Travels along the hype cycle: a set of blockchain applications and the economic processes they impact

Yuen C Lo

A report submitted in fulfillment of the requirements for the degree

Doctor of Philosophy

of

University College London

Department of Civil, Environmental and Geomatics Engineering

February 28, 2023

Abstract

Some commentators refer to blockchain as a potential General Purpose Technology. Yet despite a plethora of cryptoassets and projects, it has struggled to gain traction beyond payments and price discovery. This thesis explores how the technology is being applied to better understand the potential and risks of deploying blockchain. It examines four different use cases with econometric and case study methods: (1) Bitcoin mining as the token incentivized processing of records, (2) Initial Coin Offering tokens as a form of venture financing, (3) Uniswap the decentralized exchange and (4) Kompany improving the data integrity of compliance records via notarization to a public blockchain. It finds that blockchain enables capabilities that did not exist before, but that these capabilities are bounded by trade offs and developer priorities. Ultimately this research expands the literature on blockchain applications and argues that blockchain does not build better systems, but different systems that can achieve different objectives. It provides evidence that firms and society are gradually traversing the hype cycle, deploying blockchain, solving real world economic problems and creating value.

Keywords: Blockchain, Smart contract, Tokenomics, Decentralized exchange, Data Integrity

I, Yuen C Lo 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.

Impact statement

This thesis attempts to address the question: can blockchain solve real world problems? It provides evidence in favor of this proposition via three empirical analyses and one case study. The first empirical study examines the mechanics of the earliest application of blockchain, Bitcoin. The second and third papers explore two important assumptions in digital finance and economics. In a study of Initial Coin Offering (ICOs) tokens used for fundraising, we find evidence that there is an empirical connection between a token and its project, despite no legal connection between the two. This finding tests an important assumption often made by academic cryptoasset researchers. In a study of a decentralized exchange, we find that such marketplaces can be effective, and raise the possibility that decentralized exchanges can improve market completeness. This is important for researchers as it forms a common assumption in economic research, but can also benefit financial markets characterized by volatility arising from uneven liquidity and constrained market makers. Any improvement of market completeness implies significant benefits for participants and social welfare. In a final case study on a business know your customer application, we illustrate some of the potential benefits of applying blockchain to regulatory compliance. This may be of immediate use for regulated firms and regulators, but also provides insights for other organizations attempting to apply the power of blockchain to their data. Collectively these four analyses put forward a practical understanding of blockchain technology, expanding out from its original cryptocurrency roots to new pain points.

Three of the chapters of the thesis have been published in journals ranked by the Academic Journal Guide 2021. These are detailed in the UCL Research Paper declaration section.

Acknowledgments

I would like to express my deepest appreciation for Professor Medda. Your keen eye and guidance have been priceless. I am also grateful to Professor Okhrati and Dr Liu for their comments. Last but not least I would like to thank my wife, who has humored me throughout!

UCL Research Paper declaration

Referencing the doctoral candidates' published work

Bitcoin mining: converting computing power into cash flow	
Journal	Applied Economics Letters
DOI	10.1080/13504851.2018.1540841
Publisher	Taylor and Francis
Publication year	2018
Academic peer review	Yes
Retention of copyright	No
Multi-author statement	
Author has permission of publisher to re-use said work	
Lo, Y C: conceptualization, methodology, investigation, formal analysis, writing original/final Medda, F: supervision, writing review	
Thesis Chapter	4
Candidate e-signature	
Date	31 October 2022
Supervisor e-signature	
Date	31 October 2022

Assets on the blockchain: An empirical study of Tokenomics	
Journal	Information Economics and Policy
DOI	10.1016/j.infoecopol.2020.100881
Publisher	Elsevier
Publication year	2020
Academic peer review	Yes
Retention of copyright	No
Multi-author statement	
Author has permission of publisher to re-use said work	
Lo, Y C: conceptualization, methodology, investigation, formal analysis, writing original/final Medda, F: supervision, writing review	
Thesis Chapter	5
Candidate e-signature	
Date	31 October 2022
Supervisor e-signature	
Date	31 October 2022

