estate market was presented by McNamara in 1998 [69]. Through a survey of investment principals and agents directly involved in the transaction of investment-grade real estate on behalf of institutional investors, McNamara explored the acquisition and sale process for commercial real estate to measure typical transaction times from both a buyer and a seller perspective. The author identified three critical points in the transaction process (heads of terms/price agreement, exchange, and completion), which correspond to the three stages: search (buyer) or marketing (seller), due diligence, and settlement. The survey provides indicative times for these stages for different segments of the real estate market. According to the study, simpler and more common forms of property were faster to purchase and sell. For example, a seller was judged to need 4-6 weeks to find a buyer for high-street retail units and individual retail warehouses versus 6-8 weeks for offices and 7-9 weeks for shopping centres. Due diligence was also considered quicker at 4-6 weeks versus 12 weeks for shopping centres.[70].

Similar studies were undertaken on the buy side, where it was found that longer times were needed to allow for the search and selection of appropriate assets. There was more variability in the transaction times for larger and more complex asset types. Using data on 187 transactions collected from the records of three major commercial real estate investors for 1995-1996 and 2000-2002 [68], this study measures the average time per stage of the sale process. McNamara's stages of the sale process are extended to six: (I) the decision to sell sector, (II) pre-marketing, (III) marketing, (IV) due diligence, (V) exchange and (VI) completion. The authors

found the mean transaction time to be more than nine months and the median time greater than six months. They noted significant variability in the time taken to transact, not only in the marketing stage but also in the due diligence stages of the transaction. From the data collected, the authors found that some generalizations could be made concerning the causes of longer and shorter transaction times, highlighting the need to disaggregate the data and increase the sample size, the number of funds, and the range of ownership.

More studies are being conducted in 2013 [73]. The buy side is analyzed using data from the transaction principals and collected from the sell side as part of IPF (2004)[70]. The work concentrates on the due diligence stages of the transaction, so a comparative analysis of changes in time to transact can be made between the two periods represented in these two studies. The study finds that shorter times from the point of price agreement to the completion of the transaction are associated with greater transaction volume and steadily increasing returns, which means that the time to transact varies with overall market activity. From the interviews, a significant overestimation of asset liquidity emerges. The respondents indicated typical times that are often substantially shorter than the median times determined from the samples studied. This underestimation suggests that practitioners believe that real estate assets transact faster and are more liquid than the data indicate. However, it should be noted that the findings were based on a comparatively small number of transactions (93) and the IPF study [71] increases the sample to nearly 600 commercial real estate transactions in the UK. The IPF study provides an extended analysis of transaction times and stages for UK commercial real estate. Data were collected by approaching investment organizations willing to provide the relevant information. Based on work in the IPF study [70], the research has provided up-to-date measurements of time to transact for both sales and acquisitions, providing interesting insights [71]. The median time for purchase from introduction to completion was between three and four months, while the median time for sale from marketing to completion was four to five months. There is a lot of variation around the median times, and the market state has an important explanatory role, with slower

transaction times recorded since the UK market crash in 2007-2008. Transactions involving institutional investors appear to be more likely to complete quickly, as do transactions involving UK buyers. Lower-quality assets and portfolios of buildings took longer to transact, and price agreements were reached much more rapidly for small lot sizes (below £10m) than for properties in larger lot size bands. Overall, there was only a weak correspondence between transaction times and price, with the most significant differences arising in the introductory phase of a transaction. Location and property type also affect the time to transact, with shopping centres taking longer than standard retail units and standalone retail warehouses and offices in central London transacted more rapidly than elsewhere in the UK. Most of the findings were reasonably expected. However, surprisingly, the asset price was not found to be a significant determinant of the time to transact compared to other factors. This is interesting because liquidity is often considered a function of price: a lower price equates to greater asset liquidity. The research indicates that "a full assessment of the characteristics of liquidity in commercial real estate markets requires the study of transaction times" [71].

To summarize, most of the studies analyzed consider the time to buy/sell a property from the marketing period to the settlement. McNamara (1998) [69] breaks the sales process into three parts: marketing, due diligence, and settlement. The process is then reviewed [68] and McNamara's stages are adapted, expanding them from three to six: 'decision to sell/select sector, pre-marketing, marketing, due diligence, exchange and completion'. Other studies [70] measure the time taken per transaction, dividing the process into four main stages: Marketing to price, Introduction to price, Price to exchange, Exchange to completion. Finally, for further clarity, the IPF Study [70] measures the average time taken for seven stages: Introduction to Price Agreement, Price Agreement to Solicitor Instruction, Solicitor Instruction to Exchange of Contracts, Exchange to Completion, Introduction to Price/Solicitor Instruction (this phase combines the early parts of the transaction), Price/Solicitor Instruction to Completion (time from the price agreement and

solicitor engagement to the completion of the transaction) and Introduction to Completion (total time taken including all phases). This seven-phase model provides a more detailed view of transaction timing and allows a more accurate analysis of liquidity, delays, and inefficiencies in the property market.

2.2.1 Blockchain and new technologies in real estate

The construction industry has been slow to adopt process and technology innovations, and construction productivity has declined in some markets since the 1990s [74]. Project planning remains uncoordinated between the office and the field, and incentives for risk sharing and innovation are not included in contracts. In addition, performance management is inadequate and supply chain practices are still unsophisticated. The real estate industry has generally been slow to adopt new technologies to automate manual procedures [75], particularly the construction industry, which is considered among the weakest digitized industries. This has reduced the productivity and efficiency of this industry over time [76].

New digital technologies offer solutions to increase the efficiency and productivity of real estate activities and improve transparency. 'Globalization and the consequences of the economic and financial crisis of 2007-2008 have stimulated the interest of stakeholders in transparency in real estate markets. However, the low transparency of the real estate markets remains a problem for most countries, affecting the level of real estate investment.' [75]. In recent years, governments have paid more attention to real estate transparency and have recognized the role of transparency in facilitating new real estate investment and supporting well-being and social inclusion. Technology can improve transparency and liquidity in the real estate market, bringing lower transaction costs, which should positively impact the value of investments. Furthermore, the financial crisis of 2007-2008 motivated regulators, central banks, foreign investors, and real estate professionals to contribute to increasing transparency by publishing data. This has led to significant improvements in transaction procedures and more efficient and closely monitored lending. As a result, open data access and technological innovations have become

the new determinants of transparency in the real estate market.

There is a clear relationship between real estate digitalization and transparency. Technology and innovation constitute the foundation of a new field, 'real estate technology', also called property technology or PropTech. [75]. The emerging PropTech has driven expectations of a significant improvement in transparency as it generates large volumes of data that increase the information available on the property market. The efficient use of these data generally leads to higher returns on real estate investments. Digital data has become central to innovation in the real estate industry. In this perspective, "the real estate data become a tradeable commodity, and that data might actually become the central resource of the digitalised real estate market." [77]. Companies such as Zoopla have information technology and data at their core. Information technology enables digital business models that collect, aggregate, and process information. The processed information is essentially the service that adds value to the users. While using the service, users provide other valuable information to the firm itself, which can be the basis for novel products and services.

The high-dimensional and granular data provided by sellers and buyers of houses on Zoopla provide a unique source of market information for the platform owners. It is unknown whether the platform saw any immediate value from the user-provided data. However, over time, more sophisticated information technologies became available, and novel applications started to generate value from user data. There is significant evidence that PropTech is turning real estate into a data-driven market. It emerges that a cluster of data analytics technologies is at the core of the network of all property technologies. It is also observed that data analytics and related technologies can obtain substantially more venture capital funding than other sectors. Even though the core business of real estate remains material or space-based, the PropTech boom proves that essentially, information around using, managing, or owning real estate can be digitalized, and the Proptech phenomenon is

leading to the datafication of real estate processes. [77]. Big data analytics and machine learning technologies represent only a part of the new technologies that can disrupt the real estate industry, making it potentially more efficient and effective. A recent body of literature highlights how the development of new smart technologies, such as Building Information Modeling (BIM) and blockchain technology, can substantially benefit the industry. The current application of BIM focuses on smart energy and construction management. At the same time, there is still little attention to applying BIM to sustainable design and proposing strategies to promote the usability of these technologies in the management of building construction projects.

There is great potential for innovation in the AEC industry (Architecture Engineering Construction) by integrating BIM and blockchain technology [78]. The complete digitalization of the construction industry is still in its infancy. Great effort must be put into effectively integrating production, business and management levels, project data, and management information. With BIM technology, professionals such as architects, structural and building service engineers, and other discipline designers, including the client, can use the same BIM model for sustainable building design and planning. The BIM model functions as a faithful representation of the physical building and represents a single version to which all users can refer. In addition, the model can render a three-dimensional visualization of the building. It contains comprehensive data on size, location, relative spatial relationships, and other pertinent details. It serves as an index linking to additional information on building materials, including cost and quantity. [78]. BIM is an extremely valuable tool for promoting innovation in the AEC industry. However, there are potential challenges to the implementation of BIM in terms of legal barriers and ownership of the model, including a series of risks, such as technical, management, environmental, financial and legal risks [78]. Implementing BIM also introduces other issues and risks, such as intellectual property and cyber security, the development of comprehensive and clear reuse and adoption strategies, and finally, the level of responsibility. Integration, a characteristic of BIM, blurs the level of responsibility between different members of the project team, raising issues about trust and collab-

oration. Therefore, new contracts would be required to regulate the responsibilities, limitations, and liabilities. Interestingly, blockchain-enhanced BIM implementation could be beneficial to addressing challenges in sustainable building design by effectively managing information on the project. Combining the application and development of intelligent technologies such as blockchain, BIM can better integrate data and resources and establish clear responsibilities and contractual relationships [79].

One of the most interesting applications of blockchain is the possibility of introducing smart contracts. Smart contracts are computer programs that a network of mutually distrusting nodes can consistently execute without the arbitration of a trusted authority [80]. Smart contracts can be defined as computerized transaction protocols that execute the terms of a contract. The basic idea behind smart contracts is that many types of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the software to make a breach of contract expensive (if desired, sometimes prohibitively so) for the breached [81]. The ultimate mission of smart contracts is to replace traditional contracts with a new method of technological contracts. Through this process, smart contracts enable companies to operate with significantly fewer disputes and the need for law enforcement or court intervention. They can even negotiate with other parties autonomously (or smart contracts between other parties) [78]. Blockchain (BC) uses cryptography to store transactions in blocks of data that are replicated across multiple nodes (computers) around the world. By allowing smart contracts, the combination of BIM and BC replaces mutual trust in third-party intermediaries with an automated process where a computerized trading protocol is designed to enforce project terms. Furthermore, through the entire design-led construction phase, blockchain can be a useful tool to manage and document changes to BIM models. Smart contracts and the combination of BIM+BC could reduce technical, management, environmental, financial, and legal risks and help manage intellectual property and cyber security [78, 82].

Although the construction and project phases offer great potential for

blockchain technology applications, this study focuses only on real estate transactions and the due diligence process. As we intend to investigate how blockchain technology can help increase transparency in the sector and combat money laundering, these phases are more significant to our scope.

2.2.2 Money laundering in real estate

Money laundering in the property market has attracted significant attention in recent years. The UK has widely suggested that corrupt capital is used to buy property, often using offshore companies with non-transparent ownership [83, 84]. It is well known that the real estate sector offers multiple opportunities for money laundering, and it has been one of the most common and simplest means of laundering money for more than a century [85]. Indeed, in 2016, the then Prime Minister of the UK stated that “here in the UK, we want to clean up our property market and show that there is no home for the corrupt in Britain” [83]. A 2015 European study [86] found that the real estate sector is among the areas where money laundering was the most prevalent, together with hospitality (bars, restaurants and hotels), construction, wholesale and retail trade, and transportation. There are multiple reasons why real estate is a target of money laundering. One of the main reasons is the considerable amount of money involved in buying or renovating properties. This enables large cash transactions using illicit financial gains that can be converted into a legitimate outcome later. A second attractive feature is the relatively low levels of anti-money laundering compliance and suspicious transaction reporting currently being implemented within the sector. This poor regulatory framework prevents large cash transactions from being reported to law enforcement or financial intelligence units [87]. Another reason for targeting real estate is to minimize the risk of detection by avoiding regulated industries, such as the financial sector, characterized by high compliance standards [88]. In the context of property transactions, a proportion of the purchase price can be funded using unlawfully acquired funds, with potential tax advantages for both the purchaser and the vendor in numerous instances. Following the acquisition, property renovations can also serve as a means of facilitating money laundering. An individual may allocate a portion of the renovation expenses

using legitimate funds, while unlawfully acquired resources cover the remaining portion. Subsequently, these properties can be legitimately or fictitiously leased after the completion of the renovations. Although high-profile deals may attract attention through media coverage, small transactions are unlikely to become the subject of investigation [4].

In summary, these are some key reasons why real estate is a target of criminal activities. (I) *Large and diffuse market with low barriers to entry.* Real estate transactions represent a high-volume activity involving property acquisition and financing across a wide range of actors—from individual buyers to multinational firms. Unlike financial markets, real estate operates under less stringent oversight, allowing transactions to be conducted with considerable flexibility and limited regulatory scrutiny. These transactions are often privately negotiated, tailored to the needs of the parties involved, and rarely subject to standardised procedural frameworks. Moreover, participation in real estate activities requires no formal qualification, making it accessible to a broad pool of individuals and entities. (II) *It is considered a secure investment.* Real estate assets are widely regarded as vehicles for preserving wealth over time, as they are less directly affected by operational decisions than active businesses. The legal frameworks that guarantee the title of the property further reinforce the perception of security. However, the identity of the beneficial owner may remain concealed, complicating efforts to trace the true source of funds. (III) *Speculation.* Real estate inherently involves speculative investment strategies, allowing individuals to justify substantial increases in property value. This characteristic can be exploited by criminals who use short-term property purchases to integrate illicit funds, masking illegal gains as legitimate investment returns [89]. (IV) *Heterogeneity.* The uniqueness of each property—in terms of location, structure, and other features—makes it difficult to assess whether a transaction price reflects true market value. This complexity opens the door to price manipulation, which can be used to facilitate money laundering. (V) *Multiple actors involved.* The real estate ecosystem involves a wide variety of profes-

sionals (e.g., agents, solicitors, landlords, lenders) who carry out distinct functions. This fragmentation complicates the implementation of unified anti-money laundering practices. In the UK, for example, estate agents have expressed frustration over inconsistent guidance from regulatory bodies such as HM Revenue and Customs (HMRC) and the National Crime Agency (NCA) on the scope and execution of their AML obligations [90].

2.3 Recent changes and the role of technology

Despite persistent opacity, the art market is not a legal void as commonly believed [61]. It has recently undergone deeper scrutiny, particularly in the context of increasing concerns related to money laundering and terrorist financing. Efforts to regulate this sector have increased, and in 2018, the EU approved the Fifth AML Directive for implementation by Member States by January 2020. This Directive aims to incorporate art dealers into the scope of the regulated sector, ensuring their adherence to anti-money laundering regulatory requirements. In February 2023, the UK government approved the Guidance on anti-money laundering for the UK Art Market Participants [91], which extends AML directives to the art market, while previously, AML regulations focused on sectors such as banking, legal services, and property services (estate agents). In addition, efforts have been made to increase transparency in the insurance sector, providing more stringent regulations. Indisputable evidence substantiating ownership becomes a necessary condition to stipulate policies. Furthermore, periodic updates are required on the item appraised to adjust their value proportionally between the previous evaluation and the market value [20].

Similarly, the real estate sector has been subject to more stringent anti-money laundering regulations. The first EU Money Laundering Directive (MLD) was issued in 1991, and a twin-track approach was adopted based on criminalization and the prevention of money laundering. In 2001, the second MLD was adopted, and AML obligations were extended beyond credit and financial institutions to non-financial businesses and professions. At various times, AML efforts have been

driven more generally by the fight against organized crime and anti-corruption and antiterrorism plans, particularly after 9/11 [90]. The Fifth Money Laundering Directive (5MLD) was transposed into UK law and came into force in January 2020. It expanded the due diligence checks required by the gatekeepers of the financial system, including those involved in real estate transactions. As part of the Economic Crime (Transparency and Enforcement) Act 2022, a register must be maintained where overseas entities owning UK properties declare their beneficial owners. Interestingly, in recent years, multiple studies regarding anti-money laundering regulations have moved their focus to developed jurisdictions rather than to countries that are the source of corruption. This is because “...the bigger the financial centre, the more dirty money flows through it, including the proceeds of foreign corruption.” Therefore, endeavours to target corruption cannot merely focus on the source but must also include destination (or ‘host’) countries [90]. Although extensive international efforts have been made, the execution of money laundering in fine art and real estate remains alpracticable. White-collar criminals use straw-men and complex structures to avoid detection. This practice makes it difficult to identify the beneficial owner even when assets are identified as suspicious. To combat money laundering more effectively, greater global cooperation is needed. Money launderers can set up chains across multiple jurisdictions to obstruct law enforcement agencies, as obtaining information from another jurisdiction can take a considerably long time, even years. For this reason, if money launderers use offshore structures in multiple jurisdictions that do not cooperate promptly, law enforcement becomes almost impossible [92].

The emergence of digital art market databases has reshaped the flow of information within the art ecosystem, contributing to a specific form of transparency in an otherwise opaque market. Platforms such as Artnet, Artprice, Artsy, and Verisart offer access to auction results, provenance records, and authentication tools, thereby facilitating greater informational access for a wider range of users and institutions [93]. These platforms function as digital intermediaries that do

not necessarily replace traditional actors such as gallerists or dealers but rather reconfigure their role by aggregating data and redirecting attention, effectively engaging in a process of reintermediation [93]. While this development is often presented as enhancing transparency, its effects are uneven. The visibility provided by auction price data is frequently overinterpreted by non-expert users as objective market value, despite lacking critical contextual information such as provenance, condition, curatorial significance, or private sales dynamics [94]. This overreliance on *thin* indicators, in the absence of *thick* expert valuation, reproduces evaluative frictions and reinforces the gatekeeping role of traditional intermediaries who retain privileged access to non-public information [94]. Moreover, the epistemic authority to structure and legitimise valuation practices remains with those who control data infrastructures and performance frameworks, reinforcing asymmetries rather than eliminating them [95]. Consequently, although art market databases support greater access to information, they simultaneously enable new hierarchies of expertise and visibility, leaving intact the strategic discretion of intermediaries. This underscores the importance of architectural choices, such as the integration of cryptographic auditability, decentralised identity verification, and rules-based disclosure, within blockchain-based systems designed to mitigate information asymmetries in sectors like fine art and real estate.

Beyond its widely discussed potential to enhance transparency and efficiency in transactional systems, blockchain technology presents specific and tangible applications for anti-money laundering (AML) compliance. In the context of fine art and real estate—two sectors often characterised by opacity, fragmented oversight, and the use of high-value assets for illicit financial flows—blockchain can offer a secure and auditable infrastructure where key compliance processes are embedded at the protocol level. By enabling immutable recording of ownership history, identity verification, and transaction metadata, blockchain systems can support a rules-based framework for due diligence, including automated KYC validation, screening against PEP and sanctions lists, and audit trails for provenance verification. Smart

contracts further enhance this by allowing for the enforcement of predefined compliance logic, such as conditional execution based on risk thresholds or red-flag indicators, thus reducing the reliance on post-factum manual interventions. In addition, blockchain auditability enables continuous monitoring and retrospective investigation by regulators or auditors. In the proposed system, these features are complemented by a transaction scoring mechanism that leverages verified metadata to assess risk levels in real time, enabling early detection of suspicious activity. This data is anchored on-chain through cryptographic hashes, ensuring that verification processes are both tamper-resistant and compliant with privacy laws. This architectural model replaces ad hoc and institution-specific AML practices with a consistent, interoperable framework, thereby facilitating both cross-border cooperation and regulatory alignment, without compromising data confidentiality.

Chapter 3

Research background. Blockchain technology

This chapter examines the key characteristics of blockchain technology, providing a critical foundation to understand its core components, including blockchain types and architecture, data management, and governance. Alongside with the literature review (Chapter 2) and the case studies discussed in Chapter 4, this analysis forms a necessary precursor to the development of the Proof of Concept (Chapters 5 and 6) and the proposed blockchain solution (Chapters 7).

3.1 Blockchain across industries

Blockchain (BC) is a digital technology that has gained traction in multiple industries over the past ten years [96, 97, 98, 80], with cryptocurrency-related projects attracting an estimated amount of 17 billion US dollars in 2021 in institutional investments [99, 100, 101]. The blockchain, or distributed ledger, is a distributed database that maintains a permanent record of tamper-proof and forgery-resistant transactions. Blockchain technology utilizes a peer-to-peer system that consists of nodes that make their (computational) resources available for transaction relay and verification. Each node in the distributed network maintains a copy of the ledger to prevent fraudulent alterations of the blockchain [102, 103]. This technology is currently stimulating a broader process of social and industrial transformation, impacting several potential areas of adoption (e.g., payments, tracking and trac-

ing solutions, authenticity, etc.) [104]. Blockchain is expected to play an essential role in the sustainable development of the global economy, bringing benefits to consumers, the current banking system, and society in general [105]. “With blockchain, we can imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, protected from deletion, tampering, and revision. In this world, every agreement, every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored, and shared (...). Intermediaries such as lawyers, brokers, and bankers might no longer be necessary. This is the immense potential of blockchain” [106].

This vision of embedded trust and automation through code aligns with the principle that “code is law” [107], meaning that in blockchain systems, governance is enforced not only through institutional rules but through the software architecture itself. In such environments, the code defines what is permitted and what is not, embedding compliance, access, and verification mechanisms directly into the protocol. This marks a shift from regulation by enforcement to regulation by design, with significant implications for enhancing transparency, reducing reliance on intermediaries, and addressing vulnerabilities in sectors exposed to opacity and manipulation.

The idea of blockchain is theorized in the Bitcoin white paper by the person or group still mysteriously and pseudonymously identified as Satoshi Nakamoto [108]. The paper, published in 2008, is a revolutionary text which outlines a tamper-proof, decentralized peer-to-peer protocol that could track and verify digital transactions and generate a transparent record open for everyone to inspect in nearly real time. The blockchain protocol is a cryptographically secure system based on a Proof-of-Work algorithm. Bitcoins are ‘mined’ for a reward by individual nodes and verified by other nodes in a decentralized network. The technology can potentially replace centralized systems and change the whole industry due to disintermediation. This system contained the possibility of overcoming the need for banks and financial institutions, disrupting the siloed, monopolized field of centralized economic power.

Blockchain solutions are not limited to the exchange of cryptocurrencies. There are multiple benefits that this technology can present to businesses in different industries due to its distributed and decentralized nature [109]. Here are some examples. (I) *Greater transparency*. The transaction ledger for public addresses is open for viewing. In financial systems and businesses, this adds an unprecedented layer of accountability, making each business sector responsible for acting with integrity toward the company's growth, community, and customers. (II) *Increased efficiency*. Due to its decentralized nature, blockchain removes the need for intermediaries in many processes for sectors such as payments and real estate. Blockchain facilitates faster transactions by allowing P2P cross-border transfers with a digital currency. Property management processes can become more efficient with a unified system of ownership records, while smart contracts automate tenant-landlord agreements. (III) *Better security*. The blockchain is more secure than other record-keeping systems because each new transaction is encrypted and linked to the previous transaction. The immutable and incorruptible nature of blockchain keeps data integrity secure from falsified information and hacks. The decentralized nature also gives it the unique quality of being 'trustless', as parties do not need to trust each other to transact safely. (IV) *Improved traceability*. Each time a transaction is recorded on a blockchain, an audit trail is present to trace where the goods came from. This helps improve security, prevent fraud in exchange-related businesses, and can also help verify the authenticity of traded assets. Across different industries, this can be used to track the supply chain from manufacturer to distributor or to provide irrefutable proof of ownership. The inherent characteristics of blockchain architecture and design provide properties such as transparency, robustness, audibility, and security [104]. Companies invest in this technology because they see the potential to decentralize their architectures and decrease transaction costs as they become intrinsically safer and transparent. As a result, blockchain technology is becoming increasingly relevant. It is applied to various financial sectors, including business services, settlement of financial assets, prediction markets, and economic transactions. It is expected to play an essential role in the sustainable development of the

global economy, bringing benefits to consumers, to the current banking system, and the whole society in general [105]. Below is an overview of some of the ramifications of technology in sectors and subsectors [80], other than real estate and fine art, which will be analyzed in dedicated Chapter 4.

- *Financial applications.* Financial services have been the key sector for BC experimentation and deployments. The complexity of this sector and its structure, inherently characterised by layers upon layers and intermediaries, represent a very significant incentive to implement the new technology, which can improve margins and promote competitiveness. The global financial system explores using blockchain-enabled applications for financial assets, such as securities, fiat money, and derivative contracts. Blockchain technology promises to provide a more efficient way of performing operations such as transactions, digital payments, loans or cryptocurrency payments.
- *Integrity verification.* Blockchain integrity verification applications store information and transactions regarding the creation and lifetime of products or services. Data can be recorded in a blockchain, and since transactions on the blockchain are time-sensitive, the verification can be time-stamped after the corresponding transaction is recorded in the blockchain. This process enables users to check whether auditors perform the verifications at the prescribed time. Interesting applications are provenance, counterfeit, insurance, and intellectual property (IP) management. Implications for BC, specifically in the health insurance sector, may include the establishment of more secure data archives for medical and wellness information, for setting up alerts to take prescriptions or make regular doctor visits, facilitating pricing assessments, establishing more up-to-date risk pooling, and for allowing for more personalisation and individualised coverage [110].
- *Organization and Governance.* Governments across all countries manage and hold official records of both citizens and/or enterprises. Thanks to disintermediation, the application of BC might change the way governments at the

local or state level operate and keep records of data [111]. Improving efficiency and increasing resistance to corruption could be achieved through the accountability, automation, and safety blockchain offers for handling public records. Blockchain governance aims to provide the same services offered by the state and its corresponding public authorities in a decentralised and efficient way while maintaining the same validity.

- *Voting system.* A promising development of BC is in the voting system, as blockchain could speed up voting processes, simplify and reduce the cost of elections, and the development of stronger democracies. Existing electronic voting systems rely on a proprietary and centralised design by a single entity, characteristics that harm the trust and confidence voters have in the voting process [112]. Conversely, blockchain technology offers an open-source, peer-to-peer, decentralised network (independently verifiable) which can gain the confidence required by voters and election organisers.
- *Healthcare.* Blockchain technology could play a crucial role in the healthcare industry. Multiple areas include public healthcare management, automated health claims adjudication, online patient access, patient data sharing, drug counterfeiting and clinical trials. BC could also provide an immutable record of patient's medical records and authorizations granted to third parties to look at this data. Opening medical records through blockchain enhances the portability of personal health records, facilitating customers in moving their care from one provider to another more easily and cost-effectively. Managing patients' Electronic Healthcare Records (EHRs) is considered one of the areas with the highest potential growth [113].
- *Energy.* The potential applications of blockchain in the energy sector may have a huge impact by reducing costs and enabling new business models and marketplaces [114]. Businesses can better manage complexity, data security, and ownership. BC technology may also be used to issue certificates of origin, particularly for green energy production and renewable energy sources

for developing peer-to-peer energy transaction schemes and establishing energy management schemes for electric vehicles. BC can enhance the transparency of the energy market system by guaranteeing accountability while preserving privacy requirements. Management of the energy grid can also be empowered as blockchain offers the possibility of multilateral and dynamic energy markets, promoting direct peer-to-peer trading.

3.2 Type of blockchains, governance and network

A blockchain is public when it is built as an open network with no privileged actors, and everyone can see the records and the entire transaction history (although the identity of pseudonyms can protect the parties who are transacting) [115]. Participants can use the blockchain to perform transactions and participate in consensus and transaction validation. Network users can vote on new proposals to update or modify the underlying protocol [116]. There is no special permission to submit transactions beyond the possession of some way to pay transaction fees. Everyone is also allowed to participate in the validation of the transaction [117]. Examples of public blockchains include Bitcoin and Ethereum.

Permissioned blockchains are distributed ledger systems where participants must receive explicit authorization to read, write, or validate data on the network. This category includes both private blockchains—operated by a single organization—and consortium blockchains, governed collectively by a group of trusted entities. In contrast to public blockchains, where anyone can participate, permissioned blockchains offer enhanced privacy, control, and operational efficiency, often at the expense of decentralization. While the terms “private” and “permissioned” are sometimes used interchangeably, private blockchains typically refer to networks with a single controlling authority, whereas permissioned blockchains more broadly encompass any system that restricts access, including those shared by multiple organizations. Private/Permissioned blockchains generally have simpler consensus algorithms due to the increased trust between endorsed participants [116]. A private or permissioned blockchain does not allow open participation in the submission or participation in the transaction validation process [117]. Examples of private blockchains include Quorum, Hyperledger Fabric, and R3 Corda. Despite their appeal for enterprise and regulatory applications, permissioned blockchains face non-technical adoption challenges. A notable case is IBM’s decision to scale down its support for Hyperledger Fabric—once a leading permissioned blockchain framework—due to weak market demand and lack of commercial traction. This example illustrates that even well-designed permissioned platforms can struggle without

strong ecosystem incentives and widespread stakeholder alignment [118].

The governance of permissioned blockchains is different from that of permissionless blockchains. The major difference is that permissioned ones may have clear authorities dominating the blockchain platform. [119]. When governing permissioned blockchains, we can refer to existing centralized decision-making models, as only a few stakeholders are involved. As a result, participation permission is commonly implemented in permissioned blockchain platforms to ensure security and privacy. Roles assigned in a permissioned blockchain are typically based on off-chain entities' positions rather than being elected. On the other hand, governance in permissionless blockchains is more complex, as these platforms are characterized by a high degree of decentralization, with no central authority or controlling entity. Therefore, governance mechanisms in permissionless blockchains must be designed to accommodate the decentralized and distributed nature of the platform while also ensuring transparency, fairness, and the protection of the network's security and privacy. Additionally, permissioned blockchains have a well-defined governance structure that can be aligned with the existing off-chain institutional hierarchy.

A permissioned blockchain, as the name implies, uses an approach opposite to that of the public blockchain, since it introduces control to provide access to participants in a network, having an administrator who assigns the roles to the participants in the network. [120]. In these networks, it is essential to ensure that no attacker or unknown entity can participate in the network, nor in the validation or creation of blocks, to prevent any potential attacks. Such networks are particularly suitable where the ledger is shared exclusively within their internal network. In particular, these types of networks are not entirely immutable, and transactions can be modified with some effort. This contrasts with public blockchains, where it is nearly impossible to alter transactions once they are recorded on the network. A significant advantage of private blockchains is greater certainty in the rules that govern how these blockchain networks operate. A consortium is a hybrid solution based on a semi-decentralized blockchain. A consortium blockchain combines the favourable characteristics of both permissionless and permissioned blockchain net-

works. Rather than entrusting most tasks to a single organization, a consortium blockchain distributes the same functions to nodes maintained by multiple organizations. In these networks, also known as semiprivate networks, one part of the blockchain is private and another is public. The private part of the blockchain is controlled by a select group of individuals or entities, while the public part is accessible to anyone. This hybrid model can be useful in scenarios where the private part of the blockchain remains internal and is shared among known participants. However, anyone can still use the public part of the blockchain, with the option of mining to secure the network. As a result, the blockchain can be protected by proof-of-work (PoW), which ensures consistency and validity for both the private and public parts of the network.[120]. There are two important models of decentralized ledgers: (I) the distributed ledger model (DLT), where the trusted intermediary runs all the nodes and participants access the nodes on a software-as-a-service basis, and (II) the shared ledger model, where the trusted intermediary runs a node that hosts a full copy of the database. Participants can also run their nodes that download a partial copy of the database (this copy only includes data to which the relevant participant is a counterparty)[121]. An example of a DLT is Hyperledger.

In any type of blockchain, incentivizing stakeholders to reach a consensus is crucial. The governance structure of a blockchain must include incentive mechanisms that motivate desirable behaviours and resolve conflicts between stakeholders. These are some fundamental principles to take into consideration: [122] (I) provide incentives to achieve consensus, (II) ensure a transparent decision process to promote trust, (III) ensure accountability through both institutional and technical measures, (IV) support ecosystem-level governance, and (V) manage legal compliance and ethical responsibility. In a permissioned blockchain, incentives may be distributed off-chain, following the institutional rules established by the top executives responsible for making major decisions and setting the overall strategy for the organization. The decentralized nature of blockchain drives the need for collective decisions on governance issues. Ensuring transparency in decision-making processes is critical to allowing stakeholders to monitor whether decisions are rea-

sonable and gain the trust of the whole community. Decision-making is based on the authority, responsibilities, and capabilities of relevant stakeholders. In a blockchain platform, the majority of governance-related decisions are made by developers, who determine both on-chain and off-chain meta-rules for the platform and its community. On-chain decisions include setting blockchain infrastructure, such as block size and interval, and designing consensus and incentive mechanisms that can regulate the behaviours of other stakeholders using the blockchain. Off-chain decisions in blockchain governance involve the implementation of code, the establishment of conflict resolution rules, formal communication channels, and onboarding and exit rules for the entire community. Moreover, it is important for blockchain governance to consider various risks, such as software bugs in coding, cyber attacks during operations, and breaches of commercial contracts. Risk management in the blockchain is achieved through platform updates and evolution, which involves the approval of improvement proposals and new features. The node operators are responsible for maintaining the blockchain network. They can hold local full nodes, which store all historical ledger contents, or light nodes with compressed information, such as block headers.

Users interact with blockchain services by submitting transactions to achieve personal goals. When encountering an abnormal function/service, a user can report to the project team for improvements, while other users can then join the voting of proposed solutions. After understanding the responsibilities of the nodes operator, the question is how to make them accountable for their decisions to ensure robustness of the entire system. In the context of blockchain governance, accountability refers to the ability to identify and hold stakeholders responsible for their decisions. Explicit enforcement of accountability is necessary to allocate responsibilities and capabilities among stakeholders. Failure to enforce accountability can lead to the abuse of power and, ultimately, the collapse of the blockchain system due to the risk of centralization. Accountability in blockchain governance can be established through institutional and technical means. Institutional accountability pertains to conventional governance structures in blockchain and requires standardized docu-

mentation to report the off-chain accountability process. Technical accountability is embedded in the distributed ledger, providing evidence for on-chain accountability by recording data and operations. Compared to off-chain accountability, the on-chain accountability process is less mature and depends on how developers design the blockchain platform to minimize risks and uncertainties. The level of accountability is also dependent on the degree of decentralization of a blockchain. In permissioned blockchains, it is mandatory to conduct identity verification for entities to join the blockchain. Therefore, it requires less effort to identify individuals who are accountable for specific events or operations.

Blockchain governance is not limited to the platform itself, but encompasses a broader environment that constitutes the overall ecosystem [123, 124]. The platform is the base of the blockchain ecosystem, which includes the underlying data on the chain, the superstructure of blockchain-based application systems, and the entire community, which comprises various stakeholders. Governance rules must be applied to these multiple layers. (I) *The platform layer*. Here is where governance-related design and tactics will eventually take effect. In the preliminary planning and analysis phases of a blockchain platform, the business context is evaluated to decide the appropriate blockchain type. Subsequently, during the design phase, the blockchain architecture, complete with all on-chain self-governance attributes, is developed. This involves establishing the distribution of decision-making rights, accountability, and incentives among the stakeholders. It is worth noting that if a blockchain platform requires updates or modifications as part of a risk management process, the governance structure in permissioned blockchains enables swift responses, such as forking or protocol replacement. (II) *Data layer*. In the blockchain ecosystem, data governance is integrated into the transaction lifecycle. During the design phase of a blockchain platform, on-chain data governance is taken into account, including the implementation of a standardized format to guarantee transaction quality, access policies to ensure security and privacy, and the use of sharding techniques to improve scalability. Once a blockchain platform is operational, trans-

actions are created and distributed as users submit data to the blockchain. During blockchain operation, the focus of data governance lies in maintaining accountable access control over transactions. Capabilities to read and write to the blockchain and validate transactions are allocated to specific stakeholders based on the type of blockchain being employed. In permissioned blockchains, for instance, validators are commonly designated by authorities. (III) *Application layer*. Blockchain governance also covers the use of blockchain as a component in software application systems. Application providers are required to conduct a suitability analysis of their domain knowledge and ensure that the adoption of blockchain technology is compliant with industry standards and regulations during the initial stages. Subsequently, the implementation and testing phases rely on the APIs and testnet offered by the blockchain project team. During application operation, changes in industry regulations and specifications may necessitate new requirements, leading to upgrades of the underlying blockchain platform. (IV) *Community layer*. The commencement of blockchain platform development marks the establishment of a corresponding off-chain community. As the blockchain platform becomes officially operational, the community expands with the participation of various stakeholders, who participate in subsequent decision-making processes. With the advancement and maturation of the blockchain platform, the off-chain community gradually becomes more specialized, ultimately leading to the formation of different groups based on their roles and decision-making rights.

An additional crucial aspect is the training of blockchain practitioners, which plays a critical role in the capacity development and future growth of the workforce [122]. Equipping practitioners with the necessary expertise for the design and implementation of blockchain platforms and applications is essential to avoid potential flaws and improve trust among other stakeholders. The last principle emphasizes the importance of ensuring that all governance-related decisions and processes adhere to existing legal regulations and ethical responsibilities. Ensuring legal compliance depends on the location where blockchain platforms and applications are launched and deployed, as well as on how regulators, such as governmental institutions, de-

velop policies to protect the blockchain development process and mitigate risks and uncertainties within the overall ecosystem. Promoting and encouraging ethical principles and guidelines in blockchain governance can help support and protect human values, and the whole ecosystem will be more responsible and trustworthy. This can help to create a more responsible and trustworthy ecosystem where stakeholders can engage in ethical practices and ensure that the benefits of blockchain technology are realized while minimizing potential harm. By incorporating ethical principles into blockchain governance, the technology can be developed and utilized in a manner that prioritizes the well-being of individuals and society as a whole. For example, blockchain technology is often criticized for its energy-intensive platforms and applications, particularly those utilizing the Proof of Work (PoW) consensus mechanism. As a result, reducing energy consumption and benefiting the environment has become a significant governance topic. By incorporating ethical principles into blockchain governance, stakeholders can work together to develop and implement solutions that address energy consumption and promote sustainability, such as using alternative consensus mechanisms or adopting energy-efficient technologies. This can ultimately help mitigate the negative impact of blockchain technology on the environment and promote more responsible and sustainable blockchain governance practices. In this regard, private and semi-private blockchains are generally more energy efficient than public permissionless blockchains as they do not have to perform any PoW since all stakeholders are identified.

In summary, good blockchain governance should address the following issues [124]. (I) *Adaptability*. Blockchain technology needs to meet the specific requirements and constraints of the public and private sectors. Consequentially, stakeholders may need to modify the deployed blockchain systems significantly. (II) *Upgradability*. It refers to the blockchain capability of being upgraded in functionality by adding or replacing blockchain components. (III) *Security*. Governance needs to ensure that the daily operation of blockchain is performed in a trustworthy manner, protecting the data and digital assets against malicious attacks. (IV) *Social orders*. Effective governance in the decentralized environment of blockchains

involves pursuing collective goals and balancing power relations. A blockchain community typically encompasses various types of stakeholders. Given the complexity of the environment, governance models are necessary to establish and maintain social order among these stakeholders. (IV) *Privacy*. In a permissionless blockchain network, information is typically open and visible to all nodes that are part of the network and any devices with access to those nodes. This can pose a risk in scenarios where confidential data should only be accessible to selected participants. Therefore, governance mechanisms are necessary to safeguard sensitive data stored in the blockchain. (V) *Censorship resistance*. Permissionless blockchains represent a censorship-resistant technique which enables rules as code. The maintenance of this censorship-resistant property relies on the collective decision-making of all participants in the network. Governance can foster trust among stakeholders and enable effective coordination in a decentralized environment by providing a framework for decision-making and accountability.

3.3 Data management

Although blockchain provides a transparent, immutable and consistent data store, it also introduces new challenges in terms of data management. This technology can improve data quality, but it brings new challenges regarding privacy and security. The concept of a data-sharing ecosystem in which multiple participants participate in providing, using, and sharing data has gained wide acceptance among many organizations. However, in a blockchain environment, there remains a persistent issue of possible data breaches or abuse and misuse due to the complex nature of interactions and the sophisticated information diffusion schemes employed within these systems [124]. In this regard, the European General Data Protection Regulation (GDPR), enforced by law since May 2018, applies to any organization that interacts with data subjects located in the European Union (EU) [125]. Some of the most significant privacy requirements are the following. (I) *Access/Timeliness*. The data owner has the right to access and view their personal data. Furthermore, a request of an individual for any information about their personal data should be responded to without undue delay. (II) *Rectification*. The data owner should be able to correct inaccurate data concerning him or her. (III) *Restriction of usage*. Personal data can only be processed with the consent of the data owner. (IV) *Portability of the personal data*. The individual has the right to receive personal data in a structured, commonly used, and machine-readable format and to transmit the data to another service. (V) *Right to be forgotten*. The individual has the right to the erasure of personal data concerning him/her without undue delay.

Data privacy is still an open issue for blockchain-based systems, and there are growing concerns about whether blockchains will be able to comply with these recent regulations. In a public blockchain network, the individual whose data is stored in the system has the unrestricted right to access and obtain their personal data promptly. The absence of a “privileged” participant in a public blockchain, also known as permissionless, allows for this access. However, in a permissioned blockchain, access and timeliness of data may be restricted to those with appropriate access rights within the network. The ability to correct inaccurate data is contingent

on the ownership of the transaction record. If the individual is the owner of the transaction, they may issue another transaction to rectify the error. Otherwise, the possibility of correcting an error will depend on the transaction owner's response to a rectification request. Although blockchains do not inherently provide a mechanism for enforcing user consent for data usage, smart contracts offer a transparent way to encode and enforce access policies. Furthermore, smart contracts can specify the conditions under which data can be accessed or used, providing an additional layer of protection for users [126].

Since the introduction of the General Data Protection Regulation (GDPR), the notion of the "right to be forgotten" has gained significant attention. Because blockchain records are designed to be immutable, erasing data to comply with this requirement is impractical. However, new technologies in the blockchain environment are trying to overcome these issues. The blockchain governing body, as a platform provider, has to ensure that the platform is designed in a privacy-friendly manner using the Privacy by Design (PbD) approach. This means that privacy is embedded into the design, with end-to-end security, visibility, transparency, and respect for user privacy. Some solutions allow each user to have a separate chain and do not require full data replication across the network. This limits the distribution of data and may increase the level of privacy. [126].

A crucial aspect of data management on blockchain is ensuring that the data stored is accurate and reliable, as the value of the data depends on its quality. Therefore, it is important to define what *data quality* is. This research refers to the standard quality defined by specific institutions [127, 128]. These standards assess data quality considering a variety of dimensions, some of which are the following [128]. (I) *Consistency*. The degree to which data have attributes free from contradiction and coherent with other data. (II) *Traceability*. The degree to which data have attributes that provide an audit trail of access to data and any changes made. (III) *Availability*. The degree to which data have attributes that enable them to be retrieved by authorized users and applications. (IV) *Compliance*. The degree to which

data have attributes that adhere to in force standards, conventions, or regulations and similar rules relating to data quality. (V) *Confidentiality*. The degree to which data have attributes ensuring that they are only accessible and interpretable by authorized users. (VI) *Credibility*. The degree to which data are regarded as true and believable by users.

It is important to note that there are criticisms regarding the use of blockchain technology for data sharing, as it can be a two-edged sword in managing data quality. As a distributed database, a blockchain provides strong consistency mechanisms, reliable services, and transparency to participants, enhancing consistency, traceability, and availability. However, in blockchain applications, credibility depends on trust in external data providers [126]. The trust in data providers remains a crucial concern in both public and private blockchain contexts. This matter is intrinsically linked to the credibility of the data, a fundamental aspect of the quality of the data. The trustworthiness of data providers encompasses the notion of authenticity, which refers to the accuracy of information with respect to its origins, attributions, and commitments. Numerous potential solutions have been discussed to address this problem. For example, one solution involves procuring data from multiple oracles to minimize the hazards of relying solely on a single data source. This approach aims to prevent a single point-of-failure scenario, which could lead to significant problems in the blockchain ecosystem [126].

A critical drawback of blockchain technology is its inability to engage with the external environment, also known as the "outside world." Although the blockchain network can achieve unanimity regarding the results of a series of computations, it is restricted to operating only on data present on the blockchain [129]. In other words, the virtual machine's memory can only process information previously recorded on the blockchain before computation. The network is not inherently equipped to establish consensus concerning the veracity of this data; it can only confirm that it exists on the blockchain. To incorporate external data into a blockchain's consensus mechanism, reliable entities known as oracles must verify facts. In that sense, oracles allow a blockchain to interact with the real outside world. A solution proposed

to achieve robust security regarding the truthfulness of data is a decentralized oracle based on a voting game that decides the truth or falsity of the propositions. The oracle runs on a public ledger and utilizes human intelligence through a voting-based game. Participants within the system (ASTRAEA)[129] can assume one or more of the following roles: submitters, voters, and certifiers. Submitters are responsible for submitting Boolean propositions to the system and paying associated fees. Voters engage in a low-risk/low-reward game in which they assess the validity of a random proposition by staking a modest amount of confidence in their vote's accuracy. In contrast, certifiers engage in a high-risk/high-reward game by staking a significant amount of capital on the outcome of the voting and certification process. Because the proposition selection process is random, the voting system resists manipulation attempts by actors seeking an incorrect outcome for a specific proposition. A similar voting mechanism has been used in our research to increase the reliability of real estate asset documentation. Basically, an oracle serves as a conduit that facilitates the integration of external data sources with the blockchain network. Oracles commonly incorporate both on-chain and off-chain elements. The role of an oracle can be fulfilled by a human or a server responsible for submitting data from an external system or off-chain storage in the form of transactions. Additionally, an oracle can utilize a smart contract to enhance the quality of posted data by validating the information or adding metadata, such as the reliability or reputation of the data source.

There are different architectural design choices for storing data, including off-chain, on-chain, and a combination of both. In a public blockchain, as the sole data store, all the application data would be recorded and duplicated on all the nodes on the blockchain. However, the drawback of this approach is the lack of privacy and confidentiality, as any node can join the network and participate openly [126]. In a private blockchain network, the participation of only authorized nodes ensures confidentiality. Furthermore, the level of trust established by authorization allows the use of efficient and streamlined consensus processes, reducing the time required to accept and confirm transactions involving large amounts of data. Con-

sequently, private blockchains are typically engineered and configured to provide higher performance and scalability than their public counterparts. However, there is a requirement for pre-existing trust among participating nodes and centralization [126]. Consortium blockchains, similar to private blockchains, are engineered to provide higher performance, scalability, and confidentiality compared to their public counterparts. The key distinction between private and consortium blockchains is that a private blockchain is typically implemented within a single organization. In contrast, a consortium blockchain can involve multiple organizations that interact with each other. For instance, a Hyperledger channel can be established for two or more organizations in the same consortium blockchain to enable confidential communication between them. However, the increased performance observed in consortium blockchains is accompanied by a higher degree of centralization and a pre-existing level of trust among participants, similar to the private blockchain option [126]. Another option can be to connect more than a blockchain in a larger software system to build 'connected' data stores. The use of hybrid blockchain architectures can be motivated by a desire to utilize the security features of an existing public blockchain or to enhance the overall system's scalability. For example, an organization may store its highly sensitive data on a private blockchain it owns, while a consortium blockchain can hold essential data for business interactions between multiple entities. Anchoring data from private and consortium blockchains on a public blockchain can leverage the latter's stronger transparency and immutability properties [126]. An exciting solution can be to place data on both the on-chain and off-chain. Such a hybrid design could also overcome scalability issues resulting from full data replication and the limited computational capacity of blockchains.

By storing sensitive and time-sensitive data in off-chain storage belonging to stakeholders, this setup can offer improved confidentiality and scalability without compromising the immutability features that blockchain technology provides. The main idea of the system is to copy the blockchain data to an external database with a query layer designed outside the blockchain. This idea is most suitable for a consortium blockchain. In this solution, some information is stored in the blockchain,

while the remaining information can be stored in a central database outside the blockchain. Most information can be divided into two parts: 'core' and 'non-core.' The fields selected as core information can be packaged into one block and stored in the blockchain network. The other non-core fields can be hashed, the obtained hash results are stored in the block with the core fields, and all the information is stored in the central database.

This method can effectively reduce the amount of data in the blockchain network without compromising the functionalities with respect to data sharing. In a consortium blockchain, organizations can join the system at any time and share data according to the internal set of rules of the consortium [130]. The data's hash value can serve as a means of verifying the integrity of the data stored off-chain. Whilst off-chain storage can mitigate scalability and privacy issues, it brings new challenges, such as the integration and aggregation of data. The storage of data across multiple locations requires a mechanism for seamless consolidation of data from disparate sources. Traditional data management practices employ data warehousing technologies to integrate data from various sources into a centralized repository. In contrast, the distributed nature of blockchain data storage demands the implementation of a mechanism to effectively merge data from diverse locations [126].

Hybrid blockchains, such as consortium blockchains, can have either a listed chain as a standard blockchain system or several alliance chains. For alliance chains, each chain corresponds to a set of ledgers, and as a result, each node within the blockchain network can maintain several groups of ledgers. The structure of each chain is the same as that of a standard blockchain. To efficiently maintain multiple chains, it is crucial to enable efficient communication between them. To do so, cross-chain technology proposes to modify the architecture to enable communication between different chains. The idea is to add a data structure to the two separate chains so that they can interact with each other. For example, in the context of digital assets, if there are no barriers between different chains, it becomes possible to have cross-chain transactions of various digital assets [131].

A decentralised file storage protocol often used in conjunction with blockchain to handle large or off-chain data is the InterPlanetary File System (IPFS), a peer-to-peer protocol that enables file storage by assigning a unique cryptographic hash to each file. Although the IPFS is widely regarded as a promising solution for decentralised data storage, it was intentionally excluded from the data architecture proposed in this research due to functional and compliance-related limitations. IPFS enables content-addressable storage through a peer-to-peer network, where cryptographic hashes rather than fixed locations identify files. However, IPFS does not provide any inherent access control mechanisms [132], making it unsuitable for applications that require regulated confidentiality, such as AML frameworks in fine art and real estate transactions. Moreover, the system lacks guaranteed data persistence, since files are only retained in the network if actively “pinned” by nodes, leading to potential availability issues over time. IPFS “requires further layers for data authentication, encryption and guaranteed permanence, particularly in scenarios involving sensitive or regulated data” [132]. These characteristics stand in contrast to the requirements of this research, which prioritises institutional trust, structured lifecycle management, and legal enforceability.

Finally, it should be noted that multiple operational aspects must be considered to ensure that the blockchain network maintains performance, security, privacy, and reliability. Given the fast-paced and dynamic changes in the technological, economic, and regulatory domains, modern blockchain systems are likely to undergo substantial transformations. Blockchains are likely to eventually need to migrate to an upgraded version of the same blockchain platform, a different platform, or a different mode of hosting. However, modifying blockchains can be challenging, expensive, and risky due to differences between platforms, the compatibility of the smart contract language, and the hosting methods [133]. In conclusion, while migrating to a private or consortium blockchain could be achieved relatively easily, recreating a complete blockchain history on an existing public blockchain is impractical [126].

3.4 Blockchain potential for fine art and real estate

Blockchain technology has core use cases in the arts and real estate sectors for creating provenance and authenticity registries, promoting fractional ownership, and potentially streamlining the due diligence process. A blockchain system is attractive because it could reduce the total transaction time to complete a sale by automating the entire transaction process. It can also assist with the organization and data management of access control, distribution, and validation of information.

In the real estate sector, the importance of an ownership registry has been recognized for a long time, and most countries have a property registry which keeps track of ownership and is updated when a transaction occurs. In the UK, this task is undertaken by the His Majesty Land Registry (HMLR), which registers land and property ownership in England and Wales. These records include title registers, title plans, and title summaries. In the EU, all member states have their land register and cadaster, which contains information on real estate [134]. The European Land Registry Network (ELRN) was created in 2010 to make land registry services more accessible throughout Europe. Blockchain technology can significantly strengthen and improve the functionalities of the land registry by making information more reliable, facilitating due diligence, and potentially making real estate transactions faster and thus less expensive. In the fine art sector, blockchain technology opens multiple opportunities. Currently, there is no unique record to keep track of artwork ownership. A reliable decentralized database can help establish ownership, provenance, and authenticity. Provenance is crucial to determining the authenticity of the artwork, and it has been a vital aspect of prosperous European market centers since at least the 18th century, providing collectors with orientation and supporting art valuation. Provenance signals whether an artwork has been part of a prestigious collection or exhibition, indicating authenticity and elevated aesthetic quality. Authenticity and individual quality evaluations are crucial to determining the aesthetic and artistic merit and value of the artworks. A decentralized database can help establish the provenance and authenticity of artworks and prevent forgeries. It can also reduce insurance costs, benefiting private and public institutions such as

museums. The physical conditions of the artwork, storage and transportation requirements, previous interventions, and restorations can be recorded on the ledger, providing valuable information when considering risks and insurance premiums.

A blockchain solution would also bring another significant advantage to the fine art and real estate sector. There is a great benefit in performing automated actions based on the change in data. For example, to enhance data integrity, we can envisage a system where an automatic message is sent to all stakeholders, inviting them to check the accuracy and truthfulness of the new input when new data are recorded or updated. Establishing a resilient connection between the blockchain database and the tangible asset is crucial, as the accuracy of data uploaded to the blockchain is paramount. Blockchain is not a solution to making 'wrong information' right (a common misconception) because blockchain cannot assess whether the entered data is right or wrong. Although blockchains are well-suited for transferring assets or data intrinsic to the blockchain, their ability to assess the accuracy of externally entered data is limited. In essence, "the veracity of the ledger's contents is distinct, as a blockchain does not inherently confer trustworthiness upon the data entered, nor the parties entering it" [135]. This observation aligns with the principle of "garbage in, garbage out" (GIGO), which refers to the idea that input data quality determines output data quality. Inaccurate input is treated by a blockchain in the same manner as any other input, whereby it is hashed and recorded as a mere hash value within the blocks. The blockchain solely ensures that the data remains unchanged. Therefore, we cannot assume that 'everything on the blockchain is just *right*'. This assumption can only be made if the writing party is fully trusted by the other participants of the blockchain [136]. If not carefully checked, inaccurate or unreliable information can be stored on the blockchain and propagated across the network, negatively impacting the entire system.