Uniswap and the emergence of the decentralized exchange	
Journal	Journal of Market Infrastructures
DOI	10.21314/JFMI.2022.004
Publisher	Risk.net
Publication year	2022
Academic peer review	Yes
Retention of copyright	No
Multi-author statement	
Author has permission of publisher to re-use said work	
Lo, Y C: conceptualization, methodology, investigation, formal analysis, writing original/final Medda, F: supervision, writing review	
Thesis Chapter	6
Candidate e-signature	
Date	31 October 2022
Supervisor e-signature	
Date	31 October 2022

Contents

Chapter 1

Introduction

1.1 Problem statement

Other than speculation, what is blockchain good for? Can it solve intractable problems? Over a decade has passed since the first Bitcoin was issued on its own blockchain, yet arguably it has collected more critics than use cases. For example Roubini (2018) testified before the United States Congress and posited that cryptocurrency payment tokens and blockchain token fundraisings are inferior to the traditional financial services they compete with, in addition to being prone to fraud. In some ways, critics have their case made for them given the unsatisfied excitement epitomized by papers such as Davidson, De Filippi, and Potts (2018) that lauds blockchain as a new institutional technology. Part of the problem is that cryptoassets like Bitcoin are the default example used to explain blockchain, when one of the most important distinctions is to separate the token from the technology. The literature needs better examples to understand the capability and nuance of blockchain.

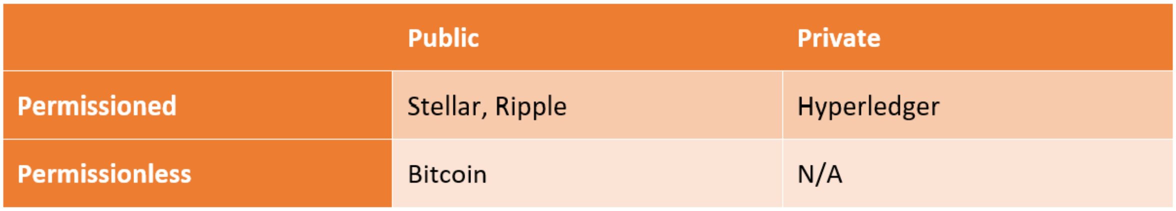
1.2 Research motivation

Litan and Leow (2021) apportions blockchain applications across the five stages of the Gartner hype cycle: innovation trigger; peak of inflated expectations; trough of disillusionment; slope of enlightenment; and plateau of productivity. It observes how Bitcoin, within the category of cryptocurrencies, has started to emerge into the slope of enlightenment. However blockchain platforms, the underlying infrastructure that was supposed to change the world, languishes in disillusionment. Despite this, many things that were difficult before have now been enabled by distributed ledger technologies such as blockchain. Bitcoin - which arguably substitutes for JP Morgan, Visa and Paypal in the payments value chain - provides a potentially cheaper way of making international payments (Kim, 2017). This has been made even easier by stablecoins linked to the value of fiat currencies such as the US dollar. TradeLens, a joint venture between IBM and Maersk, exploits the authentic shared record aspect of distributed ledgers to track the movement of 60% of the world's shipping containers - in the hopes of one day fully digitizing the global logistics network (Jensen, Hedman, and Henningsson, 2019). TradeLens fits squarely into Wust and Gervais (2018)'s argument that blockchain has a strong use case where (1) there exists data to be stored, (2) multiple writers wish to contribute, and (3) where a centralized authority either does not exist or does not add value. Bitcoin and TradeLens are examples of how distributed ledgers are impacting existing economic processes.

However, there are disadvantages with both examples. As mentioned regarding Bitcoin, many commentators struggle with separating the payment token from the payment system. The issue with TradeLens is another distinction. As a permissioned system, some would argue it is a distributed ledger, but not a blockchain (Joseph et al., 2022). Within a permissioned system, writers may vary, but the permissioner likely does not, forming a potential point of control. Pure applications of blockchain that do something that was not possible before remain poorly covered in the literature. This makes understanding the capabilities offered by blockchain somewhat abstruse. Cong (2018) opines that future research will fit within two broad categories. The first is on blockchain mechanisms and the generation of decentralized consensus. The second is on the technology's real world implications, given the functionality that blockchain provides. This thesis focuses on expanding the literature on blockchain applications. It examines four in production use cases traveling along Gartner's hype cycle. It deconstructs some of the decisions of developers in molding its trajectory. It contributes evidence to the literature that the new capabilities associated with blockchain can address multiple economic problems, such as incomplete markets and data integrity. One of the major reasons why this has been difficult to date is the slow pace of blockchain adoption beyond tokens, the reasons of which will be discussed further. An exploration of blockchain use cases can add significant insights to the mechanics of the technology. Outside of academia, this research has particular relevance to regulators who are grappling with tokens and decentralized finance, and to enterprises, which are looking for opportunities to create value with blockchain.

1.3 How blockchain changes the governance of data

A traditional ledger is defined as a book in which things are recorded, in particular business activities and funds paid and received.[1] These records are often referred to as data. Digital ledgers are somewhat more sophisticated, while distributed versions open up a panoply of options. Lipton (2018) illustrates some common ways of categorizing digital ledgers. Centralized versus distributed contrasts ledgers operated by a single entity such as a bank or government, with ledgers that have more than one point of control. Distributed ledgers are further sorted by public versus private, based on controls on data visibility. They are often delineated by permissioned versus permissionless, based on controls on agents (1.1).



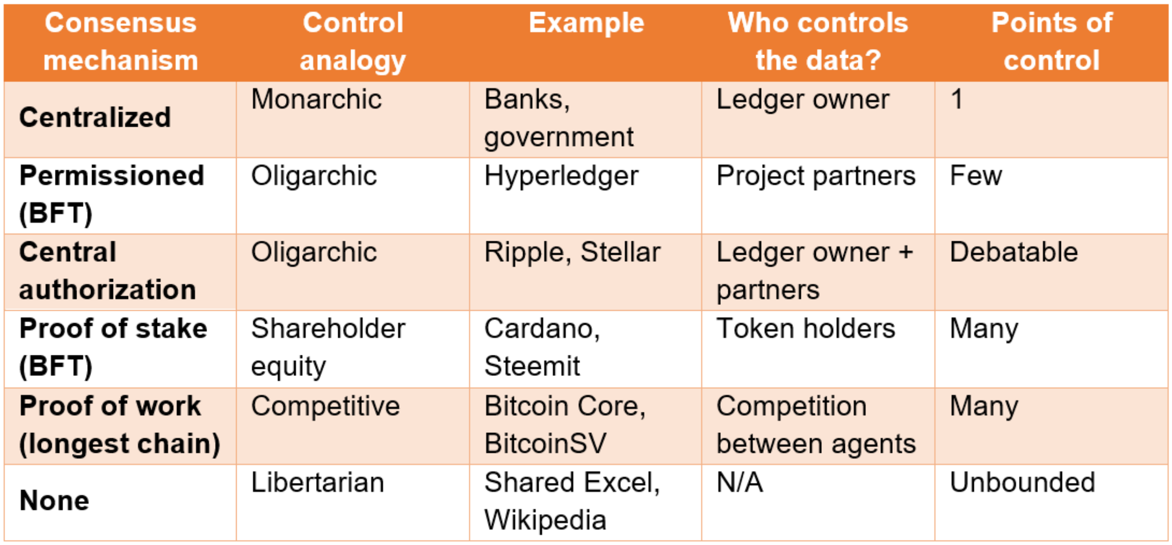
	Public	Private
Permissioned	Stellar, Ripple	Hyperledger
Permissionless	Bitcoin	N/A

Figure 1.1: Early ways of dimensioning distributed ledgers

Although each is an important variable, the problem with such schemata is that they are unable to differentiate between Proof of Work (PoW) and Proof of Stake (PoS), the two primary blockchain consensus families – short of including a consensus dimension. Furthermore, it does not capture a major change enabled by blockchain: governance and ownership of data. Tucker and Catalini (2018) argues that blockchain can address the major flaw in the economics of privacy, namely who has property rights over data. Changes in governance and ownership of data is one part of how trustless blockchains can moderate requirements for a trusted intermediary. In other words the operative function of blockchain here is data governance, with disintermediation as a consequence.