For this reason, maintaining data integrity is crucial. Data sets are susceptible to manipulation, and malicious individuals may exploit this vulnerability to their benefit, either by disseminating false information through compromised data or fraudulently claiming credit for others' work. Individuals and organizations need

rely on scientific, commercial, without concern for its integrity or trustworthiness. In response to this issue, data producers seek to ensure data integrity for their consumers and themselves, protecting against any unauthorized manipulation [137]. A method that can be used to validate the input of data in the blockchain is the hash-based system. A unique identifier representing the specific data identifies the hash. To authenticate the integrity of the data, the hash value stored for the data identifier is compared to the actual hash value of the data. A disparity between the two hash values indicates that the data have undergone modification after being included on the blockchain [137]. Nevertheless, despite this safeguard, the principle of "garbage in, garbage out" (GIGO) still applies, as false data may be introduced causing data on a blockchain simply become "immutable garbage" [138]. There is significant interest in trying to ensure the integrity and accuracy of data stored in the blockchain. Multiple industries have attempted to develop solutions to improve the provenance and integrity of data in response to the GIGO issue in the blockchain. One solution can be to have an intelligent algorithm to detect collusive behaviour with the support of a blockchain system [139]. The system and the algorithm work together to gain customers' trust during online acquisition. Based on the results, it also generates critical managerial insights for operations managers and policy makers. Integrating Internet of Things (IoT) and blockchain can also be a solution to ensure data provenance and integrity [138]. IoT devices enable data collection and transfer without physical or remote human intervention. When data collected from IoT devices is stored on a blockchain system instead of being manually input by humans, the likelihood of malicious data manipulation is significantly reduced. As a result, the integrity and reliability of the data in the blockchain system is enhanced. However, these solutions come from different industries, such as engineering [139] and food supply chain [138]. Artworks and real estate assets are unique items which require a specific and tailored approach. The issue is the relationship between the physical world and the digital ledger. Because of this, some blockchain critics argue that blockchains cannot deliver 'true provenance' because that can only be delivered via forensic or analytical science [138]. Another approach to ensure data quality is

to implement governance frameworks that define clear standards and procedures for managing data on the blockchain. This can include establishing data quality metrics, conducting regular audits to identify and resolve data quality issues, and implementing data validation checks at various stages of the blockchain transaction lifecycle.

In the context of this research, it is essential to distinguish between pure blockchain systems and oracle-assisted architectures. Pure blockchain systems execute logic and validate data entirely on-chain, without dependency on external inputs. This approach guarantees determinism, auditability, and trust minimisation, but it also presents inherent limitations—most notably, the inability of smart contracts to directly access off-chain data such as AML watchlists, valuation records, or identity documents. To bridge this gap, oracles are introduced as middleware that transmit verified external data into the blockchain environment. Leading oracle frameworks such as Chainlink and Provable (formerly Oraclize) provide cryptographic assurances of data authenticity and integrity; however, their use also entails new trust assumptions and potential security risks.

In the architecture proposed in this thesis, oracle-like components are integrated in a measured and transparent manner, limited to the verification of compliance-relevant metadata, including identity documentation, provenance records, and sanctions or PEP screening outcomes. Rather than storing sensitive information directly on-chain, the outputs of these verifications are hashed and time-stamped, ensuring tamper-proof traceability while maintaining compliance with data protection requirements. The system thus reflects a deliberate integration of off-chain verification with on-chain enforcement: third-party services authenticate the relevant documentation and communicate outcomes through secure, pre-defined input channels. These results are encoded on-chain via cryptographic fingerprints—enabling smart contracts to operate deterministically on trusted inputs, without compromising privacy. This design achieves a clear functional separation, whereby off-chain infrastructure manages regulatory-sensitive processes, and blockchain components enforce compliance rules based on immutable proofs

of verification.

Chapter 4

Case studies

The literature review in Chapter 3 highlights the inherent complexity of blockchain technology, emphasizing the need for thorough application-specific analysis and an interdisciplinary approach to effectively unlock its potential and manage associated risks. This chapter uses case studies to examine blockchain applications in the fine art and real estate sectors, while also exploring the potential risks associated with the misuse of blockchain technology. The case study analysis serves as the cornerstone for developing both the proof of concept and our blockchain solution. It provides an in-depth exploration of the chosen application, aiming to uncover key challenges such as limitations in existing blockchain implementations, regulatory risks, and adoption barriers specific to the fine art and real estate sectors. For the selection criteria of case studies, see Introduction, Section 1.4.

To ensure clarity in the analysis, the boundaries of each case study are explicitly defined. The Verisart case study (Section 4.1.1) focuses on blockchain applications for provenance and authenticity in the fine art sector, examining how digital certificates and decentralised records can enhance trust in ownership history. The analysis is limited to Verisart's architecture, data integrity features, and relevance for AML due diligence. The Maecenas case study (Section 4.1.2) explores the tokenisation of artworks and the use of blockchain to fractionalise ownership and facilitate online auctions. It focuses on compliance, investor protections, and the technical challenges of managing digital shares in fine art assets. In the real estate domain, the Due Diligence Analysis (Section 4.2.1) maps the transaction phases in

the UK context and identifies specific pain points that blockchain could address. The case is supported by the legal framework established by the Law Society Conveyancing Protocol and the HMLR Digital Street project. The Spunta Project (Section 4.2.2) is introduced as a comparative case to examine how blockchain, via Corda, is applied in interbank reconciliation. Although not directly related to real estate, it illustrates how privacy-preserving ledgers function within regulated institutional ecosystems. Finally, Tornado Cash (Section 4.3) is not analyzed as a constructive case, but as a counterexample highlighting the risks of blockchain misuse. Its role is to expose design vulnerabilities and illustrate how privacy-enhancing smart contracts can facilitate anonymity and undermine regulatory efforts when not adequately governed.

Case Study	Sector	Focus Area	Analytical Boundaries	Objective
Verisart	Fine Art	Provenance, authenticity, certification	Use of blockchain for issuing and validating certificates of authenticity; excludes commercial sales dynamics	Assess how blockchain supports tamper-proof provenance and KYC documentation
Maecenas	Fine Art	Fractional ownership, tokenised auctions	Tokenisation of artworks and share issuance via SPVs; excludes physical logistics and storage mechanisms	Evaluate how blockchain enables market access, price transparency, and investor protections
Due-Diligence Analysis	Real Estate	Conveyancing, property transactions	Focused on document-heavy due diligence workflows within the UK Law Society Conveyancing Protocol	Identify frictions in traditional property transfers that blockchain could streamline and secure
Spunta Project	Banking (Reference Case)	Interbank reconciliation via private blockchain	Application of Corda for bilateral data reconciliation; used as a technical analogue to semi-private models	Examine data integrity, privacy, and governance in distributed institutional systems
Tornado Cash	Crypto (Risk Case)	Anonymity, mixer protocols, ZKPs	Ethereum-based mixer protocol misused for money laundering purposes; analysed as a counterexample	Illustrate the risks of uncontrolled privacy features and the need for regulatory design safeguards

Table 4.1: Overview of case study boundaries and objectives

4.1 Fine art: provenance and decentralized marketplace

This section analyses applications of blockchain technology in the fine art sector, from provenance and authenticity to online sales, auctions, and NFTs. We provide an overview of the main blockchain platforms operating in the art industry and analyze in detail the functionalities of two of them, Verisart and Maecenas. The first platform tackles issues related to provenance and authenticity, while the second offers an online fine art marketplace.

In recent years, numerous blockchain-based applications have been developed in the field of cultural heritage. Blockchain has multiple core use cases in the fine art sector, from provenance and authenticity registries to digital scarcity for new media and generative art, including fractional equity and shared upside structures and new forms of copyright registry [56]. Starting from the analysis in [140] we have investigated the different types of blockchain platforms operating in the fine art sector. They can be divided into two main groups:

1. Platform with a main focus on *provenance and authenticity* certification, such as Fresco¹, Artory², Verisart³, Blockchain and Art Collective⁴, Codex Protocol⁵.
2. *Decentralised marketplaces* such as Ink Labs Foundation YAIR Your Art Is Reality, DADA⁶, Adappcity Inc, Maecenas⁷, Scarab Experiment⁸, Masterworks⁹.

The first group of solutions does not have an investment focus, but they attempt to solve issues around the provenance of traditional art pieces and the protection of digital artworks, while the second group targets investors and has the main focus on artworks as investment assets [49]. The three companies that have been the most successful in managing the provenance of valuable items via blockchain are Verisart, Artory, and Codex Protocol. All three of these services collaborate with the main auction houses around the world [56].

In the second group of platforms, blockchain technology is used to split the ownership of an artwork [141] among several investors. The decentralized marketplace comprises a network of various technological devices that enable investors to

¹<https://fresco.work/>

²<https://www.artory.com/>

³<https://verisart.com/>

⁴<https://blockchainartcollective.com/>

⁵<https://codexprotocol.com/>

⁶<https://dada.nyc/home>

⁷<https://www.maecenas.co/>

⁸<https://www.thescarabexperiment.org/>

⁹<https://www.masterworks.com/>

create markets without a centralized location. An example of this type of service is Maecenas. This company divides the ownership of artworks into fractions that can be exchanged on a global exchange platform [142]. The tokenization of physical and cultural objects simplifies investment diversification in art and, at the same time, favours fundraising by artists.

The art sector is getting increasingly crowded, and new startups are entering the market. However, our research reveals that adoption and endorsement from established art houses or collaboration with recognised institutions is crucial to success. While, for example, Artory partners with Christie's¹⁰, Maecenas with Dadiani Gallery¹¹ and Fresco with dslCollection¹², and they are thriving, other startups such as Adappcity Inc. or Scarab Experiment are struggling to make their space in the industry, and Ascribe is no longer active.

In Table 4.2 we summarize the main features of the platforms mentioned above, in particular in terms of data access (public vs. private implementation), smart contract language used and use case.

In the context of public blockchains, there are no privileged actors in the network, and anyone can see the records and the entire transaction history (although the identities of the transacting parties are usually pseudonyms) [115]. Each participant can use the blockchain to make transactions, but can also participate in the consensus process and transaction validation [117]. Network users can vote on new proposals to update or modify the underlying protocol [116]. Examples of public blockchains include Bitcoin and Ethereum.

In a private or permissioned blockchain write access is given by an organization, and read permissions can be public or restricted. In this case, the consensus process is controlled by a pre-selected set of nodes. Private / Permitted blockchains generally have simpler consensus algorithms due to the increased trust between endorsed participants [116]. A private or permissioned blockchain does not allow open participation in the submission or participation in the transaction validation process

¹⁰https://www.christies.com/?lid=1&sc_lang=en

¹¹<http://www.dadianifineart.ae/gallery-ww/home/>

¹²<https://www.glexpo.com/v3/dslcollection/>

Blockchain platforms			
Name	Blockchain type	Smart contract language	Use case
Fresco	Public (Ethereum)	Solidity	Provenance/certification
Artory	Private	non disclosed	Provenance/certification
Verisart	Public (Ethereum and Polygon)	Solidity	Provenance/certification
Blockchain Art and Collective	EVM-family blockchain	NA	Provenance/certification
Codex Protocol	Public (Ethereum)	Solidity	Provenance/certification
YAIR	NA	NA	Decentralise Marketplace
DADA	Public (Ethereum)	Solidity	Decentralise Marketplace
Adappcity	NA	NA	Decentralised marketplace
Maecenas	Public (Bitcoin, Ethereum)	Clarity, Solidity	Decentralised Marketplace
Scarab experiment	NA	NA	Decentralised marketplace
Masterworks	Public (Ethereum)	Solidity	Decentralised marketplace

Table 4.2: Summary of the main blockchain-based platforms in the art sector and main features.

[117]. Examples of private blockchains include Quorum, Hyperledger Fabric, and R3 Corda.

In the next sections (Sec. 4.1.1, 4.1.2) we will analyze in more detail how these blockchain-based platforms operate, focusing on a prominent example from group 1 (Verisart) and one from group 2 (Maecenas).

4.1.1 Verisart. Provenance and authenticity

Verisart is a blockchain-based platform that supports provenance tracking and authentication functionalities.

The company Verisart was launched in 2015 to create a trusted public database,

which provides a permanent digital art provenance record for physical artworks normally stored in galleries. Verisart is based on a peer-to-peer distributed system that allows pieces of information to be recorded in a verifiable fashion. The system uses decentralized data storage, where data are encrypted, and fault tolerance technology guarantees the resilience of the system. The fault-tolerant technology ensures that the system will continue to operate where the node(s) can fail or be malicious. This means that it can tolerate arbitrary faulty nodes and improve availability and reliability using state machine-replicated services [143]. Key cryptography is combined with a system for identification that allows the association of identities with authenticated information. Ownership and ownership transfers can be recorded on a blockchain using an agreed-upon data format. The system is described in detail in the Verisart patent [144], and is summarized below.

The blockchain can be used to record and verify the documentation of experts, appraisals or evaluations, artwork transfers or transformations, and any other actions that may occur during the lifetime of a work of art. Verisart's goal is to create a robust system to record and verify information about the creator of the artefact, its ownership, any transfer of ownership, and the condition of the artefact as evaluated by a third party, among other events. A creator can be any type of artist in principle, e.g., a manufacturer, a writer, a sculptor, a developer, or an architect. Individual parties connected to the work of art are represented by and linked to a public-private key pair. The private key is held secret by the party or on behalf of the party and used to sign information using standard techniques of digital signatures.

This platform allows for the creation of a digital certificate and/or a digital Certificate of Authenticity (COA) for both non-fungible tokens (NFTs) and physical artworks. The digital COA is based upon a combination of authentication endorsements, and it is configured to change state along a continuum of low to high confidence in authenticity based on the different layers of authentication endorsements obtained. Endorsements are weighted differently: for instance, an authentication endorsement from a creator is weighted higher than an authentication from a third party. The process to generate a COA for an NFT is structured as follows:

1. Creating a digital key for a newly registered user (i.e., any entity joining the public blockchain network).
2. Receiving a request from the user to create a relationship (such as *ownership*, *creatorship*, *endorsement*) with a creator of a collectable object (NFT).
3. Establishing a record registered on the NFT blockchain.
4. Authorizing a relationship between the user and the creator after confirming the user's ID.
5. Generating a digital key to the creator relationship .
6. Converting the NFT record to a digital COA together with a confirmation using the digital creator relationship key.

In a similar way, the platform allows the creation of a COA of a physical artwork. The objects are physical and can be collectable objects, unique individually identifiable articles created or manufactured in sequence, or digital collectable objects that exist in the real world or in the virtual world, including reality and augmented reality. In this case, the system generates a random one-time code. Then, a corresponding QR code is generated, and it is attached to the physical object. The method also includes linking the random one-time code in a database to a digital COA. Attestations by a creator, an existing owner, trusted third-party manufacturers, buyers or sellers on title transfers, combined with evidence of ownership, fractional ownership, or transfer of title are used to document and authenticate ownership and title history of the object through a link with the digital COA. The system is described in more detail in the schemes in the following.

Fig. 4.1 shows the process to authenticate attestations of an object, such as a work of art. In The example, a gallery wants to request authorization from an artist (creator) of the work of art to create a digital COA. In the first step, the gallery initiates a request via the authentication server to create a certificate of a relationship (ownership, creatorship) with the artist of the work of art. This certificate only

contains information about the artwork record and the gallery (public) key (this certificate is not a COA yet). In step 2, the authentication server verifies the gallery, approves the artist relationship between the artist and the gallery, and generates an *artist relationship key*. In step 3, the object is then transferred to a new owner together with its authenticity certificate. Once the certificate is a digital COA, further certificates created by the gallery for the same artist are preferably immediately digital COAs (unless specific restrictions apply, e.g., specific sales conditions, revocation of the gallery's mandate by the artist) and no further modification or approval from the authentication server is necessary. Step 4 shows how a collector can request an endorsement of the collectable object from the artist, via an *endorsement request*. A core principle of the authentication system design is that authenticity is based on a collection of proofs, not on a single evidence. Different confidence level on the authenticity – from low to high – can be attached to the digital certificate, depending on the proofs received (see schemes in Fig. 4.3 for further details).

Fig. 4.2 shows the process to record and verify attestations on a digital ledger (blockchain). In step 1, a hash of the certificate, initially including the user's digital key and an artist's digital key, is created. Hash functions (also called message digests or one-way encryption) are algorithms used to encrypt information. A fixed-length hash value is computed based on the plain text, making it impossible for either the length or plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's content to ensure that the file has not been tampered with [145]. In step 2, the certificate is timestamped and a record of the certificate on the distributed ledger is generated (step 3). The verification of attestation recorded on a distributed ledger (step 4) involves 3 operations: (I) The certificate held on Verisart's database is checked against previous transactions recorded on a public blockchain (in this case, the Bitcoin blockchain) to verify the timestamp of the certificate. (II) The cryptographic signatures are verified against public keys published on the websites of artists, galleries, and/or authentication services. (III) The contents of the certificate metadata and files are cryptographically verified by comparing the stored hashes against the information contained in Verisart's

archives.

Fig. 4.3 explains how confidence levels are applied to individual attestations and certificates. (I) The Registered Record (lowest confidence level) contains claims that are permanently registered on the blockchain through the authentication service's system. However, there is low confidence in their authenticity, as there is no authorization or endorsement by the artist or maker, and the issuer's identity has not been verified. (II) The COA can be authorized by the artist or (if no artist exists, or for example not alive anymore) by a verified business. Even after it meets the basic criteria of a Certificate of Authenticity, a certificate can continue to move up the ladder by accumulating additional proofs. (III) The COA Plus includes not only the previous steps but also information about the work of art (at least 2 images and an active link between the physical object and digital certificate). While the exact requirements for completeness may change over time and vary, depending on whether the work is physical or digital, the key principle is that the more descriptive information about the object is provided, the further along the classification the certificate moves.

Fig. 4.4 shows how a link between a physical object and a digital certificate is established. This step is implemented in slightly different ways depending on how the QR code is provided to users (self-printed, delivered, etc.). For simplicity, we refer only to the self-print process for sharing a QR code. In Step 1, a random code is generated and linked to a certificate in the database. For physical objects, the issuer or owner needs to have established a link between the physical object and the digital certificate. The initial implementation uses QR codes, which are printed on physical labels and attached to objects. In Step 2, a user prints and attaches the QR code to the collectable object. Once these codes have been linked to the correct digital certificate, the link is established, and the certificate moves up the ladder. This type of link is less relevant for digital objects, where other methods can be used to establish the connection between the certified item and the certificate. In Step 3, a third party follows the QR code and sees an extra security 'tick' if the code matches.

Fig. 4.5 shows a digital certificate authentication system for an NFT. In Step 1, a digital certificate is created in Verisart. In Step 2, the NFT is minted in SuperRare so that it can be bought, sold, and traded. In Step 3, the NFT details are updated in Verisart on the authentication server. The certificate automatically follows ownership changes (step 4), and in step 5, the new owner links the wallet to the manager certificate.

Although Verisart has some advantages in being publicly accessible as a database, there is a disadvantage regarding the vulnerability of vetting the initial listing of artwork on the blockchain. The record of ownership is dependent on the validity of the initial input data. Verisart allows anyone to list an artwork: In June 2018, a man named Terence Eden listed the Mona Lisa on the Verisart blockchain putting himself as the artist and 1506 as the creation date [146, 147, 56]. The platform Artory has managed to address this vulnerability, and in 2018, it became the first company to list a major auction sale on the blockchain when it became the registrar of the Ebsworth Collection, sold at Christie's New York for \$318 million on November 13, 2018. This sale included forty-two pieces of art and set numerous records [148]. Artory, built on the Ethereum blockchain, offered collectors essentially a certificate of authenticity encoded on the blockchain. Artory only lists works that have been vetted by a partner organization, for instance, an auction house or gallery, which would already be engaged in a higher level of provenance research. Artory also took the business decision to make the registry double-blind - which means that Artory itself does not know the identity of collectors, it only lists their artworks [56].

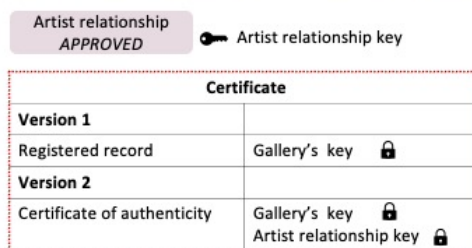
Verisart, Artory, Codex, and others face the challenge of managing the so-called "blockchain air gap," between the blockchain listing and the physical artwork [149]. To link blockchain records to physical artworks, companies have explored everything from physical tagging to DNA analysis to the ways in which the physical surface of an artwork can be recognizably photographed in the manner of a fingerprint. This challenge has not yet been fully resolved [56].

VERISART - Authentication attestations for an object such as a work of art

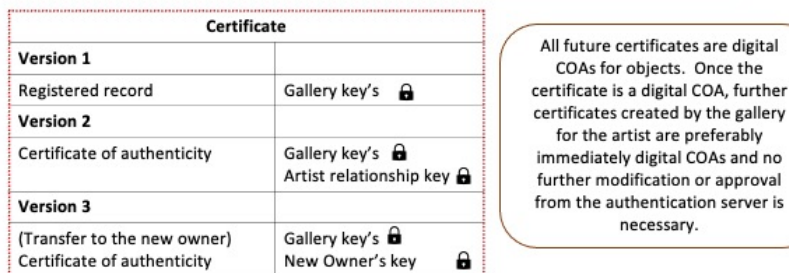
1. A gallery wants to request artist authorization from an artist (creator) of the work of art to create a digital COA.



2. The authentication server has identified and verified the gallery and approved the artist relationship between the artist and the gallery. The authentication server generated an artist relationship key.



3. Transfer of the object to the new owner



4. A collector can request an endorsement of the collectible object from the artist.

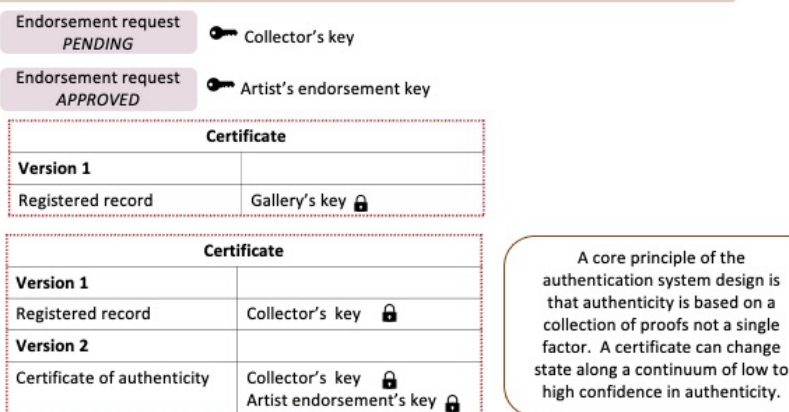


Figure 4.1: Authentication attestations for an artwork.

VERISART - Record and verify attestations on a digital ledger (blockchain)

1. A hash of the certificate in a first version including user's digital key and an artists' digital key is created.

Certificate		Hash of certificate version:
Version 1	User's key 	ab27ef128fc...
Certificate created	Artist's key 	

2. The version of the certificate is timestamped

Open TimeStamp
Merkle tree of other timestamps
1237fc814545...
abf52588rjrjdj....
628984abcf12....

3. A version of the certificate is stored on the distributed ledger

Blockchain
Transaction
628984abcf12....

4. Verification of attestation recorded on Verisart database against public record.

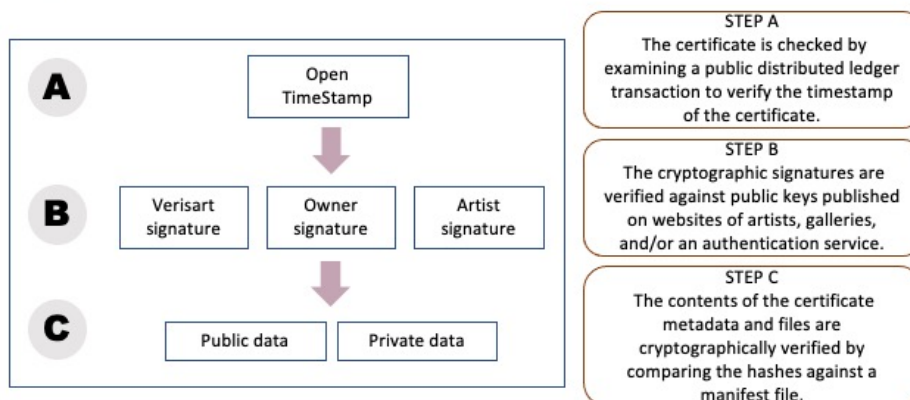


Figure 4.2: Record and verification of attestation on the digital ledger (blockchain).

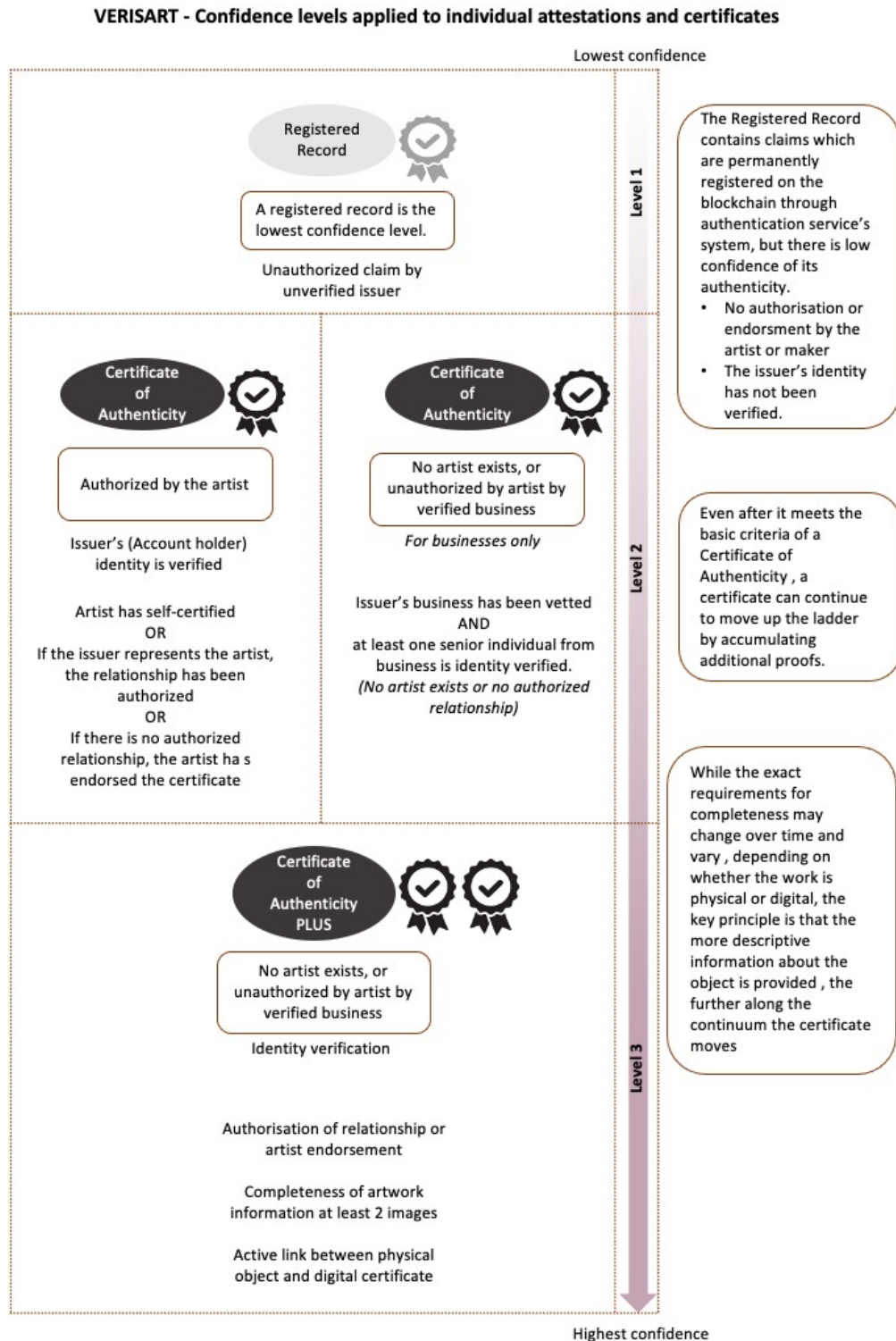


Figure 4.3: Application of confidence levels to individual attestations and certificates.

VERISART - Establishing a link between a physical object and a digital certificate

Secure self print process for printing a QR code
for attachment to a collectible object.

1. A random code is generated and linked to a certificate in database.

Code	Linked certificate
ABD 123...	1234 (cowboy)

For physical objects, the issuer or owner needs to have established a link between the physical object and the digital certificate. The initial implementation uses QR codes which are printed on physical labels and attached to the objects .

2. A user prints and attaches the QR code to the collectible object.



Once these codes have been attached to the correct digital certificate , then the link is established, and the certificate moves up the ladder. This type of link is less relevant for digital objects where other methods can be used to establish the connection between the certified item and the certificate.

3. A third-party follows the QR code and sees and extra-security 'tick' if the code matches.

https://verisart.com/works/1234&code=ABC123	
	=====
	QR VERIFIED

Figure 4.4: Creation of a link between a physical object and a digital certificate.

VERISART - Digital certification authentication system for an NFT**1. Create a digital certificate on Verisart**

Create certificate	
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----

A digital certificate is created at an authentication server.

2. Minted NFT on SuperRare

SuperRare	
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----
Authentication ID:	-----

The NFT is minted on SuperRare so that it can be bought, sold, and traded.

Description
Verisart certified:
<http://verisart.com/works/fname-lname-99a3f596-gh69-25>

3. Update NFT details on Verisart

SR SuperRare	
0xb932....b9e0	📄
22465	📄
0xb18e....5a8d	📄

The details of the NFT are updated at the authentication server

4. Certificate automatically follows ownership changes

History	
Transferred JUN 14 2021 Certificate transferred to the new owner	
NFT	
Contract:	0xb932....b9e0 📄
Token:	25315 📄
Owner:	0xb18e....83de 📄

5. The new owner links wallet to manager certificate

V	
CONNECT YOUR WALLET Claim your certificate	

Figure 4.5: Digital certificate authentication system for an NFT.

4.1.2 Maecenas. A Decentralised marketplace

Maecenas is a decentralized art gallery auction market that aims to democratize access to fine art as it allows anyone to buy, sell, and trade part ownership in masterpieces on a liquid exchange [150]. Via this platform, multimillion-dollar artworks are tokenized into “asset tokens”. Each asset token represents a share of the beneficial interest in the underlying artwork and can be traded instantly on a global exchange. Maecenas uses blockchain technology to create tamper-proof digital certificates of ownership linked to art pieces. A single artwork is broken down into thousands of certificates, similar to how a public company issues shares. Tokens represent shares of the artwork and they are traded through smart contracts following the Ethereum ERC20 standard. Smart contracts are computer programs that can be consistently executed by a network of mutually distrusting nodes without the arbitration of a trusted authority [151]. The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the software architecture in such a way as to make a breach of contract prohibitively expensive [152].

As shown in Figs. 4.6, 4.7 and 4.8 the process is structured as follows:

1. *Curation.* Maecenas identifies suitable art pieces.
2. *Due diligence.* Investors can view the painting’s details, history, condition report, high-resolution images of the artwork, and its full provenance before registering their interest to bid.
3. *Tokenisation.* “Asset Tokens” representing shared ownership in the artwork are minted on the blockchain.
4. *Sales Distribution.* Art owners can list artworks on Maecenas and sell Asset Tokens to investors. Investors can pay in any accepted fiat currency (such as USD) or cryptocurrency.
5. *Trading Exchange.* Investors can buy/sell their Asset Tokens on any exchange they are listed in.

From a collector's point of view, the possibility of fractionalizing a single artwork allows investors to diversify their art holdings in ways that are limited to the secondary art market and generally do not encompass the livelihood of artists [56]. In 2018, Maecenas purchased an Andy Warhol artwork *14 Electric Chairs* and divided it up into shares sold as ART tokens (ERC-721 non-fungible token).

The company sold 31.5 % of the \$14 million artwork [153]. By purchasing tokens, collectors can have a small investment exposure to an artwork. Such a registry of fractional shares could also enable a secondary market that allowed collectors to diversify while still rooting the art market with artists.

Artworks listed on the platform go through a bidding process (Dutch Auction Process) where investors submit private bids stating how many shares they want to purchase and for what price. The auction takes place over days or weeks to facilitate people's participation. Artworks can be listed in any fiat currency (USD, EUR) or cryptocurrencies (BTC, ETH). Any fiat money or crypto amount invested in the platform is converted into ART tokens first. After the auction, all bids are automatically analysed to determine the final share price and the amount of share each successful investor will receive. Finally, transactions issuing artwork crypto-shares to investors are settled via smart contracts. At the same time, the sellers receive either the ART token or the equivalent in cryptocurrency, depending on the agreement [154].

One of the main challenges Maecenas has faced is to structure the art investment without infringing existing financial regulations, providing security and protection for investors. To do so, the artwork or its fraction is sold to a legal entity (SVP - Special Purpose Vehicle) which issues the shares in artworks to be traded in the platform. Artworks are stored in high-security art vaults that operate as galleries where rooms are allocated for viewing. These storage facilities typically sit within internationally designated areas next to airports to avoid local tax when artworks are transacted, making them more attractive for investors. One example is the free port in Singapore, where Christie's operates their Fine Art Storage Service.

Companies such as Maecenas and Masterworks target collectors rather than

artists and emphasize art as an asset class rather than artists as producers [155]. However, fractional ownership represents a potential benefit for artists as it can facilitate resale of royalties or equity. Maecenas divides the ownership of artworks into fractions that can be exchanged on a global exchange platform [142]. The tokenization of physical, and cultural objects makes it easier to diversify the investment in art and, at the same time, favours fundraising by artists [155]. From the artist's perspective, resale royalties or equity, and the ability to resell either on an exchange, becomes a potential form of financial support for living artists.

The Maecenas platform is described in detail in [154] and it is summarised below.

Fig. 4.6 shows how the decentralized art gallery works. New artworks are continuously listed on the platform after passing a strict due diligence process detailed in Step 1 (verifying the art provenance, insurance policy, safe storage, independent valuation, artwork condition, and verification on the registry of lost and stolen art). In step 2, a single artwork is broken down into thousands of certificates (similar to how public companies issue shares). Maecenas uses blockchain technology to create tamper-proof digital certificates linked to art pieces. In steps 3 and 4, artworks listed on the platform go through a bidding process following a Dutch auction process. Investors submit private bids stating how many shares they want to purchase and at what price. This gives investors more bargaining power and provides them with a fairer and more transparent pricing mechanism. Steps 5 and 6 convert any fiat or crypto amount into ART (Maecenas native tokens). Maecenas utilized a native currency-independent token as a proxy for all currency conversions to eliminate conversion risks. Artworks can also be leased to museums for exhibitions. In step 7, The income generated from sales or leases is distributed proportionally to the holders of fractions of paintings or sculptures. Transactions are automated via smart contracts.

Fig. 4.7 explains the Dutch auction process in Maecenas. In step 1, the art owner decides to sell artwork on the Maecenas platform. For investors who want to participate in fiat currencies or other cryptocurrencies, deposits are kept in a fully

segregated virtual bank account with a unique IBAN or in a secure multi-signature cold storage. In steps 2 and 3, the art owner decides which currency to receive the proceeds in (fiat money, cryptocurrency ART tokens), and investors participate in the auction by locking ART tokens into the auction smart contract. In step 4, the Maecenas platform receives the money, allocates an equivalent amount of ART tokens to the investor, and pledges the token on the smart contract on behalf of the investor. In step 5, the Dutch auction process finishes, and the smart contract proceeds to analyze all bids to determine the final share price and the number of shares the successful investor purchases. Finally, the smart contract settles the transactions by issuing artwork crypto-shares to investors. The artwork seller receives either the ART tokens or the equivalent in currency, depending on their choice, before the auction starts (step 6).

Fig. 4.8 explains the Maecenas legal and compliance system. (I) Art experts verify artworks, a certificate is issued to Maecenas, and the certificate is archived in Maecenas. (II) Artworks are stored in high-security vaults that operate as galleries and allocate dedicated rooms for viewing. Art vaults are storage facilities typically within international airports (freeports). (III) The art owner submits provenance information to Maecenas, and (IV) sells part of the artwork to a legal entity (SPV). (V) The SPV issues shares in artwork which are transferred into Maecenas. (VI) Investors buy/sell shares.

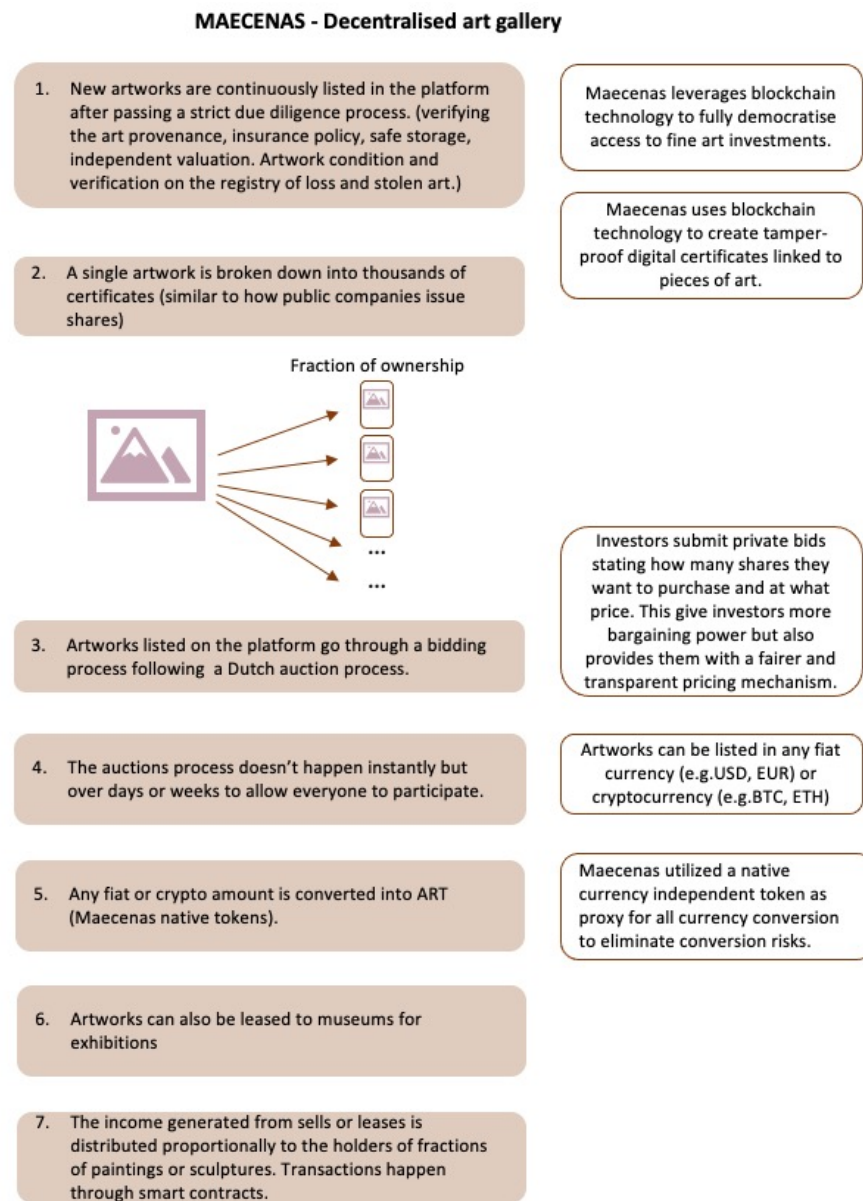
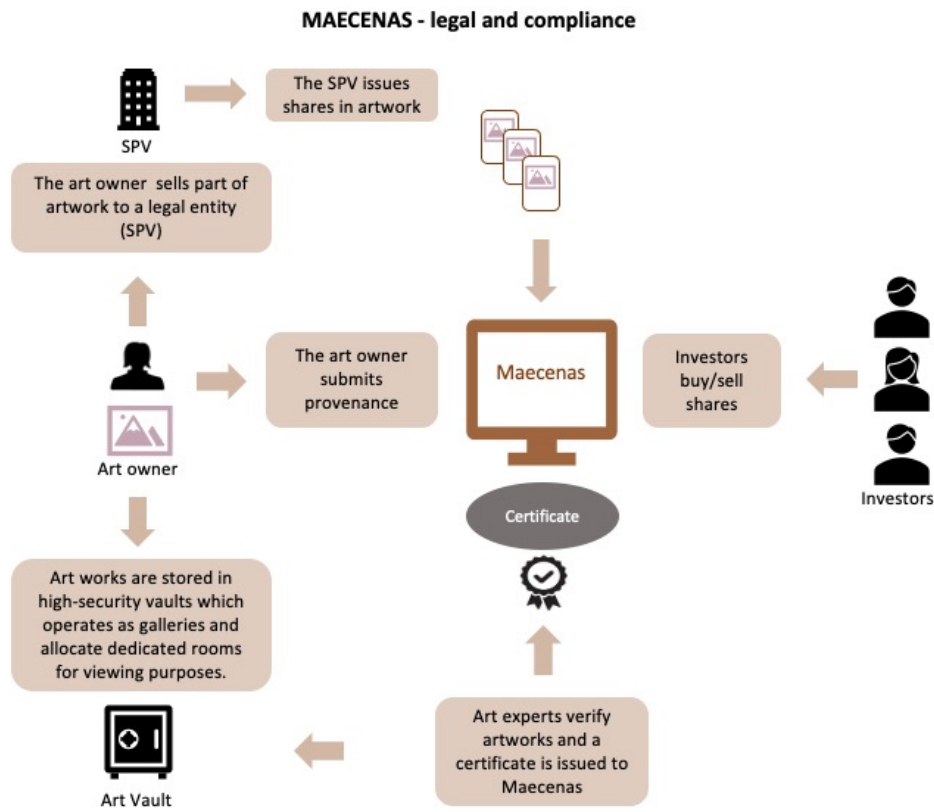


Figure 4.6: Maecenas decentralised art gallery schematic process.



Art vaults: these storage facilities typically sits within international airports (known as freeports). Valuables are kept in storage and do not attract local tax when they are transacted. In Singapore for example Christie's operates their Fine Art Storage Service (CFASS)

SPV: Special Purpose Vehicle

Figure 4.8: Maecenas. Legal and compliance

4.2 Real estate: Due diligence and transaction process

4.2.1 Due diligence analysis

The real estate transaction process is acknowledged as complex and quite convoluted (see Chapter 2, Section 2.2). For this reason, we dedicate a case study to a detailed analysis of the real estate transaction phases in the UK with the aim of understanding how due diligence works and what can be done to improve efficiency and transparency. This study is based on the material provided by the Law Society and the analysis of the Digital Street project of the HM Land Registry (HMLR) undertaken by the HMLR and the law firm Mishcon de Reya.

The literature review shows that significant work has been done on the marketing period and the relationship between price, liquidity, and marketing time. The study aims to understand crucial challenges and the main causes of delays and inefficiencies in the due diligence phase to identify the areas that could benefit more from technological innovation, especially blockchain. As mentioned in Section 2.2, successive governments have acknowledged the length and opacity of the real estate transaction process in the UK, and a digital solution has been recommended. In the UK, the due-diligence process is regulated by law, and the Law Society identifies key steps in The Law Society Conveyancing Protocol (2019). A: *Instructions*, B: *Pre-exchange - Submitting a contract*, C: *Prior to the exchange of contracts*, D: *Exchange of contracts*, E: *Completion*, F: *Post-completion*. As stated by the Law Society, “the steps in the Protocol are not exhaustive and should not be regarded as a ‘checklist’ for conveyancing. The transaction may not proceed in a fixed order and many processes can occur simultaneously or be carried out in a changed order. However, the Protocol provides a detailed description of tasks and regulatory requirements. Based on the Law Society Conveyancing Protocol and the study conducted in cooperation with HMLR (His Majesty Land Registry) [156], we provide an analysis of the crucial steps and tasks buyers and sellers must undertake

to complete the transaction process. Figs.4.9, 4.10 and 4.11.

JOURNEY MAP		
STAGE	BUYER	
OFFER	Offer made	Offer made Buyer makes an offer on the property and negotiates the sale price with the Estate Agent
	Conveyancer appointed	Conveyancer appointed. Buyer finds and appoints a solicitor to handle the conveyancing of the property.
CONTRACT	Confirmation of instruction	Confirmation of instruction. Buyer's Conveyancer confirms instruction in writing setting out the terms of business and costs.
	Monies on account	Monies on account. Buyer pays money on account to pay for searches. Likely £100s.
	Identity check	Identity check Buyer's Conveyancer meets the buyer in person and checks their ID: - Proof of identity - Proof of address Enhanced due diligence is required if the buyer is unable to meet the conveyancer or is resident overseas.
	Searches & enquiries	Searches & enquiries Buyer's Conveyancer begins due diligence on the property
		<i>Searches</i> • Local Authority Searches (LLC1, CON29R & CON29O) • Water Authority • Chancel Repair Liability • Environmental Searches (Landmark or Groundsure) • Optional & location-specific searches e.g. Coal Authority, Cheshire Brine Subsidence Area • Optional extra Local Authority searches <i>Report on title</i> • That the seller owns the property • That the seller is entitled to sell the property • The extent of the property • If anyone else needs to consent to the sale • If any legal defects in the title that need to be resolved pre- sale • If any encumbrances on the title <i>Pre-contract enquiries</i> • Restrictions on what the property can be used for • Planning restrictions • What alterations have been made • If listed or in conservation area • Compliance with all regulations • Guarantees for work done • Neighbour disputes • Rights of way/access • Obligations to contribute to repairing or maintaining other land
	Land Registry Searches	Land Registry Searches HMLR responds to search request from Buyer's Conveyancer for title register, title plan, boundaries.
	Survey	Structural survey. The Buyer decides on an RICS survey to check property condition before final value is agreed. Valuation and Certificate of title. The Lender requires a valuation survey and Certificate of Title to ensure the property is good and marketable at the offer price and/or whether the property is suitable as security for the bank at the level of the loan.
	Report on title	Report On Title. Buyer's Conveyancer produces a Report On Title confirming the property has a good and marketable title and shares with the Lender.
	Mortgage offer	Mortgage offer. The Lender reviews the Report On Title and writes to the Buyer and the Buyer's Conveyancer with details of the final mortgage offer.
	Accept mortgage	Accept mortgage. Buyer accepts the Lender's final mortgage offer and pays an arrangement fee to the Lender.
	Draft Contract received	Draft contract received Buyer's Conveyancer receives the draft contract and takes instructions from the Buyer on specific points. Bundle of documents containing: • Draft contract of sale • Property information forms • Warranties, guarantees, planning permission and building control certificates • Title plan • Official copy of Register Title • Buyer's counterpart copy of the Transfer Deed.
	Deposit payment	Deposit payment. Buyer transfers the deposit amount to their Conveyancer.
	Mortgage deed	Mortgage deed. Buyer's Conveyancer prepares the mortgage deed and sends to the Buyer for signing. Mortgage deed. Buyer signs the mortgage deed in front of a witness, dates it for the agreed completion day and sends it back to the Lender.

Figure 4.9: Buyer journey. Phases Offer and contract

EXCHANGE	Deposit payment	Deposit payment. Buyer's Conveyancer transfers the deposit amount to the Seller's Conveyancer, who confirms receipt.
	Contract exchange	Contract exchange. The Seller's Conveyancer confirms receipt of the deposit funds, and calls the Buyer's Conveyancer to date and exchange contracts Both parties now legally committed. Both parties agree date for completion.
	Standard Conditions of Sale	<i>Standard Conditions of Sale Including:</i> - date of contract - seller's details - buyer's details - property details - title number - particulars and incumbrances - completion date - contract rate - purchase price - deposit amount - contents price - balance
	Title	<i>Title Including:</i> - Official copy of Register Title - Title number - Title guarantee - Title plan.
	Transfer Deed	
	Any other information	Any other information Including: - Warranties & guarantees - Planning permission - Building control certificate
PRE-COMPLETION	Pre-completion undertakings	Pre-completion undertakings. Buyer's Conveyancer requests standard completion undertakings from the Seller's Conveyance Pre-completion undertakings • Arrangements for property keys • Confirmation of registered title deed • Completion method • Exact amount payable on completion • Bank account details • Mortgages and charges on the property • Undertaking to notify of discharge of mortgage
	Pre-completion searches	Pre-completion searches. Buyer's Conveyancer completes Land Registry pre-completion searches including: - Bankruptcy search (K16) - Land charges search (K15) - Official Search of Whole with Priority (OS1)
	Land Registry pre-comple	Land Registry pre-completion search HMLR responds to search enquiries and prevent entries being registered against the property.
	Completion statement	Completion statement. Buyer's Conveyancer receives the completion statement and forwards to the Buyer for payment. <i>Contents of completion statement</i> • Purchase price of the property • Chattels/fixtures • Stamp Duty Land Tax • Land registration fee • Solicitor's invoice • Property searches • Agents fee • Pre-completion checks (OS1 and bankruptcy).
	Mortgage	Mortgage Buyer's Conveyancer applies to the Buyer's Lender for the mortgage funds. Mortgage. Lender transfers the mortgage funds to the Buyer's Conveyancer via CHAPS (Clearing House Automated Payment System).
COMPLETION DAY	Transfer of funds	Transfer of funds. On the day of completion, the Buyer's Conveyancer sends the completion monies to the Seller's Conveyancer by CHAPS
	Insurance & utilities	Insurance & utilities. Buyer arranges utilities for new property, along with buildings insurance.
	Property keys	Property keys. Buyer collects keys from Estate Agent and moves in
	Notification of SDLT	Notification of SDLT (Stamp Duty Land Tax). The Buyer's Conveyancer notifies HMRC about the SDLT that is due.
	Stamp Duty Land Tax	Stamp Duty Land Tax. HMRC Receives notification of Stamp Duty Land Tax due on the purchase. Property
REGISTRATION	Registration of transfer	Registration of transfer. Buyer's Conveyancer sends completed TR1 to HMLR to register the transfer of ownership, along with charge, application fee and Stamp Duty Land Tax receipt.
		Registration of transfer. HMLR receives the signed TR1 and updates the register.

Figure 4.10: Buyer journey. Phases exchange, pre-completion, completion and registration

JOURNEY MAP -		
STAGE	SELLER	
OFFER	Offer accepted	"I've accepted the offer!". Offer accepted Pending contracts and searches, the estate agent accepts the offer on the Seller's behalf and removes the house from sale.
	Conveyancer search	Conveyancer search. Estate Agent advises the Seller to appoint a Conveyancer.
	Identity check	Identity check. Seller's Conveyancer meets the seller in person and checks their ID: - Proof of identity - Proof of address - Proof of ownership Enhanced due diligence is required if the seller is unable to meet the conveyancer or is resident overseas.
	Conveyancer appointed	Conveyancer appointed. The Seller appoints the Conveyancer to handle the sale. The Conveyancer confirms instructions by letter setting out the terms of business and fixed fee costs.
CONTRACT	Questionnaires	Questionnaires. Seller receives questionnaires from their Conveyancer to fill out and return. Seller's Conveyancer issues questionnaires to the Seller: •TA6: Property Information Form •TA7: Leasehold Information Form •TA10: Fittings & Contents Form •TA13: Completion Information and Undertakings form.
	Title information	Title information. Seller's Conveyancer requests all title information from HMLR (or other deed holder) to deduce title. HMLR (or other deed holder) provides the title information to the Seller's Conveyancer
	Pre-contract enquiries	Pre-contract enquiries. The Seller's Conveyancer takes instructions from the seller in relation to the questions raised. Seller receives and responds to pre- contract enquiries from Buyer's Conveyancer.
	Transfer Deed	Transfer Deed. Seller's Conveyancer drafts the Original Transfer Deed TR1 (Transfer Deed Form) and sends the original to the Seller to sign, and the counterpart to the Buyer's Conveyancer for the Buyer to sign.
	Transfer Deed - original	Transfer Deed - original. The Seller signs the original transfer deed and returns it to their Conveyancer.
	Draft contract	Draft contract. Seller's Conveyancer drafts the contract using the completed questionnaires and title information and sends it to the Buyer's Conveyancer.
	Draft contract agreed	Draft contract agreed. Buyer, Buyer's Conveyancer, Seller, and Seller's Conveyancer negotiate and agree the draft contract and date for completion.
	Final contract	Final contract. Seller's Conveyancer sends the final contract to the Buyer's Conveyancer ready for completion
PRE-COMPLETION	Pre-completion undertakings	Pre-completion undertakings. Seller's Conveyancer responds to request for standard completion undertakings
	Completion statement	Completion statement. Seller's Conveyancer prepares the completion statement outlining everything the Buyer will need to pay to complete and sends it to the Buyer's Conveyancer
COMPLETION DAY	Receipt of funds	Receipt of funds. On receipt of funds, the Seller's Conveyancer calls the Buyer's Conveyancer to complete the transfer deed. At this point, the Estate Agent is notified and can release the keys to the property.
	Property keys	Property keys. Estate Agent takes possession of the property keys for giving to the Buyer.
	Transfer deed	Transfer deed. Seller's Conveyancer sends the completed Transfer Deed to the Buyer's Conveyancer.
	Discharge of mortgage	Discharge of mortgage. Seller's Conveyancer submits form eDS1 (Electronic Discharge of Security Form) to HMLR informing of the mortgage being discharged on the property.
REGISTRATION	Discharge of mortgage	Discharge of mortgage HMLR registers the discharge of the existing mortgage on the property.

Figure 4.11: Seller journey

The analysis of the conveyance process [156] provides a comprehensive understanding of the causes of delay. It is found to be (a) slow; in the UK, it takes between 10 and 12 weeks to complete; (b) expensive; the manual, repetitive, and duplicative nature of many conveyancing steps contributes to expensive legal fees

and costly searches and surveys; and (c) stressful; the uncertainty and financial stakes involved in the conveyancing process make moving house one of the most stressful events in an adult's life. The process is linked to a variety of mental health problems, including depression and anxiety. Recent studies [157] have conducted a structured investigation of the essential causes of delay in commercial real estate transactions. Through interviews conducted among commercial real estate experts, it emerges that the process map for a transaction consists of 150 individual steps and several actors involved. Steps were grouped into five major stages such as (1) the preparation, (2) marketing (required to establish an asking price of a property), (3) the due diligence period, (4) the post-exchange period, and (5) post-completion period when the land registry collects taxes and records the legal ownership. The results show that transactions are often delayed in the current paper-based system and the time taken is beyond expectations. In the UK, delays occur in close to 40% of all transactions [158]. The lack of an up-to-date single pool of standardized property information appears to be the most critical cause of delay. More specifically, the identified causes of delay correspond to the five key stages of the transaction process as shown below.

1. *Preparation period.* Cause of delay: The vendor may not have accurate or digital records of relevant information. Data about property are often not easily available, are outdated, and are collected in different formats across several organizations. Vendors often have information stored in paper format or composed of scanned documents. Therefore, data extraction can become a tedious, time-consuming, and inefficient process. Additionally, this process is error-prone, as critical dates or changing lease clauses can easily be overlooked.
2. *Marketing period.* During the marketing stage, the vendor's lawyers make the data available to potential buyers through the data room, a single portal connecting all parties involved. Cause of delay: inconsistent approaches to data rooms. Relevant information for a potential transaction is often collected using different software with the risk of incompatible formats. The lack of a

standardized format within data rooms leads to disorganized taxonomies of content provided by third parties. Additionally, software systems at individual firms may block downloading files whose names do not meet the requirements of their cyber-security firewalls.

3. *Due-diligence period.* Cause of delay: perform adequate searches through under-resourced authorities and utility companies. The search process might create substantial delays due to inefficiencies and other reasons such as underinvestment in recordkeeping, reductions in funding of local authorities, or even a lack of motivation when the search fee does not cover the work involved. Fig.4.12 summarizes the main cause of the delays analyzed in this study.
4. *The post-exchange period.* After completion, stamp duty land tax must be paid and the title is registered at HMLR. Cause of delay: lack of transparency on requests and delays in registration. The HMLR needs to run checks on the information provided and verify any prior unresolved issues that may prevent the title's legal registration to the new owner. If the title registration cannot be validated, the buyer's solicitor raises a query ('requisition'). It can happen that substantive responses to an application are often delayed and solicitors express a lack of practical guidance to prepare applications appropriately.

As mentioned previously, this research focuses on the due diligence phase. Therefore, the Preparation and Marketing and Post-exchange period are out of scope. In the due diligence phase, the most common delays are the following. (I) *Conducting adequate searches through under-resourced authorities and utility companies.* The search process might create substantial delays due to inefficiencies and other reasons such as underinvestment in recordkeeping, reductions in funding of local authorities, or even a lack of motivation when the search fee does not cover the work involved. (II) *Identification of the correct parcel.* This problem is due to the lack of digitalization of the HM Land Registry. Inconsistencies might occur between (1) paper plans and digitized maps held by HMLR, (2) the plans in the

conveyancers possess (3) the parcels identified during site visits, and (4) the boundaries provided by geolocation or satellite imaging technology. (III) *Completion of standard enquiry forms*. Despite Commercial Property Standard Enquiry Forms or CPSEs being introduced to reduce bottlenecks (LawSociety, 2002) by providing information about potential risks involved in the property transaction, they have caused further unwanted delays. Although sellers have a duty of care, they lack the motivation to provide information relating to deficiencies that potentially reduce their negotiating power. (IV) *Reviewing and reporting using unintegrated software*. The buyer's solicitor consolidates all necessary information into one document, including planning advice, title rights and obligations, and key information on occupational leases. Extracting the relevant information for this report brings the issue of data formats. Information extraction technologies use machine learning systems to identify relevant contract terms and clauses and create digitalized copies that machines can read. However, these systems are still unable to deal efficiently with great complexity. Third parties sometimes refuse to consent to the evidence required to clear titles of historical charges and encumbrances [157]. The results of the analysis show that the main causes of delays are data storage and transfer issues. Furthermore, the caveat emptor principle, that is, the buyer is responsible for checking the quality of goods before a purchase is made, does not help to speed up the transactions. This study [157] highlights that "an openly accessible, single pool of up-to-date and standardized property information could reduce most of the causes of delay highlighted. Such property passports or data log books could be traded along with the title of a property. They could, thus, form a foundation upon which layers of digital software can be iteratively laid to transfer and process transaction-related information more efficiently". Fig.4.13 shows how smart contracts could automate and facilitate the change of information during the multiple phases of the real estate transaction.

"Building information at the right time, in the right place, in the right format, at the right level of detail, and above all, the right information" [159] is crucial for

real estate transactions to make investment decisions more rational. As mentioned above, for transactions, a data room is generally made available to ensure the availability and consistency of data. Increasing interest is in transforming these pure transaction data rooms into permanent data rooms. However, significant issues prevent a standardized pool of information for every property. The problems related to taxonomy and inconsistency in the information of data in real estate transactions have been thoroughly analyzed [68]. The study reveals that a “substantial part of all relevant digital building documents is poorly suited for automated information extraction. The availability and content of documents vary greatly from owner to owner and between document classes. The analysis has shown that the amount and quality of the documents and files are very heterogeneous and depend on the owner and authors. Currently, there is no industry-wide standard so far regarding the data and documents related to property that should be captured, managed, analyzed, and exchanged. Therefore, the structuring of the document classes differs by organization. The document’s structure is analyzed using industry-standard optical character recognition (OCR) software, and areas containing text, images, and tables are recognized. OCR technology then converts document images into editable and machine-readable text. The study shows that documents are usually rather difficult to read by a machine (for example, since a large proportion (more than 80%) of the sample was marked with handwritten notes). This means that a substantial part of relevant digital building documents is insufficient for automated information extraction. The availability and content of documents vary greatly from owner to owner, from document to document, and between document classes. However, key standardized documents, such as concession documents, official certificates, infrastructure provisions, building permit documents, commercial register extracts, and land register extracts, are easier for machines to read. Data management is critical to reducing user error and improving efficiency. In real estate transactions, transferring data from the previous to a new owner is frequently subject to an inefficient and delayed process. “Through digital processing, human capacities can be focused on value-adding processes, and efficiency can be increased” [157]. Fig.4.13 illustrates

how the integration of smart contracts can significantly enhance due diligence at critical stages of a transaction. This smart contract application contributes to the development of a property passport.

Phase	Cause of delay	Notes	
The preparation period		out of scope	
The marketing period		out of scope	
The due diligence period	Performing adequate searches via under-resourced authorities and utilities companies.	The search process may create substantial delays, due to inefficiencies and under-investment in record-keeping, cutbacks in funding of local authorities, or a lack of motivation where the search fee does not cover the work involved	Searches inefficiency
	identifying the correct parcel	Because HM Land Registry is not digitalised, there might be inconsistencies between (1) the paper plans and digitised map held by HMLR, (2) the plans given to conveyancers, (3) the parcels identified during site visits, and (4) the boundaries provided by geolocation or satellite imaging technology	HMLR - Lack of digitisation
	Completing standard enquiry forms	Commercial Property Standard Enquiry Forms or CPSEs were introduced in 2002 to reduce bottlenecks during the due diligence period (Law Society, 2002). Their rationale is that if known information about any potential risk involved in the transaction of the property were disclosed by the seller prior to exchange of contracts, this would speed up the due diligence process on the buyer's side by avoiding any late re-negotiations	Property information - Lack of transparency
	Reviewing and reporting using non-integrated software.	In reporting to the client, the buyer's solicitor will consolidate all necessary information into one document including planning advice, rights of and burdens on the title and key information on the occupational leases. Extracting the relevant information for this report, again, throws up the issue of data formats	Taxonomy issues and inconsistency between softwares
Post- exchange period	Lack of transparency over requisitions and delays in registration	When a transfer of ownership takes place, it is legally required that the new property ownership is registered through HMLR. This process is processed through the online portal or business gateway provided by the Land Registry. To ensure the validity of any transfer of title, HMLR must first run checks on the information provided and consult their database for any prior unresolved issues, which may prevent them from legally registering a new owner. Where title registration cannot be validated and therefore processed, a query ("requisition") is raised of the buyer's solicitor	Lack of transparency about property information over requisitions
ANALYSIS		Analysis Most causes for delay represent data storage and transfer issues. However, available digital technologies in commercial conveyancing have mostly focused on digitising current workflows. While this offers a more efficient transfer of information than paper-based processes, it lacks the capability of automating the full spectrum of tasks required for efficient real estate transactions. Moreover, the principle of caveat emptor (Johnson, 1985), i. e. the principle that the buyer is responsible for checking the quality of goods before a purchase is made, makes a lengthy due diligence process essential for buyers. This contributes to long transaction processes. All participants in the mapping process agreed that an openly accessible, single pool of standardised, up-to-date property information could reduce most of the causes for delay highlighted. Such property passports or data log books could be traded along with the title of a property. They could, thus, form a foundation upon which layers of digital software can be iteratively laid to more efficiently transfer and process transaction related information.	

Figure 4.12: Causes of delay

INTERDEPENDANCE	USE OF BLOCKCHAIN AND SMART CONTRACTS	
	1-Property passport	Property details • Property address, • Pictures, • Owner's details. Searches: • Local Authority Searches (LLC1, CON29R & CON29O) • Water Authority • Chancel Repair Liability • Environmental Searches (Landmark or Groundsure) • Optional & location-specific searches e.g. Coal Authority, Cheshire Brine Subsidence Area • Optional extra Local Authority searches Report on title • That the seller owns the property • That the seller is entitled to sell the property • The extent of the property • If anyone else needs to consent to the sale • If any legal defects in the title that need to be resolved pre-sale • If any encumbrances on the title Pre-contract enquiries • Restrictions on what the property can be used for • Planning restrictions • What alterations have been made • If listed or in conservation area • Compliance with all regulations • Guarantees for work done • Neighbour disputes • Rights of way/access • Obligations to contribute to repairing or maintaining other land. Vote on the property documentation (accuracy and completeness in %)
	2-Offer accepted	Parties: Buyer, Seller. Observers: Buyer's estate agent, Seller's estate agent • Property details, • Buyer's details • Seller's details • Price agreed -
	3-Buyer's conveyancer appointed	Parties: Buyer, Buyer's conveyancer • Buyer's details • solicitor's details • Property details • mandate and instructions • fees agreed • payment details
	4-Seller's conveyancer appointed	Parties: Seller, Seller's conveyancer • Seller's details, • solicitor's details • Property details • mandate and instructions • fees agreed • payment details
	5-Mortgage offer	Parties: Lender, Buyer. Observers: Buyer's conveyancer, Seller's conveyancer • Lender's details • buyer's details • property details • reviews the Report On Title • mortgage offer (amount borrowed, terms and conditions)
	6-Draft contract	Parties: Buyer, Seller. Observers: Buyer's conveyancer, Seller's conveyancer. • Draft contract of sale • Property information forms • Warranties, guarantees, planning permission and building control certificates • Title plan • Official copy of Register Title • Buyer's counterpart copy of the Transfer Deed.
	7-Deposit payment - Buyer to buyer's conveyancer	Parties: Buyer, Buyer's conveyancer. Observers: Seller's conveyancer Buyer transfers the deposit amount to their Conveyancer • Property details, • buyer's details, • buyer's conveyancer details, • seller's details.
	8-Mortgage deed	Parties: Buyer, Buyer's conveyancer Observers: Buyer's conveyancer, Seller's conveyancer • Property details • buyer's details • agreed completion day • date • agreed price
	9-Deposit payment- Buyer's conveyancer to seller's conveyancer	Parties: Buyer's conveyancer, Seller's conveyancer Observers: Buyer, Seller • Property details • buyer's details • seller's details • amount to be paid • date
10 triggers 11	10-Contract exchange	Parties: Buyer, Seller Observers: Buyer's conveyancer, Seller's conveyancer • date of contract • seller's details • buyer's details • property details • title number • particulars and incumbrances • completion date • contract rate • purchase price • deposit amount • contents price • balance Title Including: • Official copy of Register Title • Title number • Title guarantee • Title plan • Warranties & guarantees • Planning permission • Building control certificate
11 triggers 12	11-Completion statement	Parties: Buyer's conveyancer, Seller's conveyancer Observers: Buyer, Seller • Purchase price of the property • Chattels/fixtures • Stamp Duty Land Tax • Land registration fee • Solicitor's invoice • Property searches • Agents fee • Pre-completion checks (OS1- Official Search of Whole with Priority- and bankruptcy)
12 triggers 13	12-Transfer of funds	Parties: Buyer's conveyancer, Seller's conveyancer Observers: Buyer, Seller • Property details • buyer's details • seller's details • amount to be paid • date
13 triggers 14	13-Stamp Duty Land Tax	Parties: Buyer's Conveyancer, HMRC Stamp Duty Land tax Observers: Seller's Conveyancer, Buyer, Seller • Property details • buyer's details • seller's details • Notification that Stamp Duty is due
End	14-Registration of transfer	Parties: Buyer's Conveyancer, HMLR Observers: Seller's Conveyancer, Buyer, Seller • Property details • buyer's details • seller's details • TR1 to HMLR to register the transfer of ownership, charge, application fee and Stamp Duty Land Tax receipt.

Figure 4.13: 14 Steps where smart contracts can improve due diligence

4.2.2 Interbank Spunta Project. (CordaR3)

In a business environment, a distributed ledger such as the one underpinning Bitcoin can solve multiple problems, but also raises questions regarding privacy, regulations across countries, maintenance, and the actual feasibility of scaling the database, for example, to the whole financial system. For this reason, in this case study, we analyze the Corda system, a distributed ledger designed to meet the needs of regulated financial institutions and widely applicable in different sectors [160].

Corda is a blockchain-inspired system without the peculiar characteristics that make traditional blockchains inappropriate for the execution of business transactions. It is distributed ledger software for recording and processing shared data, such as contracts. The aim is to provide a new shared platform for the recording of commercial agreements and processing of business logic. The key principles underpinning the Corda platform are the following.

1. *Inclusion*. Parties can discover each other freely and transact directly in a single open network.
2. *Assured identity*. Parties have assurance over the identity of participants in the network.
3. *Privacy*. Only the parties who participate in the transaction and those who need reassurance of the transaction's provenance have access to the details of the transaction.
4. *Shared logic*. The behaviour of agreements (contracts) managed by the system is described in computer code that is shared to ensure the consistency and validity of agreements.
5. *Legal footing*. Deals recorded by the ledger are, by contract, accepted as admissible evidence and legally binding by all parties in any dispute.
6. *Authoritative*. Data recorded in the ledger are considered authoritative.

7. *Immutability.* Data recorded in the ledger are immutable; errors and unwinds must be processed through a subsequent transaction.
8. *Open.* Source, participation, development, governance, and standards are open to ensure the platform balances the needs of its diverse user base in a transparent fashion.

There are some key concepts in Corda that represent a significant difference from a shared database. Transactions occurring within a specific group of parties remain visible only to those participants. The access of another party can be granted upon verification of rights and identities. This is because, in a business environment, privacy is crucial, and parties might not want to make details public. In contrast to Bitcoin and Ethereum, Corda does not order transactions using a blockchain and does not use miners or Proof-of-Work. These two features are replaced by a notary. This notary acts as a trusted validator, ensuring that the spent assets have not been used before. It confirms this by checking the input states of a transaction. Each transaction uses only one notary. If assets from different notaries are involved, they are first moved to a single notary before the main transaction occurs. This design avoids the need for complex coordination between multiple notaries, improving efficiency.

Corda does not organize time into blocks [161]. To handle transaction ordering and timestamping, it employs notary clusters, which are a modular replacement for miners found on other blockchains. This design provides significant flexibility, allowing networks to customize their validation processes. A notary is composed of multiple mutually distrusting parties who use a crash- or Byzantine fault-tolerant consensus algorithm. They act as gatekeepers, either signing valid transactions or rejecting those with double-spend issues.

In Bitcoin, the timeline is organized into a chain of blocks, where each block points to a previous block chosen by the miner to build on. The blocks also contain a rough timestamp. The chain can be extended by the miners from any previous block. However, miners are incentivized to build on the most recently announced block, as the other nodes in the system recognize a block if it is part of a chain

with the most accumulated PoW. Because each block contains a reward, a not-recognised block is a loss, while a recognised block typically represents a profit. Bitcoin needs proof of work because the philosophy behind blockchain is to allow an unlimited number of identityless parties to join and leave the consensus-forming process. The PoW makes it hard to perform Sybil attacks. This attack refers to a situation in which a node creates a large number of pseudonymous identities or nodes to control or influence the network. These false identities, known as Sybils, are controlled by a single entity or a coordinated group. While Bitcoin is made up of nodes that cannot or do not want to commit to any long-term relationship and where there is no identity verification, Corda nodes have long-term stable identities. For this reason, Sybil attacks are blocked by the network entry process, which allows Corda to discard PoW.

A typical constraint of the Bitcoin blockchain is the difficulty of scaling the system and the nearly non-existent support for parallelism (parallelism refers to the ability to perform multiple tasks or computations simultaneously, enhancing the efficiency and scalability of the system). An advantage of Corda is that it has primary units of parallelism in Corda called flows. Many flows and, consequentially, the ledger updates can be running at the same time. The checkpointing mechanism allows flows to migrate across flow workers transparently as workers are added and removed. Notary clusters can commit transactions in batches, and multiple independent notary clusters can process transactions in parallel. Transactions can also be verified in parallel. They are not globally ordered but only relative to each other via the input list. In this way, the dependencies of a transaction do not depend on each other and can be verified simultaneously. Signature verification has historically presented a bottleneck in the process of validating blockchains, making the Corda improvement a substantial advancement.

Corda smart contracts are deliberately isolated from the underlying cryptography: they are run after signature verification and do not execute if the required signatures are missing. This ensures that signatures for a single transaction can be checked even though the smart contract code for the transaction is not accessible to

threading. In contrast to most existing distributed ledger and blockchain platforms today, Corda was built with the explicit purpose of recording and enforcing business agreements between trading partners. The system enables multiple applications and services to run across a common layer of identity, consensus, business logic, data definitions, and governance.[160].

The Corda system has been applied to interbank reconciliation in the Italian banking industry in a live application. The reconciliation process for interbank transactions (known in Italy as *spunta* has been notoriously complex. The process aims to reconcile the contracts between banks to obtain a “single version of the truth”. Multiple parties are involved and the task of identifying and addressing inconsistencies is characterized by a lack of standardization and the use of fragmented communication methods. A pioneering collaboration between R3 and several key participants in the Italian banking ecosystem has led to the development and piloting of blockchain-based solutions to transform the *spunta* process. R3 enterprise is based on the Corda system, which has emerged to be particularly appropriate for this task. R3 was designed to meet the standards of the financial services industry and is compatible with the technical competencies already in place in banks. In March 2020, the first group of 17 banking groups (corresponding to 32 different banking entities) went live on the Spunta application. According to the Italian Banking Association [162], Spunta DLT, powered by Corda Enterprise, has made the interbank reconciliation process faster, more efficient, and more transparent. Unlike the old process, transactions are reconciled daily, not monthly. The participants highlighted that the Corda system helped match the rules as they were shared and executed consistently in the Corda ledger. Reduce operational inefficiency and facilitate the real-time management of the reconciliation process. It also provided advantages by facilitating the standardization of both the process and the communication protocol. The system increased transparency by allowing full visibility of counterparty movements at any time. Finally, it enhances the tracking of communication and interactions between banks.

4.3 The misuse of blockchain technology: Tornado Cash

This case study highlights how the misuse of blockchain technology raises concerns among governments and regulators. Tornado Cash showcases the risk posed by completely anonymous payment and the importance of balancing privacy with transparency and auditability. Since its launch in August 2019, this crypto mixer has sold over \$7.6 billion worth of ether. Almost 30% of the funds sent through it have been tied to illicit actors. On 8 August 2022, Tornado faced sanctions from the US Treasury's Office of Foreign Assets Control (OFAC) for its involvement in laundering more than \$455 million dollars of cryptocurrency stolen by the North Korean organization Lazarus Group [163].

There are several hundred types of cryptocurrencies, but for the purpose of understanding potential implications on the money laundering process, we focus on Bitcoin as it remains at the forefront among cryptocurrencies in terms of market capitalization, user adoption, and widespread recognition. There are multiple reasons why Bitcoin raises concerns among governments and regulators. (I) *Pseudo-anonymity*. Although Bitcoin transactions can be linked to specific computer addresses or public keys associated with users, users are not required to disclose their real-world identities. This practice allows to retrieve the path for each transfer and backtrack to the original issuance of the coin. However, the identity of the users will not be disclosed. (II) *Peer-to-peer system*. Bitcoin was purposely designed as a peer-to-peer platform to bypass the regulatory instruments of the traditional financial sector regulated by governments. The authority of a centralized infrastructure, such as in the traditional banking system, assures users that issues with transactions and fraud on the network can be solved administratively. Even though Bitcoin provides good network security (a centralized system is also vulnerable to attacks on its infrastructure), it operates without the endorsement or regulatory oversight of a central authority [164]. (III) *Instantaneous transnational transactions*. The nature of Bitcoin transactions makes them transnational, near-instantaneous, and irreversible.

Blockchain technology allows for global transactions without geographical restrictions. Money launderers can take advantage of this feature to move funds across borders quickly and with relative ease, bypassing traditional financial institutions' scrutiny. Combined with the rapid proliferation of new cryptocurrencies, these factors have surpassed the development of policies, regulations, and law enforcement, making Bitcoin particularly attractive for terrorist financing, money laundering, and other criminal activities. [165, 166].

One of the primary features of Bitcoin that contributes to its endurance, yet simultaneously impedes efficient AML (anti money laundering) regulation, is the protocol's anonymity and resilience through flexibility. Without the possibility of establishing a definitive link between a particular Bitcoin address and an individual, tracking the injection, layering, and reentry of laundered funds can be extremely difficult for enforcement by governments and regulators [164]. Bitcoin potentially allows any user-legitimate or criminal to transfer money at near instantaneous speed at little or no cost, with very low barriers to entry, while remaining virtually anonymous, without a public paper trail. Furthermore, the capacity of users to convert bitcoins into different currencies and route transactions through several Bitcoin addresses to conceal their trail poses additional challenges for anti-money laundering initiatives. Bitcoin and analogous virtual currencies could enable money launderers to move illicit funds faster, cheaper, and more discretely than ever before [164].

Although anonymity poses significant concerns regarding money laundering and criminal activities, the reality is more complex than appearances, and most cryptocurrencies can be traced back to their original owner with a relatively high probability of success. However, the pursuit of tracing the source or creation of the coin relies on the computational capacity required to follow the sequential chain of transactions. If the investigation is limited to blockchain data, cryptocurrency trades remain shrouded in secrecy. Nevertheless, the path taken by the digital coin is likely to intersect a regulated exchange market at a given point during the lifecycle of the currency. Any entity needs to go through a crypto-to-fiat portal to convert illicit gains, incurring the risk of being identified. The gate from the encrypted world to

fiat currencies is relatively well-guarded in organized, mature markets. The wallets that contain Bitcoin, Ethereum, Litecoin, etc., are nameless, but the digital threads can be traced to a beneficial owner when the fiat threshold is crossed. [166]. Additionally, while Bitcoins theoretically enable money launderers to move illicit funds more efficiently, there is still little evidence to support claims that such illicit activities are being undertaken with cryptocurrencies. For example, in 2015, the British National Risk Assessment established that “there are only a limited number of case studies upon which solid conclusions could be drawn that digital currencies are used for money laundering and the money laundering risk associated with digital currencies is low”. [167]. However, the risk of money laundering through crypto assets has increased since 2017, with criminals increasingly incorporating them into their money laundering methodologies. The UK’s risk of using crypto assets for money laundering is now medium [168].

Tornado Cash is a smart contract mixer deployed on the Ethereum blockchain that seeks to anonymize user assets to protect their privacy. In line with the increasing use of cryptocurrencies for illicit activities, the Tornado Cash platform was repeatedly exploited to laundering misappropriated funds [169]. Crypto mixers aim to create a disconnect between the cryptocurrencies deposited by users and withdraws. They work by pooling the funds deposited by many users together, shuffling them in a seemingly random fashion, and returning the remaining funds to each depositor. Funds can be transferred from an individual’s Ethereum address into the Tornado Cash smart contracts, where they would be retained until the depositor decides to withdraw them. Generally, users might defer the retrieval of their assets for a certain time, ranging from several weeks to months or even years. An extended interval, where other participants deposit and withdraw funds, can increase the efficacy of the privacy-preserving mechanisms inherent in Tornado Cash’s design. Upon withdrawal, the protocol employed zero-knowledge proof technology to transfer funds to a new Ethereum address, thus breaking the link between the originating address used for the initial deposit and the new recipient address from which the funds were

retrieved. The Tornado Cash protocol is immutable, trustless, and fully automated. The anonymity provided by Tornado Cash depends on the fact that multiple users simultaneously use the service, breaking the connection between wallet addresses used for deposits and withdrawals. To retrieve their assets, users possess a cryptographic attestation proving ownership of the tokens deposited.

From a more technical perspective, Tornado Cash is a decentralized, non-custodial smart contract with the following characteristics. (I) *Decentralized*. The codebase is open source and managed (at least in part) by a decentralized autonomous organization (DAO). This source code was published on GitHub until the platform was removed due to the OFAC's sanctions announcement. (II) *Non-custodial*. The platform does not gain custody over its users' funds at any point during the mixing process. (III) *Based on smart contracts*. The code runs on various open public blockchains like Ethereum. The Tornado Cash's mixing process is presented below [170, 171, 172, 173, 169, 174]. The system is characterised by a high level of complexity. The analysis provides a simplified explanation as the scope is not a detailed investigation of the technology but to highlight Tornado Cash's crucial features and why they raise concerns regarding money laundering activities. The key steps of the process are listed below.

1. The user generates a *deposit note* on their local device and shares a cryptographic hash of it in a transaction with their chosen Tornado Cash pool contract. This note is a sort of *claim check* to prove they have handed over the sum of money.
2. The user's funds are sent to the contract, which pools this deposit together with other users' deposits in the denominations specified by the contract. The funds can remain in that pool for as long as users want. (Pools also exist for tokens such as USDC, USDT, DAI, cDAI, and wBTC and assets on blockchains other than Ethereum.)
3. Users then utilize their secret deposit note and some highly effective zero-knowledge cryptography to generate a transaction that proves they have the

right to withdraw the deposited value. The user can then either withdraw the funds themselves or have a *relayer* which processes the withdrawal on their behalf. A small fee (0.05% to 0.2%) is paid for the service. This relay transaction separates any direct connection between the user's deposit and withdrawal.

Fig. 4.14 provides an overview of the protocol. A user sends a fixed amount to the mixer. There are different pools (100DAI, 1000DAI) to make different deposits. The amount is a predefined unit to avoid compromising privacy. It is quite evident that if the deposit were not fixed, this would create a strong connection between the sender and the user who withdraws the money. For similar reasons, Tornado Cash suggests users allow a certain amount of time before withdrawal. The mixer receives the user's money, together with other deposits. Later, the user's money is sent to a fresh address not associated with the user himself/herself. The user has the secret key for this new address. Now, the user can purchase from an NFT marketplace while maintaining anonymity regarding their ownership.

Fig. 4.15 shows the key features of the Tornado Cash contract. Users generate a secret and send its hash (called a commitment) along with the deposit amount to the Tornado smart contract. The contract accepts the deposit and adds the commitment to its list of deposits. All Coins deposited until that moment are stored in the Merkle tree. To minimise costs, only the Coins Merkle root, which is the hash of the current state of the tree, is stored in the contract. Nullifiers are used to forbid actions like double-spending. The contract also indicates the position of the next Coin and the MerkleProof for the next Coin (number 4 in the example), which is the list of hashes from leaf 4 to the roof. When users want to withdraw, they provide proof that they possess a secret to an unspent commitment from the smart contract's list of deposits.

Fig. 4.16, 4.17 and 4.18 show more details about how deposit and withdrawal work. The deposit is shown in figure 4.16. In the example, a user wants to make

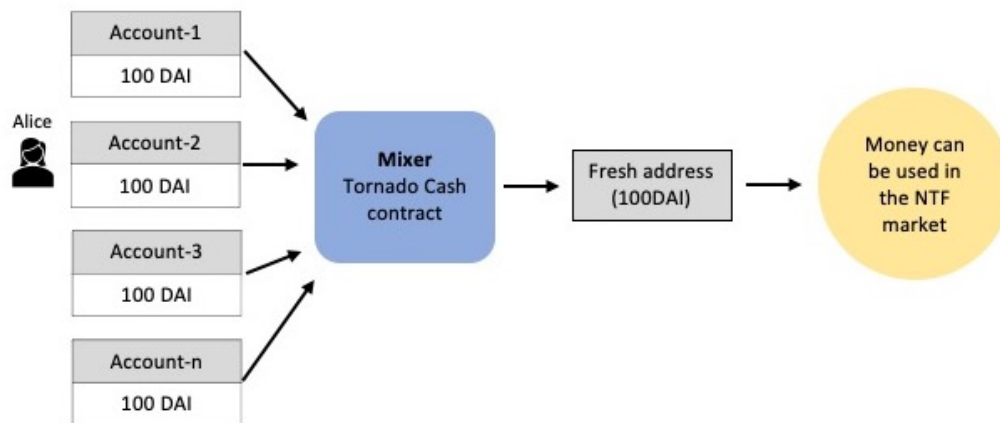
a deposit. There are already 3 Coins in the system, so they add Coin4. The user chooses two random values (K,r) and generates Coin4, which is the hash value of k,r . The hash function can be SHA256. The user writes Coin4 in leaf 4, and he/she computes the MerkleProof for Coin5, the next leaf in the tree. The user sends the contract 100DAI, Coin4 and Merkle proof (π) for position 5. At this stage, there is no privacy, and an observer looking at the tree knows who owns each leaf. The contract uses Coin4 and MerkleProof for Coin4 to compute updated Merkle root, and it verifies that the MerkleProof for Coin5 is valid. Then, it updates the state of the contract.

The withdrawal is shown in fig.4.17 and 4.18. In the example, the user wants to withdraw Coin3. The user has the secret values k',r' that he/she chose when he/she created leaf 3 (Coin3). The user withdraws Coin3 and sends funds to address A. Address A, where Tornado Contract will deposit the money, is a fresh address, and it's not related to the user in any way. The user uses K' to compute the nullifier and prove that he/she has a note for some leaf in the Coin tree and its nullifier is nf , without revealing which Coin. Nullifiers are used as a public commitment to a specific anonymous account to forbid actions like double-spending. The user builds a zero-knowledge proof π (zx-SNARK proof) composed of a public statement and a secret witness, which is used to prove the statement. The contract will verify that Coin3 is the number 3 in the root and that the note possessed by the user is the note for Coin3. Finally, the contract will verify that the nullifier is computed correctly, meaning the Coin has not been spent before. 100DAI are sent to address A, and Tornado cash is updated. The list of coins is public, but an observer does not know which Coins are spent. It is worth noting that the anonymity set for the user is basically equal to the number of people who deposited funds into the Tornado cash contract, which corresponds to around one in 1Ml.

Fig. 4.19 shows how gas fees are paid. Gas cannot be paid from the user's address otherwise, the fresh address A is linked to him/her. Tornado Cash's solution

Tornado Cash key steps

Tornado Cash is created to improve transaction privacy by breaking the on-chain link between the recipient and destination addresses. It uses a smart contract that accepts ETH deposits that can be withdrawn by a different address. Once the ETH is withdrawn, it is not possible to link the withdrawal to the deposit, ensuring complete privacy. An external observer will be unable to determine who withdrew the money.



1. Alice sends a fixed amount to the mixer. The amount is predefined to protect privacy.
2. Alice can keep the money in the Tornado Cash contract for as long as she wants. In the meantime, other users will send money to the contract.
3. When Alice wants to withdraw the money, she will prove to the contract that she owns the money zk-SNARK technology to ensure complete privacy. She will also provide an address where to deposit the fund.
4. The contract will send the money the address Alice has provided, but none will know that this address is associated with Alice.
5. Alice can use this money to buy NFTs. None will know who owns the NFTs

Figure 4.14: Tornado Cash, key steps

is to use a relay (an address which provides the service). The user sends the money to a relay, which will send the message to the Tornado Cash Contract and pay for the fees. The relay gets refunded when the user withdraws the money, so the actual amount deposited into the fresh address A is 100DAI minus gas fees.

Regarding the Tornado Cash example, some solutions have been proposed to allow privacy without compromising the traceability of funds [169]. (I) *Deposit screening*. Checking wallets making inbound transactions against blocklists and allowlists. Tornado Cash implemented a deposit screening mechanism to prevent

Tornado Cash contract

Example with 3 Coins

100 DAI Pool

Every Coin = 100DAI

H_1, H_2 = Hash functions

Tornado Cash Contract	
Treasury	300 DAI
Coins Merkle root	
Nullifier	nf_1, nf_2
Next	4
MerkleProof(C_4)	



1. The *Merkle tree* contains all the coins that have been deposited in the Contract until this moment.
2. Computing the Merkle hash of the current state of the tree, gives the *Coins Merkle root*. To minimise costs, only the *Coins Merkle root* is stored in the Contract.
3. *Nullifiers* are used to forbid actions like double spending.
4. *Next* indicates the position of the next Coin.
5. The contract also contains the MerkleProof for Coin 4, which is the list of hashes from the leaf 4 to to the roof.

Figure 4.15: Tornado Cash, contract

deposits of assets originating from individuals subject to sanctions or wallets associated with illicit activities. The solution is based on a "blocklist" where specified addresses are blocked from making deposits. (II) *Withdrawal screening*. This solution implies checking wallets requesting to withdraw funds against blocklists and allowlists. For wallet addresses that are not included on these lists, an alternative strategy for deposit screening entails the examination of oracles during withdrawal transactions. This process obstructs any withdrawal request originating from sanctioned addresses or addresses linked to unlawful activities. (III) *Selective de-anonymization*. This feature provides federal regulators and law enforcement with access to transaction information. Incorporating a mechanism for involuntary selective de-anonymization into Tornado Cash's smart contracts could potentially empower government authorities to monitor and trace illicit funds. Selective de-anonymization is a powerful instrument for preserving traceability for legitimate objectives while safeguarding privacy from malicious entities and unauthorized third parties.

Tornado Cash Deposit

Alice deposits 100DAI

1. Alice download the entire Merkle tree containing all coins that have been deposited until that moment.
2. Alice chooses random K (key), r (nonce) and compute the new coin C_4 . C_4 is the hash of K and r .
3. The coin C_4 is added in the next open slot, leaf 4.
4. Alices compute the MerkleProof for the next Coin, leaf 5. The Merkle tree for position 5 is the list of the hashes from slot 5 until the root of the Merkle tree.

Note: a nonce is an arbitrary number that is used only once

Alice sends to the Contract
100 DAI
$C_4 = H_1(k, r)$
$\pi = \text{MerkleProof}(C_5)$

What the the Tornado Cash Contract does:

1. It uses C_4 and $\text{MerkleProof}(C_4)$ to compute updated Merkle root
2. It verifies that $\pi = \text{MerkleProof}(C_5)$ is valid, meaning that it is consistent with the updated Merkle root.
3. If valid, it updates the state of the contract.

Tornado Cash Contract Updated	
Treasury	400 DAI
Updated Coins Merkle root	
Nullifier	nf_1, nf_2
Next	5
$\text{MerkleProof}(\text{Coin}_5)$	

1. The treasury is now updated to 400DAI.
2. The coin Merkle root is updated after adding Coin 4.
3. The contracts updates the next free slot to 5, and it stores the MerkleProof for leaf 5.
4. Alice stores the values K and r that she generated secretly and creates a note for K, r (note: k, r). For every Coin, one note is generated.

Note: For every deposit, a new Coin is added sequentially to the tree. At this point, an observer can see who owns which Coin. This means that an observer knows that Alice owns Coin 4.

Figure 4.16: Tornado Cash, deposit

Tornado Cash Withdrawal

Bob wants to withdraws Coin 3

1. Bob owns Coin 3, therefore he has the note for the Coin. $\text{Note}=(k',r')$
2. Bob sets the nullifier for K' , which is the hash function H_2 applied to K' .
3. Bob proves that he has a note for some leaf in the Merkle Coin tree and its nullifier is nf .

Note: Bob proves that he owns some Coin in the tree, without revealing which one.

Bob computes
$\text{Note} = (K'r')$
$nf = H_2(k')$

Bob constructs a zero-knowledge proof (zk-SNARK) that he owns some Coin in the tree

zk-SNARK Proof π	
public statement	$x=(\text{root}, nf, A)$
secret witness	$w=(K', r', C_3, \text{MerkleProof}(C_3))$

1. Bob use the secret witness to prove the public statement
2. Root is the Coin Merkle tree root.
3. A is a fresh address not associated with Bob, where Bob wants the 100DAI to be sent.

The circuit will verify the following:

Circuit(x,w) is verified if
$C_3 = (\text{leaf}\#3 \text{ of root})$
$C_3 = H_1(K',r')$
$nf = H_2(k')$

1. The Circuit will verify that C_3 is really the number 3 in the root, meaning that MerkleProof provided in the witness is a valid MerkleProof for C_3 . Now the circuit knows that the C_3 in the secret witness is really part of the Coin Merkle tree.
2. Then Circuit will verify that the note that Bob has, it is really the note for C_3 .
3. Finally, the Circuit will verify that the nullifier is computed correctly, meaning that $nf=H_2(k')$.

Note: The address A is part of the statement even though the Circuit does not run any verification about it. This is to ensure that none can change A and steal funds.

Figure 4.17: Tornado Cash, withdraw

Tornado Cash Withdrawal

Bob withdraws Coin 3 to address A:

1. Bob sends to the contract Proof π , the nullifier nf and the address A. He will send this data over TOR. The Onion Routing protocol is a method for transmitting data anonymously over the Internet by routing messages through a decentralized network.
2. The proof π doesn't reveal anything about C_3 .

Bob send to the Contract
Proof π , nf , A

What the the Tornado Cash Contract does

The contract checks

1. that Proof π is valid for (root, nf , A)
2. nf is not in the list of nullifiers.

Note: Even though it is not known what Coin is being spent, because the nf is not already in the list of nullifiers, it means that the Coin has not been previously spent.

Updated contract

1. The Contract accepts that Bob owns some Coins that has not been spent before and sends 100DAI to address A that Bob has provided.
2. The Contract adds the nullifier nf to the nullifier list.

Tornado Cash Contract Updated	
Treasury	300 DAI
Updated Coins Merkle root	
Nullifier	nf_1, nf_2, nf
Next	5
MerkleProof(Coin ₅)	

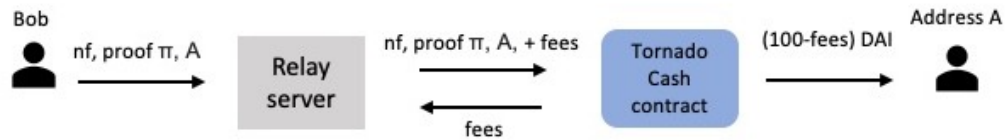
Note:

1. nf and Proof π reveal nothing about which coin was spent. However, Coin 3 cannot be spent again because $nf = H_2(k')$ is now nullified, meaning that nf is now in the list of nullifiers.
2. The Coin Merkle tree contains a public list of Coins, and it is known what Coin belongs to which user, but none knows which Coin has been spent. None knows that is Bob who withdrew a Coin and which Coin.
3. The address A where the Coin was spent, could belong to anyone who has ever deposited funds into Tornado Cash, about 1M people.

Figure 4.18: Tornado Cash, withdraw

How does Bob pay the fee to withdraw the money

Fees cannot be paid from Bob's address otherwise the fresh address A would be linked to Bob. Tornado Cash's solution is to use a relay.



1. Bob doesn't send his message to the contract directly, but he sends to a relay (a service provider) over TOR.
2. The relay sends the message to Tornado Cash and pays for the transaction. The relay gets refunded when Bob withdraw the money.

Note: Tornado Cash also charge fees, so the amount that Bob withdraws is slightly less than $(100 - \text{fees})\text{DAI}$.

Figure 4.19: Tornado Cash, fees

Although the above solutions can help significantly mitigate risks related to illicit activities, they pose additional challenges. The first question is the reliability of blockchain analytics companies in operating tools known as sanction oracles faithfully. A sanction oracle is a system or a service that provides information about addresses or entities subject to sanctions. Because Tornado Cash uses this data to prevent processing transactions from or to those entities, its compliance and operational integrity are effectively in the hands of these third-party firms. Other questions would arise, for example, about the custody of private keys, which are essential to unlock traceability and enable authorised de-anonymisation. Managing the secure custody of the private keys may introduce further complications concerning the appropriate entity responsible for their safekeeping. Consequently, the question is how innovative technological tools can be made compliant with laws and regulations to ensure that they do not become instruments to facilitate criminal activities.

The Tornado Cash analysis exemplifies the high complexity of technology, making it clear how collaboration with experts, such as cryptographers and soft-

ware engineers, is paramount. After being anonymised, illicit funds can be used to buy assets, exploiting vulnerabilities in the regulatory system or particular industries, for example, real estate and fine art, completing the laundering process. The complexity of the entire process highlights how a successful strategy to combat criminal activities must be developed within a highly interdisciplinary environment where experts from very different areas contribute to shaping effective policies and regulations. An inadequate understanding of the technology can lead to imposing ineffective and burdensome measures that do not truly impede money laundering activities. However, it is important to emphasise the distinction between blockchain as a technological infrastructure and the misuse of specific cryptocurrency services built on top of it. Blockchain is a distributed ledger technology designed to ensure transparency, immutability, and auditability of digital records. In contrast, Tornado Cash is a specific application, a smart contract-based cryptocurrency mixer, deployed on the Ethereum blockchain, whose operational logic is explicitly designed to disrupt transaction traceability. While such protocols may serve legitimate privacy-preserving functions, they have also been leveraged to conceal the origin and destination of funds, facilitating illicit financial flows. These mixers intentionally break the link between the deposit and withdrawal addresses, reducing traceability for law enforcement and regulators.

The misuse associated with Tornado Cash should therefore be understood not as a failure of blockchain technology itself, but as a consequence of how anonymisation mechanisms can be employed to circumvent compliance obligations. This distinction is essential in regulatory and policy discourse, where blockchain is often associated with cryptocurrency-related risks. In this context, it becomes clear that blockchain, if properly governed and integrated with robust compliance frameworks, can support transparency objectives. In essence, the problem lies in the unregulated or opaque use of cryptocurrency applications that deliberately undermine transparency and accountability mechanisms.

4.4 Challenges of implementing blockchain in fine art and real estate

The application of blockchain opens multiple opportunities in the fine art sector. In this section, we analyzed some of the most prominent implementations of blockchain-based platforms in these industries. The analysis in this chapter shows that there are some risks associated with the technology and difficulties with the application. The technology is still in its early stages and there are critical issues that have not yet been resolved. [175]. However, the potential of blockchain technology is becoming apparent, with platforms offering various types of services proliferating. This trend is paving the way for further technological experimentation and research, to test and devise platforms that will help gradually increase transparency and traceability.

From an anti-money laundering (AML) perspective, Verisart demonstrates promising potential as a provenance-ledger platform by recording digital certificates of authenticity on a public blockchain. This immutable and time-stamped record of ownership may strengthen due diligence processes and facilitate the traceability of artworks across multiple transactions, especially in secondary markets. Its integration of identity verification mechanisms adds a critical compliance layer by linking artworks to verified creators and owners at the time of registration. However, Verisart's capacity to prevent money laundering is ultimately constrained by the reliability of the data entered and the lack of a robust framework for ongoing validation. The platform's open architecture allows users to self-register artworks with limited third-party verification, creating the risk that fraudulent or incorrect entries become permanently embedded in the ledger. A widely cited example is the registration of the Mona Lisa by an unrelated user in 2018, an incident which illustrates the system's vulnerability to false claims in the absence of institutional oversight. Moreover, while Verisart facilitates ownership attestation and digital provenance, it does not perform or mandate Know Your Customer (KYC), beneficial ownership disclosure, or source-of-funds verification—critical components of anti-money laundering compliance. In other words, the platform cannot independently validate

the physical existence, condition, or lawful acquisition of the represented object. As such, Verisart should not be construed as an AML-compliant solution in itself, but rather as a technological layer that may enhance evidentiary support when embedded within broader compliance workflows involving regulated actors, validated identity frameworks, and institutional due diligence protocols.

It is evident that the nexus between the tangible work of art and the corresponding blockchain database represents a vulnerable point within the ecosystem. While blockchains are well-suited for transferring assets or data that is intrinsic to the blockchain or digital-only, their ability to assess the accuracy of externally entered data is limited. In essence, the veracity of the ledger's contents is a separate matter, since a blockchain does not inherently confer trustworthiness upon the data entered, nor the parties entering it [135]. The impossibility of deleting data from the blockchain makes this problem more prominent. The attribution of old master paintings, for example, is often reassessed and paintings can be identified as the work of different artists years down the line. Some artworks are sold under deliberately vague attributions ('From the School of Leonardo', for example) while research is ongoing. The closed nature of provenance-tracking on the blockchain does not allow for later amendments and may leave permanent inaccuracies related to such works. In addition, any incorrect input to the ledger would not allow modification, limiting the possibility of audit and correction over time [141]. This issue can be significant, as in the long term, the ledger might show misleading information due to the on-chain presence of outdated or incorrect information together with the right inputs. This problem also raises important questions about governance. Because blockchain is a decentralized technology, the community governance mechanisms of blockchain are critical to the system's health. These mechanisms determine who has a voice or vote in changes to the protocol or to implement solutions to problems or errors [56]. This remains a crucial challenge for Verisart and Maecenas.

Both platforms analyzed use public blockchains and allow the use of cryptocurrencies. Cryptocurrencies and NFTs are highly volatile and their value can be affected by speculative investors who just buy in the hope the price will keep rising.

Studies [176] show that pricing bubbles are possible when “attention” (which can be broadly interpreted as investors’ interests) is correlated with price movements, feeding on each other. For this reason, it might be difficult for a Maecenas investor, for example, to determine the value of their artwork shares, which may result in significant losses. As a consequence of this speculation, we have also adverse incentives for creators to focus on short-run viral content instead of its quality (e.g., creating a large quantity of low-quality NFTs). Consumers thus find themselves faced with a cluttered market difficult to navigate. NFTs make it possible for content creators to reach consumers directly, therefore the power to select content rests more with the crowd. Reducing intermediaries raises the question of how to discover and select content. As it is difficult to identify quality criteria, people might try to identify high-quality content by the sale prices [44], exacerbating the problem related to speculation and bubbles.

Some blockchains, e.g., Bitcoin in the case of Verisart, consume significant computing power and electricity due to their reliance on resource-expensive consensus algorithms. This is because the PoW, for instance, is based on a computational task that can only be solved by brute-force/iterative search of the solution, requiring substantial energy consumption. This problem is well-known in the literature. Recent research has estimated that Bitcoin mining operations produce a minimum of 22,9Mt of CO₂ per year, equivalent to the emissions produced by Sri Lanka or Jordan [177]. Although different research provides different results (because they used a different way of estimating data and a different way to geolocate the miners), all indicate a high (and increasing) level of electricity consumption [115]. Finally, there is a scalability problem as some public blockchains support a rather limited number of transactions per second to be processed, limiting a potential uptake of a large number of artworks-related transactions [175].

As mentioned in the Introduction, fine art is an attractive sector for money laundering. Astonishingly, sometimes tens of millions of US dollars can actually change hands without any formal documentation. Verisart has an ID verification mechanism embedded into the system, and artworks have to pass a strict due dili-

gence process before getting listed on the Maecenas platform (including verifying the art provenance, insurance policy, safe storage, independent valuation, artwork condition, and verification on the registry of loss and stolen art). However, the need for confidentiality and the difficulty of ensuring the truthfulness of data originating outside the blockchain leave problems related to the opacity of the sector mainly unresolved. The situation is further exacerbated by the use of cryptocurrency and the anonymity that blockchain platforms can offer. While transactions may be recorded on the public ledger, the information can be of limited use to law enforcement without knowing the true identities of the transacting parties, as individuals can mask their true identities by using different public addresses, essentially allowing transactions to be conducted anonymously [59].

Blockchain technology shows potential to improve the effectiveness and safeguard the authenticity of real estate transactions. However, there are still technical obstacles that must be overcome to ensure the widespread adoption of technology in the real estate industry. Real estate assets have unique characteristics such as high transaction costs, prolonged holding periods, rigorous regulatory oversight, and entry barriers that distinguish it from equities and bonds [63]. Real estate assets are expensive investments and this may prevent people from taking any chances with the procedures governing their trading, maintenance, or appraisal. In addition, an agency dilemma can arise, as the transaction process is dominated by professional consultants who have a vested interest in preserving their income streams, which leads chartered surveyors, brokers, and lawyers to potentially resist technological innovations that aim to disrupt their work [76]. Blockchain technology offers several advantages but has limitations, such as scalability. The real estate industry generates a significant amount of data, including property listings, transactions, and legal documents. A significant amount of storage and processing power is essential in a public blockchain network, given that verifying a new block requires all previous transactions to be presented. In this regard, permission-based blockchains such as Hyperledger Fabric could be preferable as they do not impose such a burden on the network, and therefore, they could be more efficient and have better scalability

[178]. Blockchain technology is still in its early stages of development and there is currently a lack of standardization and interoperability between different blockchain platforms. This can create challenges when trying to integrate blockchain into existing real estate systems and platforms. The number of blockchain-based applications is growing at a fast pace, creating a huge number of heterogeneous solutions. The wide diversity of implementations and features implies interoperability issues, which hinders standardization, potentially negatively impacting the efficiency of the sector [80]. Additional difficulties can be seen in the interoperability between multiple blockchain-enabled registries and jurisdictions, as a blockchain system will allow peer-to-peer transactions between platforms and countries [179]. Despite the inherent security features designed into blockchain technology, apprehensions persist about possible security breaches and hacking. Given the sensitive nature of real estate transactions, which involve the exchange of confidential financial and personal information, security becomes a crucial concern in the industry when considering adopting blockchain solutions.

Furthermore, adopting blockchain technology in the real estate industry may entail a considerable degree of technical know-how and resources, encompassing the creation of tailor-made smart contracts and applications. This may pose obstacles for small-scale companies or entities with limited resources. The technology has been frequently designated as too complex to attract a large amount of attention [180]. There is limited awareness at the organizational level and executives hesitate to embrace it. This can be attributed to scepticism about the return on investment and the lack of coherent employment of the technology. Finally, the synonymy of blockchain with Bitcoin has not helped with the widespread adoption of the technology. To address this issue, blockchain should dissociate itself from the negative connotations of cryptocurrency. A concerted effort among "knowledgeable advocates is necessary to propagate widespread awareness of the blockchain and its benefits that extend beyond cryptocurrencies" [180]. Blockchain-based technology, such as smart contracts, property passports, and blockchain land registrations, can significantly help streamline specific real estate transaction elements. How-

ever, technology is far from wide-scale adoption and the absence of standardized digital data and operational data security problems are significant barriers to adoption. [158]. Furthermore, regulatory bodies have not yet caught up with blockchain innovation, which hinders its adoption by businesses in various industries. (For example, digital currencies using blockchain have faced difficulties in achieving broader adoption, due to the lack of government and regulatory approval and support [180]). Thanks to blockchain technology, real estate transactions could be fully automated. However, they must comply with existing legislation, and some of the most ambitious innovations would require unlikely changes in contract law, which are far from happening [158].

Despite the implementation challenges identified, it is essential to recognise the comparative advantages that blockchain systems offer over traditional centralised architectures. From a systems architecture perspective, the distinction between blockchain-based infrastructures and traditional centralised systems, particularly those deployed in regulated environments such as banking, rests not solely on the presence or absence of a central authority, but on deeper differences in data governance, trust distribution, and fault tolerance. Contemporary centralised systems, including those used by banks, are often hosted on secure, scalable cloud infrastructures with built-in redundancy, granular access controls, and continuous compliance monitoring. These architectures support high throughput, regulated data protection standards, and established incident response procedures. However, such systems retain administrative centrality, meaning that control over data integrity, version history, and access policies ultimately resides with the institution or third-party service provider. In contrast, blockchain systems are characterised by distributed consensus and state replication, where data is validated and synchronised across multiple independent nodes. This design reduces reliance on institutional trust by ensuring immutability at the protocol level, verifiability through cryptographic proofs, and transparency through shared ledgers. Smart contracts further enable automatic enforcement of predefined rules without post hoc reconciliation or discretionary override. While both architectures can implement access control and audit trails,

blockchain systems provide deterministic auditability, that is, transaction history is not merely logged but cryptographically enforced and visible to authorised parties without the need for institutional mediation. Thus, although centralised cloud infrastructures can meet high standards for security and operational resilience, they cannot natively replicate blockchain's combination of decentralised trust, protocol-level finality, and autonomous execution, which are particularly advantageous in contexts demanding verifiable integrity and reduced reliance on institutional gate-keeping.

Dimension	Blockchain System	Centralised System Cloud-Based System
Control and Governance	Decentralised governance via protocol rules and consensus among distributed nodes.	Centralised control under institutional or third-party authority with administrative override capabilities.
Data Integrity and Immutability	Transactions are immutable by design; any change requires consensus and is publicly verifiable.	Data integrity is enforced through institutional policies and logging but can be altered by administrators under certain conditions.
Auditability	Deterministic and cryptographically enforced audit trails; verifiable without relying on institutional mediation.	Institutional audit logs are maintained internally; traceability relies on central control and system configuration.
Consensus and Verification	Distributed consensus (e.g., PoS, BFT, or permissioned consensus) ensures state validity without central approval.	Data verification is performed by trusted servers or system owners; consensus is implicit in system authority.
Automation and Enforcement	Smart contracts enforce rules automatically and transparently at the protocol level.	Business rules are executed through application logic or workflow engines, requiring manual oversight or triggers.
Fault Tolerance and Availability	High resilience through replication across multiple nodes; no single point of failure.	Redundancy and availability ensured via cloud infrastructure (e.g., multi-zone failover); dependent on provider resilience.
Privacy and Access Control	Selective transparency via role-based access, ZKPs, and permissioned layers.	Fine-grained access control via identity and role management; visibility controlled by system administrator.

Table 4.3: Architectural Comparison: Blockchain vs Centralised Cloud-Based Systems

Chapter 5

Proof of Concept: Fine art

In Chapter 2, we analyze the fine art and real estate sector and highlight the key characteristics that make them prone to money laundering activities. We investigated current inefficiencies and identified business bottlenecks. We also analyze some key characteristics of blockchain (Chapter 3) and the state-of-the-art of new technologies in these sectors, particularly blockchain, and identified problems that were not addressed by current solutions (Chapter 4, Section 4.4). In this chapter and in Chapter 6, we build on the work done in the previous parts of the research to design key features to enhance due diligence in fine art and real estate, thus increasing transparency.

5.1 Foundational elements of the Proof of Concept

Given the peculiar characteristics of the real estate and fine art sectors and the need for transparency as well as privacy and confidentiality, we believe a private or semi-private blockchain can be a suitable solution. There are multiple examples of firms in the financial sector and other industries using private and permissioned blockchains, such as Hyperledger Fabric, to manage their operations and store and reconcile data. The idea of using a private or semi-private blockchain was supported by UCL Business and Enterprise, which provided funding to develop an MPV (Minimum Viable Product described in Chapters 7) based on the proof of concept developed in this chapter and Chapter 6. We are aware that even though a public blockchain entails a higher degree of complexity to ensure privacy in a

completely open network, it offers greater security. For this reason, in Chapter 7 Section 7.2, we design a solution deployed on a public blockchain using zero-knowledge protocols to prove compliance with law and regulation (thereby ensuring transparency), without compromising privacy. The MVP for this second solution is outside the scope of this research and will be the topic of my postdoctoral research.

Before delving into the details of the proposed solutions, we consider the advantages and disadvantages of a blockchain solution compared to a traditional database. The latter operates on a centralized architecture with controlled access mechanisms, allowing for fine-grained privacy controls through role-based permissions and data encryption. Although this constitutes a simpler solution compared to a blockchain database, it enables data modification and deletion. Centralization introduces vulnerabilities such as the reliance on trusted administrators and the susceptibility to a single point of failure, which can compromise both transparency and data integrity. Blockchain technology can be a suitable solution when [181] (I) valuable data needs to be recorded, tracked, or logged, (II) data can change over time, (III) it is imperative to keep track of the history of changes, (IV) recorded data cannot be changed or removed, and, and (V) it is beneficial that actions are automated based on the change in data. These key points are crucial to increase transparency in the fine art and real estate sectors and make a strong case for a blockchain solution.

The proposed architecture is governed through a consortium-based model that assigns administrative roles to regulated entities. At its core, the system is governed by Main Entities (MEs), which include regulated institutions such as museums, auction houses, and land registries. These entities are responsible for validating transactions, maintaining data integrity, and executing compliance checks based on their institutional expertise. MEs are authorised to issue certifications, endorse data entries, and grant or revoke access rights under predefined smart contract logic. Surrounding the MEs are Supporting Roles, including Controllers, who manage access permissions and workflow initiation for their respective organisations, and Observers, who have read-only rights for auditing, monitoring, or external verifica-

tion purposes. This tiered role model ensures clear accountability and operational transparency while allowing for differentiated access and responsibility. Crucially, all administrative actions are logged on-chain, enabling deterministic auditability and reducing the risk of internal manipulation or unauthorised data alteration. This governance framework balances decentralized verification with institutional trust, ensuring that critical functions, such as provenance attestation or title validation, are undertaken only by parties with formal authority and domain competence.