One way to understand data governance is to juxtapose it with the diverse ways that exist to govern people, for example monarchies and oligarchies (Figure 1.2). Until blockchain, there was less diversity when it came to holding and governing data. Almost all prior large-scale records are in

[1] dictionary.cambridge.org/dictionary/english/ledger



Consensus mechanism	Control analogy	Example	Who controls the data?	Points of control
Centralized	Monarchic	Banks, government	Ledger owner	1
Permissioned (BFT)	Oligarchic	Hyperledger	Project partners	Few
Central authorization	Oligarchic	Ripple, Stellar	Ledger owner + partners	Debatable
Proof of stake (BFT)	Shareholder equity	Cardano, Steemit	Token holders	Many
Proof of work (longest chain)	Competitive	Bitcoin Core, BitcoinSV	Competition between agents	Many
None	Libertarian	Shared Excel, Wikipedia	N/A	Unbounded

Figure 1.2: Distributed ledgers as modes of data governance

two forms, collaborative or centralized. Collaborative records, exemplified by shared spreadsheets and Wikipedia, are somewhere between libertarian and anarchic, with records easily changed and reverted, and debatable reliability. Therefore unsurprisingly, the dominant container for large scale data is a centralized database or ledger, where an organization or a government can keep a record within a system under their control. A firm's double-entry accounts, the definitive list of a country's citizens, all the holders of currency deposited at a bank, are types of curated, valuable data we can refer to as centralized ledgers. Each of them reflects one rule writer, one data writer, one single point of control. Access must be rigorously regulated. Audits are complicated because the risk of tampering is clear and undefined. Users are subject to unforeseen rule changes. In many ways, Centralized ledgers are the "monarchies" of data governance.

However, that does not make PoW democracy. Rather PoW blockchains are a competitive model of data governance. We explore the consensus mechanism of PoW in Section 3.2. For now, we provide a sketch and highlight the competition inherent in having agents compete to write the next block of data to a blockchain. An intuitive component of this is the expansion of a ledger's stakeholders into a Venn diagram (Figure 1.3). The writers of the data are separated from the rule makers of the data container, and in this way give users an opportunity to be reliably assigned rights to their data. Referred to as miners, data writers on a PoW blockchain compete via hash based computational puzzles to write a block and earn a reward. This induces incentive

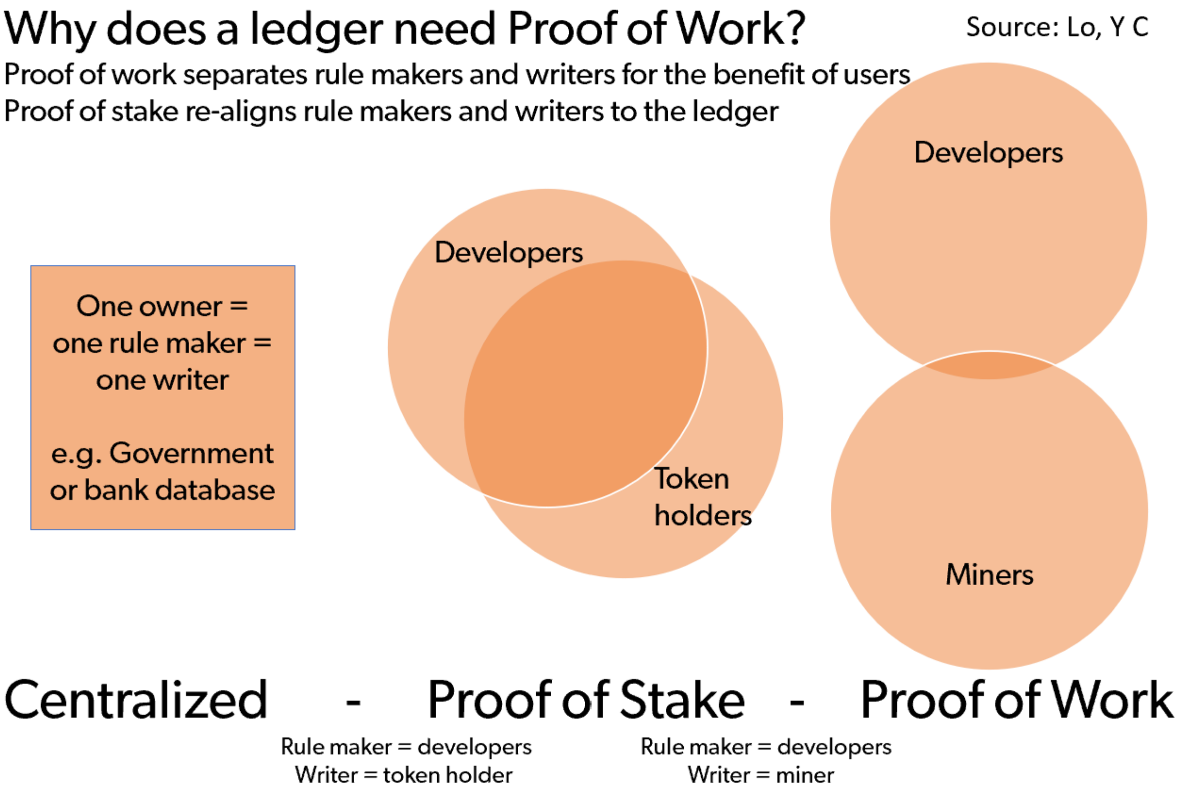

Why does a ledger need Proof of Work?
Source: Lo, Y C
Proof of work separates rule makers and writers for the benefit of users
Proof of stake re-aligns rule makers and writers to the ledger
One owner = one rule maker = one writer
e.g. Government or bank database
Developers
Token holders
Developers
Miners
Centralized - Proof of Stake - Proof of Work
Rule maker = developers
Writer = token holder
Rule maker = developers
Writer = miner

Figure 1.3: How blockchain ledgers change the distribution of control

compatibility, with free entry discouraging collusion between miners. Abadi and Brunnermeier (2018) expands on this to argue that blockchains eliminate the economic rents collected by the controller of a centralized ledger, replacing it with resource consumption by miners. However, the risk of tampering in a blockchain ledger does not disappear, it merely becomes defined. To adumbrate the size of the attack surface presented by a PoW blockchain, imagine the archetypal 51% attack on a blockchain, where the majority of mining hash power is malicious. Despite gaining considerable privileges to append data, the attacker will struggle to mint valuable new coins for themselves or change the protocol rules in its favor (Sayeed and Marco-Gisbert, 2019). If it openly does this, then the rational choice would be for users and honest miners to not follow the attacker's hard fork, leaving the attacker with nothing. Importantly honest miners are incentivized to support users by gaining the attackers block rewards. In most cases, the primary benefit of a 51% of attack is a double spend, where an attacker makes a payment and then reverses it, retaining goods and services fraudulently acquired.

Within this framework, PoS blockchains, where tokens can be staked by their holders and take turns to write to the ledger, are where the rights of the controller are passed through to equity like owners. It approximates the shareholder equity governance of data (Wright, 2019). The difference between PoW and PoS governance is illustrated by comparing Bitcoin's separation into Bitcoin Core and Cash, with the takeover of the PoS blockchain and social media site Steemit. In the former, competing groups fought via hash mining capacity, and then chose to exist separately. Fundamentally, the competition between miners circumscribes the power of the ledger's rule makers, and obliges the rule makers to compete at times of stress. Conversely, Justin Sun was able to launch and win a hostile takeover of Steemit (Copeland, 2020), by making agreements with centralized exchanges. Users are unhappy to this day. To paraphrase a common stock market aphorism, PoW is a voting machine, PoS is a weighing machine. We observe the less rigorous data guarantee of a PoS blockchain, at the same time as accepting their superior energy consumption characteristics.