The business model assumes that the network would operate as a cooperatively maintained infrastructure, where each consortium member contributes to governance and operational costs in exchange for privileged participation rights, visibility into provenance records, and access to verified documentation. Participation may also be tiered: institutional actors may pay an onboarding or node maintenance fee, while smaller market participants (e.g., individual collectors or solicitors) could access services through licensed gateways or application providers. Revenue generation mechanisms could include transaction processing fees, validation services, or the issuance of certified provenance records. Importantly, no cryptocurrency is used within the system, and value exchange occurs in fiat or off-ledger channels. This ensures regulatory compatibility and reduces volatility, while maintaining the blockchain's function as an immutable compliance and certification infrastructure. Overall, this hybrid model creates a commercially sustainable and regulatory-aligned registry for high-value asset transactions.

Participating institutions, particularly museums, galleries, and cultural organisations, are already engaged in ongoing digitisation efforts, supported by substantial public and philanthropic funding, making them prime candidates for seamless integration with blockchain registers. In the UK alone, the National Lottery Heritage Fund has invested over £2.2 billion since 1994 in museums, archives, and library digitisation projects [182]. Art Fund has recently awarded more than £800,000 through its Reimagine programme to support digital activity in 20 local institutions [183]. These initiatives reflect a strategic and funded transition toward digital record-keeping. Given these ongoing commitments, integrating blockchain inter-

faces with existing workflows incurs minimal marginal cost. More importantly, the proposed business model offers new revenue streams: verified provenance registries and certified records can be monetised through subscription or pay-per-query fees, enabling institutions to recoup investment and sustain their digitisation efforts. This financial incentive encourages positive behaviors, maintaining high-quality data, improving interoperability, and contributing to shared infrastructure. Furthermore, because institutions can license access to their data, cooperation becomes economically attractive: shared resources strengthen provenance chains across collections, enhancing reliability and cross-institutional trust. The blockchain interface itself requires no wholesale changes to internal digitisation processes; instead, it overlays cryptographic anchoring and standardised access protocols on existing systems, facilitating compliance, enabling new monetisation models, and promoting collaboration, all while aligning with funded digital strategies [184].

The HM Land Registry (HMLR) have already allocated budgets to digitisation and Research and Development (RD). For instance, HMLR's "Digital Street" project—funded through its trading fund—has piloted blockchain-based processes (via Corda) to digitally sign mortgages and reduce conveyancing times from weeks to minutes [185]. HM Land Registry (HMLR) is strategically positioned to participate in the proposed blockchain registry, building on its ongoing investment in digital transformation under the Digital Street initiative, which is funded internally through its trading model. A recent proof-of-concept led by ConsenSys and Codefi demonstrated HMLR's tokenisation of property ownership and use of smart contracts to streamline mortgage and conveyancing processes, showcasing the ability to "increase transparency and cut costs in real estate" by embedding title data and transaction metadata on a shared ledger [186]. Since HMLR's operations are funded through registration fees, integrating blockchain entails no additional external budget, while leveraging existing digital infrastructure. HMLR stands to gain operational efficiency through reduced manual reconciliation and fraud risk, support smarter public services by enabling mortgage providers and legal professionals to access time-stamped title data, and generate new revenue streams by licens-

ing authenticated land registry data and certification services to conveyancers and financial institutions. Furthermore, the shared, permissioned ledger fosters inter-institutional cooperation with banks, solicitors, estate agents, and surveyors, enhancing collaboration without compromising data governance or privacy, thus reinforcing public policy goals of modernisation, interoperability, and registry integrity.

When weighed against the projected benefits, the costs associated with consortium participation are modest and largely consistent with existing digitisation investments already undertaken by institutions. Integration with the blockchain registry requires no fundamental change to current digitisation workflows, as meta-data remains managed within institutional systems, with only cryptographic anchors and permissioned access points interfaced via the blockchain layer. Operational costs—such as hosting and maintaining a blockchain node—are minimal, typically involving lightweight infrastructure that can be deployed on institutional servers or cloud environments, depending on local IT capacity and preference. For public-sector bodies such as HM Land Registry and national museums, much of the required infrastructure, cloud hosting, data cataloguing standards, and legal review processes, is already in place and funded under national digital transformation programmes. The marginal financial cost is therefore minimal. In return, participants gain access to a secure, tamper-evident infrastructure for provenance or title records, along with monetisation mechanisms for verified datasets and a scalable platform for inter-institutional cooperation. By joining the consortium, institutions are not only aligning with compliance and transparency imperatives but also reinforcing their relevance in a data-driven ecosystem—transforming their role from static record-holders into active nodes of verification, trust, and economic value.

In this consortium-based architecture, validator roles are explicitly defined to ensure operational integrity, compliance enforcement, and institutional accountability. Validators are authorised entities responsible for verifying the authenticity, provenance, or legal status of submitted information before it is committed to the shared ledger. These roles are encoded via permissioned smart contracts that define validator permissions, obligations, and constraints, such as the ability to approve,

reject, or escalate submissions based on predefined criteria (e.g., documentation completeness, authority of the source, conflict of interest checks). Validation functions are distributed across domains: museums and archives validate provenance; legal professionals verify ownership and contractual authority; financial institutions confirm source of funds where applicable. To support sustainability and data integrity, the system incorporates a set of incentive mechanisms. Validators may receive service fees per validated transaction, recurring access fees for maintaining high-quality datasets, or revenue shares from licensed third-party queries. These economic incentives are designed to reward ongoing data stewardship and discourage passive or opportunistic participation. Validators are also reputation-sensitive: entities that consistently meet quality and auditability thresholds may gain preferential indexing, enhanced visibility, or institutional endorsement within the system. Conversely, failure to validate accurately or in good faith may lead to revocation of rights or exclusion from the network.

Criteria for validator selection include demonstrable domain expertise (e.g., curatorial authority, legal accreditation, AML compliance capacity), institutional affiliation or professional certification, digital onboarding (KYC/KYB), and commitment to network participation standards, including regular auditability and conflict of interest disclosure. All validators must agree to be subject to external peer review and dispute resolution protocols encoded in governance smart contracts. This framework ensures that validation is not only decentralised but credible, transparent, and enforceable, supporting the system's broader compliance, provenance, and trust objectives.

The first step to developing the Proof of Concept was to choose the most suitable software language. Real estate transactions are regulated by UK laws, and there are stringent requirements regarding data security and privacy. As well as real estate, the fine art sector requires a high degree of privacy and confidentiality. DAML (Digital Asset Modeling Language) is an open-source language with appropriate characteristics to develop legal smart contracts. It can be used with different types

of blockchains, such as Hyperledger Fabric, and distributed ledger technologies, such as Corda. This software language is developed by Digital Asset for creating complex and multi-purpose business applications. The primary objective of DAML is to facilitate the development of applications that require sophisticated workflows and smart contracts. DAML has an abstract ledger on which an application can be developed and integrated with various blockchain platforms, like Hyperledger Sawtooth, Hyperledger Fabric, Corda, etc. The language is developed using Scala and its compiler is written in the Haskell programming language [187]. The language allows for the assigning of fine-grained permissions and different roles to users, distinguishing between parties who can only access the ledger data and parties actively performing actions (e.g., submit or sign transactions) [188]. On this platform, endorsed parties can interact in a decentralized way. All transactions are immutably recorded and can be made accessible to the relevant stakeholders (such as the buyer, seller and estate agents, auction houses). By default, in DAML, it is possible to create three pre-defined types of parties with different privileges: (I) signatory, (II) controller, or (III) observer parties. A signatory can propose an action and sign and submit contracts to the ledger. The controller is the counterparty, who can perform actions (e.g., accept or deny) on a proposal made by the signatory. Finally, the observer is a witness (e.g., regulator, auditor) with no controlling abilities, possessing only visibility and access to transactions and data. [188]. This language allows for specifying different actions that the various parties can perform or oversee. It also has a built-in feature for testing the functionalities of prototypes by creating so-called scenarios specifying different actions performed by the parties, creating contracts and simulating real-world business applications. The platform maintains a comprehensive record of transactions and a modification history by creating a new contract for all changes and updates to existing contracts. The previous version of the transaction is archived and remains visible in the ledger as an archived contract. This process ensures that the entire history of modifications and transactions is permanently stored and readily available on the platform. There are multiple DAML use cases in the industry. In 2021, the BIS Innovation Hub launched a project in

collaboration with the Hong Kong Monetary Authority (HKMA) to improve efficiency in the distribution of green bonds and to facilitate more detailed reporting on the environmental impact of green bond proceeds [189]. In 2021, Deutsche Börse, a financial market infrastructure provider, chose DAML to develop its new fully digital post-trade platform, D7. The new cloud-backed and DLT-ready platform paves the way for same-day-issuance and paperless, automated straight-through processing for the entire value chain of issuance, custody, settlement, and asset servicing for digital securities [190]. In 2023 Goldman Sachs announces that the bank's new digital asset platform, GS DAPTM, is live. The GS DAP platform is built on top of Digital Asset's smart contract language, DAML, and Canton, a blockchain with privacy features. Tokenization platforms built using DAML, such as GS DAP, have the ability to capture the complete intricacies of asset lifecycles, encompassing rights, obligations, and cash flows. Moreover, these platforms can provide accessible and fully automated digital representations and workflows across interconnected ecosystems of distributed participants. Digital Asset's privacy protocols ensure that data is only shared with authorized stakeholders while supporting the scalability required to enable global asset connectivity [191].

5.2 Key features for a fine art decentralized registry

In Chapter 3, we analyze the current state of technology in the fine art sector. We delve into some promising blockchain-based solutions which have been recently introduced in the industry. Fresco, Artory, and Verisart offer compelling solutions for documenting the lineage of the artwork and verifying its authenticity. However, the nexus between the tangible work of art and the corresponding blockchain database represents a vulnerable point within the ecosystem, as it mainly depends on the use of a QR code that is attached to the artwork. In addition, there are doubts about the validity of the data recorded in the blockchain. While blockchains are well-suited for transferring assets or data that is intrinsic to the blockchain, their ability to assess the accuracy of externally entered data is limited. In essence, the veracity of the ledger's contents is a separate matter, since a blockchain does not inherently

confer trustworthiness upon the data entered, nor the parties entering it [135]. This observation aligns with the principle of "garbage in, garbage out" (GIGO), which posits that input ambiguity should be assumed as a given. Inaccurate input is treated by a blockchain in the same manner as any other input, whereby it is hashed and recorded as a mere hash value within the blocks. The blockchain solely ensures that the data remains unchanged.

The literature review provides evidence (Chapter ??) that unalterable databases would be valuable to avoid forgeries and to establish ownership of artworks. In the art world, the biography of artworks is deemed highly significant as it plays a crucial role in determining ownership and estimating value. Provenance is crucial to determine the authenticity of the artwork, and it has been a vital aspect of prosperous European market centres since at least the 18th century, providing collectors with orientation and supporting art valuation. The precision and abundance of information pertaining to an artwork play a crucial role in preventing fraudulent practices, such as fabricating a false history of ownership and producing counterfeit works. In addition, provenance helps researchers resolve instances of misattribution and other genuine errors. Therefore, the accuracy of the data uploaded to the blockchain is paramount. Artwork data sets are susceptible to manipulation (as demonstrated by the frequent frauds occurring in the art sector). Malicious individuals can exploit this vulnerability to their benefit, either by disseminating false information through compromised data or by fraudulently claiming credit for others' work. Individuals and organizations (auction houses, museums, investors, etc.) who rely on data expect assurance that they are reliable and trustworthy. Similarly, data producers, such as artists, seek to ensure data integrity for their consumers and themselves, safeguarding against any unauthorized tampering with their data [137]. Registries of ownership and artwork provenance represent cases where the features offered by blockchain technology are highly beneficial. A highly reliable, decentralized database would serve to deter fraudulent activity and support authorities in combating money laundering in the fine art industry. Recording the ownership of artwork would help identify assets involved in illegal activities. Keeping track of artworks'

Key parameters for art insurance		
1	Value	Valuation of the artwork
2	Location	Where the artwork is displayed
3	Type of artwork	Paintings, antiques, et al.
4	Condition	Physical condition, history of damage
5	Storage/Security	Security measures, storage conditions
6	Deductible	To pay before the coverage takes effect

Table 5.1: Key parameters for insurance companies

Most common insurance frauds		
1	Overvaluation fraud	Art value is inflated
2	False claim fraud	False claim for damage or loss
3	Restoration fraud	Damage or quality misrepresentation
4	Identity fraud	False claim of ownership, fake provenance
5	Concealment fraud	Relevant information, damages concealed

Table 5.2: Most common fine art insurance related frauds

valuations and sale prices would be beneficial in detecting illicit gains obtained through price manipulation. Additionally, recording artwork's physical condition, restorations, and damages would help reduce insurance costs by providing valuable insights when considering risks and insurance premiums. The solution can also facilitate research and encourage collaborative efforts and artwork exchanges among institutions, such as museums, by facilitating access to data and sharing information across multiple entities. Through analyzing some of the UK's leading insurance companies for fine art, we derived a list of the critical parameters (Table 5.1) for artworks' insurance. This analysis also helps us to understand the most common insurance frauds, as shown in Table 5.2 ([192, 193, 194, 195]. Analyzing the parameters for insurance and valuation and the most common insurance frauds, it emerges that an immutable and reliable data register would be beneficial as it would prevent data from being altered or omitted to carry out malicious activities.

To enhance due diligence, the proposed solution, specifically conceived for physical artworks, aims to strengthen the reliability of provenance registries. The

network is composed of verified entities, and all information input into the ledger is verified by experts and/or qualified professionals. This helps significantly reduce fraud and forgeries of artworks and increases transparency in the art sector without compromising data privacy and security. Increasing transparency greatly helps prevent money laundering activities, which find in the traditional opacity of the sector a fertile ground. The system promotes cooperation amongst private and public institutions working in the art sector by creating a shared platform with reliable information. It also incentivizes virtuous behaviours, such as entering more information, verifying existing data, and correcting genuine mistakes through a reward mechanism. Finally, it helps reduce artwork insurance costs, benefiting investors and facilitating access to fine art as an investment class.

5.2.1 The network and data input

Artworks are unique items that require a specific and tailored approach. As mentioned at the beginning of this chapter, considering the peculiar characteristics of the fine art sector, we believe that a permissioned private or semi-private blockchain can be a suitable solution. Art owners and sector stakeholders typically demand a significant level of confidentiality concerning their assets and dealings, and permissioned blockchains allow access control to admit participants into the network. They can also rely on an administrator who assigns the roles to the participants in the network [120]. It is important to note that a permissioned private blockchain or a consortium would offer significant benefits, facing less resistance from the art industry actors who might distrust a solution that shares data among unknown entities. Additionally, investors, collectors, and auction houses might welcome a technology which promises to enhance artwork's value by strengthening the trustworthiness of provenance at no compromise to privacy and confidentiality. Another advantage of private blockchains is that there is greater certainty of the rules governing how the blockchain network operates, increasing the participant's confidence in the system. However, a private blockchain offers less security than a public one and, with some effort, data can be altered. The system we design increases robustness by creating a network of trustworthy institutions, such as public organizations, museums,

well-established auction houses and asset managers regarded as trustworthy and/or mandated by law to report any suspicious activity. The consortium blockchain has multiple favorable characteristics. Rather than entrusting most tasks to a single organization, it distributes the same functions to nodes that multiple organizations maintain. To increase transparency and accountability, we make the hypothesis of a semi-private network where one part of the blockchain is private and another is public. The private part of the blockchain is controlled by a select group of individuals or entities, while the public part of the blockchain is accessible to anyone. This hybrid model can be useful in our scenario where the private part of the blockchain remains internal and is shared among known participants. However, the general public can still utilize the public part of the blockchain, with the option of mining to secure the network.

The Consortium, as shown in Fig.5.1 is composed of two levels. Level 1 is private and comprises trusted well-established institutions, such as museums and galleries, universities and auction houses, asset managers, and private banks, while Level 2 is public. A consortium blockchain with private and public levels offers a balance between privacy and transparency. Level 1 restricts access to authorized participants, ensuring confidentiality and enabling efficient, scalable operations while allowing consortium members to enforce rules and governance. Level 2, being public, provides transparency, accessibility, and decentralization. This transparent and immutable layer acts as a tamper-proof ledger to store cryptographic proofs or summaries of private transactions, ensuring their integrity without exposing sensitive details. Level 2 promotes transparency by allowing access to specific data, such as milestones or certifications. This openness builds trust among external stakeholders, including auditors, regulators, and end-users. In addition, the decentralized validation process improves security by removing the dependence on a single entity to protect records. However, we are aware that a dual-level architecture introduces complexities, such as higher development and maintenance requirements and costs. Potential security risks can be seen in the interaction between private

and public levels, which could expose vulnerabilities, such as data leakage or weak cryptographic proofs. The proposed solution can work with either a private network or a more complex architecture composed of two levels. It is not within the scope of this research to go into the technical details of different architectural solutions. We simply note that since the purpose is to increase accountability and transparency, the advantages of a dual-level architecture might be significant. The public level can bridge the private blockchain to other systems, fostering interoperability with external platforms or public blockchains. This feature supports broader collaboration and facilitates data sharing beyond the consortium's private network. The greater transparency can help promote interest towards art and culture, facilitating no-profit initiatives, sponsorships, and donations. Blockchain solutions have already been used successfully [133], demonstrating the potential of a transparent system in the management of public resources.

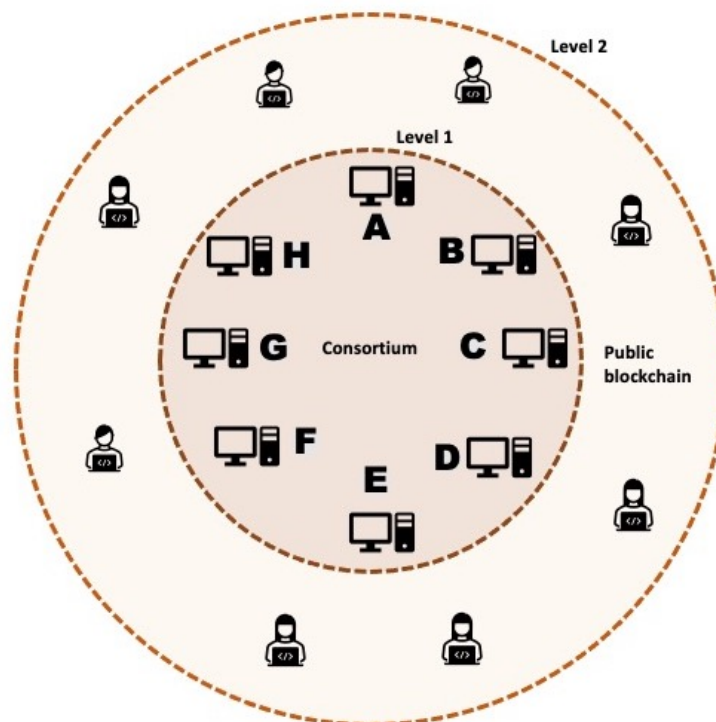


Figure 5.1: Blockchain Consortium. Level 1: Private. Participants can be museums and galleries, universities, main auction houses, asset managers, and private banks. Level 2: Public blockchain.

Before developing the code for the proof of concept, particular attention has been given to understanding what data needs to be registered in the decentralised ledger. From our research (Chapter 2 and 4), it emerges that currently, there isn't a technological solution to ensure that the provenance of the physical artworks is trustworthy and accurate. It is also difficult to unequivocally link the artwork recorded in the ledger to the physical object. In other words, the connection between the digital world of the decentralized ledger and physical work remains vulnerable. For this reason, having as much information as possible is paramount. The more data available regarding a specific artwork, the more difficult it becomes to tamper with the documentation to fake authenticity. As we acknowledged through the literature review, the provenance of artwork is paramount to support combating money laundering in the fine arts sector. By recording ownership, sale prices, interventions for restoration, physical conditions, damages, etc., we can create a complete history of artworks, thus increasing transparency and reducing opportunities for fraudulent activities. Looking at the key parameters for artwork insurance (Table 5.1), we identify the most common types of fraud (Table 5.2). This work is helpful in understanding what data is most commonly forged by malicious actors for their illicit traffic. Collecting this data can also benefit investors, collectors, and institutions such as museums as it can reduce insurance costs. The physical condition of the artwork, storage and transportation conditions, and previous interventions and restorations can be recorded on the ledger, providing valuable insights when considering risks and insurance premiums. In addition to the data above, we select other data sets that can be valuable in identifying artworks unequivocally. Information regarding the artwork's history, the artist's creative process, materials used for restorations and their chemical composition, valuations, and expert reports represents an extremely valuable resource. The possibility of relying on a robust and ample data set significantly reduces the opportunities for forgeries, as it is unlikely that the counterfeit object will match all characteristics and details recorded in the ledger. An example of the data set to be recorded in the ledger is provided in Table 5.3. Because it is crucial to keep track of all events affecting artworks'

history, this results in a significant amount of data that is difficult to store in the decentralised ledger. In the solution proposed, data can be placed on both on-chain and off-chain. By storing sensitive and time-sensitive data in off-chain storage belonging to stakeholders, we offer improved confidentiality and scalability without compromising the immutability features that blockchain technology provides. Such a hybrid design can also overcome scalability issues resulting from full data replication and the limited computational capacity of blockchains. Sensitive information can be hashed, and the obtained hash results are also stored in the ledger. This method can effectively reduce the amount of data in the blockchain network without compromising data-sharing functionalities. The data's hash value can serve as a means of verifying the integrity of the data stored off-chain.

Data	
Generic data	Identifying code, Title, Artist, Date of creation, Short description, Location
Provenance	Artist, Date of creation, Owner*, Previous owners, Exhibition history, Physical condition
Provenance documents	Documentation (list), Documentation (link)*
Restoration	Physical condition (detailed description), Materials, colours et al., Historical significance, Previous restorations, Most recent restoration detailed description (chemicals, techniques, expertise), Conservation key data
Restoration documents	Documentation (list), Documentation (link)*
Valuation	Most recent valuation*, Valuer*, Valuation description*, Previous valuations*
Valuation documents	Documentation (list), Documentation (link)*
Insurance	Insurance company*, Insurance details*
Insurance documents	Documentation (list), Documentation (link)*
Note 1	* - Only available with the owner's permission
Note 2	1 - Only available upon request as per agreement between parties

Table 5.3: Artwork's data to be recorded to ledger

5.2.2 Proof of concept

The proposed solution aims to strengthen confidence in the data recorded in the decentralized ledger. For this reason, we create a trusted environment where data are input by trusted nodes and qualified experts can assess the information, thus significantly increasing reliability. As shown in Fig. 5.2, all parties are subject to approval before being admitted to participate in the ledger. One of the Consortium members, for example, Entity A, uploads data regarding the artwork they want to register in the ledger. A message is automatically sent to the entire network to ensure that all members are aware of the change in the data. If data needs to be verified, a panel of experts is automatically created by random selection from a list of professionals previously approved by the Consortium. To ensure that the assessment is reliable, it is crucial that experts sign their assessment with their digital signature. If none of the panel members accept to validate the data, they are replaced through a new random selection. Validation fees can be agreed on the blockchain and paid offline. At the end of the process, the validated artwork data set is uploaded to the decentralized ledger with the approval of the panel. If the data have not been verified, they are recorded in the blockchain only with the endorsement of the proposer, Entity A in the example of Fig.5.2. Although experts are recommended to verify the data, the lack of this assessment does not prevent the data from being recorded in the ledger. This choice aims to avoid bottlenecks in the system without compromising data quality. The fact that only Consortium members can actively interact with the data in the ledger offers good reassurance about the quality of the input. Additionally, for many artworks, provenance and authenticity have already been evaluated offline and accepted by the scientific and expert community. Mandatory verification will create unnecessary workload and expense. However, expert assessment remains crucial for the future of the system and its long-term success.

The consortium structure can allow members to derive financial benefits from their data. This opportunity is crucial to promoting virtuous behaviour among the

consortium members incentivizing data sharing. Investors, collectors, and other actors operating in the sector need reliable data to make informed decisions. However, collecting and structuring these data might be expensive and time-consuming. If this work is not compensated, it is difficult to imagine that any members would proactively share their data. Due to the trust implied in the Consortium, there is no need for cryptocurrency payments, and transactions can occur via traditional payment gateways. Sending an automated notification when data are uploaded significantly contributes to maintaining awareness of the Consortium members, who are encouraged to check the new inputs. The proposed solution improves the reliability of the decentralized database without compromising privacy. Sensitive data are not shared in the ledger and are stored in the institution's archive to which they belong. Access to these data from other institutions is granted upon request and with the permission of the parties involved. This feature facilitates due diligence processes while preserving confidentiality. Importantly, it also promotes transparency in the fine art sector by providing authorities with trustworthy information regarding provenance, artwork prices, and valuation. If an artwork is suspected of being involved in illicit activities, authorities can be granted access to the system, significantly increasing the speed of the traditionally long and complex investigation processes. Moreover, relying on a systematic and robust database provides unprecedented transparency and audibility.

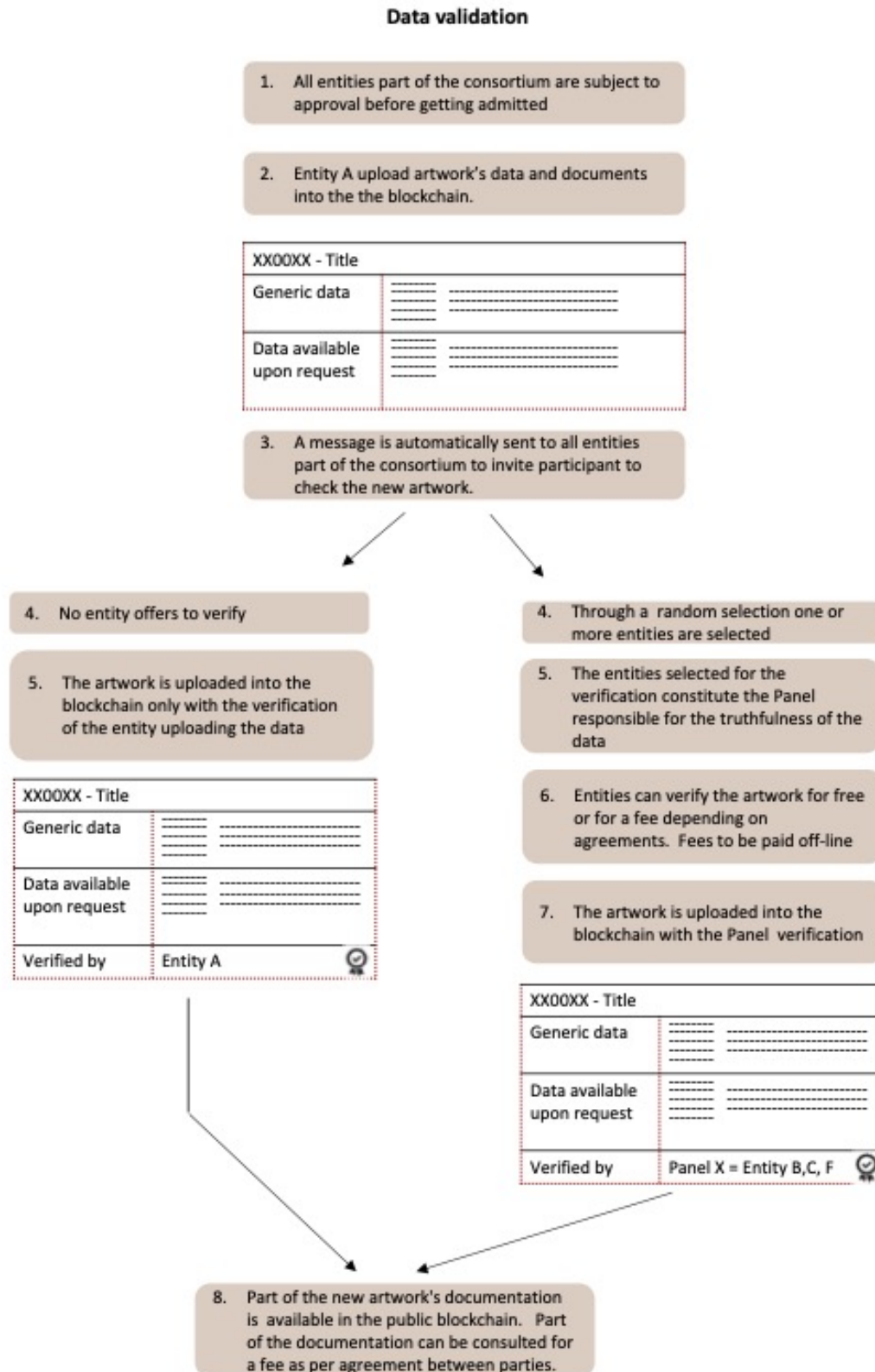


Figure 5.2: Input and validation

Step 1. Create panel

The first step is to create an asset (asset refers to a physical artwork) and input the data. Any entity member of the Consortium, for example, entity **A**, can create a new dataset for an artwork or update existing ones. Identifying the entity that interacts with the ledger is crucial to ensure data reliability. The process of creating and updating assets is similar to the one described in Chapter 6 for real estate transactions (Section 6.2). Therefore, to avoid redundancy, we refer to that section for the details. However, for clarity, a high-level view of the system is provided in Fig. 5.3. Entity **A** inputs information about the artwork. When a new asset is uploaded to the ledger, a message is sent automatically to all other entities (Consortium members). If the Entity uploading the data believes that the documentation needs to be verified, they send a request for assessment. Requesting a verification or endorsement is not mandatory. If the documentation is considered satisfactory, the artwork is uploaded to the ledger with only the endorsement of Entity **A**. When there is a request for evaluation, an invitation to participate in the process is sent to all entities of the Consortium that can accept or reject it. Members who agree to participate in the assessment accept the invitation and propose a qualified expert from a list of professionals. Subsequently, an expert panel with qualified professionals is created by randomly selecting a maximum of five professionals. The number of professionals in the panel is fixed in small numbers to avoid excessive complexity. The proposer entity receives the offer to assess the documentation and can accept or reject it. In case of no answers, they can opt to send another round of invites.

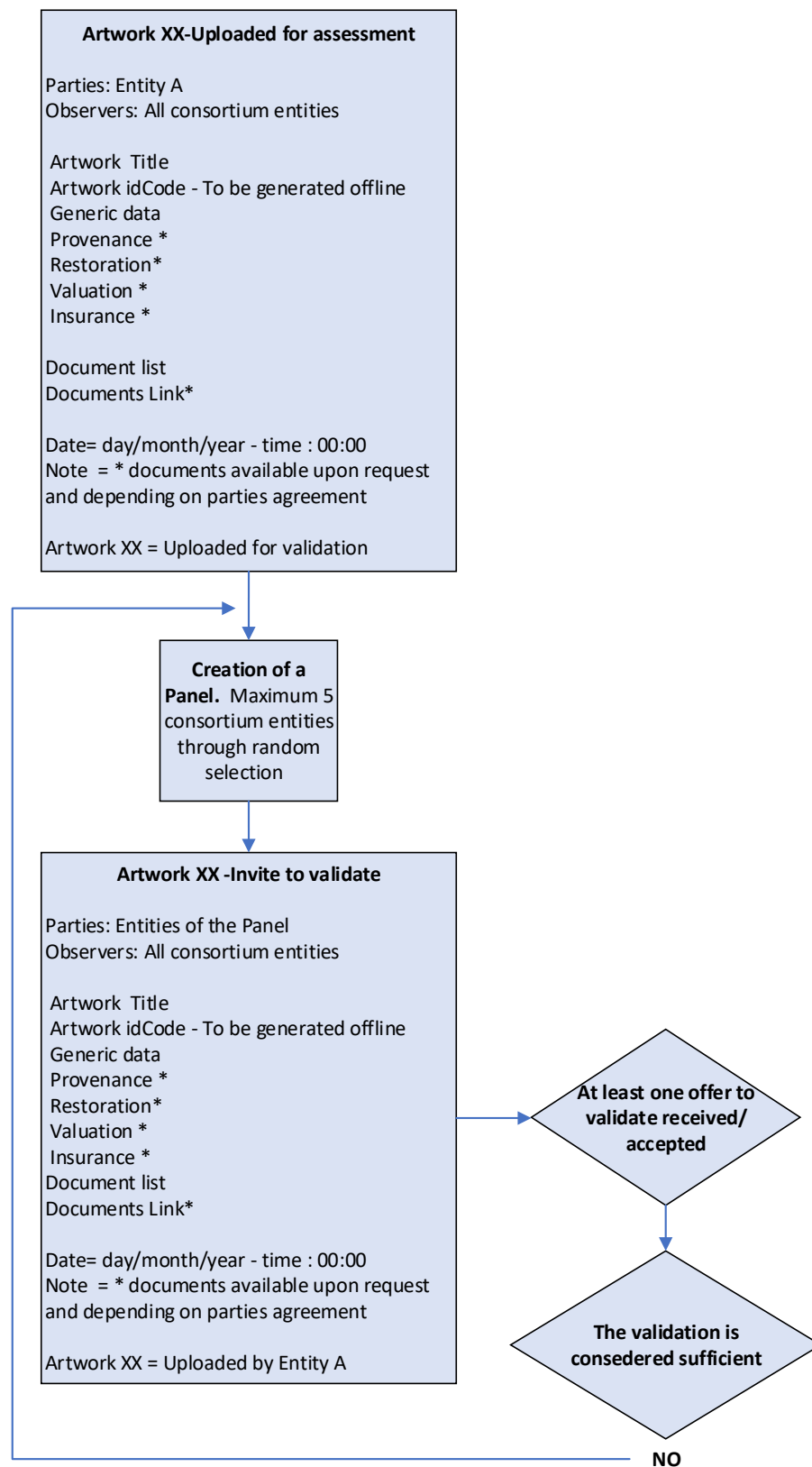


Figure 5.3: Creating asset and expert panel

Step 2. Weighting professionals

Transactions in the fine art sector are not as regulated as in real estate, where the sale/purchase of properties follows predetermined phases and is under the supervision of solicitors mandated by law to act according to the regulations. The sale/purchase of an artwork or a collection does not have to follow a particular structure of steps, and professional qualifications are not so strictly defined as for solicitors. In the fine art world, there is no register of qualified professionals or a professional body for art experts. Nevertheless, experts play a crucial role in art transactions, and choosing the right professional can be challenging. For these reasons, we introduce a mechanism to weigh the endorsement provided by the professional. Based on key criteria such as experience and qualifications, Consortium members assign a score to professionals. This score is then used to weigh all assessments provided by that professional, providing valuable insight regarding the prestige and reliability of the endorsement. For transparency, professional curriculum vitae and qualifications can be consulted in the ledger. As a positive side effect, the weighted score encourages young professionals to enter the fine arts sector. From our research, it emerges that the connection with established players is crucial to penetrating and succeeding in the art sectors. This penalizes young professionals with small or inefficient networks. Depending on the complexity of the task, investors or collectors might opt for a less expensive service, increasing opportunities for young professionals. It is worth noticing that professionals interact with the ledger through the members of the Consortium. This choice aims to provide increased trustworthiness as the expertise of young a professional is endorsed by at least one of the entities. In addition, professionals are always identifiable and sign reports with their digital signature.

The code below creates a smart contract to allow consortium entities to score professionals before adding them to the list of experts. The first step is to identify the parties involved. The entity initiating the process is the `inviter`, while invited entities are the `invitee`. The `inviter` sends an invitation (`Makeinvitation`)

to another consortium member, the `invitee`, to score a professional. It is important to note that to maintain privacy, DAML allows the assignment of different roles to the parties involved, which correspond to different levels of privileges to access data and perform actions. In this case, the `invitee` is an observer, meaning that he/she can witness the process and perform only some predefined actions. The `signatory` controls the process. Once professionals have been added and assigned a score, they can be easily found in the system. The `key` allows to retrieve them, for example, using their score to facilitate the selection of professionals based on their skills and expertise. The `maintainer` is the party responsible for keeping the `(score)`. The function `ensure`, specifies the score boundaries. In this case, it is established that `score >1` and `score <=10`. There is also a possibility for the `inviter` to leave a note to facilitate communication between the parties.

```
template InviteProfessionals
  with
    score : Int
    inviter : Party
    invitee : Party
    notes : Text
    date : Time
  where
    signatory inviter
    observer invitee
    ensure (score >1 && score <=10)
    key (inviter , score) : (Party , Int)
    maintainer key._1
```

The auxiliary template below allows us to retrieve professionals according to their scores. The function `fetchByKey` looks for the score selected in all contracts created with the template `GiveScore`.

```
template AssetHelper
  with
```

```

    caller : Party
where
    signatory caller
    choice GetProfessionalByScore : ( GiveScoreId , GiveScore )
        with
            score : Int
            controller caller
        do
            fetchByKey @GiveScore ( caller , score )

```

After a Consortium member accepts the invitation to score a professional, the score is assigned using the smart contract below. The process is undertaken by one of the members (`mainEntity`) who is identified as a `Signatory`. For transparency, other entities can witness the process and participate as `observer`. The code ensures the score is valid by rejecting negative values (`ensure (score>=0)`).

```

template GiveScore
    with
        mainEntity : Party
        score : Int
        scoreNotes : Text
        entity: Party
        entityIdCode: Text
        date: Time
    where
        signatory mainEntity
        observer entity
        ensure (score >=0)
        key (mainEntity , score) : (Party , Int)
        maintainer key.\_1

```

If professionals gain more experience or new qualifications, their score

can be updated by exercising the same choice used to assign the score (AssignScore).

```
choice AssignScore
  : GiveScoreId
  with
    weightedScore : Int
    scoreComment : Text
    updatedDate : Time
```

Once the scores are received, the `mainEntity` assigns a category to the professional. In the solution proposed, the list of experts is divided into three categories according to their score: junior professionals, experienced professionals, and top professionals. For transparency, there is the possibility to insert a comment on the score and the corresponding category `scoreComment`, and the date when the score is last updated `updatedDate`. Only Consortium entities are allowed to participate in the process. To avoid controversies, professionals are not involved. A professional is assigned to a category using the smart contract below. The multiple-choice (MultiWayIf) assigns a score between 0 and 4 to Junior professionals, 4 and 7 to experienced professionals and greater than 7 to top professionals.

```
if | weightedScore >= 0 && weightedScore <= 4 &&
scoreComment == "Junior professional" ->
  create this with
    score = weightedScore
    scoreNotes = scoreComment
    date = updatedDate

| weightedScore > 4 && weightedScore <= 7 &&
scoreComment == "Experienced professional" ->
  create this with
    score = weightedScore
    scoreNotes = scoreComment
```

```

        date = updatedDate

| weightedScore>7 \&\& weightedScore<=10 \&\&
scoreComment == "Top professional" ->
    create this with
        score = weightedScore
        scoreNotes = scoreComment
        date = updatedDate
| otherwise -> abort "The score must be an integer
between 0 and 10"

```

Step 3. Create an expert panel

Once professionals are assigned a score and added to the system, upon request, the smart contract creates a panel of experts selected from the list. In the example below, we add a professional from the “top professional” category to the panel. Because the subset of the expert panel with top professionals will contain more than one party, the `topPanel` is identified as a collection of parties `Set party`. The smart contract ensures that the professional possesses the right score to be inserted in this category (between 7 and 10 in the example). Finally, the panel of top professionals is updated by inserting the new member (`Set.insert chosenProfessional topPanel`).

```

controller scoreGiver
do
    assertMsg "The score must be an integer between 7
and 10" $ (score>7 && score<=10)
    create this with
        topPanel = Set.insert chosenProfessional
topPanel
        notes = updatedNote

```

Step 4. Testing

After creating the smart contracts, we test the code using hypothetical scenarios. Firstly, we allocate parties using the function (`allocatePartyWithHint`). In the example, the Consortium Entity responsible for the process is an asset manager, while the professionals are identified with numbers from 1 to 5.

```
assetManager <- allocatePartyWithHint "Asset Manager"
  (PartyIdHint "Asset Manager")
professional1 <- allocatePartyWithHint "Professional 1"
  (PartyIdHint "Professional 1")
```

The manager assigns a score to the five professionals. The base case is set to 0, and then we simulate scenarios where the professional's score is 4, 5, or 8, corresponding to three different categories, to verify that the smart contract works correctly and adds the professional to the right category. The entity that assigns the score is always identifiable through the unique `entityIdCode`.

```
startingScore <- submit assetManager do
  createCmd GiveScore with
    mainEntity = assetManager
    score = 0
    scoreNotes = "Base case"
    entity = professional1
    entityIdCode = "XX123YY"
    date = time
```

In the scenario below, a professional with a score equal to 4 is assigned to the junior category.

```
juniorProfessional <- submit assetManager do
  exerciseCmd startingScore AssignScore with
    weightedScore = 4
    scoreComment = "Junior professional"
```

```
updatedAt = time
```

The categories are assigned correctly to the professionals, and now we test the search mechanism to retrieve professionals from the systems based on their scores. The function `queryContractId` allows searching in contracts using the contract `IdCode`. The function `GetProfessionalByScore` search for a professional with a score of 8.

```
Some professional <- queryContractId assetManager
goodProfessional (currentScoreId , currentScore)
<- submit assetManager do
  createAndExerciseCmd (AssetHelper asset manager)
  GetProfessionalByScore with
    score = 8
```

The code below tests the smart contract with the entity “asset manager” that invites the professional with a score of 8 to join the expert panel in the category “top professional.”

```
invite <- submit assetManager do
  createCmd InviteProfessionals
  with
    score =8
    inviter = assetManager
    invitee = professional1
    notes = " Only Top professionals panel"
    date = time
```

Finally, we test whether the expert panel is created correctly. In the test scenario below, the entity Asset Manager wants to add a professional to the panel. The Professional 4 has a score equal to 8, so he/she will be added to the top professional category. This action is performed by exercising the command `createPanel` using the choice `AddProfessional`.

```
addProfessional <- submit assetManager do
```



```
exerciseCmd createPanel AddProfessional
with
  score = 8
  chosenProfessional = professional4
  newDate = time
  updatedNote = "Professional XX added to panel"
```

When another professional needs to be added to the panel, the same process is repeated through `addAnotherProfessional`. In this case, the Asset Manager exercises the command `addProfessional`. The score of the new professional is 9, so he/she gets added to the top professional category.

```
addAnotherProfessional <- submit assetManager do
  exerciseCmd addProfessional AddProfessional
with
  score = 9
  chosenProfessional = professional3
  newDate = time
  updatedNote = "Professional YY added to panel"
```

Scenario testing gives the correct results, which means that the code compiles correctly. DAML provides script results to show what happens behind the scenes. Figures 5.4 and 5.5 present script outputs from the DAML-based implementation of two key smart contracts: `CreatePanel` and `ScoreWeighting`. These figures illustrate how blockchain mechanisms are used to manage contractual logic, participant roles, and the lifecycle of data states within a permissioned ledger. Each row in the figures represents a contract instance, with `signatories` (S) or `observers` (O) denoting the roles of the involved parties. These roles are assigned at the smart contract level and determine which entities are authorised to initiate, validate, or view the contract's evolution. The crossed-out contracts indicate archived states, highlighting blockchain's append-only model, where updates do not overwrite prior data but instead archive the previous contract and generate a new state. This reflects the immutability and traceability inherent in distributed ledger systems. In Fig.5.4,

the creation of a panel involves multiple parties with defined access and validation rights, captured directly in the contract metadata. Fig. 5.5 shows the assignment of score weights to experts, again using signed commands that ensure only authorised validators can submit or update scores. Both figures show the principles of role-based permissions, deterministic execution, and tamper-evident state transitions, demonstrating how blockchain enforces process integrity and auditability in multi-stakeholder workflows.

It should be noted that parties do not obtain any information about contracts in which they are not involved. For example, Professional3 will not have any knowledge of the data contained in the contract of Professional4. This is crucial as it shows how the system allows for transparency without compromising privacy. As per our hypothetical scenario, the entity Asset Manager scores a professional and updates his/her score over time according to his/her new experience and qualifications. The asset manager controls the process, and the professional is only notified of the update. This is clear from the script as the professional is assigned the role of `observer (o)`, while the Asset Manager is the `mainEntity` with `signatories` `priveledges`. (In all script results, the archived contracts are shown crossed).

CreatePanel:Panel

id	status	scoreGiver	topPanel.map
#7:0	archived	'Asset Manager'	GenMap[]
#8:1	archived	'Asset Manager'	GenMap['Professional 4'->{}]
#9:1	active	'Asset Manager'	GenMap['Professional 3'->{}, 'Professional 4'->{}]

date	notes	Asset Manager	Professional 3	Professional 4
1970-01-01T00:00:00Z	"Panel creation"	S	-	-
1970-01-01T00:00:00Z	"Mr Al pacino added to panel"	S	-	O
1970-01-01T00:00:00Z	"Mrs Julia Roberts added to panel"	S	O	O

Figure 5.4: Create Panel and invite professional, scrip results

WeightedScore:GiveScore

id	status	mainEntity	score	scoreNotes
#0:0	archived	'Asset Manager'	0	"Base case"
#1:1	archived	'Asset Manager'	4	"Junior professional"
#2:1	archived	'Asset Manager'	5	"Experienced professional"
#3:1	active	'Asset Manager'	8	"Top professional"

entity	entityIdCode	date	Asset Manager	Professional 1
'Professional 1'	"XX123YY"	1970-01-01T00:00:00Z	S	O
'Professional 1'	"XX123YY"	1970-01-01T00:00:00Z	S	O
'Professional 1'	"XX123YY"	1970-01-01T00:00:00Z	S	O
'Professional 1'	"XX123YY"	1970-01-01T00:00:00Z	S	O

Figure 5.5: Weighted score, scrip results

Chapter 6

Proof of Concept: Real estate

In Chapter 5 Section 5.1, we outlined some foundational considerations for the Proof of Concept regarding the choice of semi-private blockchain and the software language chosen (DAML) that also apply to the real estate Proof of Concept described in this chapter. For this reason, we refer to Chapter 5 for these underpinning analyses.

In regulated markets such as fine art and real estate, where data integrity, auditability, and confidentiality are paramount, decentralised blockchain registries can offer significant advantages over traditional centralised solutions. Modern centralised systems, particularly those deployed by financial institutions, offer robust access control, high availability, and well-audited data management protocols. These systems are typically hosted in secure cloud environments with granular identity management, encryption, and logging mechanisms that support regulatory frameworks such as GDPR and AML directives. However, they retain an inherent reliance on institutional trust and administrative enforcement: the authority maintaining the system governs access, updates, and the audit trail, introducing a single point of control and, potentially, a single point of failure.

Conversely, a decentralised blockchain registry distributes control across multiple permissioned entities, embedding compliance and privacy mechanisms directly into the protocol layer. Decentralisation reduces the reliance on a single institution to maintain trust, which is particularly relevant in cross-jurisdictional con-

texts. For example, in a permissioned blockchain network, institutions such as museums, land registries, and financial intermediaries can co-govern a shared ledger, while maintaining differentiated access to private or institution-specific data. In such systems, data modifications and access rights are governed through deterministic smart contracts, reducing reliance on discretionary administrative processes. Critically, all updates are append-only and cryptographically time-stamped, enhancing auditability and evidentiary robustness. In scenarios where multiple institutions must cooperate, such as provenance certification across museums or title validation across borders, decentralised registries can reduce duplication, minimise reconciliation delays, and provide shared visibility without requiring full data disclosure. Privacy is preserved through selective disclosure mechanisms (e.g. role-based access, data partitioning, and cryptographic proofs), ensuring that sensitive data remains confidential while still verifiable.

6.1 Foundational elements of the Proof of Concept

The analysis undertaken in Chapter 2 highlights that the real estate sector is particularly vulnerable to money laundering. From our research, it also emerges that the lack of transparency in the transaction process can cause significant delays and transaction failures, negatively impacting market liquidity. In the UK, in 2017, the Government acknowledged that “the current home buying and selling process in England is not fit for purpose. It is stressful, time-consuming and costly for buyers and sellers alike – with over a quarter of house sales falling through each year” [64]. The vulnerability of the real estate sector to money laundering and the characteristics of the property transaction process make the UK context particularly interesting for a blockchain-based solution. Thanks to this technology, transactions can be stored in transparent shared databases, protected from deletion, tampering, and revision. Ownership, prices, asset valuations, and other crucial information can be stored securely in the decentralized ledger, facilitating the identification of assets involved in illicit activities. A blockchain system is also attractive for real estate because it could reduce the total transaction time to complete a sale [66] by automating

multiple steps of the transaction process. The combination of blockchain technology and smart contracts can potentially reduce the need for multiple intermediaries that, in the current process, increase transaction costs [67].

In this section, we propose a blockchain-based solution for the UK context to help improve the real estate transaction process. In the UK, solicitors are key actors. The buyer and seller do not interact directly, but through their solicitors, who are legally responsible for following the procedure of the transaction process. The UK Law Society clearly identifies and defines every step. Before the sale/purchase is concluded, all relevant documents of the property must be collected and become part of the contract. These property searches take time and are generally repeated before a sale, even if the property was recently transacted. As shown in the analysis in Chapter 2 and Chapter 4 Section 4.2.1, causes of delay are often connected with search inefficiency. Moreover, to reduce the possibility of transaction failure, professional bodies suggest signing a legal agreement at an early stage of the process to secure the sale. However, buyers are reluctant to commit before receiving the complete documentation of the property, since the agreement requires a deposit. The proposed solution aims to create a trusted environment where properties' documentation is stored safely and securely, allowing parties to easily consult data, thus significantly increasing transparency and reducing transaction time. Providing information upfront accelerates the transaction process and may contribute to enhancing the property's value. A property that is easy to transact is a more liquid asset and may be more appealing to investors as it reduces risks due to fluctuation of the price and the overall uncertainty of the transaction process.

The code presented in this chapter reflects the implementation of smart contract logic using DAML, a domain-specific language designed for modelling financial workflows with deterministic execution and granular role control. The structure of the code follows key blockchain smart contract principles: contractual terms are codified as logic-bound templates; data is immutable once committed; and updates follow a lifecycle governed by signed transaction flows. In particular, the design pattern aligns with DeFi-inspired mechanisms such as escrow functionality, where

assets (e.g., ownership titles, authentication tokens) are conditionally held until pre-defined conditions are met. Within the DAML environment, this is operationalised through contract states and choice bindings, whereby certain parties (e.g., buyers, sellers, certifiers) are authorised to exercise contractual "choices" (e.g., release, cancel, endorse) only when the conditions encoded in the contract logic are satisfied. This mirrors the function of on-chain escrow contracts in public DeFi systems, but within a permissioned and auditable ledger context suited for regulated markets.

For example the *AssetProposal* contract acts as the initial escrow container, binding together the asset, the intended recipient, and the compliance conditions to be satisfied (e.g., identity verification or documentation checks). The contract is not executable by either party independently, following the custodial neutrality of a DeFi escrow, and must first receive explicit approval via the *AcceptAssetProposal* choice. The choice can be exercised by an authorised signatory (e.g., an institution or validator), triggering the creation of a new ownership state and archiving the previous contract. This reflects deterministic state progression, a defining property of blockchain smart contracts. Throughout, DAML enforces role-specific permissions, ensuring that only designated parties (as defined in the contract metadata) can view or interact with a given contract. This structure replaces traditional intermediaries with code-based conditionality and role-enforced execution, aligning with blockchain's broader objective of automating trust while preserving institutional oversight. Thus, the implemented code not only supports the functional requirements of regulated asset exchange, but also embeds the operational logic of DeFi escrow contracts within a permissioned, auditable framework.

6.2 Key features for a real estate decentralized registry

The proposed solution aims to create a property passport or data log that could be traded along with the title of a property. It is also worth noting that it fits into the UK's current regulatory frame because it reproduces the transaction process in the digital world as it happens in the physical world. This aspect is significant because it could facilitate the adoption of the proposed solution in the sector. The system dramatically improves transparency and efficiency. In addition, it could help governments and authorities in combating money laundering by helping to identify assets suspected of being involved in illicit activities. If necessary, authorities and regulators can have access to the decentralized property database, significantly reducing the investigation time and facilitating the sharing of information between institutions. Finally, the solution benefits society by improving the real estate transaction process, as required by the UK Government's Call for Action [64].

This proof of concept is conceived to be deployed on a private blockchain or a consortium where all parties are identified and approved before being admitted. Trusted nodes can be solicitors, public institutions such as the His Majesty Land Registry (HMLR) and professional bodies such as the Royal Institute of Charter Surveyors (RICS). Because blockchain does not have the ability to assess whether entered data are right or wrong, the quality of input data determines the quality of output data (garbage in, garbage out). Therefore, ensuring that the data stored in the ledger are correct becomes paramount. To achieve maximum reliability, firstly, we ensure the correctness of the input data. In the UK, solicitors are legally mandated to be truthful and legally responsible for misconduct. For this reason, they are the only parties allowed to upload data to the ledger. Replicating the real-life process ensures that the data stored in the digital ledger have the same level of trustworthiness as in the physical world. Secondly, we maintain trust over time. Although buyers, sellers, and other parties, such as estate agents, can be involved as witnesses, lawyers are the only parties allowed to update and modify the data. To

further enhance data reliability, we propose a scoring system in which solicitors are invited to assess the accuracy and completeness of documentation. This assessment is valuable because it allows for an accurate estimate of the time and costs of the transaction, helping people and investors make informed decisions. For example, let us make the case that a buyer or investor has time constraints to buy a property or evaluate the opportunity to invest in certain assets. The time taken by the due diligence process is a crucial factor in determining which property(s) is more suitable. In addition, documents can be easily retrieved whenever needed, making due diligence significantly more efficient.

6.2.1 Network and input data

The structure of the network participating in the decentralized ledger can be similar (with different institutions and actors involved) to the one proposed for fine art (section 5.2.1). For this reason, to avoid repetition, we will briefly describe the network and focus on other aspects of the proposed solution. The system is conceived to be deployed on a private blockchain or a consortium. Even though solicitor firms can benefit from creating a private blockchain to store their clients' property data and documentation, it is worth highlighting that a private blockchain has lower security compared to a public blockchain. Additionally, if only one organization stores and maintains data, manipulation might be possible. However, we note that this is unlikely to happen. Solicitors are regulated professionals mandated by law to follow ethical and professional standards and face severe sanctions for misconduct. The system replicates in the digital world the real-life process, making solicitors responsible for ensuring the truthfulness of data. Therefore, even with a private blockchain, the probability of tampering with the data is not higher than in the physical world. However, to improve security, we propose creating a Consortium of trusted nodes. Professional bodies such as RICS, solicitors' firms, institutional bodies such as HMLR, and others can be part of the consortium to increase the ledger security, making malicious alteration of the data very unlikely. To enhance privacy, if required, the Consortium can establish separate channels to allow confi-

dential communications between members. In real estate transactions, parties need to exchange sensitive data that cannot be publicly available in the ledger.

Transactions produce a significant number of documents in the form of reports, surveys, pictures, etc., which increase over time. Storing these data in the blockchain would significantly raise costs and negatively affect the scalability due to data replication and the limited computational capacity of blockchains. For these reasons, we propose to store the data outside the ledger, making them available upon request and only with the permission of the parties involved. Some core information can be stored in the blockchain, while a large amount of information can be stored in a central database outside the blockchain. Data stored off-chain are hashed, and the obtained hash results are stored in the blockchain. The data's hash value also allows to verify the integrity of the data stored off-chain. Because different data cannot have the same hash value, a disparity between the two hashes indicates that the data have undergone modification after their inclusion on the blockchain. Figure 6.1 provides a high-level description of the system. Upon request, parties can retrieve documents from the ledger through a Remote Process Call (RPC). RPC is a communication protocol that facilitates the invocation of a procedure or subroutine located on a remote system over a network. This allows a program to execute a service provided by another program, even when they are geographically distributed and operate on different networks. In this protocol, the caller is not required to have any knowledge of the underlying network details or physical location of the callee. RPC enables transparent communication between distributed programs, which can work together as if running on the same system. Through the common user interface, solicitors, estate agents, buyers, and sellers can interact with the system. Solicitors have full access privileges, which allow them not only to consult the ledger but also to upload and modify documents. Buyers, sellers, estate agents and other users have restricted access, and they can consult only the transactions where they are involved and the documents for which they have permission.