To this framework we add one more category of data governance: oligarchic. Hyperledger can be described as an "oligarchic" ledger where a set of organizations take on the role of rule making and permission data writing. Although oligarchic ledgers like Hyperledger are replicated and append only, one or more key sponsors have development and rule-making rights over the ledger. Therefore their tamper resistance is administratively weaker. Ripple is an "oligarchic" ledger where they retain rule making rights and permission a list of data writers with additional privileges. With this intuition, the ledger design space can be characterized as Libertarian, Competitive, Equity, Oligarchic and Monarchic (Figure 1.2). Data transparency is a design feature available to them all, but the independent data guarantee associated with each is correlated with the number of separate points of control (with the exception of Libertarian - though some might argue it has none). We draw out these points as an area for future research, noting that its theoretical basis is consistent with the existence of checks and balances within political systems (Acemoglu, Robinson, and Torvik, 2013).

In terms of scaling, the inverse correlation between transaction throughput and the number of nodes is well covered in the literature, notably when linked to the use of sharding to split up groups of nodes to boost throughput e.g., Dang et al. (2019). The value of nodes that are not points of control, with respect to decentralization, is not so clear cut. Such arguments revolve around non-miner nodes collectively rejecting inappropriate rule changes even when the latter are supported by miners.[2] It is unfortunate for proponents of such logic that there are numerous examples of the criticality of miner choices (e.g., Ethereum Classic's split from Ethereum), and relatively fewer where non-mining nodes have prevented a rule change. The case that nodes, that are not points of control, are important for use cases such as digital gold is easier to make. The software run by such nodes enable users to personally verify their own transactions.

Concluding this section, we argue that only competitive ledgers offer the potential for unconflicted data verification via reliably assignable, and potentially user-centric, governance of data. Other ledgers have the potential for control to be suddenly reassigned by their rule makers, specifically in a way that is difficult to resist. It is from this new data control paradigm that each use case for blockchain emerges. Reliably assigned rights (e.g. "Code is law") means that users have increased confidence in shared data - they become shared facts. Smart contracts extend this to shared rules, in particular regarding the ex post consequences of future actions. Circumventing intermediaries can be understood as a corollary of user centric data, and a potential use case.

1.4 Research questions

We summarize the introduction so far as arguing that the science of blockchain revolves around the invention of a new data control paradigm. A new way to store and agree facts. This simplifies blockchain down to a record keeping technology with reduced cost of verification. The most important measure of a blockchain's differentiation is decentralization of control - and this metric is defined wider than the number of nodes / miners / validators that contribute to consensus. Multiple applications, or capabilities, emerge from blockchain, including: payment systems, tokens, trustless systems, identity wallets, disintermediation and smart contracts. Some of these existed previously, and some did not. With that we move on to research questions.

The over arching research question is can blockchain solve real world economic problems? Ultimately this question addresses the key critique of blockchain, that it is an overhyped technology of little incremental value. Conversely high incremental value is a corollary of solving real world economic problems. A good starting point for addressing the high level question is to formulate a

[2] vitalik.ca/general/2021/05/23/scaling.html

better understanding of blockchain systems, with our focus being on PoW blockchains. Our first, of four, sub-question tackles this.

- What are the drivers of Bitcoin mining revenues? How does this relate to transaction processing capacity?

  This question will be examined in Chapter 4. A version of this has been published in the journal Applied Economics Letters (Lo and Medda, 2018). The question is important as Bitcoin is a dominant pole in the blockchain literature, as well as the cause of critiques related to its low transaction processing capability. This thesis adds to the literature an empirical study of Bitcoin mining, a critical element of the economics of PoW. It finds that mining revenue is highly correlated to the price of Bitcoin, and less correlated to transaction volumes - up until capacity constraints become binding. We argue that the low scalability of Bitcoin is primarily a design choice that is appropriate for a digital gold use case. We differ with arguments that low scalability is a function of decentralization, as we care about the benefits of decentralization, not the number of nodes. Resource intensity is a feature of PoW, but low transaction processing capacity is a design choice that preferences the number of nodes.