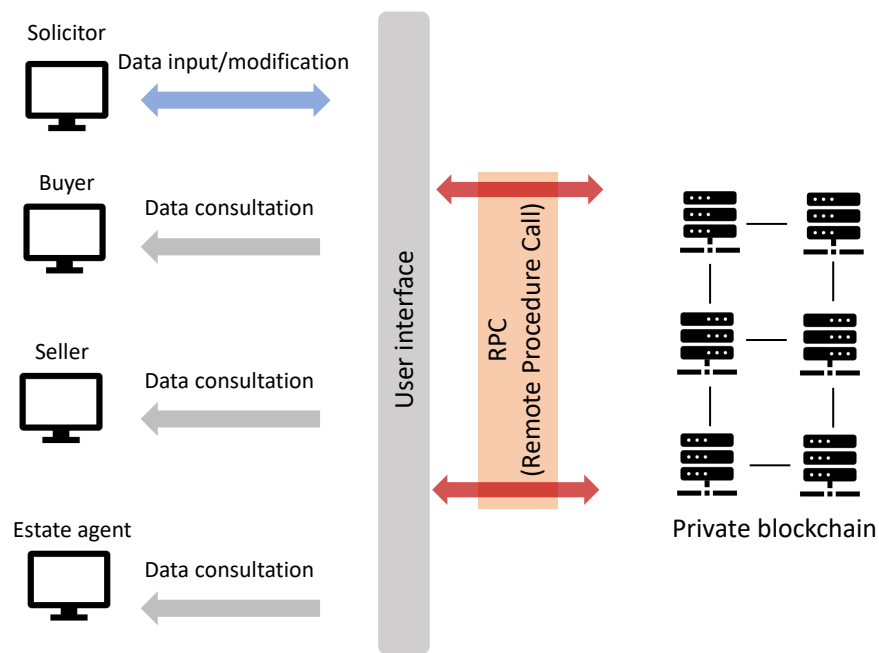


Figure 6.1: High-level description of the system. The figure shows how users have different access privileges. Through the user interface, users can retrieve documents from the ledger through a Remote Process Call (RPC)

6.2.2 Proof of concept

To develop the proof of concept, we chose DAML as a software language because it is open-source and has the appropriate characteristics to develop legal smart contracts. The language makes it easier to implement complex workflows and agreements directly into smart contracts, which can then be deployed on a private blockchain such as Hyperledger Fabric or distributed ledgers like Corda. DAML language is influenced by Haskell, a functional programming language known for its expressiveness and suitability for formal reasoning. Functional programming encourages the use of descriptive function names, which can make code more readable and self-documenting. The use of higher-order functions allows for the creation of abstractions that can describe *what is being done* rather than *how it is done*. This can lead to code that reads like a series of operations or transformations applied to the data, similar to a sentence describing a process in English. This type of code allows for a high-level understanding of the actions undertaken through smart contracts, fostering an interdisciplinary approach to problem-solving by facilitating the

dialogue between technologists and other areas of expertise.

Real estate transactions in the UK are heavily regulated with respect to privacy and confidentiality. To enhance privacy, DAML allows the creation of three pre-defined types of parties with different privileges: (I) signatory, (II) controller, or (III) observer parties. A signatory can take action and sign and submit contracts to the ledger. The controller is the counterparty who can perform specific actions (such as accepting or rejecting an offer) made available for him/her. The observer is a witness with no controlling abilities, possessing only visibility and access to transactions and data. DAML has a built-in feature for testing the functionalities of prototypes by creating scenarios that simulate real-world business cases. The platform maintains a full record of the transaction history. Once a contract is updated, the previous version is archived, but remains in the ledger, providing a track of any change.

Step 1. Create and update assets

The first step is to register an asset in the blockchain (`create an asset`), as shown in Fig.6.2. An asset refers to any real estate property. With the asset owner's permission, qualified solicitors collect the documents and upload the hash of the corresponding package into the ledger while the hashed documents are stored in an off-chain archive. The property is registered with all relevant information, such as the address, a short description, the list of documents available, etc. For certain types of real estate assets (such as luxury properties), the registry can include a list of valuables associated with the property, such as paintings or any valuable item. The form also specifies all parties involved (solicitors, auction houses or estate agents, buyer and seller) and the time when the asset is created.

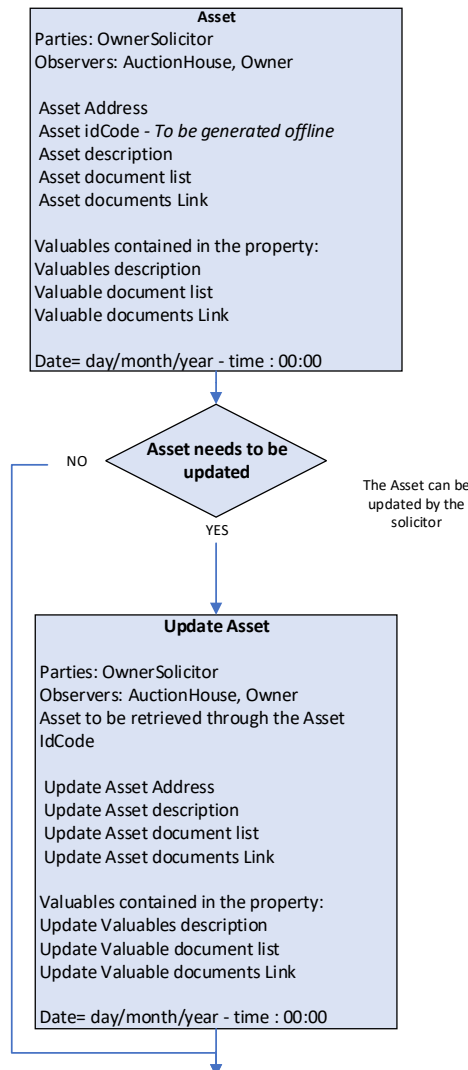


Figure 6.2: The figure illustrates Step1, create and update an asset.

The actions shown in Fig. 6.2 are executed using the following code. In DAML, *templates* define the structure and behaviour of smart contracts, while *choices* specify the operations that can be executed on contracts instantiated from a template. Choices are a powerful feature, as they determine how contracts can evolve over time by specifying possible operations like creating new contracts, modifying existing ones, or archiving contracts. The template *Asset* defines the behaviour of the smart contract to create assets. To ensure transparency and privacy, parties are identified and their role is specified. The asset's owner solicitor is a *signatory*, meaning that he/she has the authority to take actions, such as creating the asset and uploading documents. The asset owner and other third par-

ties, such as an auction house or a real estate agency, can be involved in the process as `observers`, which means that they can witness the process but cannot take action. The fact that solicitors in the UK are mandated by law to be truthful is important because it ensures that the data entered in the ledger are correct from the first step. Each asset is identified by a unique `IdCode` generated offline, which allows for retrieval of the asset. There could be other ways to retrieve an asset, for example, through the number of the contract. However, this option is not viable because the same asset can undergo several updates and/or resales. Because these actions are implemented through smart contracts, the same asset is likely to have multiple contract numbers, making the search impractical.

```

module Asset where
type AssetId = ContractId Asset
template Asset
  with
    ownerSolicitor : Party
    owner : Party
    auctionHouse : Party
    address : Text
    idCode: Text To be generated offline
    a_description : Text
    a_documents : [Text]
    a_docLink : Text
    v_description : Text
    v_documents : [Text]
    v_docLink : Text
    date: Time
  where
    signatory ownerSolicitor
    observer owner, auctionHouse
    key (ownerSolicitor, idCode) : (Party, Text)

```

```
maintainer key._1
```

The asset is identified through the `IdCode`, and the function `FetchByKey` ensures that it can be retrieved from the ledger even when new transactions occur. It is worth noting that the section `key` in the above code clarifies not only the key parameter univocally associated with the asset (`IdCode`) but also the party responsible for maintaining this key. The solicitor is held responsible for the task because of his/her legal role.

```
choice GetAssetByIdCode : (AssetId , Asset)
  with
    idCode : Text
  controller caller
  do
    fetchByKey @Asset (caller , idCode)
```

The code below shows how solicitors can update, consult, and download documentation. It is often beneficial for the asset owner to give estate agents and potential buyers permission to view and download documentation. However, to ensure the integrity of the data, these parties are not allowed to interact with the ledger actively. This condition is expressed by adding these new parties as `observers`, who can only be witnesses, while the owner's solicitor, the `signatory`, can upload and modify documents in the ledger. The operation of updating an asset is performed through the choice `UpdateAsset`, where the `signatory` (the solicitor) can make changes to the required fields.

```
choice UpdateAsset
  : ContractId Asset
  with
    updated_address : Text
    updated_a_description : Text
    updated_a_documents : [Text]
```



```
updated_a_docLink : Text
updated_v_description : Text
updated_v_documents : [Text]
updated_v_docLink : Text
updated_date : Time

controller ownerSolicitor
do
  create this with
    address = updated_address
    a_description = updated_a_description
    date = updated_date
```

Step 2. Sell assets

When the asset's owner decides to sell the asset, his/her solicitor sends the documentation to the potential buyer's solicitor for review. The smart contract described in this section allows the current owner's solicitor to invite additional parties, such as the potential buyer and his/her solicitor, his/her auction house, or estate agent, to view and download the documents. The smart contract also allows one to insert notes to improve communication between parties. The potential buyer has the option, through his/her solicitor, to review the proposal, as shown in Fig.6.3.

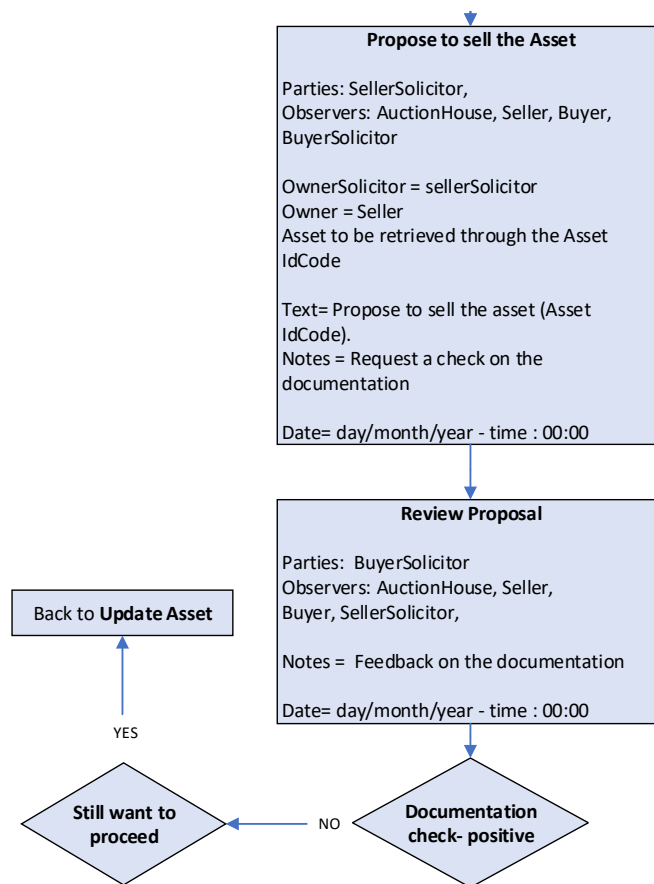


Figure 6.3: The figure illustrates the key steps to propose to sell the asset. Propose to sell and review the proposal.

The code below shows how the actions described in Fig. 6.3 are translated into smart contracts. In the template `AssetProposal`, the `proposerOwner` (potential buyer), and `proposerOwnerSolicitor` (potential buyers' solicitor) are added as parties as observer. It is worth noticing that the `ownerSolitor`

is still the `signatory`. This is because, until the sale happens, the control is still in the owner's hands, who exercises this power through his/her solicitor.

```
template AssetProposal
  with
    idCode : Text
    proposerOwnerSolicitor : Party
    proposerOwner : Party
    notes : Text
    date : Time
    ownerSolicitor : Party
    owner : Party
    auctionHouse : Party
  where
    signatory ownerSolicitor
    observer owner , proposerOwner , auctionHouse ,
    proposerOwnerSolicitor
    key (ownerSolicitor , idCode) : (Party , Text)
    maintainer key._1
```

The choice `MakeAssetContractOffer`, exercised on the template `Asset`, allows the owner's solicitor to make the offer to sell the asset to the potential buyer.

```
choice MakeAssetContractOffer
  : AssetProposalId
  with
    assetproposal : Text
    controller ownerSolicitor
  do create this
```

Fig. 6.4 shows the process of reviewing, accepting, or rejecting a proposal. Once the proposal to sell the asset has been created, the potential buyer, through his/her solicitor, has some choices. If the documentation is incomplete or not con-

sidered satisfactory, he/she can ask for the proposal to be reviewed. In this case, the seller's solicitor can update the asset documentation and provide the clarification required through the smart contract. Other choices are to reject or accept the proposal. If the proposal is accepted, a smart contract to sell assets is created.

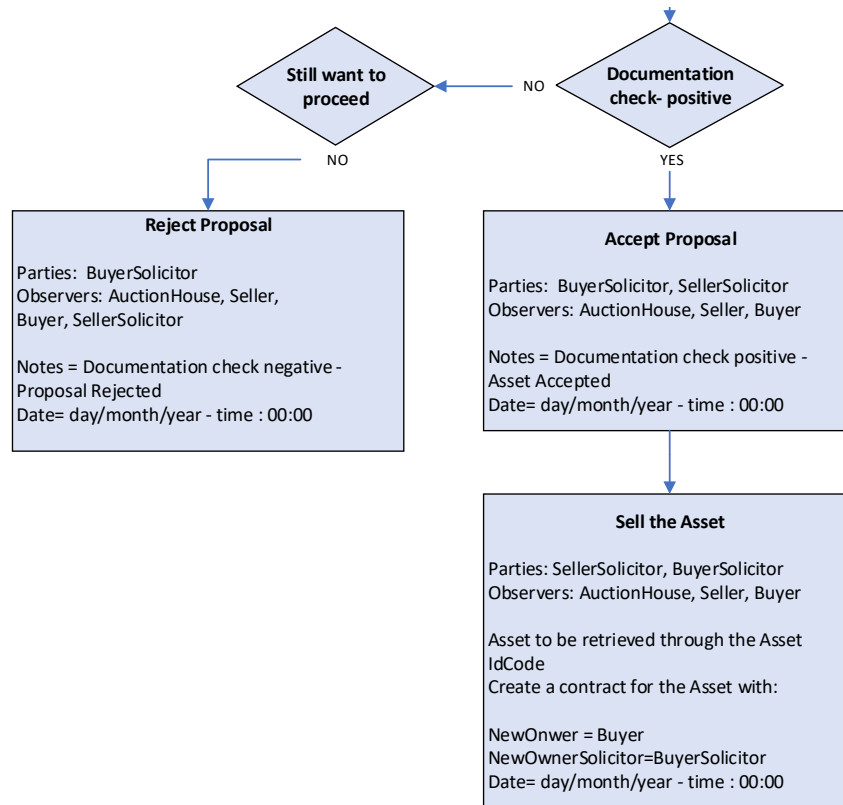


Figure 6.4: The figure illustrates the key steps to propose to sell the asset. Accepting/rejecting an offer.

The code below creates the smart contracts to review and reject the offer. These options are expressed through `ReviseAssetContractOffer` and `RejectAssetContractOffer`, which create smart contracts corresponding to the different choices from the template `AssetProposal`. The option of accepting or rejecting an offer is exercised by the `proposerOwnerSolicito`, who is identified as the `controller`. He/she can also add some notes for clarity, for example, adding details regarding what documents need to be updated or what information is missing.

`choice ReviseAssetContractOffer`

```

      : AssetProposalId
    with
      offerRevision : Text
    controller proposerOwnerSolicitor
    do create this with
      notes = offerRevision
choice RejectAssetContractOffer
  : AssetProposalId
  with
    feedback : Text
  controller proposerOwnerSolicitor
  do create this with
    notes = feedback

```

The option to accept the offer is exercised through `AcceptAssetProposal`. Interestingly, the conciseness of the DAML language allows us to shorten the code by omitting the choice `AcceptAssetContractOffer`. This choice is redundant because accepting the offer can be actioned by directly originating a new contract where the sale is finalised.

```

choice AcceptAssetProposal
  : AssetContractId
  controller proposerOwnerSolicitor
  do
    create AssetContract with
      idCodeAsset = idCode
      buyer = proposerOwner
      seller = owner
      buyerSolicitor = proposerOwnerSolicitor
      sellerSolicitor = ownerSolicitor
      contractNotes = notes
      contractDate = date

```

```
auctionHouseInContract = auctionHouse
```

The sale is finalized through the template `AssetContract` and by exercising the choice `AcceptAssetProposal` on this template. In the new contract, the `proposerOwner` is now identified as the `buyer`, and the `proposerOwnerSolicitor` is now `buyerSolicitor`. Because the sale must be signed by both parties (buyer and seller), the buyer's solicitor must be added as signatory. All other parties remain observers. It is important to note that the asset has been sold, and now the `sellerSolicitor` becomes responsible for maintaining the unique code which identifies the asset. However, the `idCode` has not changed, allowing the asset to be retrieved through multiple smart contracts.

```
template AssetContract
  with
    idCodeAsset : Text
    buyer : Party
    seller : Party
    buyerSolicitor : Party
    sellerSolicitor : Party
    contractNotes : Text
    contractDate : Time
    auctionHouseInContract : Party

  where
    signatory buyerSolicitor , sellerSolicitor
    observer buyer , seller , auctionHouseInContract
    key (buyerSolicitor , idCodeAsset) : (Party , Text)
    maintainer key._1
```

In this proof of concept, we only deal with aspects related to the due diligence and property documents. The actual sale of real estate assets is outside the scope of this project. In the solution proposed, because of the trusted relationship between

parties, the money exchange can happen offline (as per the usual procedures currently in place). This option facilitates the adoption in the industry, as it does not involve the use of cryptocurrencies. Buying and selling real estate assets involves significant sums of money, and investors, buyers, and sellers are likely to distrust new payment methods supported by a technology that is still *mysterious* to the general public. Additionally, the solution designed does not require any change in the current regulatory framework to be implemented or any behavioural changes from the actors in the real estate industry.

Step 3. Scoring system

We create a scoring system to enhance the reliability of the information stored in the decentralized ledger. Fig. 6.5 shows the key steps of this tool. Upon the request of the asset's owner, solicitors are invited to assess the asset's documentation. The score concerns the accuracy and completeness of the documentation, and it provides potential buyers with a very clear idea of how long due diligence might take on the asset. The score is between 0 and 5, with 0 being the lowest. There is also the possibility for the solicitor to give more details about the score assigned, further increasing transparency. Solicitors' fees for assessment are settled offline. Because the solution is deployed on a private blockchain or a consortium, the nodes trust each other, allowing traditional offline payments without the use of cryptocurrencies.

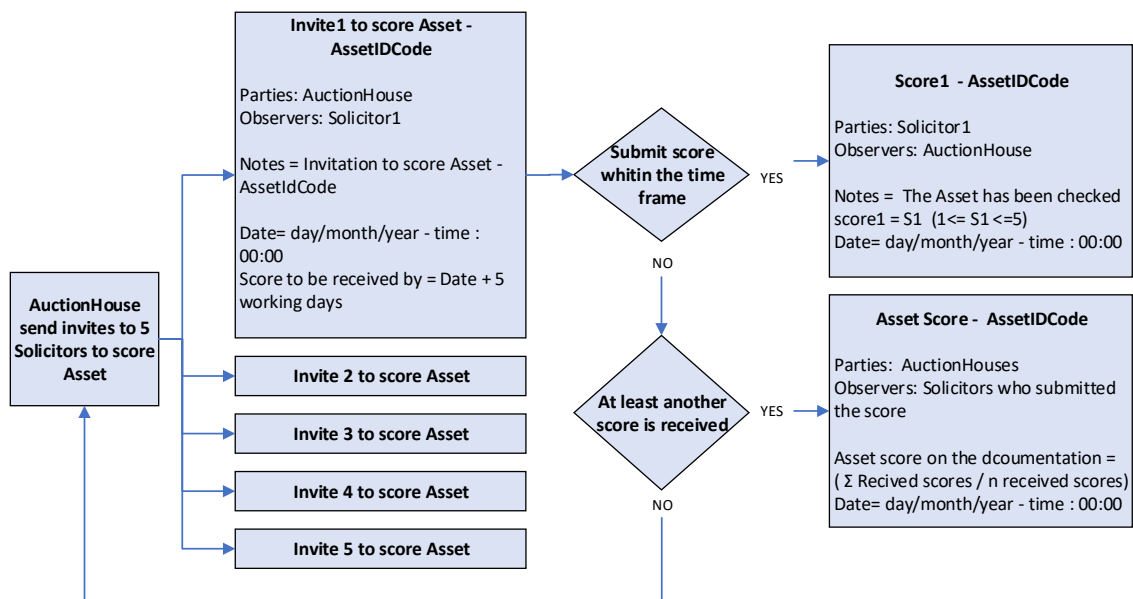


Figure 6.5: The figure illustrates the scoring system

The code below creates the smart contract to score the asset. The asset is univocally identified through the `assetidCode`, the parties are the `scoreCalculator`, the `scoreVoters` (the group of solicitors who have been selected to provide the score) and the `alreadyVoted` (the group of solicitors who have already given their score). To express that these groups are constituted by more than one party, they are identified as a set (`Set Party`). In this design, the score

calculator party can access the Score contract at any time. If `calculatedScore` is zero, no votes have been submitted. If it is more than zero, then at least one voter submitted their individual score. To further enhance transparency and reliability, it was considered to create a panel of experts through a random selection of lawyers. However, this is challenging, as DAML does not provide a random number generator. The reason is that computations must be deterministic and always produce the same result given the same input values. Consequently, the only way to create the group of professionals selected randomly is to determine the composition of these groups off-ledger. This task would entail creating a ledger client application, where it is possible to use a random number generator and compose groups through a random selection of members of the network. Subsequently, these groups can be stored on the ledger by creating contracts with the groups of pre-determined members. However, this additional feature is beyond the scope of this proof-of-concept.

`template Score`

`with`

```
assetidCode: Text
scoreCalculator: Party
calculatedScore: Decimal
scoreVoters: Set Party
alreadyVoted: Set Party
```

`where`

```
signatory scoreCalculator
observer scoreVoters
```

The `scoreCalculator` initially sets the `calculatedScore` to zero (`calculatedScore == 0.0`) and the group of parties who have already voted to empty (`alreadyVoted /= Set.empty`).

```
ensure (intersection scoreVoters alreadyVoted
== Set.empty) && (alreadyVoted /= Set.empty
|| calculatedScore == 0.0)
```

Voters can submit their individual scores by exercising the choice `Score-Vote` on the contract `Score`. Every time the choice is exercised, the `calculatedScore` is updated with the average value of all individual scores submitted thus far.

```
choice Score_Vote: ContractId Score
with
  scoreVoter: Party
  score: Int
```

To prevent voters from voting more than once, the choice also removes the voting party from the set of allowed voters and adds it to the set of parties that already voted. This action is implemented through the functions `assertMsg`, which also verifies that the score follows the required criteria `assertMsg score>=1 && score<=5`.

```
controller scoreVoter
do
  assertMsg "The score must be an integer between 1&5" $
    (score >=1 && score <=5)
  assertMsg "The voter is not on the list of allowed
    voters" $ (Set.member scoreVoter scoreVoters)
  create this with
    calculatedScore = (intToDecimal score + calculatedScore
      * intToDecimal (size alreadyVoted))/ (intToDecimal
      (size alreadyVoted) + 1.0)
    scoreVoters = Set.delete scoreVoter scoreVoters
    alreadyVoted = Set.insert scoreVoter alreadyVoted
```

Step 4. Testing, script results

To test the code, we create a hypothetical scenario where the owner of a villa is a client of an auction house and wants to sell the property with some valuable paintings. The first step is to assign a name to the parties created in the smart contracts. This action is performed through the function `allocatePartyWithHint`. The code below allocates the parties where (I) the asset owner's solicitor is `Solicitor 1`, the asset owner is `Mrs Owner`, the auction house is `Auction House`, the potential buyer's solicitor is `Solicitor 2` and the potential buyer is `Mr Buyer`.

```
s1 <- allocatePartyWithHint "Solicitor 1"
(PartyIdHint "Solicitor 1")
mrsOwner <- allocatePartyWithHint "Mrs Owner"
(PartyIdHint "Mrs Owner")
time <- getTime
```

The code below tests the template `Asset`. The property is identified through the `uniqueIdCode XX23225XXX`. Documents are listed, hashed and stored off-chain. The hash value is added to the smart contract to allow parties to retrieve the documentation. The destruction of documents also protects them from tampering, ensuring the correspondence between the data stored off-chain and the hash stored in the chain.

```
assetId <- submit s1 do
  createCmd Asset with
    ownerSolicitor = s1
    owner = mrsOwner
    auctionHouse = ah
    address = "Mulholland Drive"
    idCode = "XX2325XXX"
    a_description = "Villa by the sea"
    a_documents = ["VillaDoc1", "VillaDoc2", "VillaDoc3"]
    a_docLink = "Hash_RE_Documents"
    v_description = "Portrait of Adele"
```

```

Bloch-Bauer , Klimt"
v_documents = ["KlimtDoc1", "KlimtDoc2",
"KlimtDoc3"]
v_docLink = "Hash_FA_Documents"
date = time

```

Then we proceed to test the smart contract `UpdateAsset`. The action `updateAsset` is exercised by the owner solicitor `s1` on the action `assetId`. The code below tests how the fields that require changes are updated and the new smart contract is created with the updated asset.

```

updateAsset <- submit s1 do
  exerciseCmd assetId UpdateAsset with
    updated_address = "Mulholland Drive 135"
    updated_a_description = "Villa by the sea with a
wonderful view"
    updated_a_documents = ["VillaDoc4", "VillaDoc5",
"Villa6" ]
    updated_a_docLink = "Hash_RE_Documents_Updated_1"
    updated_v_description = "Klimt Portrait of Adele
Bloch-Bauer and Le Moulin de la Galette-Renoir"
    updated_v_documents = ["Renoir1", "Renoir2",
"Renoir3"]
    updated_v_docLink = "Hash_FA_Documents_Updated_1"
    updated_date = time

```

The code below tests the functionality to retrieve the asset. Through the auxiliary template `AssetHelper`, the owner's solicitor `s1` uses the function `GetAssetByIdCode` specifying the `idCode`.

```

(currentAssetId , currentAsset) <- submit s1 do
  createAndExerciseCmd (AssetHelper s1)
    GetAssetByIdCode with idCode = "XX2325XXX"

```

In this hypothetical scenario, the potential buyer's solicitor *s2* asks to review the proposal with the motivation that the documentation is incomplete. After the asset owner's solicitor updates the documentation, the offer is accepted. Solicitor *s1* creates the proposal on the template `AssetProposal` and creates the action `makeoffer` where the command `createproposal` is exercised on the template `MakeAssetContractOffer`. Similarly, the code is tested for reviewing and rejecting the offer where the buyer's solicitor *s2* calls the action `reviseoffer` and `rejectprop`. The test for reviewing the documentation upon the buyer's solicitor's request and accepting the offer are omitted as they follow processes already explained above. In the code below, we verify the functioning of the scoring system. The scenario is created with 5 voters and the case of the score list being 1, 2, 3, 4, 5. The calculated score is the score average.

```
pSC <- allocateParty "Score Calculator"
p1 <- allocateParty "Party1"
p2 <- allocateParty "Party2"
p3 <- allocateParty "Party3"
p4 <- allocateParty "Party4"
p5 <- allocateParty "Party5"
s <- submit pSC do
  createCmd Score with
    assetidCode = "XXX"
    scoreCalculator = pSC
    calculatedScore = 0.0
    scoreVoters = Set.fromList [p1,p2,p3,p4,p5]
    alreadyVoted = Set.empty

let counterList = [0..4]
let scoresList = [1,2,3,4,5]
let partiesList = [p1,p2,p3,p4,p5]
foldlA (\s x -> submit (partiesList !! x) do
```

```

exerciseCmd s Score_Vote with
    scoreVoter = partiesList !! x
    score = scoresList !! x)
s counterList

```

The code compiles correctly, and the script results are shown in Fig.6.6, 6.7, 6.8 and 6.9. The script results show details of what is happening behind the scenes. Once a contract is executed, it is archived. However, for transparency, it is always possible to see the previous contracts and keep track of all changes. Traceability is important to prevent money laundering activities. Keeping a record of sale prices will reduce the risk of price manipulation for money laundering activities, while the history of transactions supported by reliable documentation can facilitate the identification of assets involved in suspicious activities. Interestingly, the increased transparency does not compromise privacy. The possibility of assigning different rights and roles to parties allows different privileges to consult/modify data. The script results show all parties involved in a particular contract and who is allowed to view and/or take action. Parties not involved in a specific smart contract will have no knowledge of the data.

The script results in Fig. 6.6 show results from the smart contracts created with the template `Asset`. The first smart contract (0:0) is the creation of the asset. The contract shows the data uploaded, the asset `IdCode`, data and time. The last part of the script results shows the parties involved in the contract and their roles. The contract behaves as expected. The solicitor is the `signatory (s)` while the auction house and the asset owner are `observer (o)`. Because the `Solicitor 1` updated the field `A-description`, the original contract (0:0) is archived, and a new contract (1:1) is created. This second contract is archived because the `Solicitor 2` asked for a review of the proposal 6.7 as some documents were missing (“The plan of the first floor is missing. Please update the documentation”). Therefore, the active contract is the third one (7:1), created after the last update.

Asset:Asset

id	status	ownerSolicitor	owner	auctionHouse	address	idCode	a_description	a_documents
#0:0	archived	'Solicitor 1'	'Mrs Owner'	'Auction House'	'Mulholland Drive'	'XX2325XXX'	'Villa by the sea'	["VillaDoc1", "VillaDoc2", "VillaDoc3"]
#1:1	archived	'Solicitor 1'	'Mrs Owner'	'Auction House'	'Mulholland Drive 135'	'XX2325XXX'	'Villa by the sea with a wonderful view'	["VillaDoc1", "VillaDoc2", "VillaDoc3", "VillaDoc4", "VillaDoc5", "Villa6"]
#7:1	active	'Solicitor 1'	'Mrs Owner'	'Auction House'	'Mulholland Drive 135'	'XX2325XXX'	'Villa by the sea with a wonderful view'	["VillaDoc1", "VillaDoc2", "VillaDoc3", "VillaDoc4", "VillaDoc5", "Villa6", "VillaDoc4", "VillaDoc5", "Villa6", "Plan 1st Floor"]

a_docLink	v_description	v_documents	v_docLink	date	Auction House	Mrs Owner	Solicitor 1
"Hash_RE_Documents"	"Portrait of Adele Bloch-Bauer - Klimt"	["KlimtDoc1", "KlimtDoc2", "KlimtDoc3"]	"Hash_FA_Documents"	1970-01-01T00:00:00Z	O	O	S
"Hash_RE_Documents_Updated_1"	"Klimt Portrait of Adele Bloch-Bauer and Le Moulin de la Galette - Renoir"	["KlimtDoc1", "KlimtDoc2", "KlimtDoc3", "Renoir1", "Renoir2", "Renoir3"]	"Hash_FA_Documents_Updated_1"	1970-01-01T00:00:00Z	O	O	S
"Hash_RE_Documents_Updated_2"	"Klimt Portrait of Adele Bloch-Bauer and Le Moulin de la Galette - Renoir"	["KlimtDoc1", "KlimtDoc2", "KlimtDoc3", "Renoir1", "Renoir2", "Renoir3", "Renoir1", "Renoir2", "Renoir3"]	"Hash_FA_Documents_Updated_2"	1970-01-01T00:00:00Z	O	O	S

Figure 6.6: Scrip results for smart contracts Asset

The script results in Fig.6.7 show the test for the smart contract Asset Proposal. Solicitor 2 asks for multiple updates, which leads to the smart contracts being archived. As expected, there is no active contract for the asset proposal as the smart contract to accept the offer is redundant. This is because, once the last review is completed, the sale is undertaken directly through the smart contract Sell Asset (Fig. 6.8). The proposal to sell involves other parties, which are listed in the script results. All new stakeholders, such as the potential buyer and his/her solicitor, have been added as observer.

SellAsset:AssetProposal

id	status	idCode	proposerOwnerSolicitor	proposerOwner	notes
#3:0	archived	"XX2325XXX"	'Solicitor 2'	'Mr Buyer'	"Offer for Mulholland Drive 135"
#4:1	archived	"XX2325XXX"	'Solicitor 2'	'Mr Buyer'	"Offer for Mulholland Drive 135"
#5:1	archived	"XX2325XXX"	'Solicitor 2'	'Mr Buyer'	"The documentation is incomplete."
#6:1	archived	"XX2325XXX"	'Solicitor 2'	'Mr Buyer'	"The plan of the first floor is missing. Please update the documentation"
#8:1	archived	"XX2325XXX"	'Solicitor 2'	'Mr Buyer'	"The plan of the first floor is missing. Please update the documentation"

date	ownerSolicitor	owner	auctionHouse	Auction House	Mr Buyer	Mrs Owner	Solicitor 1	Solicitor 2
1970-01-01T00:00:00Z	'Solicitor 1'	'Mrs Owner'	'Auction House'	O	O	O	S	O
1970-01-01T00:00:00Z	'Solicitor 1'	'Mrs Owner'	'Auction House'	O	O	O	S	O
1970-01-01T00:00:00Z	'Solicitor 1'	'Mrs Owner'	'Auction House'	O	O	O	S	O
1970-01-01T00:00:00Z	'Solicitor 1'	'Mrs Owner'	'Auction House'	O	O	O	S	O
1970-01-01T00:00:00Z	'Solicitor 1'	'Mrs Owner'	'Auction House'	O	O	O	S	O

Figure 6.7: Scrip results for smart contract Asset Proposal

When the proposal to sell is accepted, the code creates the smart contract `SellAsset`. The scrip results in Fig. 6.8 show that the contract `SellAsset` (9:1) is active and states the parties involved `Soliciotr 1`, `Soliciotr 2`, `MrBuyer`, `Mrs Owner` and the `Auction House`. Because both parties (the buyer and the seller) must be involved in the contract, both solicitors are now signatories.

SellAsset:AssetContract

id	status	idCodeAsset	buyer	seller	buyerSolicitor	sellerSolicitor	contractNotes
#9:1	active	"XX2325XXX"	'Mr Buyer'	'Mrs Owner'	'Solicitor 2'	'Solicitor 1'	"The plan of the first floor is missing. Please update the documenta"

contractDate	auctionHouseInContract	Auction House	Mr Buyer	Mrs Owner	Solicitor 1	Solicitor 2
1970-01-01T00:00:00Z	'Auction House'	O	O	O	S	S

Figure 6.8: Scrip results for the smart contracts Sell Asset

The script results in Fig.6.9 show the smart contracts created to score the asset. As in any contract, `IdCode` identifies the asset. The voters enter their score, the

previous contract is archived, and the calculated score is updated. It should be noted that voters are identified as `observers`, but the party that submits the score is a `witenss`. The difference is that observers are entitled to observe a transaction or a contract but may not necessarily have the authority to act upon the contracts involved. Witnesses are parties who need to authorize an action, such as creating a contract or exercising a choice. These are the parties whose consent is necessary for the transaction to be valid. The authorization of the solicitor who submits the score is necessary to proceed; therefore, he/she is identified as `witenss(w)`. After all parties have submitted their score, the calculated score is updated and a new contract (15: 1) is created, which is the only active contract. (In all script results, the archived contracts are shown crossed).

Scoring:Score

id	status	assetidCode	scoreCalculator	calculatedScore	scoreVoters.map
#10:0	archived	"XX2325XXX"	'Score Calculator'	0.0000000000	GenMap['Party1'->(), 'Party2'->(), 'Party3'->(), 'Party4'->(), 'Party5'->()]
#11:1	archived	"XX2325XXX"	'Score Calculator'	1.0000000000	GenMap['Party2'->(), 'Party3'->(), 'Party4'->(), 'Party5'->()]
#12:1	archived	"XX2325XXX"	'Score Calculator'	1.5000000000	GenMap['Party3'->(), 'Party4'->(), 'Party5'->()]
#13:1	archived	"XX2325XXX"	'Score Calculator'	2.0000000000	GenMap['Party4'->(), 'Party5'->()]
#14:1	archived	"XX2325XXX"	'Score Calculator'	2.5000000000	GenMap['Party5'->()]
#15:1	active	"XX2325XXX"	'Score Calculator'	3.0000000000	GenMap[]

	Party1	Party2	Party3	Party4	Party5	Score Calculator
alreadyVoted.map						
GenMap[]	O	O	O	O	O	S
GenMap['Party1'->()]	W	O	O	O	O	S
GenMap['Party1'->(), 'Party2'->()]	-	W	O	O	O	S
GenMap['Party1'->(), 'Party2'->(), 'Party3'->()]	-	-	W	O	O	S
GenMap['Party1'->(), 'Party2'->(), 'Party3'->(), 'Party4'->()]	-	-	-	W	O	S
GenMap['Party1'->(), 'Party2'->(), 'Party3'->(), 'Party4'->(), 'Party5'->()]	-	-	-	-	W	S

Figure 6.9: Scrip results for the smart contracts Scoring

Step 4. Testing, implementation of the simple ledger

The simple ledger implementation (Sandbox) enables rapid application prototyping by simulating a DAML Ledger. The Sandbox is a lightweight, in-memory ledger where developers can deploy and interact with DAML contracts without setting up a full ledger or blockchain infrastructure. It offers a safe and isolated environment for the test and provides a close approximation of how contracts and transactions would behave on an actual ledger. The Sandbox includes support for testing privacy and authorization features of DAML contracts, allowing the simulation of different parties with different rights. Because the implementation of the simple ledger for the fine art proof of concept is very similar to one for the real estate, to avoid redundancies, we chose to show only the one on real estate.

The scenario created in the real estate proof of concept is now used to simulate the execution of transactions on the ledger, which helps to comprehensively test the logic of smart contracts. The ledger implementation correctly shows all parties involved in the transaction as set up in the DAML code Fig.6.10.

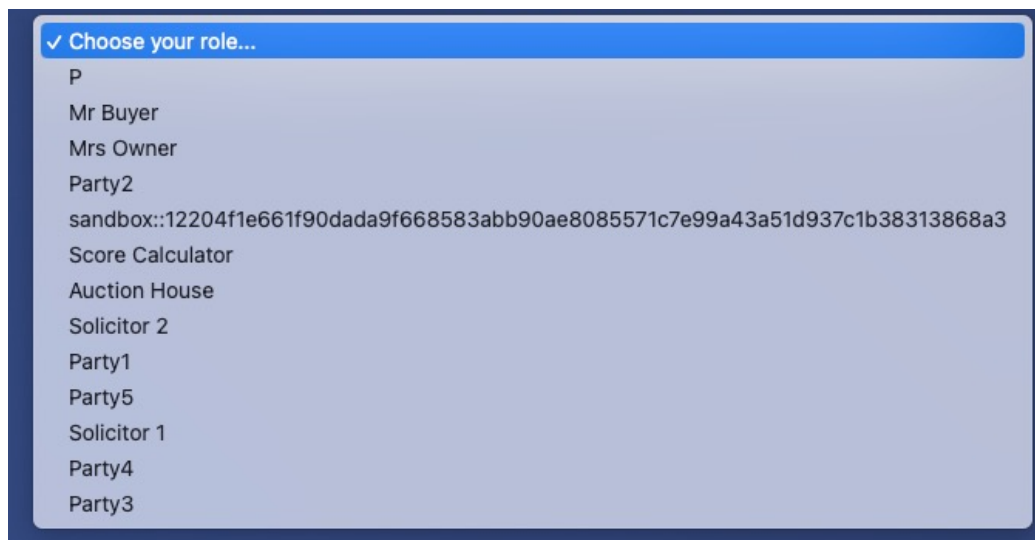
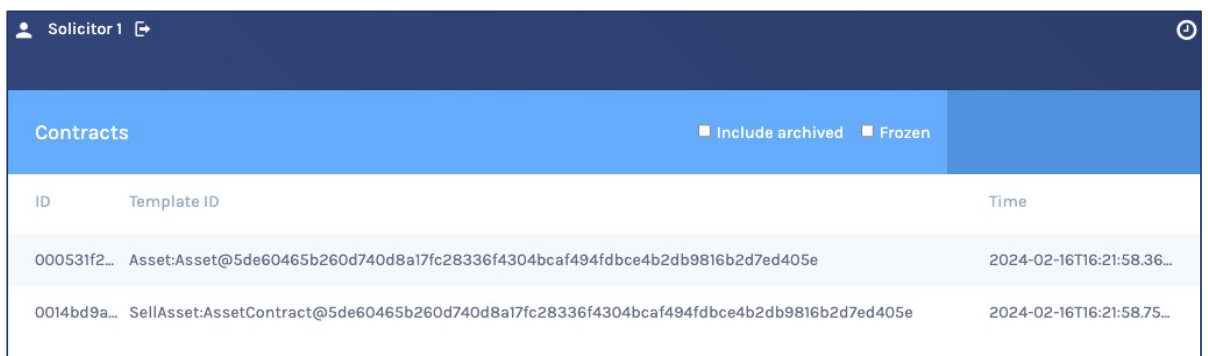


Figure 6.10: Parties set up in the DAML Sandbox

The Sandbox allows playing different roles to test the functioning of the system from the different perspectives of the parties involved. If we choose to act as `Solicitor 1`, (Fig.6.11), as expected, we will see two active contracts,

one `Asset` corresponding to the last update of the asset and the second one `SellAsset` corresponding to the sale. Archived contracts are available on request. Fig. 6.12 shows the data in the contract `Asset`. As per the code developed, the observers are the `Auction House` and `Mrs Owner`, while `Solicitor 1` is the signatory. The `Contract Key` correctly states the `IdCode` and that the maintainer is `Solicitor 1`. By opening the contract details, we can see all documents uploaded for the property, the corresponding hashes and the date/time.



Contracts		
ID	Template ID	Time
000531f2...	Asset:Asset@5de60465b260d740d8a17fc28336f4304bc494fdbce4b2db9816b2d7ed405e	2024-02-16T16:21:58.36...
0014bd9a...	SellAsset:AssetContract@5de60465b260d740d8a17fc28336f4304bc494fdbce4b2db9816b2d7ed405e	2024-02-16T16:21:58.75...

Figure 6.11: Smart contracts active in the Sandbox for Solicitor 1

Solicitor 1

Contract 000531f22409...

UpdateAsset

Archive

Template > Asset:Asset@5de60465b260d740d8a17fc28336f4304bc4f494fdbce4b2db9816b2d7ed405e

Signatories

Solicitor 1::12204fle661f...

Observers

Auction House::12204fle661f...

Mrs Owner::12204fle661f...

Contract key

_1

Solicitor 1::12204fle661f...

_2

XX2325XXX

Contract details

ownerSolicitor

Solicitor 1::12204fle661f...

owner

Mrs Owner::12204fle661f...

auctionHouse

Auction House::12204fle661f...

address

Mulholland Drive 135

[9]

Plan 1st Floor

idCode

XX2325XXX

a_docLink

Hash_RE_Documents_Updated_2

v_description

Klimt Portrait of Adele Bloch-Bauer and Le Moulin de la Galette -Renoir

v_documents

[0]

KlimtDoc1

a_documents

[0]

VillaDoc1

v_docLink

Hash_FA_Documents_Updated_2

date

2024-02-16 16:21

Figure 6.12: Details of the smart contract Asset

Chapter 7

A proposal for a fine art and real estate blockchain registry

In Chapter 5 and 6, we provide the proof of concept for crucial features to enhance due diligence in fine art and real estate, thus significantly increasing transparency. In this chapter, based on this proof of concept, we design a solution for the first blockchain registry for fine art and real estate. From our research, it emerges that the real estate and fine art sectors share some crucial characteristics that suggest the possibility of building a solution suitable for real estate assets and physical artworks. Both industries deal with valuable physical assets; due diligence can be quite complex and require the involvement of professionals to verify and endorse data. These industries are particularly vulnerable to money laundering and need increased transparency to prevent criminal activities. They also require a high level of privacy and confidentiality.

This chapter consolidates the design outputs developed in Chapter 5 and 6 by embedding them within a systematic structure informed by the design thinking methodology and supported by both primary and secondary data sources. The primary data, semi-structured interviews with industry professionals across the fine art, legal and technology sectors (Table 1.2), served a central role in the Empathize and Define stages of the design thinking framework. These interviews provided qualitative insights into user pain points, compliance challenges, and technologi-

cal barriers, particularly around provenance, KYC (Know Your Customer) procedures, and transaction integrity. Their feedback directly informed the functional requirements and architecture of the MVP described in Section 7.1 and visualised in Figures from 7.1 to 7.13. The secondary data, such as technical documentation, the detailed case studies presented in Chapter 4, and relevant legal and regulatory reports, played a crucial role in supporting the Ideate and Prototype phases of the design thinking process. These sources provided industry benchmarks, identified limitations of existing solutions, and offered regulatory context. This information helped shape the solution proposed and validate the feasibility and compliance of the blockchain architecture.

The solution for a public blockchain architecture (Section 7.2) also reflects this iterative, human-centred process: for example, Figures 7.14 and 7.15 translate artwork, client and transaction verification requirements derived from expert interviews into automated workflows. Additionally, Figures 7.16 to 7.20 illustrate how zero-knowledge proof (ZKP)-based architectures were used to address user concerns about privacy and regulatory compliance, themes that were consistently raised by legal and technology stakeholders. Furthermore, the due diligence matrix in Tables from 7.3 to 7.5 and the red flag taxonomy in Tables 7.6 to 7.8 are direct outcomes of synthesising interview content and existing AML guidance into usable, auditable frameworks for smart contract deployment. These structured outputs, summarised in fig. 7.14 and 7.15 are cleanly mapped to the test phase, where experts' insights were embedded into the solution design to increase its robustness and real-world applicability. All steps of the solution design are interlinked using the design thinking methodology, not just as a framing device but as a systematic analytical pathway. This approach ensured that the resulting blockchain registry solutions are not only technically feasible but also aligned with the practical, institutional, and legal realities of the fine art and real estate sectors.

In summary, the development of the blockchain prototype was guided by a structured application of the design thinking methodology. During the Empathize phase, qualitative insights were gathered through stakeholder and expert interviews,

involving professionals at professional bodies, auction houses, a national museum registrar, solicitors, and asset managers. These interactions uncovered critical operational bottlenecks, such as fragmented provenance validation, inconsistent KYC documentation, lack of interoperable audit trails, and duplicated due diligence processes, which directly informed the system's architecture. The design of smart contract templates, user roles (signatory vs observer), and validation checkpoints was structured to respond to these domain-specific frictions. In the Test phase, the prototype was evaluated through code-level simulation and walkthrough testing using realistic transaction scenarios that reflected the challenges articulated during the Empathize stage. This included simulations of provenance endorsement, conditional transfer using escrow logic, and weighted scoring across multiple validators. The focus was on validating the internal logic of the smart contracts, assessing role-based permissions, and ensuring alignment between intended institutional behaviours and contract outcomes. However, a full second round of interviews or structured user feedback on the final prototype was considered out of scope for this research. The primary objective of the Test stage was to confirm that the implemented contract logic was capable of executing the workflows defined in earlier stages, in line with regulatory expectations and domain constraints.

Design Thinking Stage	Primary Data (Semi-Structured Interviews)	Secondary Data (Case Studies, Technical and Legal Sources)	Outputs and Implementation (Chapters 5 to 7)
Empathize	Insights from experts across fine art, legal, and tech sectors (Table 1.2). Identified pain points in KYC, provenance, and due diligence.	—	Functional needs defined for compliance workflows. Influenced MVP architecture (Figures 7.1–7.13) and risk flag taxonomy.
Define	Stakeholder-driven articulation of workflow frictions and system goals. E.g., fragmented provenance, poor audit trails.	—	Requirements consolidated into feature sets (e.g., smart contract roles, user permissions). Mapped to Tables 7.3–7.5.
Ideate	—	Analysis of existing technical documents, regulatory frameworks, and Chapter 4 case studies.	Benchmarked current systems, identified gaps, and proposed design innovations (e.g., escrow, endorsement logic).
Prototype	Feedback from experts helped simulate role-based interactions and scoring logic.	Architecture structured using insights from legal and technical constraints.	Developed smart contracts in DAML for fine art and real estate (PoC1 and PoC2). Visualised in Figures 7.14, 7.15.
Test	Scenario testing based on user input (provenance endorsement, ZKP-based scoring). Interviews informed logic (new feedback round out of scope).	—	Internal validation of contract logic. Figures 7.16–7.20 demonstrate regulatory alignment and ZKP-based privacy mechanisms.

Table 7.1: Integration of Primary and Secondary Data Across the Design Thinking Framework

In order to advance the contribution of our findings and offer structured insights to both researchers and practitioners working in other regulated sectors, we examined the interview data related to risk evaluation in depth. This analysis led to the formulation of three key design principles aimed at supporting the develop-

ment of compliance risk scoring systems that are suitable for algorithmic expression. As a result, these systems can be aligned with automation objectives and support the application of secure computation techniques, including zero-knowledge proofs (ZKPs). The abstraction level of these principles allows the artefact to be positioned for broader academic discussion and facilitates its adaptation in domains where risk-based compliance frameworks are essential [30, 31]. Furthermore, these principles offer applicability beyond the original domain and can be extended to areas like private equity and venture capital. While initially derived in the context of blockchain technologies and the anticipated use of ZKPs, specifically with components such as digitally signed provenance trails and identity attestations managed through digital wallets, they also have relevance for traditional environments that rely on rule-based automation. This is especially pertinent given the increasing integration of compliance procedures with AI and machine learning models, which continue to raise concerns about transparency, reliability, and explainability.

Design Principle 1: Feedback loops of developing algorithmic compliance checks. Many operational contexts, including the fine art sector, are characterised by limited transparency and a lack of formal structure. This contributes not only to increased complexity and cost in conducting compliance verifications but also to inconsistencies across institutions, professionals, and jurisdictions. Such variability can undermine the broader acceptance of risk assessments, whether across individuals, organisations, or regulatory regions, and introduces potential investor exposure and reduced market competitiveness due to inefficiencies. Several interviewees recognised the value of automating compliance procedures as a means to systematically capture existing due diligence practices, organise data inputs, and enhance procedural transparency through the adoption of a structured, threshold-based model. As ExpertB noted, the absence of recognised credentials for art professionals and the lack of a centralised registry of expertise mean that actors can claim specialist knowledge without oversight. Artworks may be transferred privately, with no public record of the transaction or official change of ownership, as sales are not required to pass through public notaries or registries. This regulatory

vacuum creates vulnerabilities in the sector, particularly regarding forgery and misrepresentation. In line with this, ExpertC emphasised the absence of a formalised due diligence process in the art industry. Against this backdrop, the framework we propose introduces the first consolidated set of verifiable requirements that could support the creation of a standardised approach for assessing anti-money laundering risk, offering the potential for machine-verifiable adoption in practice.

Design Principle 2: Risk assessments are not one-dimensional. Effective compliance risk evaluation typically relies on a wide array of inputs sourced from diverse registries and institutional actors. This multi-dimensionality makes confidentiality a critical requirement, necessitating the integration of advanced privacy-preserving technologies such as zero-knowledge proofs (ZKPs). Expert O raised specific concerns regarding the handling of sensitive data, noting that a public blockchain solution would only be viable if strong technical safeguards are in place to ensure that privacy is not compromised. However, applying threshold-based scoring models in combination with secure computation frameworks introduces further complexity, particularly in scenarios requiring ex-post auditability, which may involve third parties who act as custodians of confidential records. This observation reflects a broader regulatory tension: the need to promote transparency and accountability while simultaneously protecting individual privacy. Similar challenges have been highlighted in other areas, such as the regulatory discourse on gatekeeper data-sharing obligations under the Digital Markets Act [196].

Design Principle 3: Facilitate spot checks. Rule-based compliance models are typically optimised for the most frequent transaction types and risk scenarios. As a result, they often fail to detect edge cases or recognise patterns of illicit behaviour that only become apparent after the fact. This limitation underscores the importance of designing systems that anticipate the need to revise and update risk scores dynamically, especially when implemented within static environments such as blockchain-based smart contracts. Furthermore, technologies like zero-knowledge proofs (ZKPs), while preserving confidentiality, inherently restrict the ability of auditors to retrieve contextual data unless the relevant parties, such as ex-

perts or financial institutions, are actively involved. To address this, systems should include mechanisms that allow for controlled stakeholder engagement during investigations or audits. Such capabilities would support accountability by enabling the reconstruction of decision-making processes and the verification of stakeholder actions against publicly anchored cryptographic records. In this context, features like multi-signature workflows and encrypted escrow schemes can be instrumental in securely managing sensitive data, ensuring it remains inaccessible except under lawful and procedurally authorised conditions.

Design Principle 4: Handling the incompleteness of digital records. Given that digitisation in the fine art sector often occurs retrospectively, and risk evaluation criteria are subject to ongoing refinement, it is essential to design systems capable of accommodating new parameters as they emerge. As Expert B points out, no single data element can definitively establish provenance; instead, it is the aggregation of diverse and independent data points that increases confidence in an artwork's authenticity. As they put it, "all data in fine art can be manipulated," whether it relates to valuations, ownership history, or material characteristics. Therefore, the more comprehensive the dataset, the closer one can get to an informed, trustworthy assessment. In light of this, risk scoring models must remain adaptable, enabling future expansion while maintaining cryptographic linkage to the original transaction. Even in cases where data is not initially disclosed or used in the risk calculation, anchoring it securely within the system supports later verification and audit. For smaller actors entering the market, adopting a practice of capturing and anchoring as much relevant information as possible early on can significantly enhance the credibility and robustness of future compliance checks.

Design Principle 5: Supporting adoption through institutional alignment and incentives. The successful deployment of compliance technologies, particularly in sectors like fine art that have historically been resistant to digital transformation, depends not only on technical robustness but also on the degree to which the solution integrates with existing practices and offers tangible benefits to its users. As Expert G notes, many galleries and clients remain sceptical of new systems and

prefer conventional methods due to concerns about trust, usability, and perceived complexity. Therefore, adoption must be supported through clear alignment with familiar procedures and value propositions that reflect institutional priorities. Positive feedback from Experts H and I, gathered during the demonstration of the prototype, suggests that transparency-enhancing features are viewed favourably when they are shown not to compromise privacy or disrupt core workflows. In addition, Expert N points out that while larger, well-established institutions often already adhere to best practices, small and medium-sized market actors operate with fewer formal controls, highlighting the importance of a flexible architecture that can scale across different organisational contexts. To address these dynamics, the proposed system is designed to mirror key elements of current workflows, such as certification, provenance logging, and approval chains, while offering additional automation, traceability, and optional monetisation of high-quality records. This approach lowers the barrier to entry, builds on institutional logic already in use, and helps generate buy-in from stakeholders with varying degrees of digital maturity.

Table 7.2: Mapping of Expert Insights to Design Principles

Design Principle	Relevant Expert(s)	Explanation / Link
1. Feedback loops for developing algorithmic compliance checks	A, B, C, D, F	Expert A suggests that blockchain can support emerging artists in managing and structuring their work. Expert B notes the absence of professional accreditation and structured practices. Expert C discusses the lack of formal due diligence procedures. Expert D describes informal, trust-based systems in small galleries. Expert F points to museum protocols as references for standardisation. These insights underscore the need for repeatable, evolving compliance mechanisms grounded in real-world practice.
2. Risk assessments are not one-dimensional	C, E, O, P	Expert C and O raise privacy concerns related to public blockchain visibility. Expert E notes that decentralised systems may lack a clearly accountable human authority. Expert P highlights the emerging relevance of ESG and its intersection with AML, reinforcing the need to combine multiple sources and criteria in compliance risk modelling.
3. Facilitate spot checks	C, D, F, L, M	Expert C observes that art transactions may proceed despite suspicion. Expert D discusses informal verification norms. Expert F emphasises auditability requirements. Experts L and M highlight GDPR considerations and the need for lawful mechanisms to review decisions retrospectively. These opinions support the inclusion of flexible, auditable pathways in rule-based frameworks.
4. Handling the incompleteness of digital records	B, C, Q	Expert B states that all data in the fine art world is prone to manipulation, requiring accumulation of partial data points. Expert C notes the lag in information availability. Expert Q highlights the expense and complexity of verifying artworks, underscoring the need to accommodate evolving and incomplete provenance documentation.
5. Supporting adoption through institutional alignment and incentives	G, H, I, N	Expert G identifies resistance to technological change in the sector, especially among more traditional clients. Experts H and I respond positively to the prototype and note its potential for improving transparency. Expert N states that established actors already follow strict processes, but smaller galleries often do not. These views point to the importance of aligning technical solutions with institutional workflows and building adoption incentives through familiarity and perceived utility.

7.1 HP1. Solution to be deployed on a private blockchain

Due diligence and KYC (Know Your Client) procedures are crucial to combating money laundering and establishing good practices for robust governance. Keeping track of ownership and recording key information can facilitate the identification of properties and artworks suspected of being involved in illicit activities. Additionally, the cross-national nature of blockchain can help in tracing transactions globally, dramatically reducing the time it takes for bureaucratic paperwork to access information. The endorsement mechanism with qualified professionals and experts helps maintain data integrity and increase reliability. Enhancing due diligence in fine art and real estate can help attract more investment to these industries. This aspect is not of secondary importance. Combating money laundering is an arduous task and public funding, although necessary, will not be sufficient. Therefore, the contribution of businesses and private individuals is paramount. For this reason, when designing a solution to increase transparency and help prevent criminal activities, we carefully considered the business' perspective to incentivize adoption and reduce entry barriers.

The proposed solution aims to solve this seeming contradiction between two apparently opposite requirements: privacy and transparency in public blockchain. We designed two different systems, one to be deployed on a semi-private blockchain (HP1) and the second for a public blockchain (HP2). Real estate and fine art are not particularly receptive to new technologies. A solution based on a semi-private blockchain could penetrate the market more easily, as the involvement of trustworthy institutions provides reassurance regarding the correct data management, participation in the network, and governance. Nevertheless, semi-private blockchains exhibit reduced security compared to public blockchains and are more vulnerable to cyber-attacks. Because the network is composed of a reduced number of nodes, with "some" effort, the data can still be altered. Considering the pros and cons of the two solutions, we decided to explore both scenarios, HP1 (solution to be deployed on a public blockchain) and HP2 (solution to be deployed on a public

blockchain). Although the solutions are conceived to be suitable for both the fine art and the real estate sector, to avoid redundancy, we decided to develop the HP1, showcasing the application in real estate, and the HP2, the application in fine art.

Based on the Proof of Concept described in Chapter 5, and 6 we design a solution for the first blockchain registry for fine art and real estate to be implemented on a semi-private blockchain. This research was selected by UCL Business and Enterprise and received funding to build an Minimum Viable Product (MVP) to be deployed on Hyperledger Fabric. This platform for distributed ledger solutions is underpinned by a modular architecture which can provide high degrees of confidentiality, resiliency, flexibility, and scalability. The platform is designed to support the implementation of different components and accommodate the complexity of industries across the economic ecosystem. Compared to other permissioned blockchains such as Corda or Quorum, which are mainly designed for the finance industry, Fabric offers a broader range of industrial applications. Additionally, Hyperledger Fabric uses smart contracts to deliver greater flexibility and a pluggable consensus model which allows enterprises to define their rules to achieve consensus over transactions. Finally, it is a very well-known and established platform that facilitates finding qualified and experienced developers.

7.1.1 The network

The solution is designed for a Consortium blockchain. All participants in the network must be identified and granted permission to join. Organizations or members participating in the network have their certified identities released by Certificate Authorities which provide a public and private key forming a key pair that can be used to prove identity. However, this identity needs to be recognized by the network to ensure that no outsider interacts with the ledger. Fabric provides a Membership Service Provider (MSP) that contains a list of permissioned identities. While the peer certificate public key is used to verify the validity of the signature in the transaction, the MSP ensures that the rest of the network recognizes this identity and can be trusted. Interestingly, the MSP assigns a role to an identity, specifying their

privileges and restrictions on acting on the network. This feature is important for our case because the real estate and fine art sectors are less homogenous ecosystems than, for example, the financial sector. In these industries, actors' qualifications and expertise can span multiple backgrounds, from history and valuation to law and finance, and it is crucial that their different roles are reflected in the way they interact with the network and with the blockchain.

Although real estate and fine art share similarities, they remain separate industries. The proposed solution considers this factor and allows flexibility. For this reason, the network is divided into two channels, one for real estate and one for fine art. Channels can have different participants, and each channel has a completely separate ledger. However, applications and smart contracts can communicate between channels so that ledger information can be accessed between them. This feature is quite significant. It can happen that properties (especially luxury real estate) may be sold with some valuable assets, such as artworks, sculptures, and similar. Communication between channels provides increased transparency as both assets are identified through their unique IdCode allowing easy and complete traceability of provenance and ownership. The blockchain network is entirely customizable. However, for this research, we propose some members for the real estate and fine art channels, prioritizing the maximum benefit for society. Trusted institutions and regulators should play a significant role not only because they confer authority and reputability to the registry but also because they can ensure transparency by contributing to the network governance. For the real estate channels, some of the key participants could be (I) His Majesty Land Registry (HMLR), (II) regulators, such as Financial Conduct Authority (FCA) and Solicitor Regulation Authority (SRA), (III) professional bodies such as the Law Society and the Royal Institute of Trusted Surveyors (RICS), well-established solicitor firms and wealth and asset managers. Similarly, for fine art, some key participants can be (I) The British Art Market Federation (TBAMF), (II) the established Museums and Museum Association, (III) the Department for Culture, Media and Sport, and (IV) the Established Auction Houses

and galleries. Members can also be part of both channels, such as regulatory bodies, such as the FCA.

7.1.2 The Minimum Viable Product (MVP)

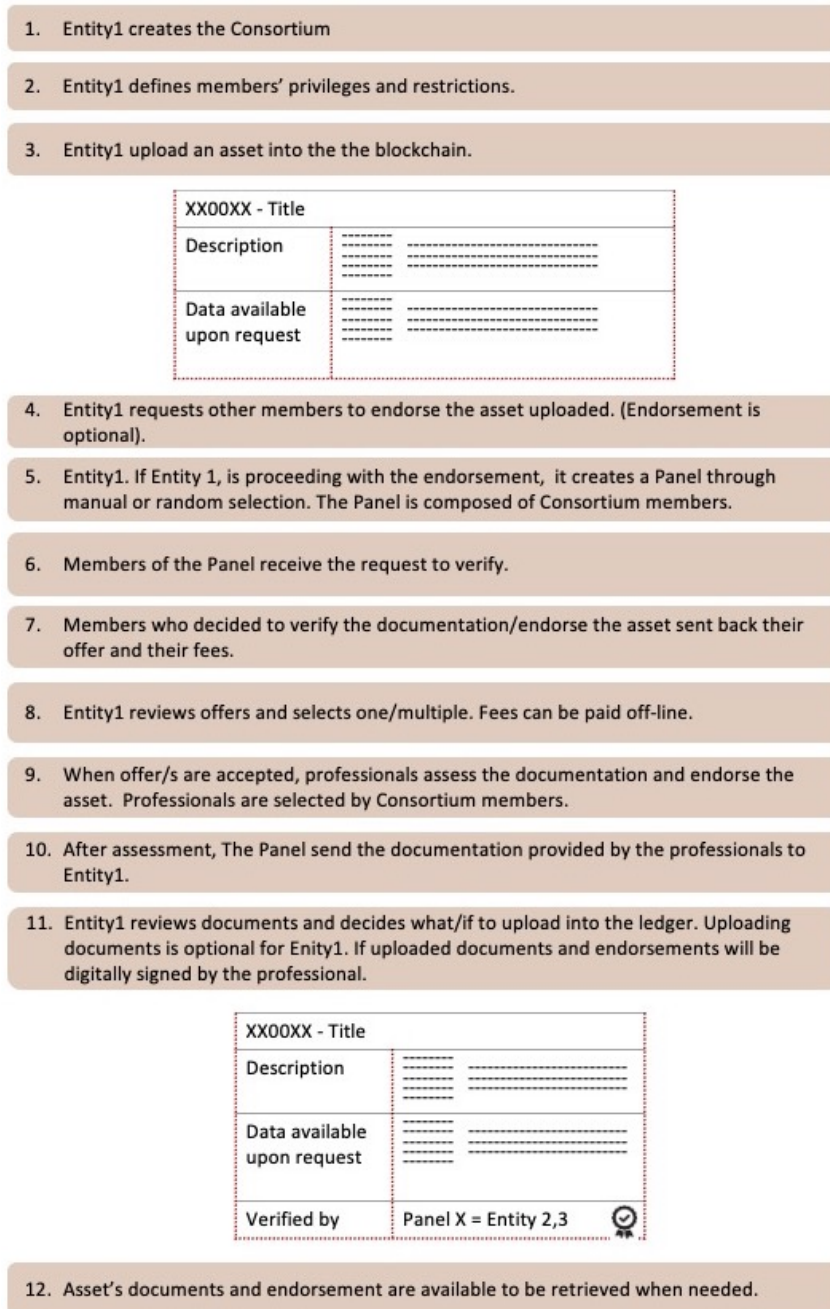
The MVP was developed in 2023/2024 thanks to UCL funding made available by UCL Business and Enterprise. The solution has been built following the DAML code developed in Chapter 5 and 6. For the development of the MVP, I highly benefited from my start-up experience, which I gained in the years 2021-2023 by running my real estate startup (RelAi), which was RICS TechPartner, selected for the CMS Cameron McKenna Equip Start-up program, and YCombinator Startup School. The MVP development follows Stanford University's Design Thinking methodology, as described in the Introduction, Section 1.4. This solution-based approach to solving problems has proven effective in improving, accelerating, and visualising creative processes, particularly in multidisciplinary research. According to this methodology described, the prototype development followed the following phases. (I) *Emphasize. Identification of the problem.* Alternative Assets represent a significant portion of investors' portfolios. Investors, buyers, and sellers must rely on accurate information to make informed decisions. Therefore, due diligence is crucial. Real estate is typically opaque, scarcely digitized, and prone to money laundering. Access to data is time-consuming as information is mainly disaggregated and often offline. (II) *Define. Research data is analysed to find a solution.* The literature review, case studies analysis, and interviews with experts highlighted that to increase transparency in the sector, we need to enhance due diligence by providing more accurate and reliable information. (III) *Ideate. Identifying a solution.* We identified a possible solution to the problem by building a blockchain register to provide a reliable, easy-to-access source of information. The register would significantly increase transparency, thus helping combat money laundering. Data reliability can be enhanced through an endorsement mechanism relying on qualified professionals. Among other options, blockchain represents a valuable solution for the problem identified because (a) valuable data need to be recorded, tracked or logged. (b) data can change over time, (c) it is imperative to keep track of the history

of changes, (d) recorded data cannot be changed or removed, and (e) it is beneficial to automate some actions based on the change in data. (IV) *Prototype. MVP developed with UCL funding.* The prototype creates a reliable database of information using blockchain technology. When needed, data are assessed by qualified professionals, thus increasing the reliability of the information. The MVP is coded in Java and developed to be deployed in Hyperledger Fabric (HF), a private, permissioned system in which only trusted members can participate in the network. Members of the network enrol through a trusted Membership Service Provider (MSP) so that protocols like “proof of work” are not required. The possibility of creating different channels for communications between members and private data collections allows selective access to data and a customisable degree of privacy, which is a crucial requirement in real estate. (V) *Test.* The prototype went through several cycles of testing and de-bugging with the UCL engineering but also with external developers to ensure correct functioning. A round of tests with professionals could not be included in this part of the research as the funding was not sufficient to implement changes to include feedback from the industry. However, this test is crucial and will be part of my post-doctoral research.

How it works

The blockchain is private and permissioned. To increase transparency, we propose a consortium blockchain; however, the system can work with just one Entity and be entirely private. For example, the HMLR could decide to develop its blockchain system, enhancing the existing registry (HMLR has demonstrated interest in blockchain projects, as shown in Chapter 4, Section 4.2.1 *Real estate due diligence analysis*). Data are entered into the blockchain only by trusted parties. Other entities can participate in the blockchain with limited privileges. To improve the reliability of the database, a scoring system allows qualified professionals to assess and score asset documentation. Data can be divided into core and non-core data. The first one can be publicly visible as it contains generic information to identify the asset. Non-core data (all documents) are hashed and stored off-chain in a separate archive to reduce block sizes. Fig. 7.1 explains the crucial steps to endorse

assets. With Main Entities (ME) we identify trustworthy institutions that control the network governance, access, and privileges. Privileges and limitations can be related to data visibility/ copy of the documents and/or transactions. One Entity starts the process by inviting other trusted entities to the blockchain. The group of entities with full privileges decides the privileges and limitations of the other entities invited to the blockchain. When an Entity requires an assessment of an asset (Entity 1 in the figure), the group of MEs create a Panel of experts to start the process. They have the choice to create the Panel manually or through a random selection. The panel is composed of a minimum of one member. The Panel assesses the documentation and provides an overall score (from 1 to 5). The Score is visible upon request of the MEs or other participants if permission is granted. Professional fees can be paid off-line. Given the trustworthiness relationship between the members of the network, there is no need to use cryptocurrency. Once the asset is verified, the endorsement is complete and all documents are uploaded to the ledger. The source of data and the professionals responsible for the endorsement are always recorded to ensure transparency. Due to the unique code assigned to every asset, documentation can be retrieved from the ledger upon request. Other participants (PAs) in the chain do not have the same privileges as MEs. Their access to data and transactions is restricted and their actions are limited. Examples of other participants can be estate agents, insurance companies and professional bodies.

**Figure 7.1:** MVP. Workflow figure

As mentioned, the prototype is created to be deployed on Hyperledger Fabric which we found particularly suitable for our purpose. An exciting feature of this platform is the ability to create channels, allowing participants to have a separate ledger of transactions. This is an important option for the MVP to provide different levels of privacy. Because privacy and confidentiality are paramount in fine art and

real estate, we require a system that allows granular access control to data. When two or more participants create a channel, only those participants, and no others, have copies of the ledger for that channel. However, creating separate channels for every case entails additional administrative work (maintaining chain code versions, policies, MSPs, etc). The platform offers the ability to create private data collections, allowing a subset of organizations on a channel to endorse, commit, or query private data without creating a separate channel. This feature is of great interest for our use case, as real estate and fine art transactions may require some participants to see that a transaction has happened without being granted permission to access the data, which remain private. Hyperledger Fabric smart contracts are written in Chaincode and invoked by an external application to the blockchain when it needs to interact with the ledger. Chaincode can be implemented in several programming languages, such as Go, Node.js, and Java. Compared to DAML, Java, the software used for the proof of concept, has a large community of users and developers, open-access resources, and libraries. For this reason, for the development of the prototype, this language was preferred over DAML. Interestingly, Hyperledger Fabric is designed to allow network starters to choose a consensus mechanism that best represents the relationships between participants. In our case, this role is with the trusted institutions, which are identified in the network as Main Entities. Some of these Entities can be selected to ordering nodes and form an ordering service. Fabric design is based on deterministic consensus algorithms so that any block validated by the peer is guaranteed to be final and correct. Additionally, ledgers cannot fork like in many other distributed and permissionless blockchain networks.

Although the MVP is created to be deployed in Hyperledger Fabric, for economic reasons the software runs on a local server simulating a network. Please note that some features are not available in a simulated environment and might display an error. Fig.7.2 and 7.3 show how assets are created. By selecting the function "createAsset", we input the data (as per the proof of concept developed in Chapter 5 and 6), such as the unique asset IdCode, name of the solicitors and the auction

house, the asset's address, asset's description, documents, and documents' links. The verified descriptions refer to reports and notes signed or verified by qualified professionals. For privacy reasons, it is not mandatory to fill in all fields. For example, the link to the documents might not be provided, or access can be restricted to some network members.

Asset Interaction App

Select the Environment

dev

Select the Chaincode Function

CreateAsset

ID Code

123XZ

Owner Solicitor

Owner Solicitor_NAME

Owner

Owner_NAME

Auction House

Auction House_NAME

Address

ADDRESS

Asset Description

ASSET_DESCRIPTION

Asset Documents (JSON Array format or add document names separated by commas)

ASSET_DOC1, ASSET_DOC2



Figure 7.2: MVP. Create asset. (Part. I)

Once the form is submitted, the system creates the asset. Fig. 7.4 shows that the system has correctly created the asset identified in the example with the IdCode "123XZ", displaying all information input in Fig.7.2 and 7.3. Fig.7.4 illustrates the internal contract structure governing the association between a digital asset and its supporting documentation, as implemented within the permissioned smart contract

Asset Documents Link (add links separated by new lines or commas)

ASSET_DOC1_link, ASSET_DOC2_link

Choose a file for Asset Documents

Drag and drop file here
Limit 200MB per file

Browse files

Verified Description

VERIFIED DESCRIPTION

Verified Documents (JSON Array format or add document names separated by commas)

V_ASSET_DOC1, V_ASSET_DOC2

Verified Documents Link (add links separated by new lines or commas)

V_ASSET_DOC1_link, V_ASSET_DOC2_link

Choose a file for Verified Documents

Drag and drop file here
Limit 200MB per file

Browse files

Date

2024/09/12

Submit

Figure 7.3: MVP. Create asset (Part. II)

model. This linkage mechanism is central to the workflow integrity of the registry, ensuring that each asset is cryptographically tied to one or more evidentiary records (e.g. provenance, valuation, or compliance documents). This contract-to-contract linkage is consistent with blockchain workflow principles: each state transition is signed, time-stamped, and committed to the ledger, ensuring traceability and tamper-resistance. Furthermore, the role-based access logic embedded within the template restricts who can view or modify document links, reflecting institutional permission boundaries. As such, Fig.7.4 represents a key technical enabler for ensuring that every registered asset within the system maintains a verifiable, immutable association with its supporting documentation, an essential requirement

in regulated environments where auditability and document provenance are legally binding.

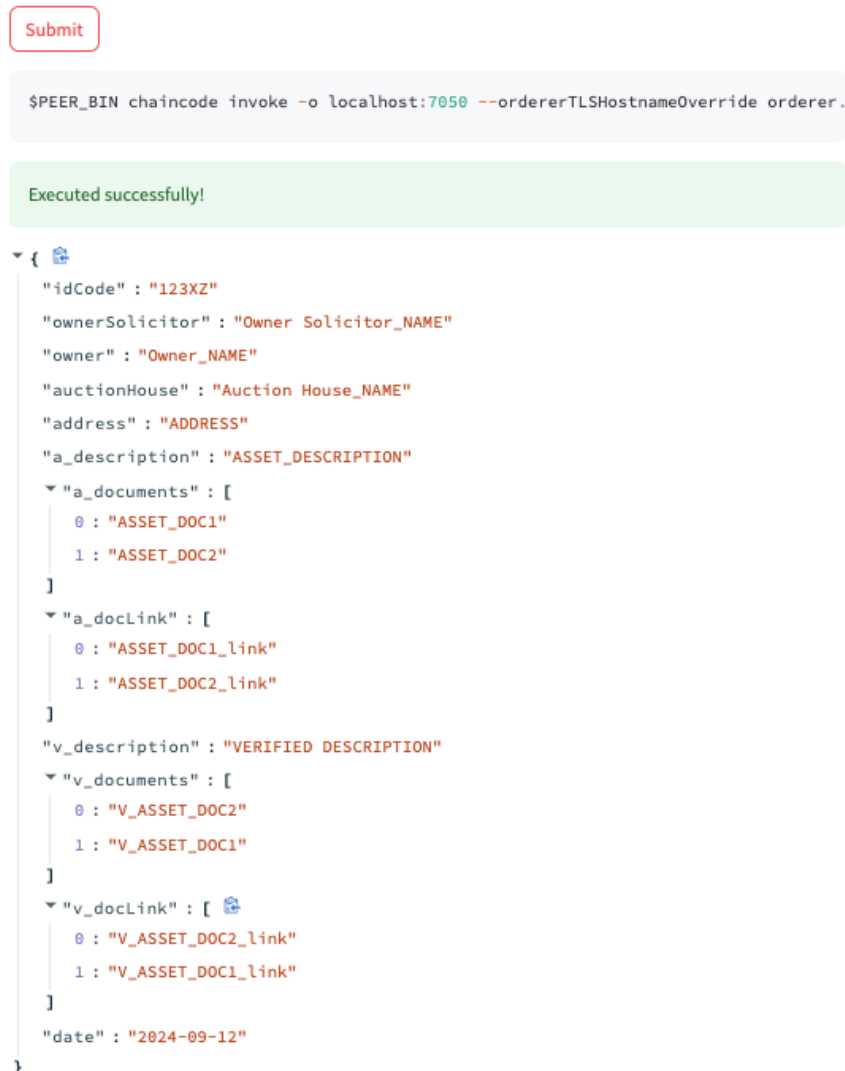


Figure 7.4: MVP. Asset created

Now that the asset is created, qualified professionals can score the asset's documentation. Because the score is assigned by qualified professionals, it provides a reliable evaluation of crucial aspects, such as market value, physical conditions, etc. The score is assigned to the asset through the unique IDcode ("123XZ" in the example). One of the members of the Consortium is identified as the Score Calculator and decides the number of professionals who are invited for the assessment. These professionals are the voters. In the test, we chose to have three voters. Fig.7.5

shows that voter3 has input his/her vote with a vote value equal to 5. We now verify that the MVP correctly translates from the DAML proof of concept, the function to avoid double-voting. The system is working correctly, and when we attempt to insert a second vote for Voter 3, the system shows an error with the message “the voter has already voted”. When all voters have input their vote, the score is automatically calculated, as shown in Fig.7.6. An additional function (as per the DAML proof of concept) allows selected qualified network members to score professionals based on their qualifications and experience. This function is important because it allows the weighting of the asset’s documentation score, creating a more balanced result that considers the professional’s experience and qualifications. The system is designed to be used both in real estate and in fine art. While established professional bodies ensure high professional standards in real estate, the fine art sector is less structured. Fine art experts are not required to hold specific or mandatory qualifications. For this reason, it is crucial to weigh the scores assigned by the professionals based on their experience.

The screenshot displays a web form for submitting a vote. It includes a text input field for 'Voter ID' containing 'Voter3', a text input field for 'Vote Value' containing '5', and a 'Submit' button. Below the form, a terminal window shows a command: `$PEER_BIN chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.`. A red error message box states 'Command execution failed!'. At the bottom, a log entry reads: 'nt failure during invoke. response: status:500 message:"The voter has already voted"'.

Figure 7.5: MVP. Already voted

Voters are always identifiable. Functions such as “UpdateVoterMetadata” and “ReadVoterMetadata” allow voters to input their unique ID and create their digital identity. Their digital signature is also required. The system is running successfully and a professional identity is registered. For simplicity, in the tests, we show the

registration using simple data, such as name and ID (Fig.7.7).

```
$PEER_BIN chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.
```

Executed successfully!

```
{
  "alreadyVoted" : [
    0 : "Voter2"
    1 : "Voter3"
    2 : "Voter1"
  ]
  "assetidCode" : "123XZ"
  "calculatedScore" : 3.6666666666666665
  "scoreCalculator" : "ABC"
  "scoreVoters" : []
}
```

Figure 7.6: MVP.Score vote

Voter Name

Voter_EMAIL

Voter Email

claudiagiannoni.16@gmail.com

Submit

```
$PEER_BIN chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.
```

Executed successfully!

```
{
  "email" : "claudiagiannoni.16@gmail.com"
  "id" : "Voter1"
  "name" : "Voter_NAME"
}
```

Figure 7.7: MVP.Update Voters metadata

When multiple voters are invited, it can be difficult to understand who has already voted. Functions such as "GetPendingVoters" (Fig.7.8) help identify professionals who were invited to vote and have not voted yet. When all votes are collected, if the system is interrogated again by calling the same function, the system shows a successful execution message and provides the voters' list.

Select the Environment

dev

Select the Chaincode Function

GetPendingVoters

Asset ID

123XZ

Submit

```
$PEER_BIN chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.
```

Executed successfully!

```
[
  0 : "Voter1"
]
```

Figure 7.8: MVP.Get pending

Once the voting process is completed, the function "GetTotalScoreForAsset" (Fig.7.9) allows us to show the asset's total score using the asset's unique ID.

Select the Chaincode Function

GetTotalScoreForAsset

Asset ID

123XZ

Submit

```
$PEER_BIN chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.
```

Executed successfully!

```
{
  "assetidCode" : "123XZ"
  "totalScore" : 3.6666666666666665
}
```

Figure 7.9: MVP.Get total score

Assets can be retrieved at all times with the function "ReadAsset", using the unique asset ID code. By calling the function "GetAllAssets" (Fig.7.10), the system provides a list of all assets created.

**Figure 7.10:** MVP.Get all assets

Until now, we have explained how assets are created, updated, retrieved, and the voting system. We now show how the system allows one to make an offer to sell an asset. According to the proof of concept developed in Chapter 5 and 6 only identified and permissioned members of the network can actively interact with the ledger. This solution allows for the preservation of data quality and integrity as all information is verified before it is uploaded into the ledger. The function "MakeAssetContractOffer" (Fig.7.11) creates an offer to sell the asset identified through the unique ID Code. As we can see, the offer presents crucial information such as the owner, the owner's solicitor, date etc. as per guidance provided by the UK legal authorities for real estate transactions. The offer created can be accepted or rejected by the other party through their solicitor.

Select the Chaincode Function

MakeAssetContractOffer

Asset ID

123XZ

Proposer Owner Solicitor

ProposerOwnerSolicitor_NAME

Proposer Owner

ProposerOwner_NAME

Notes

Notes

Date

2024/09/12

Owner Solicitor

OwnerSolicitor_NAME

Owner

Owner_NAME

Auction House

AuctionHouse_NAME

Press Enter to apply

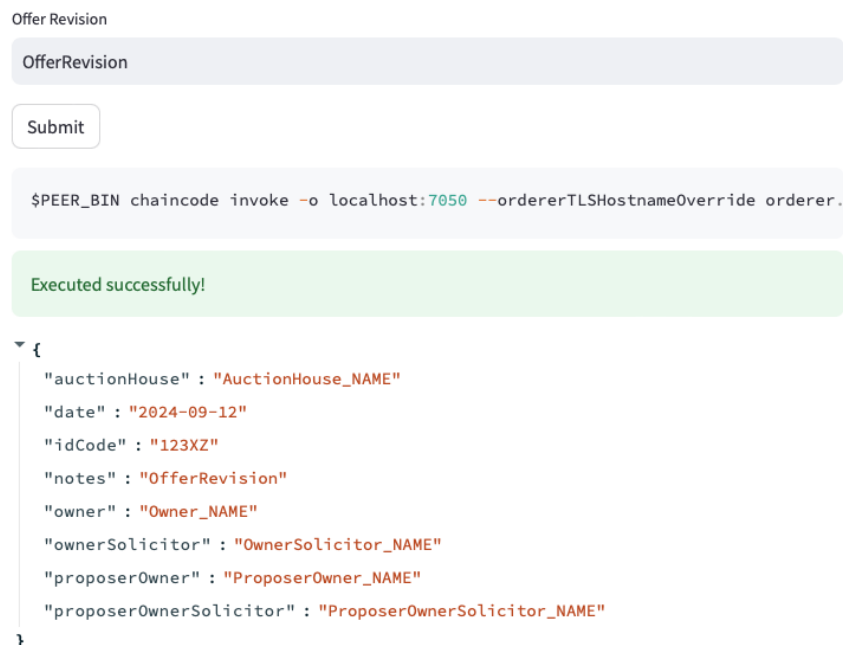
Submit

Figure 7.11: MVP. Create an offer

The function "ReviseContractOffer" allows parties to interact before deciding to accept or reject an offer. Through the "offer revision" field, parties can ask for clarification or request more documents. Additional documents can be uploaded into the ledger by retrieving the asset through the IDcode and recalling the function "Create Asset". In this case, this function is used to update the information. When data is updated, the offer revision is submitted as shown in Fig.7.12.

Fig.7.12 illustrates the contract lifecycle associated with offer revisions in the proposed blockchain-based transaction workflow. In this architecture, each offer has a distinct smart contract template containing details such as asset identifier, counterparty roles, pricing terms, and conditional clauses. When an offer is revised, either due to negotiation, compliance checks, or valuation adjustments, the original contract is not modified directly. Instead, it is archived and replaced by a new instance

with the updated parameters, preserving a cryptographically verifiable history of all prior states. This versioning mechanism reflects a core principle of blockchain systems: immutability through state transition rather than overwrite. Each revision is authorised by role-specific signatories (e.g., seller, compliance officer), and all state transitions are timestamped and auditable. This process guarantees that no historical terms can be retrospectively altered, and ensures full traceability of negotiations or compliance-related adjustments. The contract identifiers and archival links act as a hash-linked chain of custody for offer states, which is particularly valuable in regulated sectors where pre-contractual transparency and auditability are essential. As such, Fig.7.12 handles revisions using deterministic blockchain logic, aligning with both business negotiation practices and regulatory documentation standards.



Offer Revision

OfferRevision

Submit

```
$PEER_BIN chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.
```

Executed successfully!

```
{
  "auctionHouse" : "AuctionHouse_NAME"
  "date" : "2024-09-12"
  "idCode" : "123XZ"
  "notes" : "OfferRevision"
  "owner" : "Owner_NAME"
  "ownerSolicitor" : "OwnerSolicitor_NAME"
  "proposerOwner" : "ProposerOwner_NAME"
  "proposerOwnerSolicitor" : "ProposerOwnerSolicitor_NAME"
}
```

Figure 7.12: MVP. Revise an offer

The offer can be accepted using the function "AcceptAssetProposal" (Fig.7.13). The system will then store in the ledger the accepted offer stating the date, the buyer's and seller's names and their solicitors, and other parties involved (for example, the auction house), date and notes. As we can see, the asset ID Code has not been modified after the sale, allowing retrieval of the asset through multiple sales. To reject the offer, we can call the function "RejectAssetContractOffer". The

process is similar to the accepted offer, but the offer is archived as rejected.

Select the Chaincode Function

AcceptAssetProposal

Asset ID

123XZ

Buyer

Buyer_NAME

Seller

Seele_NAME

Buyer Solicitor

BuyerSolicitor_NAME

Seller Solicitor

SellerSolicitor_NAME

Contract Notes

Contract_NOTES

Contract Date

2024/09/12

Auction House In Contract

AuctionHouseInContract_NAME

Press Enter to apply

Submit

Executed successfully!

```
{
  "idCodeAsset" : "123XZ"
  "buyer" : "Buyer_NAME"
  "seller" : "Seele_NAME"
  "buyerSolicitor" : "BuyerSolicitor_NAME"
  "sellerSolicitor" : "SellerSolicitor_NAME"
  "contractNotes" : "Contract_NOTES"
  "contractDate" : "2024-09-12"
  "auctionHouseInContract" : "AuctionHouseInContract_NAME"
}
```

Figure 7.13: MVP. Accept an offer

The test was successful in showing that the MVP functions correctly. The prototype provides a solution for a reliable database to facilitate due diligence in fine art and real estate. Because blockchain technology cannot guarantee the truthfulness of data originating outside the ledger, the MVP provides a solution in which the data

content is evaluated by qualified professionals. This provides a robust source of information to support authorities and investors in their decision-making process. The endorsement performed by qualified professionals enhances the reliability of the data further by leveraging the accountability of the professionals and their commitment to high-quality standards.

7.2 HP2. Solution to be deployed on a public blockchain

In Section 7.1 we designed a solution for a fine art and blockchain registry conceived for a semi-private blockchain. In this Section, we explore the possibility of creating a decentralized registry for these industries to be deployed on a public blockchain. As mentioned in Section 7.1 both solutions (HP1 and HP2) are designed to be suitable for both the real estate and fine art industry. However, because in HP1 we showcased the solution for real estate, in HP2 (described in this Section), we work in the fine art sector.

Permissioned blockchains balance transparency and confidentiality by limiting replication and visibility to a select group of predefined nodes. This design restricts access to the blockchain, ensuring that only authorized participants can engage in the consensus process and access transaction histories. This model is particularly advantageous in enterprise settings, where transparency is necessary for auditing and compliance, but sensitive information must remain confidential within a trusted group. However, this increased privacy comes at the cost of reduced security and decentralization. In public blockchains, security relies on the large number of nodes participating in the consensus process. The more distributed and independent the network, the harder it becomes for malicious actors to compromise it. In contrast, permissioned blockchains operate with fewer nodes, often managed by a consortium or a single entity. This smaller, semi-centralized structure makes the network more vulnerable to targeted attacks, such as collusion between participants or exploitation of administrative privileges. Furthermore, reliance on predefined trust among participants in a permissioned blockchain shifts the security model away from trustless verification, which is characteristic of public blockchains. Although this trust-based approach simplifies governance and transaction efficiency, it introduces potential risks. It is important to note that if the centralized authority managing access permissions is compromised, the integrity of the entire network could be at stake. In essence, permissioned blockchains, even though they provide a solution to combine privacy and transparency, reduce the robust security that defines public

blockchains.

In public blockchains, the data are shared between multiple nodes (which could also be in different countries), potentially creating a problem regarding privacy and confidentiality which remain key requirements for fine art and real estate. For this reason, before designing the solution, we decided to investigate in great detail what data can be publicly visible and therefore, do not pose a confidentiality risk. There are sensitive data, though, that under no circumstances can be stored in the public ledger, such as financial information and individuals' private data. Storing these data on a public blockchain would also infringe GDPRs, which, especially in European markets, are particularly stringent. For this reason, in this solution, we propose the use of zero-knowledge proofs (ZKPs) to ensure transparency without compromising privacy. These mathematical proofs, introduced in 1985, are a special class of proofs that reveal no information beyond the truthfulness of a statement. This means that the verifier does not learn anything apart from the fact that the statement is true. In these proofs, input variables, intermediate results, and outputs of an algorithm can be hidden from the verifier unless explicitly shared. In other words, if the data are not collected, they cannot be stolen.

In HP2, we put a strong focus on due diligence as a key instrument to combat money laundering. A registry for fine art and real estate on a public blockchain has great potential to become a valuable instrument to prevent criminal activities. The cross-national nature of blockchain could foster collaboration among different countries and provide authorities with easy and fast access to information that is currently accessible only after long bureaucratic procedures. However, the complexity of this due diligence in the context of a public blockchain is significant and cannot be underestimated. To ensure that the solution has a strong ground in the real world, we conducted multiple interviews with key players in the fine art industry, such as art experts, galleries, auction houses, and private banks.

7.2.1 A rigorous fine art due diligence

As mentioned in Chapter 2, the fine art and real estate sectors share some key characteristics such as inefficient due diligence processes and vulnerability to money

laundering. The real estate sector is a more structured environment, where transactions are regulated by law and recorded. The Land Registry in the UK or similar cadastral registries in other countries keep records of transactions and ownership titles. The fine art sector is a less regulated sector and does not have a central organization like the Land Registry to record transactions and title of ownership for artworks. In order to understand how a new technological solution would be received in such an unstructured environment, we decided to sustain our research with several interviews with industry experts. We believe that this step was necessary to incorporate real-world business perspectives and assess the feasibility of the proposed solution. Experts were selected based on their expertise to cover the following areas: provenance and valuation, technology, laws and regulations, and risk management/KYC procedures (Introduction, Section 1.4, Table 1.2). Interviews of around 60/70 minutes were conducted in person or through video calls by the same individual to ensure consistency. Given the different backgrounds of the interviewees, we preferred not to adopt a standard interview methodology in favour of a more flexible approach. This allowed us to calibrate the interviews case by case to capture nuances and perspectives that otherwise would be missed. We need to note also that interviews belong to the fine art, financial, and consulting sectors, where privacy is crucial. For this reason, their identities are not disclosed.

Through these interviews, we identified three main areas where the experts' perspective is paramount to shaping technological solutions able to solve real-life problems: (I) provenance and artwork due diligence, (II) transaction and client due diligence, and (III) blockchain technology in the art industry.

Artwork due diligence.

Artwork due diligence is paramount to reduce the risks of forgeries and counterfeiting. Institutions and well-renowned established businesses provide guidance to promote responsible practices to manage these risks. However, the art industry is not homogeneous, and it contains very different realities, from international auction houses to small galleries, secondary vs. primary market dealers and businesses,

private collectors, foundations and public institutions. These realities have different needs, and any solutions aiming to facilitate the artwork's due diligence should be aware of their intrinsic peculiarities. In addition, the contemporary art market has different characteristics from the art and antiques market. The first is generally more dynamic and volatile, while the second is slower and more stable.

To understand how to perform accurate artwork diligence, we created a comprehensive list of tasks following the recommendations of experts, public institutions and established businesses in the art sector, such as the Responsible Art Market (RAM), Collection Trust (UK), USEUM and World's Art Museum. The experts selected to investigate this topic, work in different areas of the industry (sales, art curation, art valuation, etc.) to ensure we capture different perspectives.

Interviewees A and F belong to academia and bring an institutional view of the topic, interviewee B is an expert in art and antiques and appraisal, interviewee C is an expert in contemporary art and appraisal, interviewee D is a small gallery owner and interviewee E is a curator. Expert F brought an institutional perspective and explained the documentation and procedures required for collection management used in many countries. Museum procedures have been analysed to identify high-quality standards and compare them with art business guidelines and recommendations. Organisations such as Collection Trusts (UK) aim to better connect audiences and collections and provide detailed information regarding acquisition procedures, movement control, inventory, cataloguing and more. To understand which data can be openly shared in the blockchain, expert F suggested viewing the work undertaken by organisations such as USEUM, a digital World's Art Museum. Expert D also agrees to follow museums' recommendations and operating methods to identify the information to be displayed. Experts E and C point out that simple information, such as size, material, colours, and general characteristics recorded on the blockchain, could help identify fakes. Surprisingly, more often than we might think, to increase prices, forgeries have bigger sizes than the original artworks. Expert A pointed out how a blockchain solution to record artwork data can not only facilitate due diligence but also help young artists manage and promote their work.

Expert B provided us with a comprehensive understanding of crucial peculiarities of the fine art world. It is important to note that the art sector is not regulated like others, such as the financial sector. From this perspective, even the real estate industry, which shares similar risks with the fine art sector regarding money laundering, exhibits more structured procedures. Real estate transactions are generally regulated by law, and professionals and experts (for example, valuers, architects and engineers) possess specific qualifications. The cadastral registry, present in many countries, ensures all transactions are registered, and property titles are recorded. This is not the case for the fine art sector. Expert B highlights that there are no specific qualifications to identify as an art expert, and there isn't a professional register. Art sales can be registered at a notary but can also happen privately, without involving any public institution and without the transfer of ownership being recorded anywhere. This lack of structure makes the fine art sector a fertile ground for forgeries and counterfeiting. Expert B highlights that there is not a single piece of data which can ensure the truthfulness and accuracy of provenance but a plurality of information. As they put it, "all data in fine art can be manipulated", from sales prices and valuations to authenticity. The more information we have about an artwork, the closer we are to the truth. For example, even if it is true that prices published, for example, on specific databases (Artprice.com, Artnet.com), can be manipulated, more information about exhibitions, previous sales and ownerships can significantly help establish the truth (where the truth is an honest estimate or a truthful provenance). Expert C reviewed the checklist we created in detail to perform accurate artwork due diligence. The checklist is paramount as it constitutes the base for our proposed design solution. Expert C finds the list comprehensive and states that the proposed checks are effective and feasible. No further comments or changes were proposed to the list. A high-level and a detailed list of verifications for artwork due diligence are shown in Table 7.3 and Fig.7.14.

Client and transaction due diligence

Expert C reviewed in detail the checklist we created to perform accurate client and transaction due diligence. They found the list comprehensive and stated that the

proposed checks were effective and feasible. Regarding the client identity verification, they suggested including the driver's licence. Regarding the verification of the source of funding, they suggested including the wire transfer while the bill of lading was added to the artwork transportation documentation. Expert C also suggested including a red flag related to the client's behaviour. From their experience, it emerges the client's conduct is a good indicator of suspicious activities. Pushing for a fast transaction, insisting on showing the artwork only at very specific unusual conditions, and providing evasive answers are a good example of what can be considered suspicious. Overall, expert C thinks that our work is very comprehensive and accurate and covers all crucial aspects for good artwork and client and transaction due diligence. Like expert B, expert C agrees that there's no structured process for due diligence in the art world. Expert C states that if an art dealer or an expert suspects that, for some reason, the transaction is illegitimate, they have to alert the client, but there are no other obligations, and the transaction can happen despite this red flag. Expert C works in the US, where EU regulations do not apply. However, the US is one of the biggest art markets in the world, and because money laundering activities can be cross-national, expert C's view and knowledge are of great interest to this research. Expert D also (active in the EU) states that small businesses have no stringent obligations regarding artwork, client, and transaction due diligence. Expert N highlights that well-established auction houses and galleries follow more strict procedures. However, Eurostat estimated that in 2021, there were half a million active enterprises in creative, arts and entertainment activities. For this reason, the modus operandi of small galleries and art dealers is not negligible. Expert D states that small galleries work mainly on trust. The lack of structured procedures is compensated by the personal relationship with clients who are well known to the gallery and with whom there is generally a long-time acquaintance. The expert highlights that genuine businesses deal only with legitimate transactions. However, malicious activities are possible for dishonest actors in the industry. They also note that cash payments are infrequent, with a maximum limit of 1.000 Euro per transaction. Nevertheless, it is possible to pay in instalments (generally up to 10) for

each artwork. Expert C agrees that cash payments are infrequent, but they highlight how cryptocurrencies have become the "new cash" to hide the source of funds and prevent tracking payments. In their view, cryptocurrency payments represent a red flag and need careful due diligence. Because of the associated risks, many art businesses do not accept this type of payment. Like expert B, expert C thinks that in the art sector, prices are easy to manipulate, but they also point out that there is not necessarily a "right" price. There are many legitimate cases where the price of an artwork is higher or lower compared to the corresponding market segment. In these cases, it is important to understand how the price is justified considering exhibitions, previous sales and similar artworks. A high-level and a detailed list of verifications for client and transaction due diligence are shown in Table 7.4, Table 7.5 and Fig.7.15.

Experts' perspective on Blockchain technology in the art industry

The fine art sector is not particularly receptive to technological innovation. Because of the high volume of transactions, actors (from UHNIs to collectors and various art dealers) are more concerned with privacy and security than with the modernisation of the industry. However, there is an increasing need for transparency due to new AML laws and regulations. Additionally, new technologies can facilitate due diligence, increase liquidity and bring more investments. Experts in the financial and law sectors have been selected to have their views regarding the feasibility of a blockchain solution, particularly regarding data security. The private banking expert also brings the perspective of their UHN clients which otherwise would be impossible to acquire. Expert Q provided great insights into how the art industry deals with innovation. They share a similar perspective as Expert B when highlighting that in the art sector, all data can be manipulated. For this reason, proving authenticity is challenging and expensive. Art galleries can charge up to 30% of the sale price and actors in the market are looking for alternatives to facilitate the clearance of artworks. Significant barriers to new technologies can be seen in the resistance to technological changes exhibited by clients and some galleries and auction houses which are more anchored to conventional *modus operandi* and less

aware of changes. Nevertheless, Expert Q emphasizes that things are changing in the art industry and actors who do not adapt might become obsolete shortly. Experts C and E think that a blockchain solution can be very useful in tracking provenance and facilitating due diligence. Expert E sees barriers in the high cost of technology and the decentralised nature of blockchain which entails that there isn't a physical person directly responsible for the management of the blockchain. This characteristic might be a deterrent to adoption as clients will be required to trust a technology perceived as mysterious and difficult to understand. In this regard, Expert C highlights the client's concerns regarding privacy. Even though blockchain can offer high data security and increased privacy thanks to cryptography, the challenge will be to convince clients to trust the technology. Data privacy and confidentiality are paramount in the art sector and clients would rather continue with that traditional *modus operandi* than embark on a due diligence process controlled by an unknown technology. The blockchain solution HP1 developed in Section 7.1, was presented at the Tech Italia event on the 7th of March 2024 in London. During the event, the solution was explained in detail and well received by Experts I and H who provided good feedback. They agree that this blockchain solution can effectively help increase transparency in the fine art sector without compromising privacy. Experts L and M provided precious insights regarding new AML laws and regulations and the legal implications of new technological solutions. GDPR give customers rights to their data, such as access, change, and right to be forgotten, which need to be carefully considered when designing a blockchain solution. They also underlined how KYC procedures currently in place in the physical world can be used as a base for digital solutions. For these reasons, the solution proposed is based on current artwork client and transaction due-diligence procedures and works with zero-knowledge protocols to overcome the challenge of providing transparency while ensuring GDPR compliance. Experts O and P highlight that anti-money laundering laws and regulations are crucial to good practices in governance, and they are becoming even more essential now that environmental, Social, and Governance (ESG) criteria have emerged as critical indicators for evaluating long-term companies' re-

Artwork due diligence
Identification. Physical examination and high-resolution images
Trade restrictions. Verification if the artwork is subject to trade sanctions in any of the jurisdictions covered by the transaction
Ownership. Obtain details of the legal owner and all other persons who have a legal interest in the artwork
Provenance and exhibition history. Establishing the historical record of ownership and if applicable, exhibition history
Artwork locations and recent movements. Verification of location and tax status of the artwork and if applicable its last country of export
Authenticity. Verifying authenticity, with the help of expert opinion, provenance and art historical research and scientific testing
Physical conditions. Analysis of materials used, artwork's condition and the presence of any restoration

Table 7.3: Artwork due diligence

Client due diligence
Individual. Verification of identity
Company or other legal entity. Verification of identity to prove these entities are properly formed and exist. Physical identities of people with significant roles are also verified
Client's role. Verification if there are one or more intermediaries
Client's authority to act. Verification if the artwork is owned jointly by two or more individuals, e.g. married couples, siblings following the death of a parent, etc.

Table 7.4: Client due diligence

silence and investments' ethical implications. Expert O believe that a blockchain solution to facilitate due diligence and asset clearance would be well received by their UHN clients. Wealth managers would be glad to offer their clients a solution to securely store asset data to allow faster transactions and increase their investment liquidity. However, Expert O remains concerned about privacy. For this reason, a solution based on a private blockchain might be easier to promote. nevertheless, they highlight that provided that privacy is not compromised, a solution based on a public blockchain might be beneficial if it ensures higher security.

Transaction due diligence
Purpose of the transaction. Verification of the client's background, such as his/her collection, previous sales, his/her professional activities and personal wealth.
Form of the transaction. Verification of the form and structure of the transaction, such as the use of intermediaries and other non-face-to-face methods, unusually complex structures or Unusual payment structures, conflict of interests, and artificially low or inflated prices
Source of funds. Verification of payments such as cash payments, third-party payments, Payments from bank accounts located in non-AML regulated jurisdictions, and payments with digital currencies.
Documentation. Verification of documents regarding the transaction such as consignment, sale and purchase, loan or exchange of artworks and artwork movements such as export and import permits, bills of lading and delivery notes.

Table 7.5: Transaction due diligence

7.2.2 Identifying and investigating red flags

Thanks to the literature review and the interviews with industry experts, we identify the most significant red flags which make an artwork suspicious of being involved in illegal activities. We also considered the guidelines provided by established institutions such as the Responsible Art Market (RAM), which has developed accurate recommendations for combating money laundering and terrorist financing in the art industry. Depending on the circumstances, the verifications listed may not be appropriate or practicable or, in some cases, sufficient. However, these recommendations aim to raise awareness of the threats and risks related to criminal activities and provide a framework of suggested measures designed to combat both money laundering and terrorist financing.

As emerges from the previous section, before an artwork is sold/purchased, it is highly recommended to perform accurate due diligence. This entails obtaining as much information as possible about the parties involved in the transaction, the artwork, and the details of the transaction itself. To summarise, the artwork due diligence process has been divided into three groups: (I) Artwork due diligence, (II) Client due diligence, (III) Transaction due diligence (Table 7.3, 7.4, 7.5). The artwork's due diligence concerns information about the nature of the artefact, its characteristics, provenance, and authenticity. The client's due diligence aims to acquire information about the client, whether he/she is a well-known existing client or a new one. It concerns his/her identity (in the case of an individual) or the company's (or trust/association or other legal entity) legal documentation, main shareholders, directors, beneficiaries, and controlling owners. It includes verifications on the client's role in the transaction and his/her authority to act. Transaction due diligence concerns the type of transaction and whether the sale/purchase occurs through intermediaries, face-to-face, or over the Internet. Accurate due diligence is also recommended in several situations, such as acquisitions, sales, donations, loans, and exchanges of artworks, as well as management of art collections by fiduciary service providers and advisors. It is also advised in the case of financial transactions and investments involving artworks when loans are secured against

artworks, the curation of exhibitions and art fairs, and when arranging insurance, storage, and/or transportation of artworks. It is important to highlight that accurate due diligence is beneficial for all parties involved in art transactions to manage reputational and financial risks. The list of recommended checks adopts a “risk-based” approach to help determine the level of due diligence required when entering a specific art transaction. From interviews with industry experts, we understand that while international auction houses have an internal compliance department, small dealers, galleries, or collectors do not have the same resources. Therefore, the due diligence process must be tailored and adjusted case by case. The purpose is not to overwhelm businesses with unrealistic tasks but to ensure that all parties involved understand the risks to which they are exposed and take commensurate measures to mitigate them effectively and efficiently.

A structured onboarding process is essential to ensure that all participating clients in the registry—whether collectors, dealers, or institutional buyers—are subject to consistent and verifiable compliance checks. The framework outlined in Table 7.4 provides a step-by-step guideline for client onboarding, beginning with the initial identity verification through official documentation (e.g., passport, national ID, or driver’s licence), and followed by a source of funds assessment. This includes the collection of verifiable financial information, such as bank wire records or transaction histories, to establish transparency and legitimacy. Where applicable, additional layers such as PEP screening and sanctions list checks are triggered based on the client’s profile or transaction context. Once the client has been verified, transaction-level due diligence procedures, detailed in Table 7.7, are applied to assess the legitimacy of each specific artwork-related activity. These include documentation of transportation and insurance (e.g., bill of lading, invoices, and certificates of origin), provenance history, and pricing justification mechanisms. The framework also integrates behavioural indicators as red flags—for instance, clients insisting on rushed deals, limited viewing options, or use of privacy-centric payment methods such as cryptocurrency. These patterns are flagged for enhanced

review and, where applicable, further validation through institutional endorsement. Together, Tables 7.4 and 7.7 provide a compliance blueprint that maps onto the proposed smart contract infrastructure.

The themes presented in Table 7.7 were derived through expert interviews conducted during the Empathize phase of the design thinking process. These themes include identity verification, source of funds validation, transaction behaviour monitoring, and provenance, each emerging from multiple interviewees working across legal, curatorial, financial, and regulatory roles. This thematic structure aligns with established compliance literature, particularly the Financial Action Task Force (FATF) guidelines on Customer Due Diligence (CDD) and Know Your Customer (KYC) principles, which emphasise the importance of identity checks, beneficial ownership tracing, and ongoing transaction monitoring. It also reflects insights from sector-specific studies [197], [198]. Sector-specific studies, such as the Basel Art Trade Anti-Money Laundering Principles [199], further underscore the importance of provenance tracing and price justification in the fine art context. However, our thematic framework extends beyond procedural checklists: interview feedback highlighted behavioral indicators, such as rushed negotiations, unusual payment methods (e.g., cryptocurrency), and intermittent disclosures, which are not commonly addressed in standard AML frameworks. This divergence is supported by recent studies on network analytics in AML, which advocate for flagging anomalies and illicit payment patterns [200].

Once complete due diligence is performed (artwork, client, and transaction), some *red flags* may emerge, which could be indicators of suspicious activity. It is important to specify that these flags need to be read simply as warnings, not as proof of some illegitimate activity. A transaction can have multiple red flags and still be legitimate. The purpose is to identify key characteristics that are recurrent in transactions involved in money laundering activities. Multiple warnings should encourage deeper investigation. Some factors which can be considered high risk are clients who are Politically Exposed Persons (PEPs) or associated with PEPs, artworks without a verified provenance, and transactions which take place entirely via

Artwork red flags
Limited or no documentation or provenance. No recent provenance or provenance with unexplained gaps
artwork sourced from a country which is or has been in recent conflict
Artist or the object known to be forged and/or adverse information from the market regarding its existence/authenticity
Documentation for the artwork (e.g. authorisations, export licences, provenance documents) limited or inexistent or appearing to be false
Contradictory/unclear information about how the seller acquired the artwork
The artwork is subject to trade restrictions
The artwork presents signs of an attempt to hide details or restoration or with unexplained or extensive restorations, or where the original canvas and tacking edges cannot be accessed
High-value artworks, with no insurance and/or storage records

Table 7.6: Artwork red flags

Client red flags
The client is a Politically Exposed Person (PEPs) or he/she is closely associated with PEPs
The client operates through offshore structures (such as companies or trusts) which exist to hold assets only
The client is known to be involved or (or associated with persons involved) in a criminal or regulatory investigation, prosecution or conviction
The client is an agent for undisclosed buyers or sellers
The client operates through multiple private investment companies or offshore structures whose ownership, control and/or beneficiary structure is opaque.

Table 7.7: Client red flags

non face-to-face means or are unusually complex. In contrast, some lower risk factors can include long-standing clients with a clean transaction record, authenticated artworks with verified provenance, transactions occurring face-to-face, or which involve low-value artworks. According to expert C, currently, one of the main risks is represented by payments using cryptocurrencies. If cash payments have become less frequent due to more strict regulations, cryptocurrencies are becoming the new way to bypass restrictions and elude controls. For this reason, they suggested considering high-risk any transaction of significant value involving cryptocurrencies. A fairly comprehensive list of red flags is shown in Table 7.6, 7.7, 7.8.

As mentioned above, these red flags serve as warnings, prompting the involved

Transaction red flags
The client provides vague or appearing to be false information about their identity or the artwork and artwork documentation
The client is unwilling to provide adequate proof of ownership for the artwork
The client insists on paying large amounts in cash or making multiple low-value cash payments for a single transaction or connected transactions
The client insists on paying with an anonymous credit card (e.g. China Union Pay Card, which does not include the holder's name) or cash card, or by a cheque drawn on a bank located outside the FATF (Financial Action Task Force)
The client shows unusual interest in the art business' procedures for reporting suspicious activity and/or financial matters to tax authorities
The client willing to sell at an artificially low or inflated price
The client insists on using unusually complicated structures for the purchase or sale
Payments or transactions arranged through a third party
The seller and buyer (or their intermediaries) are connected
The client's profile or business structure is not consistent with the transaction
Parties to the transaction have conflicts of interest

Table 7.8: Transaction red flags

parties to conduct further checks to rule out any potential criminal activity associated with the transaction. In case of suspicious activity, parties are strongly advised to alert authorities. Once potential red flags have been identified, it is important to know what and how to verify the transaction's legitimacy. In this section, we describe how some of the crucial information can be verified. Client and transaction verifications present some overlap and, for convenience, they have been grouped. Most of these verifications have been conceived for art and antiques. However, industry experts confirmed that these checks are appropriate for physical artworks in general. Experts also highlighted that, even though these verifications represent a wide spectrum for accurate due diligence, cases may be different and must be evaluated individually Fig. 7.14 and 7.15 provide an accurate summary of key due diligence steps, crucial aspects to be investigated and how to find the information needed for the verification.

Regarding provenance due diligence (Fig. 7.14), a significant concern is the lack of specificity and references such as *private collection*, not supported by adequate documentation. Antiquities often have customs clearance in their history and they should be accompanied by documents from legal authorities in the corre-

sponding jurisdictions. Again, incomplete or vague information should raise concerns. All available documentation should be checked, and unclear aspects should be questioned and further investigated. It is evident that if the artwork's provenance is endorsed by a well-known and recognized organization or expert, such as a well-established auction house or foundation or a renowned art expert, it is considered more reliable and carries more weight. When available, a Certificate of Authenticity endorsed by a trustworthy organization or expert can be of significant help. It offers valuable information about materials used to create the artefact and generally provides information on provenance. It is worth noticing that even though scientific analysis of materials and physical conditions can give important information regarding authenticity, accurate analysis goes beyond physical aspects to consider the artist's culture and background and his/her way of working. The exhibition history and the scholarly reputation of any attribution are also paramount in assessing the artwork's authenticity. Besides verifying documentation, it is important to consult databases of lost and stolen, such as Interpol's "Works of Art" database, the ICOM (International Council of Museums) Red Lists Database, and the Art Loss Register. It is also crucial to check the location of the artwork and recent movements. Particular attention should be paid to objects that come from known conflict zones. Even when dealing with commercial centres outside the area of conflict, it should be verified that objects are not connected to objects in an otherwise lawful location. For this purpose, UNESCO's World Heritage in Danger list is instructive.

Crucial information can be deducted from the artwork's insurance if available. Data included in the insurance can vary depending different companies, but generally include artwork's valuation, movements and loans, location, current physical conditions, conditions required for the artwork's storage, damages and or previous restorations. According to industry experts (Expert B, F and C in Table 1.2), consulting data from public websites is also important as it can help verify the consistency of information and address lacunae in the provenance documentation. Furthermore, artwork's valuation and data about previous sales are also valuable. Websites like Artnet and Artprice can be valuable resources as they provide a compre-

hensive record of art sales. When data are not available, these art price databases are very useful to get a better understanding of the art market and identify the artwork's market segment 7.14.

Beside provenance, client and transaction verifications are of the utmost importance (Fig.7.15). Parties' identity should be verified using official identity papers (e.g., passport or national ID card) and cross-checked with other reliable, independent documents, such as a copy of a bank statement or utility bill for proof of address. As mentioned above, internet searches are recommended, and specialist screening services (screening against up-to-date PEP and sanction lists) can also be used to verify a client's identity. In the case of companies, trusts or other legal entities, identity should be verified based on official documents and data proving these entities were properly formed and currently exist (e.g., the certificate issued by the relevant company registry including details of directors and/or shareholders, trustees, beneficiaries if the case). It is recommended to verify the company's controlling owner and its majority shareholder(s). For accurate due diligence, it is crucial to identify the "Beneficial Owner", that is to say, the natural person who enjoys the ultimate benefit of ownership of the artwork. To emphasise the importance of this point, it is worth noticing that established institutions such as the RAM (Responsible Art market) suggest that best efforts should be made to identify the Beneficial Owner even if the client raises confidentiality concerns to ensure the transaction is not associated with any money laundering activities or terrorist financing schemes. Company registries are generally available for consultation in many countries, and efforts are being made (for example, in the UK and EU) to develop beneficial ownership registries.

Once the client's identity is verified, the client's role in the transaction and his/her authority to act needs to be investigated. The transaction might involve one or more intermediaries, such as an art advisor or agent. There are multiple reasons why intermediaries are involved. For example, in the case of jointly owned artworks, the executor of a deceased person's estate and the agent acting on behalf of a principal owner. In these cases, it is important to check in what capacity

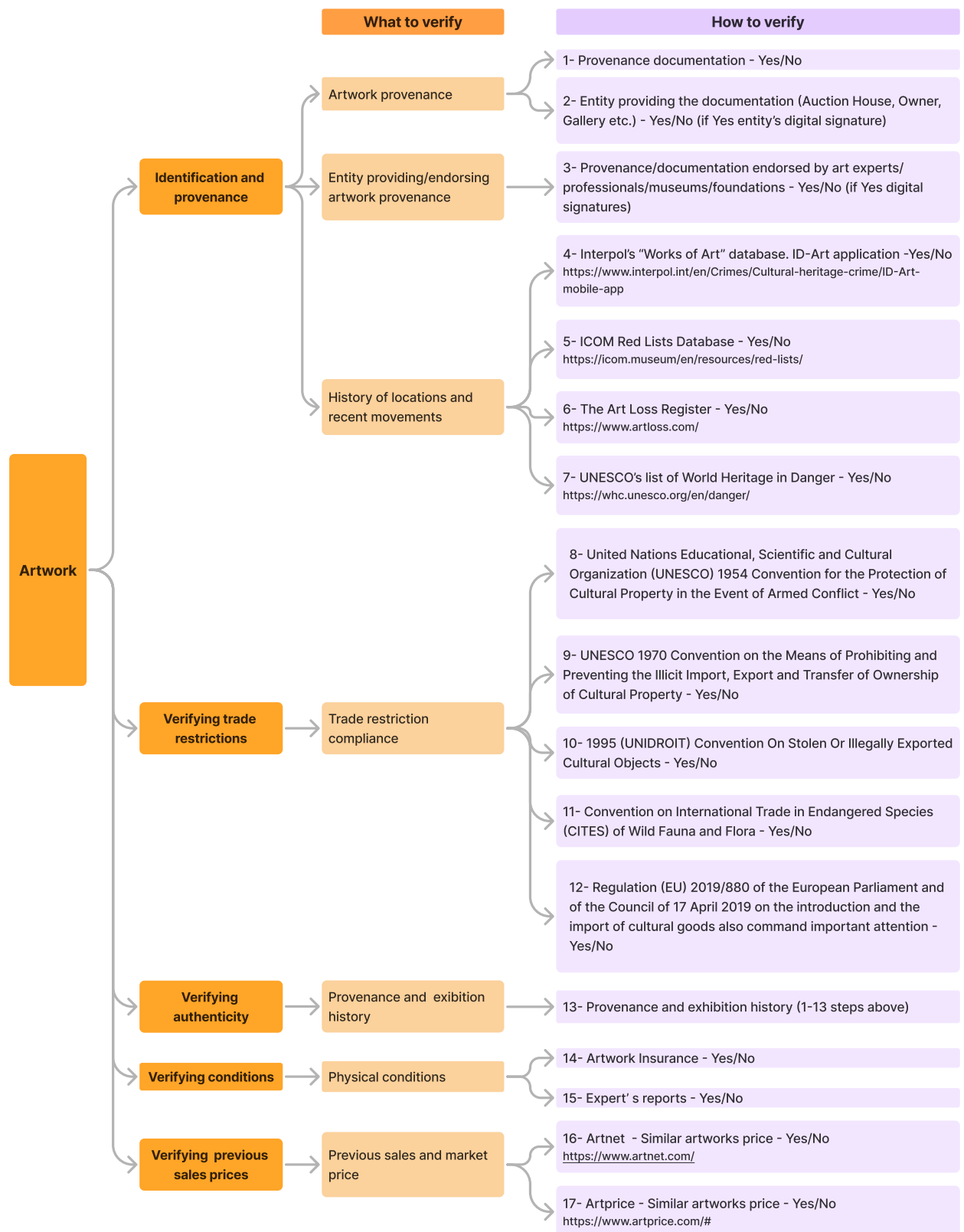


Figure 7.14: Artwork due diligence and verifications.

these intermediaries are acting and that they have the authority to act. Importantly, the RAM highlights that if the transaction is taking place through intermediaries or entirely non-face-to-face, there is a risk that the information provided cannot be properly verified and that the transaction is used in an illegal scheme. Unusually complex structures where the client operates through multiple private investment companies or offshore entities whose opaque structure suggests caution. Similarly, if the client is willing to sell or buy at an artificially low or inflated price or proposes multiple low-value cash payments for a single or series of connected transactions without providing logical business reasons, it is recommended to undertake further investigations to obtain comfort that the transaction is not part of an illegal scheme. Finally, further concerns arise if it emerges that the seller and buyer (or their intermediaries) are connected because of the potential conflict of interest and situations of potential bribery, which might take place behind the scenes.

Particular attention should be paid to the source of funds used in the transaction. Cash payments should generally be discouraged as the source cannot be traced and is not guaranteed to be legitimate. Single or multiple cash payments above the legally imposed threshold should never be accepted. Similarly, payments from third parties without legitimate reasons are highly suspicious. According to Expert C, payments with cryptocurrencies are becoming a significant warning, as they represent "new cash". There is a plethora of cryptocurrencies, and many are not controlled or regulated. They cannot be tracked and it is very difficult to verify that the source of funds is legitimate. For similar reasons, payments through anonymous credit cards should be carefully vetted. Transactions where the source of funds comes from banks located in non-AML regulated jurisdictions should also be carefully considered. The Financial Action Task Force (FATF) lists countries that do not adhere to international standards to prevent global money laundering and terrorist financing. Finally, the artwork's transactions and movement documentation must be exhaustive and clear. Complete transport documents (including export and import permits, bills of lading, and delivery notes) prove an artwork's legal import and export and can include statements of origin and destination, de-

tails of the consignor, consignee, and transporter, dates, and vehicle/flight details. The artwork must be clearly identified through high-definition pictures and accurate descriptions, including size, materials, and physical conditions.

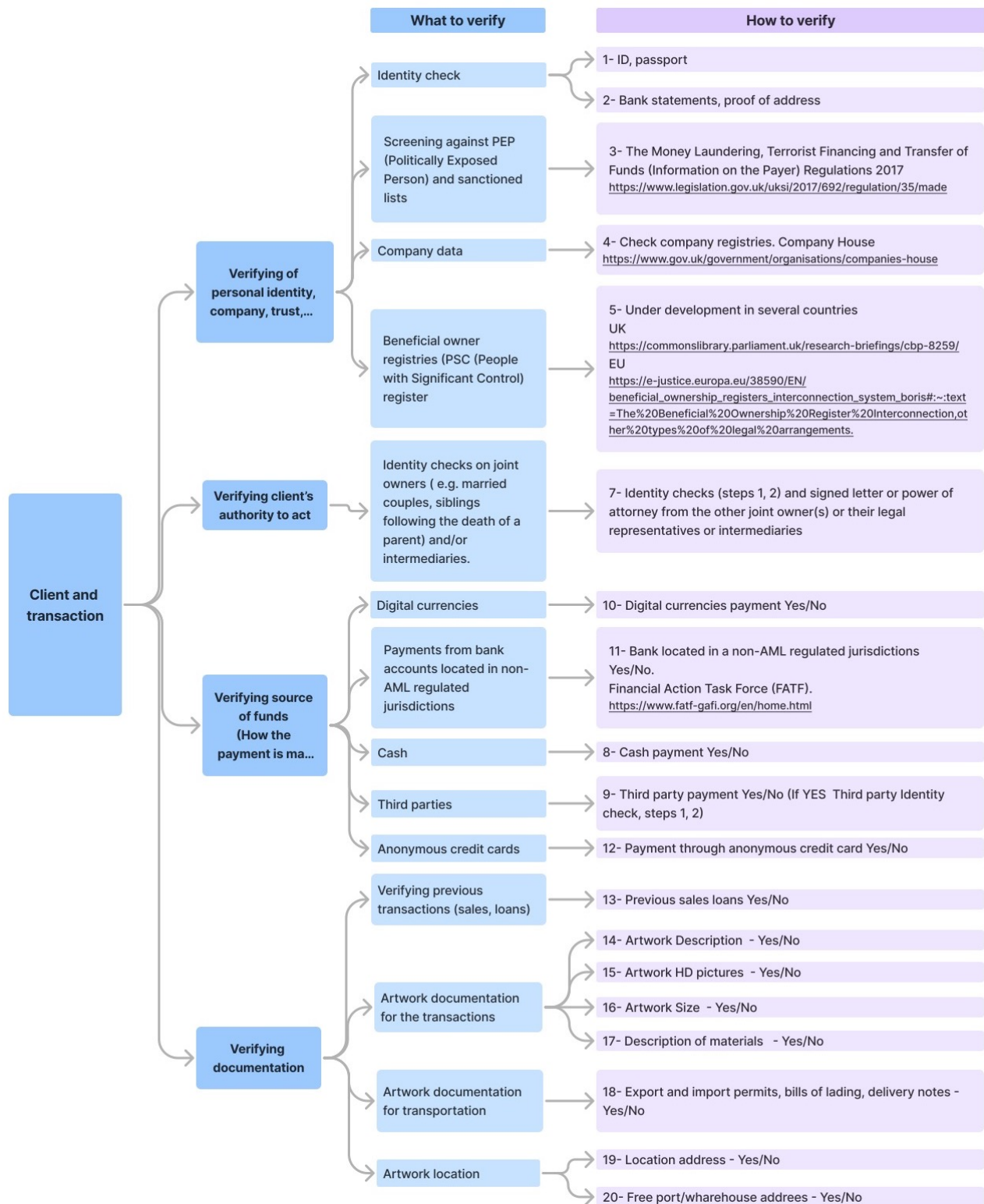


Figure 7.15: Client and transaction due diligence and verifications.

7.2.3 Solution design. Blockchain registry and ZKPs

The need for aggregated and reliable data in fine art is perceived as a need in the industry. Currently, online research through multiple websites is one of the most common tools to gain and cross-check information regarding artworks and antiques. To provide some examples, websites such as USEUM [201] provide images of paintings by artists and museums around the world. Through the Spectrum project [202] Collections Trust provides management standards and guidance in many countries. Art UK [203] brings together art from multiple British institutions, showing more than 300,000 works by more than 50,000 artists. Finally, towards National Collection [204] is a project funded by the UKRI Arts and Humanities Research Council that breaks down the barriers between the outstanding collections of British cultural heritage. However, none of these websites or projects provides a complete set of information regarding artwork transactions, ownerships, and valuations. Data collected through online research are unstructured, maybe contradictory, and unverified, making the diligence inefficient and time-consuming.

In addition, due diligence for clients and transactions involves collecting and holding sensitive data, which burdens art businesses with additional responsibilities regarding data protection and exposes them to the risk of data leaks. Art businesses are strongly recommended to perform accurate due diligence to protect themselves from legal actions and the potential reputational damage that might occur if they get involved in illicit activities. To manage these risks, they are obliged to collect many documents with highly sensitive and personal data from individuals, incurring data protection obligations, and consequentially other legal risks. It is recent news that Christie's has been subject to a class action lawsuit over the exposure of clients' personal data (including full names, genders, birthdates, birthplaces and a variety of information from their passports) in a cyberattack [205]. The breach could directly have resulted from the auction house's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its clients. Christie's clients may be threatened by multiple forms of identity theft, from malicious actors opening fraudulent financial accounts to using data from exposed parties to illegally

secure government benefits, acquire driver's licenses, and more.

A blockchain registry can significantly help create a reliable source of information, dramatically improving due diligence. The proposed solution entails cryptographic endorsements by experts or established institutions that can be algorithmically verified, e.g., via a smart contract. While manipulations of individual documents can also be detected when only digital signatures are used, a blockchain can make it clear when certain documents are added or removed and establish a chronological event log that is publicly verifiable. In our system, transparency does not come at the cost of privacy. We design a privacy-by-design solution that stores verifiable documents in a decentralized, non-replicated way using digital wallets. (Solutions based on digital wallets are, for example, currently being implemented in the European Union). Based on authentic identity data and obfuscated transaction histories on-chain, investors can demonstrate that they have all the documents required to prove that a certain investment in an artwork is legitimate. This approach keeps sensitive data confidential while providing a transparent record on-chain. This record proves that the transactions were legitimate and complied with all the rules specified by a smart contract using zero-knowledge proofs. Based on this on-chain record of obfuscated history, investors can also prove compliance with authorities and collect documents in their wallets facilitating future transactions. This solution brings transparency to the industry by facilitating due diligence and dramatically reducing the risk of data breaches.

Registering an artwork

When an artwork is sold/purchased or whenever the art owner wants to register his/her artwork or collection, he/she or whoever is acting on his/her behalf (for example, an auction house) accesses the blockchain and inserts the first set of data (Fig.7.16). Like the data contained in artwork labels commonly used in museums and galleries, these data provide high-level information, such as a short description, the name of the artists, size and materials, year and collection. Although this information is simple, as it emerges from interviews with industry experts, it is important because it can help, for example, identify forgeries. If needed, some information

can be offuscated, such as the location in Fig.7.16, and made available on request only to selected parties. Once the artwork is registered, multiple sets of data can be recorded. Every due diligence is case-specific, and some checks may be irrelevant or non-applicable. However, key verifications apply to any artwork, such as provenance and authenticity proof, source of funds, and identity checks. Fig.7.16 shows the set of verifications that can be performed after registering an artwork. Information can be made publicly available or offuscated, disclosing only the hash of the data. Sensitive data are not collected in any form and verifications are undertaken through ZKPs. Figs.7.17 and 7.18 show the verification that can be undertaken, respectively, for the artwork and for the client and the transaction. As we can see, these verifications closely reflect the key due diligence steps and the method for verifications described in in Figs. 7.14 and 7.15. Information can be made visible with the owner of the artwork's permission. Once the artwork is registered, the system assigns a weight to each verification to provide a *transaction score* that allows authorities and investors to understand the level of risk associated with that transaction. Documents and proofs supporting verifications have a positive score, while a negative score reflects a risk. An overall low score does not automatically mean that the transaction is not legitimate. It simply means that a risk has been detected and a more in-depth examination is recommended. The proposed blockchain solution is not designed to take automatic actions, such as blocking transactions with a low score. This is because the fine arts sector is highly complex and any decision should be subject to human scrutiny. The score is meant to be a tool to help identify risks efficiently. The score also allows comparison between transactions, facilitating investors' decision-making process. It also provides institutions and regulators with valuable information to decide if a transaction needs to be further investigated for money laundering purposes. The scoring mechanism is described in detail in the next section.

Scoring transactions to identify risks

Based on research and expert interviews, the verifications have been divided into groups to reflect their relevance (Fig. 7.19). The first group constitutes the core

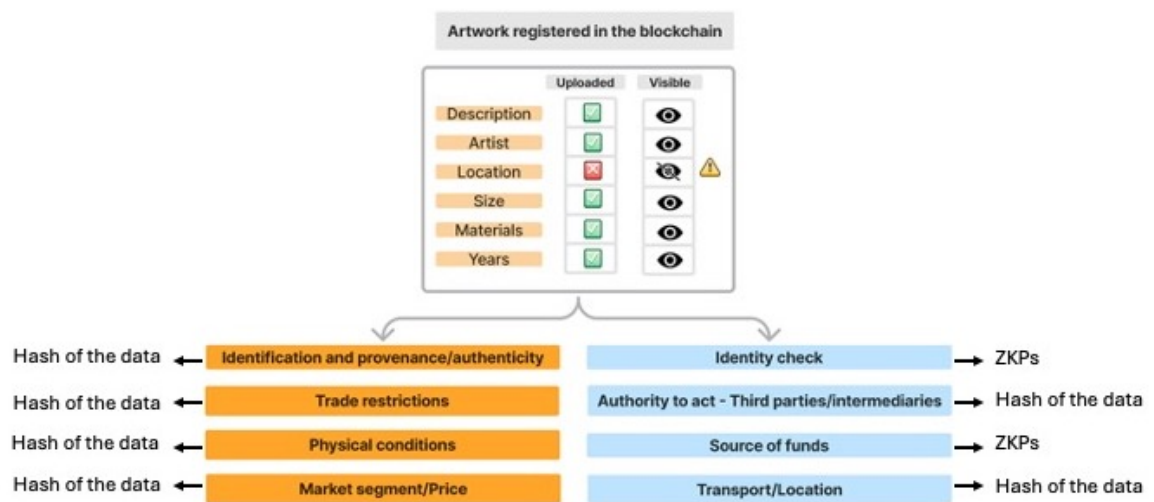


Figure 7.16: BC solution using ZK protocols

of due diligence and is considered a barrier before proceeding to the next step. This is because (I) the Provenance and authenticity of the artwork, (II) the client's identity check, and (III) the source of funds are fundamental for risk assessment. Transactions with unsatisfactory scores in these categories should not be processed without further investigation. As explained in the previous section, this is a strong recommendation, but no automatic action is undertaken by the system, except signalling the transaction with a warning. The transaction score is structured to assign the same value to the documentation (for example, the provenance report) and the proof supporting the truthfulness of the documents (for example, the expert's digital signature). The identity check follows the same steps to verify the client's identity in the UK, and it includes all physical parties involved, including intermediaries. Suppose that we are not dealing with a physical person. In that case, verifications are undertaken on the company or other legal entity through the company registries and by identifying the owner/beneficial owner identity. The system ensures that potential intermediaries have their identities fully verified to prevent malicious actors from bypassing the verification using an empty structure of Chinese boxes. For this reason, the lack of a valid power of attorney (or authority to act) authenticated by a valid digital signature or the failure to identify even one intermediary leads to an unsuccessful identity check. Similarly, identifying the source of funds is

Identification and provenance/authenticity			Trade restrictions		
Provenance	Uploaded	Visible	Laws, regulations	Yes/No	Visible
Hash of the report	☒	☒	UNESCO 1954 Convention [1]	☒	☒
Digital signature/s	☒	☒	UNESCO 1970 Convention [2]	☒	☒
Queries	Yes/No	Visible	UNIDROIT 1995 Convention [3]	☒	☒
Art Loss Register	☒	☒	CITIES [4]	☒	☒
Interpol - Stolen Works of Art Database	☒	☒	Regulation (EU) 2019/880 [5]	☒	☒
International council of Museums- Red Lists	☒	☒			
UNESCO- List of World Heritage in Danger	☒	☒			

Physical conditions			Market segment/Price		
Insurance	Yes/No	Visible	Artwork valuation	Yes/No	Visible
Hash of the report	☒	☒	Hash of the report	☒	☒
Digital signature/s	☒	☒	Digital signature/s	☒	☒
Queries - KN protocol			Queries		
Insurance cover amount	☒	☒	Artnet/Artprice	☒	☒
Artwork pictures			Queries - KN protocol		
HD pictures	☒	☒	Previous sales	☒	☒
LD pictures	☒	☒			

[1] United Nations Educational, Scientific and Cultural Organization (UNESCO) 1954 Convention for the Protection of Cultural Property in the Event of Armed Conflict

[2] UNESCO 1970 Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property

[3] 1995 (UNIDROIT) Convention On Stolen Or Illegally Exported Cultural Objects

[4] Convention on International Trade in Endangered Species (CITES) of Wild Fauna and Flora

[5] Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the introduction and the import of cultural goods also command important attention

Figure 7.17: Artwork verifications in the blockchain

Identity check		
ID Check - KN protocol	Uploaded	Visible
Passport/ID		
Bank statement/ energy bill		
	Yes/No	Visible
Queries		
Company Registries		
Beneficial ownership Registries [7]		
Laws, regulations		
AML Laws and regulations [8]		

Authority to act - Third parties/intermediaries		
ID Check - KN protocol	Yes/No	Visible
Passport/ID		
Bank statement/ energy bill		
Power of attorney/ signed letter		
Hash of the document		
Digital signature/s		

Source of funds		
Queries - KN protocol	Yes/No	Visible
Amount of money		
Cryptocurrency		
Cash/anonymous payment/debit/credit card		
Funds from non AML jurisdictions [8]		

Transport/Location		
Transport documentation	Yes/No	Visible
Hash of the documents		
Digital signature/s		
Location/custody		

[6] Under development in several countries, UK Registers of beneficial ownership, EU Beneficial ownership registers interconnection system (BORIS)

[7] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations

[8] Bank located in a non-AML regulated jurisdictions according to Financial Action Task Force (FATF).

Figure 7.18: Client and transaction verifications

paramount. The Financial Action Task Force (FATF) is a global organization that promotes international standards to mitigate the risks related to money laundering and terrorist financing. Payments from countries that do not meet FATF standards constitute an additional risk, so they are assigned a negative score. All payments need to be traceable. Therefore, a negative score is assigned when the funding source (sender and receiver) cannot be identified. As recommended by experts, in this case and the transaction is signaled as high risk even in absence of other *red flags*. Multiple transactions are legal and allowed. However, they represent a risk because large payments can be hidden behind a series of small payments). The negative score ensures that if the transaction presents another risk point, such as payments from non-FATF countries, the overall score will be below the minimum, and the transaction is signalled for further investigation.

If a transaction passes the first verification group, it is transferred to the second group of verifications, which are (IV) trade restrictions checks, (V) physical condition assessment, (VI) market segment/price and (VII) transport/location documents. Some artworks are subject to trade restrictions and are exposed to the risk of illegal sales/purchases. This risk is reflected in the negative score assigned to the category. As in other cases, a risk is reflected by a negative score, which is returned to zero if the verification through international registries is successful. The physical conditions of the artwork can be verified through insurance documents (such as reports endorsed by digital signatures) and images (where high-definition pictures are regarded as more reliable and therefore have a higher score). To prevent price manipulations, it is essential to understand if the artwork's sale price is aligned with previous sales or the market segment. It is worth noticing that artwork prices can legitimately vary; nevertheless, if this happens without a reasonable justification, it can signal a risk of money laundering activities. It is evident that an expert-endorsed valuation is more reliable than identifying the market segment through online research. This consideration is reflected in the higher score assigned to expert valuations, verification of previous sales, and digital signature endorse-

ments. Finally, documents regarding the artwork's transport, location, or custody are examined, considering the presence of an endorsement of the parties involved in the transportation or custody.

At the end of the verification process, the system outputs a YES/NO answer as a result of the first group of verifications (I-provenance and authenticity of the artwork, II-client's identity check, III-source of funds). A negative response means that the transaction is automatically signaled as high risk and notifications are sent to the parties involved recommending that they perform additional checks. A positive answer will make the transaction proceed to the second group of verifications (IV-trade restrictions checks, V-physical condition assessment, VI-market segment/price and VII-transport/location). This second step of the transaction scrutiny results in an overall score (Low/Good/Excellent), where excellent represents a transaction with complete positive verifications. Fig.7.19 is an example of how the transaction score can work and exemplifies how the weight is assigned to different verifications. It is important to note that the 100-point score assigned to each verification group is arbitrarily decided to ease the calculation. However, the parameters in each group do not require any interpretation as they can be represented as Boolean variables. Consequently, assigning a different weight to categories would not affect the transaction score, provided that the overall criteria and proportions are maintained. The resulting score represents a valuable guide for investors and authorities regarding the transaction and its risk of being involved in illicit activities.

TRANSACTION SCORE (TS)	
I - Provenance and authenticity	100
Provenance report	25
Expert's digital signature	25
Authenticity report	25
Expert's digital signature	25
II - Identity check	100
<i>Physical person</i>	
Passport/ID	50
Bank statement/energy bill	50
	OR
<i>Other legal entity</i>	
Company registry	20
Beneficial owner Passport/ID	40
Beneficial owner Bank statement/energy bill	40
	AND/OR
<i>Intermediaries</i>	
NO intermediaries	0
NO Power of attorney/signed letter/authority to act AND/OR NO Intermediary identification + digital signature	-100
III - Source of funds	-100
Funds from non FATF countries	-30
Multiple transactions	-20
Source of funds not traceable (cryptocurrencies/cash/ anonymous payment)	-50
TS<200	Additional investigation needed
TS=200	Pass
IV - Trade restrictions (check not performed=0)	100
Proof of verification for: UNESCO 1954/UNESCO1970 /UNIDROIT 1995/UNIDROIT 1995/CITIES/Regulation EU 2019/880	100
Presence of any trade restriction	-50
V - Physical conditions	100
Insurance documents report/expert report	40
Digital signature	25
HD Pictures	25
LD Pictures	10
VI - Market segment/price	100
Expert Valuation/previous sale	55
Expert Digital signature	25
Market segment	20
VII - Transport/Location	100
Transportation documents/location/custody	50
Digital signature	50
200<TS<400	Low
400 <=TS<=550	Good
TS>550	Excellent

Figure 7.19: Transaction Score

Technical implementation

Zero-Knowledge Proofs (ZKPs) are cryptographic protocols that allow one party (the prover) to demonstrate to another party (the verifier) that a given statement is true, without revealing any underlying data or the proof itself. This unique property makes ZKPs particularly valuable in compliance scenarios where sensitive information must be validated, but confidentiality must also be preserved.

In the context of regulatory due diligence, ZKPs can be used to prove that a client has passed a Know Your Customer (KYC) check, that funds originate from a legitimate source, without disclosing personal identity documents, bank account numbers, or underlying score components. This ensures that verifications are conducted transparently and verifiably, while maintaining GDPR-compliant data minimisation. Within the proposed system architecture, ZKPs support the implementation of selective disclosure: compliance validators can attest to specific attributes (e.g., "the client is not a politically exposed person" or "the valuation range is consistent with prior sales") without revealing full documentation. This mechanism enables privacy-preserving validation of identities, provenance, and risk scores on both private and public blockchains, removing the need to broadcast sensitive data while maintaining cryptographic assurance of correctness. Thus, ZKPs serve a dual purpose in the compliance process: they enforce accountability by ensuring validations are auditable, and they maintain privacy by ensuring that only authorised conditions, not underlying inputs, are exposed in the verification process. For example, Zero-knowledge proofs (ZKPs) can be applied to verify the source of funds, which is one of the most crucial verifications for AML compliance.

In traditional financial due diligence, the buyer must disclose sensitive information (e.g., bank account balances, transaction history) to the seller or auction house to demonstrate that funds are legitimate. However, this process creates significant privacy and security concerns. ZKPs offer a cryptographic alternative: they allow the buyer (prover) to prove that their funds meet the necessary legal and financial conditions, for instance, they are from a legitimate bank account and do not exceed a given threshold (e.g. $\text{transaction} < \text{£}10.000$), without revealing any

underlying data. The process involves three main components: (I) *Commitment Generation*: The buyer's bank generates a cryptographic commitment to the underlying financial details, such as account balance and source of funds, concealing the actual data while securely binding it to the proof. (II) *Proof Construction*: A ZKP is then generated (by the bank) to prove that the committed data satisfies a regulatory condition (e.g., "Transaction < £ 10.000") without revealing the actual value. (III) *Verification*: The auction house, acting as the verifier, checks the validity of the ZKP using public parameters (e.g., a verification key), without learning the buyer's private financial details or the original data behind the commitment. This approach ensures that the integrity and compliance of the transaction are maintained while giving the buyer full privacy over their financial position. The result is a privacy-preserving, cryptographically secure system for anti-money laundering (AML) and Know Your Customer (KYC) compliance that aligns with the confidentiality needs of high-net-worth individuals and institutions operating in opaque markets such as fine art.

We assume that all stakeholders, investors, artists, fine arts experts, and auction houses have a digital identity wallet that stores cryptographic keypairs and digital attestations [206]. Such digital identity wallets are currently being explored globally. For example, the European Union is working to provide their citizens with a digital identity wallet that stores not only national identity cards but also further electronic attestations of attributes, such as digital driver's licenses, membership cards, etc. [207]. Similar digital identity wallets are already available to Bhutan and Canadian citizens and are being developed in Switzerland and Korea [208]. Many of these projects are designed to provide institutional wallets to businesses and other types of organizations. The Global Legal Entity Identifier Foundation (GLEIF) [209] is currently working on a system that enables clear and unique identification of legal entities that participate in any transaction globally. This solution Facilitates surveillance activities such as Know-Your-Customer (KYC) and Anti-Money Laundering (AML) processes to ensure counterparty transparency across many sectors, including financial services, supply chain, trade finance, and payments. Furthermore,

many of these wallets already implement special forms of ZKPs (for example, the verifiable organization network of Canada) or will probably support ZKPs in the near future [210] for example, the European Digital Identity Wallet (EUDIW). This European Union initiative aims to provide citizens, residents, and businesses with a secure digital identity fully controlled by the owner. The wallet allows individuals to store and manage personal information, such as identification cards, diplomas, and bank details, facilitating access to public and private services for EU members. The European Commission has recognized the potential of ZKPs to enhance privacy and is planning the future integration of this technology. This proactive approach is testified by the Commission's call for tenders to develop privacy-preserving solutions, such as mechanisms to verify age using ZKPs [211].

Based on the consideration above, we make the assumption that all stakeholders involved in the fine arts market have digital attestations confirming their digital identity. These digital identities have multiple uses in the proposed solution. Investors can provide evidence of their nationality and use this proof to demonstrate that they are not on the sanction lists [206]. Fine arts experts can demonstrate their professional background by means of their digital diplomas or employment certificates. They can also certify the authenticity of the artworks through digital attestations that can be issued to their respective owners [212]. Storing identity-related information on a blockchain is not particularly useful because its authenticity and integrity are already ensured by digital signatures and trusted systems such as today's Web PKI (Public Key Infrastructure) that already enable secure communication over the Internet by using digital certificates and encryption. However, for information that needs to be verified by multiple stakeholders, such as proving the artwork's provenance or the correct processing of transactions, the blockchain can add value by enhancing transparency and providing verifiable proof.

Here, we provide a description of what the lifecycle of an individual artwork could look like. For simplicity, we do not consider fractional ownership and assume that every artwork is owned by a single investor [213, 214]. Although we want to use the blockchain network to cryptographically anchor the transaction history of

artwork for public verifiability, we also note that public visibility of information such as the owner or the price paid is, in general, not desirable. Therefore, we only publicly obfuscated (hashed) data on the blockchain while keeping sensitive information off-chain and only disclosing ZKPs for the correct processing of these transactions in case this is required. The lifecycle of an artwork starts with its registration. This registration is handled by a smart contract that can access external data via an Oracle. For example, it can retrieve public keys from a registry maintained by a consortium of auction houses, as well as access lists of accredited experts, organizations, and public sanctions. This registry can also include a revocation list to make sure that, for example, stolen or lost ID cards and other credentials relevant to individuals and organizations in art markets can be reported to prevent future use. Any certified expert can submit the registration of an artwork that is accepted by the smart contract. The expert has two options: they can either sign the transaction directly, which reveals their identity, or they can generate proof of membership within the set of authorized public keys. The latter option allows them to remain anonymous, preventing disclosure of the total number of artwork registrations they have conducted, which could reveal sensitive business information. Experts may include additional information about the artist and their qualifications for the registration, documentation supporting the provenance of the work, and information about the current owner if authorized. The smart contract will store an obfuscated cryptographic fingerprint (hash) of all of these data. To prevent a preimage attack (cryptographic attack in which an attacker attempts to find an original input *-preimage-* that produces a given hash value), a randomly generated number *-entropy-* should be added to the document before hashing. This ensures that no meaningful information about the original document can be inferred from its hash. In addition, experts or anyone who owns the data can decide to disclose additional information from these documents or statements derived from them. These statements, known as 'predicate proofs,' allow them to prove certain facts without disclosing the full content of the documents using ZKP. For instance, while the identity of the initial owner will usually remain confidential, it may be helpful to disclose their nationality or proof that

the initial owner is not on a sanctions list to which the smart contract also has Oracle access. For example, Eden Network (multichain infrastructure platform [215]) uses a smart contract to track sanctioned entities. Investors can prove they are NOT on the sanctions list using a digital wallet containing government-issued identity data. A zero-knowledge proof (ZKP) system ensures they can prove this without exposing their full identity. The figure in Fig. 7.20 summarises the concepts above showing how data can be verified using ZKPs.

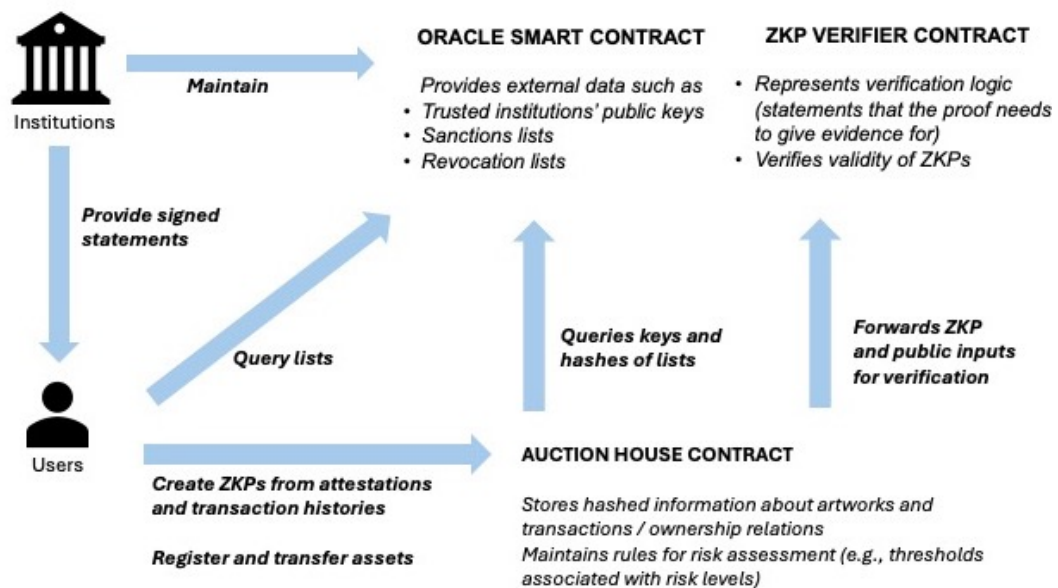


Figure 7.20: Example of verification using ZKPs

This proposed solution highlights that machine-verifiable provenance records and identity attestations can create a strong foundation to assess compliance. However, these verifications are only part of the solution. We propose a risk-based approach that is widely used in other sectors, such as finance. Our risk-based model integrates automatic verifications with contextual risk assessment, evaluating the likelihood and impact of potential risks. This means that compliance is not just about confirming identities or verifying provenance through automated processes; it also involves expert judgment, regulatory interpretation, and risk management.

Chapter 8

Conclusions

8.1 Answer to the research question

The purpose of this study was to (I) understand if and how blockchain technology can help increase transparency in fine art and real estate, and (II) design a blockchain-based solution to increase transparency, thus helping authorities and investors identify and mitigate risks of money laundering.

The first part of the research question brings the following granular questions. (Ia) What are the key features of the fine art and real estate industries and what makes them vulnerable to money laundering? (Ib) What characteristics of blockchain technology make it a valuable tool to enhance transparency?

We answered these questions through a thorough analysis of blockchain technology and the fine arts and real estate sectors, undertaken in Chapter 2, 3 and 4. Although real estate and fine art represent two different categories of alternative assets, they exhibit some similarities, such as relative illiquidity (compared especially to stock and bonds), the presence of intermediaries, and the large amount of information required to conclude a transaction. Additionally, they are both well-known targets for money laundering activities because of the large monetary transactions involved and the relative ease of disguising illicit funds. From the research, it also emerged that both sectors can benefit from a system that allows easy and reliable verification of ownership, clients' identity, beneficiaries and intermediaries, source

of funds, and record of transaction history. Blockchain can significantly benefit the fine art and real estate industry by improving efficiency and transparency and enhancing due diligence. In fine art, provenance is crucial to establishing ownership and is paramount in estimating artwork's value, as stated by the International Valuation Standard Council (IVSC). Provenance is also central to museum practice as institutions rely on it for their collections. In real estate, a blockchain system is attractive because it could reduce the total time to complete a sale by automating the entire transaction process. Combining blockchain technology and smart contracts can reduce the time and costs of transactions, facilitate due diligence, and promote transparency. This research delves into the potential of the technology beyond cryptocurrency, highlighting how Blockchain has core applications in real estate and fine art. It can increase transparency and traceability by creating immutable records of provenance and ownership, thus facilitating the identification of assets involved in illicit activities. The technology can increase the efficiency of due diligence processes by facilitating verifications, thus promoting good governance practices. Privacy and confidentiality are paramount in fine art and real estate. The combination of blockchain and cryptography techniques, such as zero-knowledge proofs, promises to address the seemingly binary trade-off between transparency and privacy. It is important to highlight that these technologies entail a high degree of complexity, requiring the skills and knowledge of highly specialized software engineers, cryptographers, and developers. From the analysis of the case studies, it is clear that an interdisciplinary approach and a comprehensive analysis of key aspects of the technology are decisive factors in unlocking the full potential of blockchain. In addition, the knowledge and expertise of regulators and policymakers are necessary to create effective regulatory frameworks to ensure that technology benefits society, preventing misconduct and improper use of the technology.

The second part of the research question is to (II) design a blockchain-based solution to achieve increased transparency, thus helping authorities and investors identify and mitigate risks of money laundering. This part presents the following

granular questions. (IIa) What are the key features that a blockchain solution should have to help increase transparency in fine art and real estate? (IIb) What factors should a proposed solution take into account to ensure its practical applicability in the fine art and real estate sectors, rather than remaining purely theoretical?

We answer these questions by identifying crucial features to address some of the most prominent issues in the fine art and real estate industry (Chapter 5 and 6) and designing our proposed solution (Chapters 7). The Proof of Concept constitutes the basis of the proposed blockchain solution (HP1 and HP2). One of the key components is the scoring system that allows qualified professionals (both for fine art and real estate) to assess asset documentation. This solution is essential to ensure the quality of the data input in the ledger and maintain it over time. Qualified professionals can be invited to assess the documentation provided for a property or artwork and assign a score. This indicator (score) provides a clear idea of the accuracy and completeness of the documentation, allowing us to estimate the duration of due diligence and identify potential issues with the asset before embarking on a transaction. In real estate, this feature aligns with the need to improve the real estate transaction process, as stated by the UK government on multiple occasions. Assessing the asset's documentation at an early stage would not only facilitate due diligence but also make it possible for the buyer to legally commit to the purchase at an early stage. A presale contract can avoid gazumping, which negatively affects the market and is a common reason for transaction failures. In fine art, similarly to real estate, qualified professionals can score artwork documentation to facilitate due diligence and help identify items potentially involved in money laundering activities. It is also possible to assign professionals a score based on their experience and qualifications. This score is then used to weight professionals' assessments of artworks' documentation. This is important because fine art is less regulated and systematized compared to real estate, and there are no professional bodies that act as guarantor of professional and ethical standards. Finally, The registration and collection of artwork data meets the demand for aggregated and reliable information that is acutely perceived as a need in the industry, as emerges from interviews with

fine art experts (Chapter7).

After developing the Proof of Concept, it appears that a blockchain-based registry can be a promising solution to enhance due diligence and considerably contribute to increased transparency in fine art and real estate. For this reason, based on the key features developed in the Proof of Concept, we design a blockchain solution to build the first blockchain registry for fine art and real estate. The real estate sector is more structured than fine art and many countries already have a property registry. The His Majesty Land Registry (HMLR) in the UK has existed for around 160 years and has been a critical institution protecting property rights. Keeping a record of the ownership of the property allows the property to be transacted securely. New technologies have opened great opportunities to increase efficiency, and the HMLR is exploring solutions to enable properties to be bought and sold digitally, provide near real-time property information, and accessible digital register data [216]. More specifically, these are some of the HMLR's most compelling goals. (I) Improve speed of the service, (II) automate and personalize conveyancing services, (III) increase resilience to fraud and cyber threats, (IV) explore mapping unregistered land to increase transparency, (V) make the process of buying and selling property digital, (VI) complete automation of all information services, (VII) develop greater transparency and online access for people and businesses, and (VIII) promote research to take advantage of emerging technologies. The solution we designed aligns with the HMLR's main goals and expands the scope of a real estate registry to include fine art, designing the first decentralized register that records real estate and fine art transactions. Even though fine art and real estate are separate and different types of assets, they share some characteristics (as described in Chapter 2) that suggest the possibility of creating one technological solution applicable to both sectors. The fine art industry in the UK (and elsewhere) lacks a unique register to keep track of transactions, record ownership, and provide reliable information to facilitate investors' decisions. Additionally, like real estate, large amounts of money are transacted across countries, making the sector a target for criminal activities. It is also worth noting that artwork and antiques represent a unique and

invaluable inheritance of a nation and must be protected. Keeping track of ownership and recording artwork data is imperative to prevent losses and illegal trading. In the proposed solution, museums, institutions and collectors can also benefit from registering their collections in the ledger to increase visibility, facilitate due diligence and artwork loans, and easily track and prove ownership. The register also helps to prove authenticity, as qualified professionals can assess and digitally sign documents. For particular assets, such as luxury real estate or museums, artworks can be linked to the property they belong to facilitate traceability. This option can reduce the risk of losses and misappropriation of valuable items. The increased transparency provided by the proposed solution can significantly help authorities identify properties potentially involved in illicit activities. Money laundering prospers in opaque environments, as funds unlawfully acquired need to be hidden behind multiple intermediaries, unidentified companies, beneficial owners, inflated valuations, and untraceable sources of funds. Moreover, the cross-national nature of the blockchain allows a faster and easier collaboration between countries to join forces to fight these criminal activities. The proposed blockchain registry provides a transaction score (Low, Good, Excellent) based on a clear and comprehensive assessment of the risks associated with the asset, whether in real estate or fine art. The transaction score for fine art and real estate is a key mechanism that helps investors and authorities identify assets potentially involved in money laundering. The score is divided into two main steps. The first consists of evaluating the most critical parameters, such as provenance, client identity, and source of funds. If the score in this first step does not reach a minimum threshold, the transaction is automatically signalled as high-risk and strongly recommended for further investigations. If this first phase gives a positive outcome, other criteria are evaluated, such as physical condition, value according to the market segment, and more in order to provide the final score. It is worth highlighting that if a transaction does not pass the first verification step, it does not mean that it is automatically associated with illicit activities. Fine art and real estate are highly heterogeneous sectors, each encompassing a wide range of distinct cases and it is important to allow some flexibility. However, the

score signals that the verification is not satisfactory and a deeper scrutiny is highly recommended.

It is important to note that a blockchain solution that permanently records data might infringe privacy rights and compromise the confidentiality so much needed in the real estate and fine art sectors. These aspects are easier to manage on the permissioned blockchain as the network is composed of only trusted nodes. This hypothesis is explored in the HP1 (Chapter 7, Section 7.1). In this case, the decentralized ledger is shared among a network of trusted members, such as public institutions and authorities, for example, the HMLR, the relevant UK Ministry and professional bodies. This solution was selected for the UCL Knowledge Exchange Program to develop a Minimum Viable Product (MVP) funded by UCL Business and Enterprise. The MVP was developed in Java to be deployed on Hyperledger Fabric, a private blockchain that is particularly suitable for this case. Among other advantages described in Chapter 7, Fabric offers flexible solutions to guarantee the privacy of data and transactions, which allows the creation of an environment particularly suitable for fine art and real estate registries.

The awareness that private blockchains provide weaker security than public ones has motivated us to develop a fine art and real estate registry optimized for a public blockchain. This hypothesis is explored in HP2 (Chapter 7, Section 7.2). The main challenge lies in the apparent contradiction between privacy and transparency, arising from the need to share and store due diligence information while maintaining confidentiality. In this hypothesis, we use zero-knowledge proofs to enable private transactions on a public blockchain. Fundamentally, a zero-knowledge proof constitutes a method in which an individual (the *prover*) persuades another party (the *verifier*) that a particular statement is true while revealing no information about the underlying data that proves the truth of the assertion. The proposed solution allows for a public register for fine art and real estate on a public blockchain, ensuring high security and privacy. Given the crossnational and potentially global nature of the blockchain network, it will also enhance the collaboration between countries to prevent money laundering and other criminal activities. The solution does

not rely only on machine-verifiable data and identity attestations, but introduces a risk-based approach as implemented in other industries, such as the financial sector. However, due to the peculiarities and heterogeneity of the fine arts and real estate sectors, transactions pose additional complexities. For this reason, the expertise of industry professionals was essential in developing a due diligence mechanism and a scoring system that ensures compliance, improves efficiency, and helps mitigate risks.

The two proofs of concept developed in this research (Chapters 5 and 6) serve as the technical foundation for the proposed solutions HP1 and HP2 (Chapter 7). The first focuses on the fine art sector, where it develops key features such as provenance certification, risk scoring, and conditional asset transfer through smart contracts written in DAML. The second focuses on the real estate sector, implementing domain-specific smart contracts for title verification, document validation, and escrow-style workflows, also using DAML. Both PoCs showcase essential features through smart contracts required for a blockchain-based compliance registry and form the basis for the proposed hybrid solution (HP1), which evolves into a minimum viable product (MVP) on a permissioned blockchain. Simultaneously, they underpin the theoretical design of HP2, which explores how the registry could be extended to operate on a public blockchain infrastructure with privacy-preserving guarantees. Together, these implementations ensure that the proposed architectures are not only conceptually sound but also technically grounded and reproducible.

The two proposed architectures, HP1 (semi-private blockchain) and HP2 (public blockchain with ZKP), (Table 8.1) do not differ in asset class (both can be used for fine art and real estate) but in their foundational governance and technical models. HP1 relies on a permissioned architecture governed by identifiable institutions and actors such as solicitors, professional bodies, or land registry. This structure ensures strong legal accountability and supports compliance with regulations, for examples, the UK laws. HP2, in contrast, envisions a decentralised registry where transactions are verified on a public blockchain using zero-knowledge proofs. This

model enhances cross-jurisdictional auditability and anonymity while maintaining verifiability, but requires more advanced cryptographic infrastructure and stakeholder coordination. Technically, HP1 is easier to deploy using established tools such as DAML and Hyperledger Fabric, whereas HP2 introduces greater complexity due to ZKP implementation. From an adoption perspective, HP1 is more feasible in near-term regulatory contexts, while HP2 aligns with longer-term ambitions around scalability, interoperability, and cross-national cooperation. In practice, HP1 is better suited to high-trust environments involving licensed actors, clear jurisdictional control, and formal legal registries. HP2 becomes preferable when dealing with international asset transfers, multiple regulatory regimes, or low-trust contexts where privacy-preserving compliance is paramount. Together, these models offer a dual-path framework adaptable to both institutional settings and future decentralised ecosystems.

The blockchain architecture presented in this thesis offers a transformative contribution to anti-money laundering (AML) efforts in fine art and real estate by enabling a digital infrastructure where compliance becomes a built-in feature of the transaction process rather than a retrospective investigation. Through structured data layers and programmable workflows, the system introduces algorithmic verifiability of ownership, identity, and provenance, reducing opportunities for manipulation and anonymity that are commonly exploited for criminal activities. The integration of a scoring mechanism for transactions enables contextualized risk evaluation, while automated alerts and red-flag triggers help institutions respond proactively to suspicious patterns. Importantly, this increase in transparency does not come at the cost of privacy: using RBAC (HP1) and ZKPs (HP2), the platform ensures data confidentiality and compliance with GDPRs and other international privacy standards. By offering a common data structure and verification logic, the solution facilitates cross-border information sharing and harmonization of due diligence practices, addressing one of the most persistent weaknesses in global AML enforcement. In doing so, this research contributes not only a novel artefact but also a replicable governance framework capable of improving compliance, trust, and oversight in

two historically opaque markets.

	HP1 (Section 7.1)	HP2 (Section 7.2)
Type of Blockchain	Private/ Consortium	Public
Governance model	Centralised or semi-centralised	Decentralised
Level of development	MVP	Theoretical investigation
Funding	UCL Innovation and Enterprise	No
Privacy and confidentiality	Role-Based Access Control (RBAC)	Zero Knowledge Proof (ZKPs)
Registry for both fine art and real estate	Yes	Yes
Solution showcased for	Real estate	Fine art
Real-world readiness	High	Lower due to the complexity of decentralised architecture
Security	More vulnerable due to semidecentralised architecture	High
RedFlags and transaction scoring	Yes	Yes

Table 8.1: Comparative analysis Proposals (HP1, HP2)

A comparative analysis of public versus semi-private blockchain infrastructures reveals distinct trade-offs in terms of governance, scalability, privacy, and regulatory alignment. Public blockchains (e.g., Ethereum, Bitcoin) offer full decentralisation, immutability, and censorship resistance, making them suitable for use cases that benefit from open verification and global accessibility. However, they pose limitations for compliance-sensitive domains due to their inherent transparency, limited throughput, and challenges around GDPR compliance and data erasure. (For this reason, in HP2 we explore the use of ZKPs to ensure compliance with regulations such as GDPRs and maintain privacy). In contrast, semi-private (or permissioned) blockchains, such as those built using DAML on Canton or Hyperledger Fabric (HP1), enable finer control over participant access, role-based visibility, and transaction privacy. These features make them more appropriate for applications where data confidentiality, role attribution, and legal enforceability are essential, such as client onboarding, escrow execution, and multi-party compliance verification. In

such contexts, validators are known entities (e.g., museums, auction houses, or legal bodies), and consensus is achieved through trusted cooperation rather than open mining or staking. Selection criteria between public and semi-private models should include: (1) the sensitivity of the data to be stored or referenced; (2) the need for interoperability with external actors or registries; (3) the level of regulatory oversight and auditability required; and (4) the ability to enforce off-chain contractual obligations.

Dimension	Public Blockchain	Semi-Private Blockchain
Governance Model	Decentralised, open participation; consensus by anonymous nodes (e.g., PoW, PoS)	Permissioned governance; validators are known, trusted entities
Data Transparency	Fully transparent and publicly readable	Granular access control; data visible only to authorised roles
Privacy and GDPR Compliance	Challenging due to immutable and public data; right to erasure is problematic	Privacy-preserving by design; supports selective disclosure and controlled data retention
Transaction Throughput and Scalability	Often limited (e.g., 10–30 TPS on Ethereum); subject to congestion and fees	Higher performance; optimised for enterprise-scale use and regulated environments
Security Model	High cryptoeconomic security through decentralised consensus; resistant to collusion and censorship	Relies on institutional trust and legal governance; more vulnerable to internal misbehaviour but easier to audit and control
Example Platforms	Ethereum, Bitcoin, Tezos	DAML on Canton, Hyperledger Fabric, R3 Corda

Table 8.2: Comparison of Public vs Semi-Private Blockchain Architectures

8.2 Challenges and limitations

Blockchain technology has increasingly gained traction in multiple industries in recent years. Although blockchain has various applications, its popularity is mainly associated with cryptocurrencies such as Bitcoin and Ethereum. Unfortunately, they are often associated with negative connotations. One of the main reasons for distrust is that blockchain technology allows for global transactions without geograph-

ical restrictions and in complete anonymity. This is not the case for the proposed solution, where parties can be identified before being admitted to the network (HP1, permissioned blockchain) or through ZKPs (HP2, public blockchain). However, although substantial, these differences may be perceived as technical details without significant impact on the acceptance of technology. Additionally, blockchain technology is characterized by a high degree of complexity that requires trust in a system that remains substantially unknown. Technology has been frequently designated as too complex to attract a large amount of attention [180]. Key actors in the fine art sector, such as collectors, investors, and auction houses, may not be willing to trust the solution with their data, thus hindering its adoption. In fine art, other difficulties might lie in the peculiar characteristics of physical artworks. The attribution of old Master paintings, for example, is often reassessed, and paintings can be identified as the work of different artists years down the line. Artworks are sometimes sold under deliberately vague attributions ('From the School of Leonardo', for example) while research is ongoing. The closed nature of provenance-tracking on the blockchain does not allow for changes and may leave permanent inaccuracies. Any erroneous input to the ledger would not allow modification, limiting the possibility of audit and correction [141]. Because data can be updated but not cancelled, in the long term, the ledger might show misleading information due to the on-chain presence of outdated or incorrect information and the right inputs. Other barriers to entry for the proposed solution might be related more generally to the relative novelty of blockchain technology. The lack of standardization and interoperability between different blockchain platforms can create challenges when integrating blockchain into existing systems and platforms currently used in the sector. Although blockchain technology shows potential to improve real estate transactions, obstacles might impede or delay the widespread adoption of the technology in the industry. The real estate sector is well known to resist change and be allergic to the adoption of new technologies [217, 218]. The adoption of blockchain technology may involve a considerable degree of technical know-how and resources, encompassing the creation of tailor-made smart contracts and applications. As such, this

may pose obstacles for small-scale companies or entities with limited resources.

Despite the inherent security features designed into blockchain technology, apprehensions persist about possible security breaches and hacking. Given the sensitive nature of real estate and fine art transactions, which involve the exchange of confidential financial and personal information, ensuring security becomes a crucial concern. The technology uses private keys which serve the dual purpose of decrypting encrypted data and generating digital signatures by encrypting a document's hash value. These keys are complex alphanumeric strings that require secure storage. The absence of a backup in the event of loss of a private key results in permanent denial of access to the data encrypted with that key. Moreover, quantum computing poses an additional threat to network security. Using the principles of quantum mechanics, quantum computers process large amounts of data in parallel. In future, they could theoretically compromise digital signatures by reverse computing hash values and forging transactions [135]. Finally, there are some considerations to take into account with respect to ZKPs. Although zk-SNARKs are efficient to verify, one limitation is that generating these proofs is computationally intensive. The process requires reformulating the algorithm so that the correct execution can be represented by properties of polynomials that are evaluated using complex cryptographic techniques. This means that while the verifier does not need high computational power, the process of ensuring compliance can be expensive for the prover, hampering the widespread adoption of the technology.

8.3 Final considerations and further studies

Despite the challenges, we believe that a blockchain registry for fine art and real estate has the potential to significantly increase transparency. This solution would be beneficial in combating money laundering as it provides a source of reliable and accurate information for authorities and regulators. In addition, having an immutable sales record would make it difficult to manipulate prices to hide illicit gains. In fine art, other benefits can be seen in improved cooperation between institutions fostered by increased transparency. Exchanges between museums and

exhibitions can be facilitated thanks to the blockchain registry which makes due diligence faster and more efficient. Relying on extensive information about artwork can also help reduce insurance costs by allowing an accurate estimation of risks. The research shows how blockchain technology can increase transparency in real estate transactions by providing secure and decentralized data storage. Ownership, prices and all relevant information can be collected in an immutable register, where the truthfulness of data is ensured by the solicitors who, in the UK, are responsible for driving the real estate transaction process. The ledger keeps track of ownership and all parties involved in the transaction, together with a transaction timestamp, making it easier for authorities to track and identify assets involved in illicit activities.

This research contains the theoretical framework for the first public blockchain registry for fine art and real estate. Building on this study and the knowledge acquired with the first MVP funded by UCL, the next step will be to further develop the MVP including the implementation of ZKPs. For this purpose, I am working to create partnerships with established auction houses and public authorities. I firmly believe that increasing transparency in fine art and real estate is crucial for the betterment of society, to foster robust governance, and prevent criminal activities.

The study has also highlighted the importance of an interdisciplinary approach to harnessing the potential of blockchain. A high level of complexity characterizes the technology, and the knowledge and expertise of specialized software engineers are paramount. Moreover, to ensure compliance with the regulatory frame, the contribution of policymakers and regulators is crucial.

Finally, from a more general perspective, an interdisciplinary approach is required to understand the ramifications of technological power within society. The influence of technology in shaping human perceptions, cognition, and behavior is a complex subject beyond the scope of this research. Here, we simply observe that recent studies have analyzed the relationship between democracy and technology [219]. They highlight the fundamental challenges that the power of digital tech-

nologies can pose to democracy by possibly controlling human activity through code and large-scale data collection. This potential raises questions concerning the inherently political nature of technological power, despite assertions of being completely neutral made by the technology industry. Furthermore, the concentration of technological power in the hands of a minority, the potential misalignment with the public interest, and the lack of mechanisms for democratic oversight can exacerbate these concerns. As technology, including blockchain, should aim to benefit society, a thoroughly comprehensive and interdisciplinary approach should include a more political perspective to address the potential influence of technology on democratic structures. The foundation is that technology is a public good for the betterment of society and cannot be considered a prerogative of expert technologists.

Appendix A

Glossary and terminology

1. **Bitcoin.** The concept of Bitcoin was first introduced by an unknown individual (or a group of people) named Satoshi Nakamoto before it was released as open-source software in 2009. Bitcoin is a peer-to-peer cryptocurrency and a decentralized worldwide payment system for a digital currency where transactions take place among users without any intermediary. Bitcoin transactions are performed and verified by network nodes and then registered in a public ledger (blockchain) [220]. Even though the question "What is Bitcoin?" may seem naive, the answer is not trivial, and a comprehensive definition of Bitcoin can be problematic[221]. Bitcoin is usually referred to as cryptocurrency and is perceived as money by its users and supporters. Conversely, from national currencies, bitcoin is not a legal tender in any country, and there isn't a clear definition of the users' community. The community is open, and users may be virtually anyone. Moreover, the theoretical definition of money implies the perception of money as an asset, which presents additional difficulties in the case of Bitcoins. In the case of Bitcoin, it is impossible to require an exchange of issued money for another asset by the central bank and to have this relationship displayed in the bank's balance sheet. Bitcoin is not significantly associated with the banking system; there aren't Bitcoin term deposits or securities issued in Bitcoin. Even from a legal perspective, the definition of Bitcoin raises some issues as Bitcoin does not meet the criteria for the legal category of money. Bitcoin cannot be considered equal to electronic money

as it does not meet the key criteria for monetary value, such as representing a claim to the issuer, being stored on an electronic means of payment, being issued against receiving of funds in the value not less than the value of issued electronic money, being accepted as means of payment by persons other than the issuer[221]. In conclusion, despite Bitcoins being intuitively considered money, it is not possible to consider virtual currency as money.

2. **Blockchain & Cryptocurrency.** Blockchain is a digital technology that over the past ten years has increasingly gained traction in multiple industries [96, 97, 98]. The blockchain, or more generally the distributed ledger, It is a decentralized database for maintaining a permanent tamper-proof and forgery-resistant record of transactional data. Blockchain technology utilizes a peer-to-peer system that consists of nodes that make their (computational) resources available for transaction relay and verification. Each node in the distributed network maintains a copy of the ledger to prevent fraudulent alterations of the blockchain and all copies are updated and validated simultaneously [102]. Cryptocurrencies are exchanged peer-to-peer over distributed ledger platforms [222]. This process requires distributed verification of transactions without a central authority. Transaction verification confirms transaction amounts and whether the payer owns the currency they are trying to spend while ensuring that currency units are not spent twice. This verification process is called mining and is an integral part of the systems. The mining process adds records of past transactions to the distributed ledger (Blockchain), allowing users to reach a secure, robust consensus for each transaction. The Bitcoin network is secured by individual miners (any machine in the Bitcoin network can act as a miner) who are watching Bitcoin transactions continuously and trying to verify them. A block is only considered valid when it has proof of work. In an average of 10 minutes, a new transaction block is added to the blockchain in the network. The miner who mines the block gets a reward in Bitcoins, and transaction fees are obtained from all the transactions included in the block. This motivates the miners to continuously compete in

the race for finding a valid block [223].

3. **Cryptography.** The Concise Oxford Dictionary (2006) defines cryptography as the art of writing or solving codes. However, in the late 20-th century, cryptography radically changed, and a rich theory emerged, enabling the rigorous study of cryptography as a science. Modern cryptography can be defined as the scientific study of techniques for securing digital information, transactions, and distributed computations [224]. Cryptography protects the data from theft or alteration and can be used for user authentication. We will focus on the following cryptographic algorithms: public key (or asymmetric) cryptography and hash functions. The initial data is referred to as plaintext, while the encrypted text is referred to as ciphertext [145].

- **Public Key Cryptography (PKC):** uses one key to encrypt the plaintext and another to decrypt the cyphertext. One of the keys is designated as the public key and can be publicly shared and advertised. The other key is designated as private and is never revealed to third parties.
- **Hash functions:** Hash functions (also called message digests or one-way encryption) are algorithms used to encrypt information. A fixed-length hash value is computed based on the plain text, making it impossible to recover either the length or plaintext. Hash algorithms are typically used to provide a digital fingerprint of a file's content to ensure that the file has not tampered with [145]. A cryptographic hash function—such as the widely used SHA-256 algorithm— is mathematically irreversible: for a given output y , it is impossible to calculate an input x such that $h(x) = y$. This ensures the confidentiality of the information stored in the condensate. Additionally, it is mathematically impossible to find in advance two inputs of the hash algorithm yielding the same output, i.e., have two distinct inputs x and x' such that $h(x') = h(x)$.

4. **Non-Fungible Tokens (NFTs)** All information recorded on a blockchain can be considered a digital asset (or token), and the record of these assets is

immutable and tamper-proof. Through smart contracts, parties can create new types of digital assets with custom-defined parameters and properties. These tokens can then be transacted, and each transaction is recorded on the blockchain. A token's fungibility is a token feature that shows whether assets can be totally exchanged throughout the trading process. A fungible token is equivalent to other tokens of the same type and can be divided into smaller units. An example fungible token is the Ethereum native currency ETH, where each ETH token is of identical value. On the other hand, non-fungible tokens have unique value and cannot be divided. These have also been used to represent unique assets such as collectables, certificates, deeds/rights, artwork, etc. Consequently, a non-fungible token (NFT) is unique, indivisible, and distinct from other tokens of the same kind.

5. **Smart contracts.** Smart contracts are computer programs that can be consistently executed by a network of mutually distrusting nodes without the arbitration of a trusted authority [151]. The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the software architecture in such a way as to make a breach of contract prohibitively expensive [152]. The ultimate goal of smart contracts is to replace traditional contracts, enabling companies to operate with significantly fewer disputes, and minimizing the need for law enforcement or court intervention [78].
6. **Consensus algorithm.** A consensus algorithm is a protocol which ensures a common, unambiguous ordering of transactions and blocks and guarantees the integrity and consistency of the blockchain across geographically distributed nodes [225]. The consensus algorithm ensures that the transactions emerge from a legitimate source, as every participant has consented to the state of the distributed ledger. This makes the blockchain a trustless, secure, and reliable digital-transition technology. Distinct consensus mechanisms follow different principles, enabling network participants to agree on a shared history of transactions following a different set of rules. Popular ex-

amples of consensus mechanisms are proof of work (PoW) and proof of stake (PoS) [226]. For instance, the Proof of Work (PoW) is based on a computational task that can only be solved by brute force. Blockchain technology adds a new block of a transaction to the network through mining. The PoW consists of a complex cryptographic puzzle where miners try to find a value called a nonce (number used once). When the nonce is hashed with an algorithm used for hash functions (Bitcoin uses SHA-256), the resulting hash begins with a prescribed number of zeros. The average work required is exponential to the number of zeros the correct hash starts with. This shows that the Proof of Work requires high computational cost in the verification process [223]. To contain energy use while at the same time guaranteeing acceptable levels of security, some blockchains use different consensus mechanisms alternative to the Proof of Work, such as the Proof of Stake (PoS). Instead of relying on computational power as the “scarce resource”, the resource that the network security depends on is ownership of the coin itself [222]. Hence, in order to verify a transaction and receive the coin reward (whether new coins or transaction fees), a miner must own some coin himself. The probability of success in creating a new block is a function of the number of coins miners own, not computational power. Therefore, there are much lower energy costs in this transaction.

7. **Public permissionless vs Private permissioned blockchain.** A blockchain is public when it is built as an open network with no privileged actors, and everyone can see the records and the entire transaction history (although pseudonyms can protect the identity of transacting parties) [115]. Each participant can use the blockchain to carry out transactions and participate in the consensus and transaction validation. Network users can vote on new proposals to upgrade or modify the underlying protocol [116]. There is no special permission to submit transactions beyond the possession of some way to pay transaction fees. Everyone is also permitted to participate in validating the transaction [117]. Examples of public blockchains include Bitcoin and

Ethereum.

A blockchain is private (or semi-private) if the consensus process can only be achieved by a limited and predefined number of participants. Write access is given by an organization, and read permissions can be public or restricted. In this case, the consensus process is controlled by a preselected set of nodes. The private blockchain does not necessarily use mechanisms based on cryptography. Private/permissioned blockchains generally have simpler consensus algorithms due to the increased trust between endorsed participants [116]. A private or permissioned blockchain does not permit open participation in submitting or participating in the transaction validation process [117]. Examples of private blockchains include Quorum, Hyperledger Fabric, and R3 Corda.

8. **Zero-knowledge proofs.** Zero-knowledge proof (ZKP) is a cryptographic technique that permits selective disclosure of the information necessary to assess policy compliance without exposing all of the underlying information. This property may be used to ensure compliance while preserving privacy. An interesting use case is the so-called anonymous credentials, where a trusted party can attest that a user credential contains attributes whose values are correct, allowing to prove certain properties in zero knowledge way [227]. Zero-knowledge proofs enable private transactions on a public blockchain. Fundamentally, a zero-knowledge proof constitutes a method wherein an individual (the *prover*) persuades another party (the *verifier*) that a certain statement is true while revealing no information about the underlying data proving the truth of the assertion. For example, a person can prove they are old enough to buy alcohol or vote without revealing the name and date of birth printed on their ID documents. Technically, they would prove, in zero knowledge, that they have documents verified by the government, where the date of birth establishes the requisite age of the person. The proof convinces the verifier that this fact is true without revealing any other information [169].

9. **Merkle tree.** Merkle trees (or hash trees) play a significant role in verifying and retrieving data for blockchain implementation, allowing efficient and secure verification of the contents of large data structures. A Merkle tree is essentially a binary tree. Specifically, the tree's top node is called the root, and each node has two child nodes. Each node (including the root) is a cryptographic hash of its child nodes. The terminal nodes of the tree are called leaves, and it is where the actual data or its hash values are stored [228].

Appendix B

Acronyms

AML Anti Money Laundering

AEC Architecture Engineering and Construction

API Application Programming Interface

BIM Building Information Modeling

BC Blockchain

BCT Blockchain Technology

ESG Environmental Social Governance

FCA Financial Conduct Authority

GDPR General Data Protection Regulation

HMLR His Majesty Land Registry

HMRC His Majesty Revenue and Customers

IoT Internet of Things

IVSC International Valuation Standard Council

KYC Know Your Customer

KYB Know Your Business

POW Proof Of Work

POS Proof Of Stake

ZKP Zero Knowledge Proof

Appendix C

DAML code

In Chapter ?? we describe and explain some crucial parts of the DAML code developed for the Proof of Concept (Fine Art and Real Estate). The complete version of the code can be found here. <https://github.com/ClaudiaGiannoni/PhD-DAML-Code/tree/main>

Appendix D

Colophon

This document was set in the Times Roman typeface using $\text{\LaTeX}$ and $\text{\BibTeX}$, composed with a text editor.

Bibliography

- [1] Statista Research Department. Global art market volume of transactions from 2007 to 2021. <https://www.statista.com/statistics/885518/global-art-market-volume-of-transactions/>. [Accessed on 20 January 2023].
- [2] Statista Research Department. Sales value of the art market worldwide from 2007 to 2021. <https://www.statista.com/statistics/883755/global-art-market-value/>. [Accessed on 15 December 2022].
- [3] Statista Research Department. Real estate investment management market size, 2024. [Accessed: 22 October 2024].
- [4] Fabian Maximilian Johannes Teichmann. Twelve methods of money laundering. *Journal of Money Laundering Control*, 20(2):130–137, 2017.
- [5] UBS; Art Basel. Global art market volume of transactions from 2007 to 2021(in millions). Global art market volume of transactions from 2007 to 2021(in millions), 2022. [Accessed on 15 December 2022].
- [6] ArtBaselUBS. Sales value of the art market worldwide from 2007 to 2023. <https://www.statista.com/statistics/885531/global-art-market-share-by-country/>, 2023. [Accessed on 04 January 2025].
- [7] EPRA. Real estate investments on the European market. <https://www.statista.com/study/39150/investment-in-properties-in-europe-statista-dossier/>, 2024. [Accessed on 10 January 2025].
- [8] UBS; Art Basel. Distribution of online and offline sales volume at fine art auctions in selected countries worldwide in 2021. Distribution of online and

offline sales volume at fine art auctions in selected countries worldwide in 2021, 2021. [Accessed on 04 December 2022].

- [9] Natalie Chladek. What are alternative investments? <https://online.hbs.edu/blog/post/types-of-alternative-investments>. [Accessed on 20 September 2023].
- [10] Guy Fraser-Sampson. *Alternative assets: investments for a post-crisis world*. John Wiley & Sons, 2010.
- [11] H Kent Baker and Greg Filbeck. *Alternative investments: Instruments, performance, benchmarks, and strategies*. John Wiley & Sons, 2013.
- [12] BlackRock. Alternative investments in modern portfolios. <https://www.blackrock.com/institutions/en-us/insights/portfolio-design/alternatives-in-modern-portfolios>. [Accessed on 20 September 2023].
- [13] Statista. Composition of alternative investors' portfolio worldwide in 2020, by asset class and investor type. <https://www.statista.com/statistics/1230272/portfolio-composition-by-investor-type/>. [Accessed on 04 October 2023].
- [14] Mark JP Anson. *The handbook of alternative assets*. John Wiley & Sons, 2003.
- [15] Noël Amenc, Lionel Martellini, and Mathieu Vaissié. Benefits and risks of alternative investment strategies. *Journal of Asset Management*, 4:96–118, 2003.
- [16] IVSC. Perspectives Paper: The Art of Valuing Personal Property with IVS. 2021.
- [17] Dror Poleg. *Rethinking real estate: A roadmap to technology's impact on the world's largest asset class*. Springer, 2020.

- [18] Mark JP Anson, Frank J Fabozzi, and Frank J Jones. *The handbook of traditional and alternative investment vehicles: investment characteristics and strategies*, volume 194. John Wiley & Sons, 2010.
- [19] Savills. Change in real estate investments worldwide in 1st half 2020, by region. <https://www.statista.com/statistics/1192037/real-estate-investments-change-worldwide/>, 2022. [Accessed on 10 January 2025].
- [20] Fausto Martin De Sanctis. *Money Laundering Through Art A Criminal Justice Perspective*. Springer International Publishing Switzerland 2013, 2013.
- [21] Pablo Cortés. Scope of Application. *The Singapore Convention on Mediation*, 1937(I):63–85, 2023.
- [22] Tim Edmonds. *Money Laundering Law*. House of Commons Library, 2018.
- [23] Office on Drugs and Crime. Money Laundering. <https://www.unodc.org/unodc/en/money-laundering/overview.html>. [Accessed on 23 June 2023].
- [24] Vandana Ajay Kumar. Money Laundering : Concept , Significance and its Impact. 4(2):113–120, 2012.
- [25] Allison Worldwide. September 20. The Golden Age of Proptech - Knowledge Hub - Allison. https://www.allisonworldwide.com/the-golden-age-of-proptech-is-upon-us/?utm_source=chatgpt.com, 2023. [Accessed on 16 June 2023].
- [26] Ledger Insights Blockchain for Enterprise. August 2. Latest German Real Estate Tokenization on Public Blockchain Involves Deutsche Boerse Affiliate 360X. https://www.ledgerinsights.com/real-estate-tokenization-public-blockchain-360x/?utm_source=chatgpt.com, 2023. [Accessed on 16 June 2023].
- [27] Shirley Gregor and Alan R Hevner. Positioning and presenting design science research for maximum impact. *MIS quarterly*, pages 337–355, 2013.

- [28] Uchendu Eugene Chigbu, Sulaiman Olusegun Atiku, and Cherley C Du Plessis. The science of literature reviews: Searching, identifying, selecting, and synthesising. *Publications*, 11(1):2, 2023.
- [29] Hannah Snyder. Literature review as a research methodology: An overview and guidelines. *Journal of business research*, 104:333–339, 2019.
- [30] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS Q*, 28:75–105, 2004.
- [31] Ken Peffers, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. A design science research methodology for information systems research. *J Manag Inf Syst*, 24:45–77, 2007.
- [32] Christoph Meinel and Larry Leifer. Understanding innovation, 2011.
- [33] Johannes Eekels and Norbert FM Roozenburg. A methodological comparison of the structures of scientific research and engineering design: their similarities and differences. *Design Stud*, 12:197–203, 1991.
- [34] John Venable and Richard Baskerville. Eating our own cooking: toward a more rigorous design science of research methods. *Electron J Bus Res Method*, 10:141–153, 01 2012.
- [35] Alan R. Hevner. A three cycle view of design science research. *Scand J Inf Syst*, 19, 2007.
- [36] Roman Beck, Sven Weber, and Robert Wayne Gregory. Theory-generating design science research. *Information Systems Frontiers*, 15:637–651, 2013.
- [37] Richard Baskerville, Abayomi Baiyere, Shirley Gregor, Alan Hevner, and Matti Rossi. Design science research contributions: finding a balance between artifact and theory. *Journal of the Association for Information Systems*, 19:358–376, 2018.
- [38] Statista Research Department. Total online sales of the art and antiques market worldwide from 2013 to 2021. <https://www.statista.com/statistics/886776/online-art-and-antiques-market-total-global-sales/>. [Accessed on 15 November 2022].

- [39] UBS; Art Basel. Distribution of sales value at fine art auctions in selected countries worldwide in 2021, by offline and online market. <https://www.statista.com/statistics/1236560/online-and-offline-sales-share-fine-art-auctions-in-selected-global-countries/>, 2021. [Accessed on 04 December 2022].
- [40] Johannes Gramlich. Reflections on Provenance Research: Values – Politics – Art Markets. *Journal for Art Market Studies*, 1(2):322–327, 2017.
- [41] Masne de Chermont and Laurence Sigal-Klagsbald. *À qui appartenait ces tableaux ? / Looking for owners*. Reunion des musées nationeaux Paris, 2008.
- [42] Laney Salisbury and Aly Sujo. *Provenance: How a con man and a forger rewrote the history of modern art*. Penguin, 2009.
- [43] Pi Hsia Liang and Yan Ping Chi. Influence of perceived risk of blockchain art trading on user attitude and behavioral intention. *Sustainability (Switzerland)*, 13(23), 2021.
- [44] Nikhil Malik, Max Wei, Gil Appel, and Lan Luo. Blockchain technology for creative industries: Current state and research opportunities. *International Journal of Research in Marketing*, 2022.
- [45] Georg Franck. The scientific economy of attention: A novel approach to the collective rationality of science. *Budapest Scientometrics*, 55(1):3–26, 2002.
- [46] Alessia Zorloni and Antonella Ardizzone. The winner-take-all contemporary art market. *Creative Industries Journal*, 9(1):1–14, 2016.
- [47] Andy Warhol’s 14 Small Electric Chairs To Be Sold in Blockchain Art Auction. <https://blog.maecenas.co/andy-warhols-14-small-electric-chairs-to-be-sold-in-blockchain-art-auction/>, 2018. [Accessed on 05 January 2023].
- [48] Christie’s. Results: An american place: The barney a. ebsworth collection — part one achieves \$317.8 million. <https://www.christies.com/about-us/press-archive/details?PressReleaseID=9215lid=1>. [Accessed on 5 December 2022].

- [49] Lorenzo Mucchi, Matilde Milanesi, and Claudio Becagli. Blockchain technologies for museum management. The case of the loan of cultural objects. 2022.
- [50] Susan E Brabenec. The art of determining stolen property: United states v. portrait of wally, a painting by egon schiele. *U. Cin. L. Rev.*, 69:1369, 2000.
- [51] Ariel A Furman. Saving Adele: A History of the Portrait of Adele Bloch-Bauer I. *Quest*, 3:2019.
- [52] Nicholas M. O'Donnell. A tragic fate : law and ethics in the battle over Nazi-looted art. page 418.
- [53] Beeple. Everydays: The first 5000 days. <https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924>. [Accessed on 20 December 2022].
- [54] Lennart Ante. Non-fungible token (NFT) markets on the Ethereum blockchain: Temporal development, cointegration and interrelations. *SSRN Electronic Journal*, (22):1–23, 2021.
- [55] Amy Whitaker, Anne Bracegirdle, Susan De Menil, Michelle Ann Gitlitz, and Lena Saltos. International Journal of Cultural Policy ISSN: (Print) (Online) Journal homepage: <https://www.tandfonline.com/loi/gcul20> Art, antiquities, and blockchain: new approaches to the restitution of cultural heritage. 2020. [Accessed on 20 January 2023].
- [56] Amy Whitaker. Art and Blockchain: A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts. *Artivate*, 8(2):21–46, 2019.
- [57] Jingwen Zhang, Meiting Guo, Biyan Li, and Ruimin Lu. A transport monitoring system for cultural relics protection based on blockchain and internet of things. *Journal of Cultural Heritage*, 50:106–114, 2021.
- [58] Henry Lydiate. Money Laundering. <https://www.proquest.com/docview/2554602626?pq-origsite=gscholarfromopenview=true>. [Accessed on 6 December 2022].

- [59] George Forgang, Greg Forgang, and Integrative Capstone. Money Laundering Through Cryptocurrencies. [Accessed on 18 December 2022].
- [60] T. Burroughs. US and EU Efforts to Combat International Money Laundering in the Art Market are no Masterpiece. *Vanderbilt Journal of Transnational Law*, 52:1061–1096, 2019.
- [61] Saskia Hufnagel and Colin King. Anti-money laundering regulation and the art market. *Legal Studies*, 40(1):131–150, 2020.
- [62] Erin Thompson. The Relationship Between Tax Deductions an the Market for Unprovenanced Antiquities. *Columbia Journal of Law and the Arts*, 33(2):241–265, 2010.
- [63] Hugo Pieter Wouda and Raymond Opdenakker. Blockchain technology in commercial real estate transactions. *Journal of Property Investment and Finance*, 37(6):570–579, 2019.
- [64] Communities Ministry of Housing and Local Government. Improving the home buying and selling process Summary of responses to the Call for Evidence and government response. 2018.
- [65] Hannah Cromarty. Improving the home buying and selling process in England, 202.
- [66] Atefeh Mashatan and Zachary Roberts. An enhanced real estate transaction process based on blockchain technology. *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation*, 2017-Augus(Swan 2015):1–5, 2017.
- [67] Marco Iansiti and Karim R. Lakhani. The truth about blockchain. *Harvard Business Review*, 2017(January-February), 2017.
- [68] Neil Crosby and Patrick McAllister. Liquidity In Commercial Property Markets: Deconstructing The Transaction Process. (rep-wp2004-07), 2004.
- [69] P McNamara. Exploring Liquidity. 1998.

- [70] Steven. Devaney and David Scofield. Time to Transact: Measurement and Drivers. *IPF Research Programme*, (September 2014), 2014.
- [71] Steven Devaney, Nicola Livingstone, Pat McAllister, and Anupam Nanda. Unravelling Liquidity In International Commercial Real Estate Markets. *Investment Property Forum Research Programme*, (March):2011–2015, 2016.
- [72] Shaun Bond, Neil Crosby, Soosung Hwang, Tony Key, Colin Lizieri, George Matysiak, Patrick McAllister, and Charles Ward. Liquidity in Commercial Property Markets. 1(5):117, 2004.
- [73] David Scofield. Time to completion liquidity in UK commercial real estate investment: 2000-2008. *Journal of European Real Estate Research*, 6(1):34–47, 2013.
- [74] José Blanco, Andrew Mullin, Kaustubh Pandya, and Mukund Sridhar. The new age of engineering and construction technology. *McKinsey & Company*, (July):1–16, 2017.
- [75] Elena Ionaşcu and Ion Anghel. Improvement of the real estate transparency through digitalisation. *Proceedings of the International Conference on Business Excellence*, 14(1):371–384, 2020.
- [76] Andrew Baum, Saul Saull, and Fabian Braesemann. Proptech 2020: the Future of Real Estate. page 107, 2010.
- [77] Fabian Braesemann and Andrew Baum. PropTech: Turning Real Estate Into a Data-Driven Market? *SSRN Electronic Journal*, pages 1–22, 2020.
- [78] Alireza Shojaei, Ian Flood, Hashem Izadi Moud, Mohsen Hatami, Xun Zhang, and M E Rinker. An Implementation of Smart Contracts by Integrating BIM and Blockchain. 2020.
- [79] Malachy Mathews, Dan Robles, and Brian Bowe. Bim+ blockchain: A solution to the trust problem in collaboration. *CITA BIM Gathering*, 11:2017, 2017.

- [80] Fran Casino, Thomas K. Dasaklis, and Constantinos Patsakis. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36:55–81, 3 2019.
- [81] Nick Szabo. The idea of smart contracts, 1997, 1997.
- [82] Charles Kerrigan. *Artificial intelligence: Law and regulation*. Edward Elgar Publishing, 2022.
- [83] Transparency International UK. Transparency International gives qualified welcome to new UK Anti-Corruption Strategy. <https://www.transparency.org.uk/transparency-international-gives-qualified-welcome-new-uk-anti-corruption-strategy>. [Accessed on 21 June 2023].
- [84] Ilaria Zavoli and Colin King. New development: Estate agents’ perspectives of anti-money laundering compliance—four key issues in the UK property market. *Public Money and Management*, 40(5):415–419, 2020.
- [85] J D Agarwal. *Keynote Address on Money Laundering : The Real Estate Bubble 1 Money Laundering : The Real Estate Bubble*. Number August. 2007.
- [86] Riccardi Michele Savona Ernesto Ugo. From Illegal Markets to Legitimate Businesses: The Portfolio of Organised Crime in Europe - Final Report of Project OCP Organized Crime Portfolio. <https://hdl.handle.net/10807/121534>. [Accessed on 21 June 2023].
- [87] Mohammed Ahmad Naheem. Money laundering and illicit flows from china-the real estate problem. *Journal of Money Laundering Control*, 20(1):15–26, 2017.
- [88] Fabian Teichmann. Recent trends in money laundering. *Crime, Law and Social Change*, 73:237–247, 2020.
- [89] M Maloney, T Somerville, and B Unger. Combatting money laundering in BC real estate: Expert panel on money laundering in BC real estate. *Victoria, BC: Ministry of Finance, Government of British Columbia*, pages 1–176, 2019.

- [90] Ilaria Zavoli and Colin King. The challenges of implementing anti-money laundering regulation: An empirical analysis. *The Modern Law Review*, 84(4):740–771, 2021.
- [91] Guidance On, Anti Money, Approved By, and H M Treasury. BRITISH ART MARKET FEDERATION. (February):1–116, 2023.
- [92] Fabian Maximilian Johannes Teichmann. Twelve methods of money laundering. *Journal of money laundering control*, 20(2):130–137, 2017.
- [93] Marios Samdanis. Platformisation and transparency in the global art market. In *Global Art Markets*, pages 219–231. Routledge, 2024.
- [94] Erica Coslor. Transparency in an opaque market: Evaluative frictions between “thick” valuation and “thin” price data in the art market. *Accounting, Organizations and Society*, 50:13–26, 2016.
- [95] Erica Coslor and Christophe Spaenjers. Organizational and epistemic change: The growth of the art investment field. *Accounting, Organizations and Society*, 55:48–62, 2016.
- [96] Stefania Fiorentino and Silvia Bartolucci. Blockchain-based smart contracts as new governance tools for the sharing economy. *Cities*, 117:103325, 2021.
- [97] Mohamad Kassab, Joanna DeFranco, Tarek Malas, Phillip Laplante, Giuseppe Destefanis, and Valdemar Vicente Graciano Neto. Exploring research in blockchain for healthcare and a roadmap for the future. *IEEE Transactions on Emerging Topics in Computing*, 9(4):1835–1852, 2019.
- [98] Shuchih E Chang and Yichian Chen. When blockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE Access*, 8:62478–62494, 2020.
- [99] Institutionalisation of crypto-assets and defi–tradfi interconnectedness, 2022. Accessed: 2022-11-20.

- [100] Jack Neureuter. The institutional investor digital assets study. Technical report, Fidelity Digital Assets, 2021.
- [101] Luca Mungo, Bartolucci Silvia, and Laura Alessandretti. Cryptocurrency co-investment network: token returns reflect investment patterns. *arXiv preprint arXiv:2301.02027*, 2023.
- [102] Daniel Drescher. *Blockchain basics*. Apress, 2017.
- [103] Jerome Kehrli. Technological Thoughts by Jerome Kehrli. Niceideas.Ch:Blockchain ExplainedBlockchain explained. 2025.
- [104] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4:2292–2303, 2016.
- [105] Quoc Khanh Nguyen. Blockchain-A Financial Technology for Future Sustainable Development. *Proceedings - 3rd International Conference on Green Technology and Sustainable Development, GTSD 2016*, pages 51–54, 2016.
- [106] Marco Iansiti and Karim R. Lakhani. The Truth About Blockchain. 2017. [Accessed on 04 January 2023].
- [107] Lessin L. Code is law.on liberty in cyberspace. <https://www.coindesk.com/business/2021/02/01/ibm-blockchain-is-a-shell-of-its-former-self-after-revenue-misses-job-cuts-source>, 2012. [Accessed on 16 June 2023].
- [108] S Nakamoto Decentralized Business Review and undefined 2008. Bitcoin: A peer-to-peer electronic cash system. *debr.io*.
- [109] Nicolas Kube. Daniel Drescher: Blockchain basics: a non-technical introduction in 25 steps. *Financial Markets and Portfolio Management*, 32:255, 2018.
- [110] Blockchain in insurance. Turning a buzzword into a breakthrough for health and life insurers. *Deloitte Center for Health Solutions and the Deloitte Center for Financial Services.*, 2016.

- [111] Wessel Reijers, Fiachra O’Brolcháin, and Paul Haynes. Governance in blockchain technologies & social contract theories. *Ledger*, 1:134–151, 2016.
- [112] Teogenes Moura and Alexandre Gomes. Blockchain voting and its effects on election transparency and voter confidence. In *Proceedings of the 18th annual international conference on digital government research*, pages 574–575, 2017.
- [113] Paul Tak Shing Liu. Medical record system using blockchain, big data and tokenization. In *Information and Communications Security: 18th International Conference, ICICS 2016, Singapore, Singapore, November 29–December 2, 2016, Proceedings 18*, pages 254–261. Springer, 2016.
- [114] Kashif Bilal, Saif Ur Rehman Malik, Osman Khalid, Abdul Hameed, Enrique Alvarez, Vidura Wijaysekara, Rizwana Irfan, Sarjan Shrestha, Debjyoti Dwivedy, Mazhar Ali, et al. A taxonomy and survey on green data center networks. *Future Generation Computer Systems*, 36:189–208, 2014.
- [115] Christophe Schinckus. The good, the bad and the ugly: An overview of the sustainability of blockchain technology. 2020.
- [116] Dominique Guegan. Public blockchain versus private blockchain. 2017.
- [117] Siamak Solat, Philippe Calvez, and Farid Naït-Abdesselam. Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice. *Journal of Software*, (December):95–106, 2021.
- [118] Ian. CoinDesk Allison. IBM Blockchain Is a Shell of Its Former Self After Revenue Misses. <https://www.coindesk.com/business/2021/02/01/ibm-blockchain-is-a-shell-of-its-former-self-after-revenue-misses-job-cuts-sources>, 2023. [Accessed on 16 June 2023].
- [119] Rowan van Pelt, Slinger Jansen, Djuri Baars, and Sietse Overbeek. Defining Blockchain Governance: A Framework for Analysis and Comparison. *Information Systems Management*, 38(1):21–41, 2021.

- [120] Jersain Zadamig Llamas Covarrubias and Irving Norehem Llamas Covarrubias. Different types of government and governance in the blockchain. *Journal of Governance and Regulation*, 10(1):8–21, 2021.
- [121] the Law Society Conveyancing Protocol. 2019.
- [122] Yue Liu, Qinghua Lu, Guangsheng Yu, Hye Young Paik, and Liming Zhu. Defining blockchain governance principles: A comprehensive framework. *Information Systems*, 109:102090, 2022.
- [123] Yue Liu, Qinghua Lu, Guangsheng Yu, Hye-Young Paik, and Liming Zhu. Bgra: A reference architecture for blockchain governance. *arXiv preprint arXiv:2211.04811*, 2022.
- [124] Yue Liu, Qinghua Lu, Liming Zhu, Hye Young Paik, and Mark Staples. A systematic literature review on blockchain governance. *Journal of Systems and Software*, 197(November 2020):111576, 2023.
- [125] European Commission. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). <https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04>, 2016. [Accessed on 31 March 2023].
- [126] Hye Young Paik, Xiwei Xu, H. M.N.Dilum Bandara, Sung Une Lee, and Sin Kuang Lo. Analysis of data management in blockchain-based systems: From architecture to governance. *IEEE Access*, 7:186091–186107, 2019.
- [127] ISO. ISO/IEC 38505-1:2017 Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data. <https://www.iso.org/standard/56639.html>, 2022. [Accessed on 31 March 2023].
- [128] ISO. The ISO/IEC 25000 series of standards. <https://iso25000.com/index.php/en/iso-25000-standards>. [Accessed on 31 March 2023].

- [129] John Adler, Ryan Berryhill, Andreas Veneris, Zissis Poulos, Neil Veira, and Anastasia Kastania. Astraea: A Decentralized Blockchain Oracle. *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*, pages 1145–1152, 2018.
- [130] Jian Chen, Zhihan Lv, and Houbing Song. Design of personnel big data management system based on blockchain. *Future Generation Computer Systems*, 101:1122–1129, 2019.
- [131] Qian Wei, Bingzhe Li, Wanli Chang, Zhiping Jia, Zhaoyan Shen, and Zili Shao. A Survey of Blockchain Data Management Systems. *ACM Transactions on Embedded Computing Systems*, 21(3), 2022.
- [132] Christian Bieri. An overview into the interplanetary file system (ipfs): use cases, advantages, and drawbacks. *Communication Systems XIV*, 28, 2021.
- [133] H M N Dilum Bandara, Xiwei Xu, and Ingo Weber. Patterns for Blockchain Data Migration. 2020(July):1–40, 2020.
- [134] European e Justice Portal. Land registers in EU countries (2017), 2017.
- [135] Floor Seuren. Introducing Blockchain to Commercial Real Estate: Exploring the applicability of blockchain technology in lowering transaction costs of the commercial real estate due diligence process. page 144, 2018.
- [136] F Seuren, Floris. Exploring the applicability of blockchain in lowering transaction costs in the commercial real estate due diligence process: a case study research. *SSRN Electronic Journal*, (Dd), 2017.
- [137] Rosco Kalis and Adam Belloum. Validating data integrity with blockchain. *Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom*, 2018-Decem(August):272–277, 2018.

- [138] Warwick Powell, Marcus Foth, Shoufeng Cao, and Valéri Natanelov. Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains. *Journal of Industrial Information Integration*, 25(July 2021), 2022.
- [139] Xiang Chu, Rui Wang, Yan Lin, and Yantong Li. Building trust in online trade-in programs with a blockchain-enabled system. *Transportation Research Part E: Logistics and Transportation Review*, 164(October 2021):102833, 2022.
- [140] Yo-Seob Lee. Analysis on Trends of Artworks Blockchain Platform. *International Journal of Advanced Culture Technology*, 7(3):149–157, 2019.
- [141] Zohar Elhanani. How Blockchain Changed The Art World In 2018. *Forbes*, 2018.
- [142] Laura Lotti. The Art of Tokenization: Blockchain Affordances and the Invention of Future Milieus. *Media Theory*, 3(1):287–320, 2019.
- [143] Libo Feng, Hui Zhang, Yong Chen, and Liqi Lou. Scalable Dynamic Multi-Agent Practical Byzantine Fault-Tolerant Consensus in Permissioned Blockchain. *Applied science, MDPI*, 2018.
- [144] Bradford Lindsley Schlei, C A Us, Shelley Ann, London Gb, John Wood, London Gb, and Marcus Ramsden. *United States Patent*, volume 1. 2021.
- [145] Gary C Kessler. An Overview of Cryptography (Updated Version. (January):1–65, 2019.
- [146] Terence Eden. How I became Leonardo da Vinci on the Blockchain. <https://shkspr.mobi/blog/2018/06/how-i-became-leonardo-da-vinci-on-the-blockchain/>. [Accessed on 22 January 2023].
- [147] Wilma Woo. Leonardo da Vinci’ Puts Mona Lisa Painting on the Blockchain. <https://bitcoinist.com/leonardo-da-vinci-mona-lisa-blockchain-verisart/>. [Accessed on 3 December 2023].
- [148] Eileen Kinsella. New Auction Records for Hopper and de Kooning Lead Christie’s Booming \$318 Million Barney Ebsworth

- Sale. <https://news.artnet.com/market/edward-hopper-barney-ebsworth-sale-christies-1395328>: :text=The 20sale 20of 20late 20business-man,estimate 20of 20about 20 24258.3 20million., 2018. [Accessed on 10 January 2023].
- [149] Tim Schneider. Cryptocurrencies, Explained: How Blockchain Technology Could Solve 3 Big Problems Plaguing the Art Industry. <https://news.artnet.com/art-world/cryptocurrencies-explained-part-three-1248863>, 2018. [Accessed on 02 December 2022].
- [150] Maecenas, The Art Investment Platform.
- [151] Massimo Bartoletti, Stefano Lande, Livio Pompianu, and Andrea Bracciali. A general framework for blockchain analytics. *SERIAL 2017 - 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, Colocated with ACM/I-FIP/USENIX Middleware 2017 Conference*, 2017.
- [152] Nick Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9):1–33, 1997.
- [153] Georgina Adam. Interested in a square inch of a Warhol? Fractional ownership hits the art market. <https://www.theartnewspaper.com/2018/10/04/interested-in-a-square-inch-of-a-warhol-fractional-ownership-hits-the-art-market>, 2018. [Accessed on 15 November 2022].
- [154] Maecenas. Maecenas, The Decentralised Art Gallery. <https://www.maecenas.co/whats-maecenas/>. [Accessed on 15 January 2023].
- [155] Lauren Van Haaften-Schick, Amy Whitaker, and Amy Whitaker@nyu Edu. From the Artist’s Contract to the blockchain ledger: new forms of artists’ funding using equity and resale royalties. *Journal of Cultural Economics*, 46:287–315, 123.
- [156] Mishcon De Reya. Buy-Sell-Journey. (July):2018, 2018.

- [157] Saull Andrew and Baum Andrew. The Future of Real Estate Transactions Report Summary The future of real estate transactions: Technology, innovation and the real estate conveyancing process. 2020.
- [158] Andrew Saull, Andrew Baum, and Fabian Braesemann. Can digital technologies speed up real estate transactions? *Journal of Property Investment and Finance*, 38(4):349–361, 2020.
- [159] Royal Institution of Chartered Surveyors (RICS). The Value of Information Management for Surveyors. <https://ww3.rics.org/uk/en/journals/construction-journal/the-value-of-information-management-for-surveyors.html>, 2022. [Accessed on 10 January 2023].
- [160] Richard Gendal Brown. The corda platform: An introduction. *Retrieved*, 27:2018, 2018.
- [161] Mike Hearn and Richard Gendal Brown. Corda: A distributed ledger. *Corda Technical White Paper*, 2016, 2016.
- [162] R3 Team. Fast and transparent interbank reconciliation powered by distributed ledger technology. 2020.
- [163] Chainalysis Team. Understanding Tornado Cash, Its Sanctions Implications, and Key Compliance Questions. <https://blog.chainalysis.com/reports/tornado-cash-sanctions-challenges/how-it-works>. [Accessed on 28 July 2023].
- [164] Danton Brytas. *Bitcoin and Money Laundering : Mining for an Effective Solution*, volume 89. 2014.
- [165] Emily Fletcher, Charles Larkin, and Shaen Corbet. Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance*, 56(January):101387, 2021.
- [166] Daniel Dupuis and Kimberly Gleason. Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*, 28(1):60–74, 2021.

- [167] HM Treasury. *UK National money laundering and terrorist financing risk assessment*. Number February. 2015.
- [168] HM Treasury and Home Office. *National risk assessment of money laundering and terrorist financing 2020*. Number December. 2020.
- [169] Joseph Burleson, Michele Korver, and Dan Boneh. Privacy-protecting regulatory solutions using zero-knowledge proofs, 2022.
- [170] GitHub. Tornado Cash Privacy Solution. <https://github.com/tornadocash/tornado-core/blob/master/README.md>. [Accessed on 28 July 2023].
- [171] Tornado Cash. Introducing Private Transactions On Ethereum now! <https://tornado-cash.medium.com/introducing-private-transactions-on-ethereum-now-42ee915babe0>. [Accessed on 28 July 2023].
- [172] Dan Boneh. Anonymous payments. <https://youtu.be/Z0s4W3UBxM8>. [Accessed on 31 July 2023].
- [173] Alexey Pertsev, Roman Semenov, and Roman Storm. Tornado Cash Privacy Solution Version 1.4. 1(1):4–6, 2019.
- [174] Stanford University. The 13th biu winter school on cryptography, stanford university aug 28-30, 2023. [Accessed on September 2023].
- [175] Edoardo D’Andrassi and Francesca Ventimiglia. The use of blockchain by different art market players: Current applications and risks. *2021 IEEE International Conference on Technology Management, Operations and Decisions, ICTMOD 2021*, pages 1–7, 2021.
- [176] Z. John Zhang. Cryptopricing: Whence comes the value for cryptocurrencies and NFTs? *International Journal of Research in Marketing*, 2022.
- [177] Christian Stoll, Lena Klaaßen, and Ulrich Gellersdörfer. The Carbon Footprint of Bitcoin. *Joule*, 3(7):1647–1661, 2019.

- [178] Alireza Shojaei, Jun Wang, and Andriel Fenner. Exploring the feasibility of blockchain technology as an infrastructure for improving built asset sustainability. *Built Environment Project and Asset Management*, 10(2):184–199, 2020.
- [179] J Michael Graglia and Christopher Mellon. Blockchain and property in 2018: At the end of the beginning. *Innovations: Technology, Governance, Globalization*, 12(1-2):90–116, 2018.
- [180] Vikram Sadhya and Harshali Sadhya. Barriers to Adoption of Blockchain Technology Barriers to Adoption of Blockchain Technology Completed Research. 2018.
- [181] Daml. Daml documentation. <https://docs.daml.com/>. [Accessed on 15 March 2023].
- [182] The National Lottery Heritage Fund. Museums, libraries and archives. https://www.heritagefund.org.uk/our-work/museums-libraries-and-archives?utm_source=chatgpt.com, 2025. [Accessed on 24 June 2025].
- [183] Art Fund. October 31. Art fund awards £1m to local museums. https://www.artfund.org/professional/news-and-insights/art-fund-reimagine-grants?utm_source=chatgpt.com, 2024. [Accessed on 24 June 2025].
- [184] A. 2024. Morrison. An enormous milestone for museums’: Platform designed to host 100 million object records launches in uk. https://www.theartnewspaper.com/2024/09/17/enormous-milestone-museums-platform-designed-host-100-million-object-records-launches-uk?utm_source=chatgpt.com, 2024. [Accessed on 24 June 2025].
- [185] GOV.UK. Hm land registry to explore the benefits of blockchain. https://www.gov.uk/government/news/hm-land-registry-to-explore-the-benefits-of-blockchain?utm_source=chatgpt.com, 2018. [Accessed on 24 June 2025].
- [186] Consensys. Hmlr: Blockchain case study for real estate tokenization in the uk. https://consensys.io/blockchain-use-cases/finance/hmlr?utm_source=chatgpt.com, 2025. [Accessed on 24 June 2025].

- [187] Md Tauseef Alam, Sujit Chowdhury, Raju Halder, and Abyayananda Maiti. Blockchain Domain-Specific Languages: Survey, Classification, and Comparison. *Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain 2021*, pages 499–504, 2021.
- [188] Candidate Number. On Blockchain and Non-Fungible Tokens (NFTs): opportunities , challenges and the emergence of a new asset Supervised by Dr Silvia Bartolucci. 2022.
- [189] Emanuel Kohlscheen, Marco Lombardi, and Egon Zakrajsek. BIS Working Papers. *Globalization*, 19(943):20, 2021.
- [190] Digital Asset. Deutsche Börse Names Digital Asset Strategic Technology Partner for its New Digital Post-trade Platform. <https://www.digitalasset.com/use-cases/custody-safekeeping>, 2021. [Accessed on 15 March 2023].
- [191] Digital Asset. Goldman Sachs’ Tokenization Platform GS DAP™, Leveraging Daml, Goes Live. <https://www.digitalasset.com/use-cases/tokenization>, 2023. [Accessed on 15 March 2023].
- [192] Hiscox UK. Hiscox UK Art Insurance, 2024. [Accessed: 25 September 2024].
- [193] Gauntlet. Fine Art Collections Gauntlet, 2024. [Accessed: 25 September 2024].
- [194] Chubb. Fine Art Collections Gauntlet, 2024. [Accessed: 25 September 2024].
- [195] Brownhill Insurance Group. The Realist’s Guide to Art Insurance, 2024. [Accessed: 25 September 2024].
- [196] Linda Weigl, Tom Josua Barbereau, Johannes Sedlmeir, and Liudmila Zavolokina. Mediating the tension between data sharing and privacy: The case of DMA and GDPR. In *Proceedings of the 31st European Conference on Information Systems (ECIS)*, 2023.
- [197] Responsible Art Market. Guidelines on combatting money laundering and terrorist financing. <https://www.responsibleartmarket.org/guidelines/guidelines-on->

- combatting-money-laundering-and-terrorist-financing/., 2025. [Accessed on 24 June 2025].
- [198] Deloitte. 8th deloitte private and arttactic art finance report. <https://www.deloitte.com/lu/en/services/financial-advisory/research/art-finance-report.html>, 2023. [Accessed on 24 June 2025].
- [199] Basel Institution of Governance. Basel art trade anti-money laundering principles. https://baselgovernance.org/publications/basel-art-trade-anti-money-laundering-principles?utm_source=chatgpt.com., 2018. [Accessed on 24 June 2025].
- [200] Bruno Deprez, Toon Vanderschueren, Bart Baesens, Tim Verdonck, and Wouter Verbeke. Network analytics for anti-money laundering-a systematic literature review and experimental evaluation. *arXiv preprint arXiv:2405.19383*, 2024.
- [201] USEUM. Interactive fine art gallery museum useum. <https://useum.org/>. [Accessed: 17 September 2024].
- [202] Collection Trust. Spectrum collections trust. <https://collectionstrust.org.uk/spectrum/>. [Accessed: 17 September 2024].
- [203] ArtUK. Art uk. <https://artuk.org/>. [Accessed: 17 September 2024].
- [204] Towards a National Collection. Towards a national collection. <https://www.nationalcollection.org.uk/>. [Accessed: 17 September 2024].
- [205] T. Schneider. Christie’s hit with class action lawsuit over exposure of clients’ personal data in cyberattack. <https://www.theartnewspaper.com/2024/06/04/christies-cyberattack-class-action-lawsuit-data-breach>. [Accessed: 28 June 2024].
- [206] Tom Barbereau, Johannes Sedlmeir, Reilly Smethurst, Gilbert Fridgen, and Alexander Rieger. Tokenization and regulatory compliance for art and collectibles markets. In Mary Lacity and Horst Treiblmaier, editors, *Blockchains and the Token Economy: Studies in Theory and Practice*, chapter 8. Palgrave Macmillan, 2022.

- [207] Blaž Podgorelec, Lukas Alber, and Thomas Zefferer. What is a (digital) identity wallet? A systematic literature review. In *46th Annual Computers, Software, and Applications Conference*, pages 809–818. IEEE, 2022.
- [208] André Kudra, Alexander Rieger, Johannes Sedlmeir, Gilbert Fridgen, and Amber G. Young. Digital identity wallets: How public and private sector organizations can implement the EU’s new identity mode. *Information Systems Journal*, 2025. Forthcoming.
- [209] GLEIF. [Accessed on 8 March 2025].
- [210] Raúl Ramos Fernández. Evaluation of trust service and software product regimes for zero-knowledge proof development under eIDAS 2.0. *Computer Law & Security Review*, 53:105968, 2024.
- [211] EU Digital Identity Wallet. [Accessed on 8 March 2025].
- [212] Mary Lacity and Erran Carmel. Self-sovereign identity and verifiable credentials in your digital wallet. *MIS Quarterly Executive*, 21(3), 2022.
- [213] Amy Whitaker and Roman Kräussl. Blockchain, Fractional Ownership, and the Future of Creative Work. *Management Science*, pages 1–33, 2018.
- [214] Matthias Babel, Vincent Gramlich, Marc-Fabian Körner, Johannes Sedlmeir, Jens Strüker, and Till Zwede. Enabling end-to-end digital carbon emission tracing with shielded NFTs. *Energy Informatics*, 5, 2022.
- [215] Eden Network. Multichain Infrastructure for Maximal Value. [Accessed on 8 March 2025].
- [216] HM and Land Registry. Enabling a world-leading property market strategy 2022+. 2022.
- [217] McKinsey Company. Imagining construction’s digital future, 2016.
- [218] Avi Spielman. *Signature redacted – Signature redacted – Signature redacted*. Number 2000. 2017.

- [219] Jamie Susskind. *The digital republic: on freedom and democracy in the 21st century*. Bloomsbury publishing, 2022.
- [220] Mohamed Rahouti, Kaiqi Xiong, and Nasir Ghani. Bitcoin Concepts, Threats, and Machine-Learning Security Solutions. *IEEE Access*, 6:67189–67205, 2018.
- [221] Max Kubát. Virtual Currency Bitcoin in the Scope of Money Definition and Store of Value. *Procedia Economics and Finance*, 30:409–416, 2015.
- [222] Ryan Farrell. ScholarlyCommons An Analysis of the Cryptocurrency Industry An Analysis of the Cryptocurrency Industry. 2015.
- [223] Suman Ghimire and Henry Selvaraj. A survey on bitcoin cryptocurrency and its mining. *26th International Conference on Systems Engineering, ICSEng 2018 - Proceedings*, 2019.
- [224] Huy Tran and Main Sam Cheng. Book-introduction to modern cryptography Related papers Design of Secured Protocols Kart heek D N.
- [225] Arati Baliga. Understanding Blockchain Consensus Models - White paper. 2020.
- [226] Sarwar Sayeed and Hector Marco-Gisbert. Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences (Switzerland)*, 9(9), 2019.
- [227] Eduardo Morais, Tommy Koens, Cees Van Wijk, and Aleksei Koren. A survey on zero knowledge range proofs and applications. *SN Applied Sciences*, 1:1–17, 2019.
- [228] Haojun Liu, Xinbo Luo, Hongrui Liu, and Xubo Xia. Merkle tree: A fundamental component of blockchains. In *2021 International Conference on Electronic Information Engineering and Computer Science (EIECS)*, pages 556–561. IEEE, 2021.