- Do blockchain tokens, and the project that issues them, have an observable economic connection?

  This question will be addressed in Chapter 5. A version of this has been published in the journal Information Economics and Policy (Lo and Medda, 2020). One important capability of blockchain is its ability to formulate tokens that are easily sent and traded. Papers such as Catalini and Gans (2016) provide strong arguments regarding the benefits of tokens, but there is less literature on what blockchain tokens are. We identify a key assumption underlying that literature: that there is a link between a token and the issuing project, in the absence of any legal connection. In this Chapter we categorize tokens by function and find that token function dummies have a statistically significant impact on their trading price. This provides evidence of an economic connection. That this connection exists is necessary for token use cases such as venture funding.

- Can blockchain improve the completeness of a financial market?

  This question will be addressed in Chapter 6. A version of this has been published in the Journal of Financial Market Infrastructures (Lo and Medda, 2022). Incomplete markets are a real world problem, reflecting a major gap between reality and the assumptions of many economic models. We add to the literature a study of the price of Ether on a DEX and the price of Ether on centralized exchanges. We find that they are cointegrated, which is a necessary condition for DEXs to be effective. We explore the automated market maker mechanism used and argue that a corollary of liquidity pools are that they provide continuous liquidity. If they do so when market makers are absent or withdraw, then DEXs may improve market completeness.

- Can blockchain improve data integrity?

  This question will be addressed in Chapter 7. Data integrity is a problem that has been explored by the literature, and that blockchain has the potential to improve. We use a case study methodology to discuss a real world example of an enterprise using notarization, to a public blockchain, in order to improve data integrity and therefore its reliability. This work is beneficial to companies which can use a similar notarization process to improve the integrity and auditability of its internal data. We put forward three internal data use cases that are highly suited to blockchain notarization: regulatory process, employee fraud prevention and dispute mitigation. This chapter provides an example of blockchain moving from primarily price speculation based use cases typified by tokens, to more nuanced utility applications consistent with Gartner's slope of enlightenment.

1.5 Thesis contribution

Arguing that blockchain can solve real world problems, the central question of this thesis, is not as clear cut as proponents of the technology would like to make out. Part of this relates to some of the limitations of early blockchains. If blockchains are only capable of 5 transactions per second, the answer is likely no. If blockchain tokens have no connection to their underlying ventures, then the answer is likely no. If blockchain digitization of facts and centralized digitization of facts are the same then the answer is no. These are some of the doubts that justify the high level question. In order to examine this, the four narrower questions (1) review the mechanics of proof of work, (2) test a key assumption of the token literature, and (3) juxtapose two real world problems with two blockchain based solutions.

The findings arising from these questions makes a number of contributions to the literature. We focus on three. Firstly is the evidence that it is valid to assume a token is connected to its issuing project. There are many papers, such as Catalini and Gans (2016), that build theory and evidence regarding the benefits of tokens. Many token markets are visibly driving economic behavior. Much of this research and activity depends on the assumption that tokens are connected to the underlying project, despite the lack of a legal connection.

The second contribution relates to decentralized exchanges. Unlike with payments and price discovery, this application of blockchain was not commercialized previously in a centralized form. Although it directly competes with centralized exchanges, never before had we seen liquidity pool based markets which react passively to the behavior of other traders. Decentralized exchanges, such as Uniswap V2, enable trades at any volume and any price (with an inverse relationship), filling gaps that may exist on other venues. Chapter 6 contributes evidence of effectiveness, and therefore that such decentralized exchanges can improve market completeness. The latter is a critical real world problem and a major assumption across the field of economics.

The final contribution relates to the field of data integrity. This thesis adds a case study of a real world, revenue generating application of blockchain to the literature, that is not dependent on tokens and price. The case study explores the use of blockchain for Know Your Customer / Anti Money Laundering purposes, which improves process and auditability. It then discusses applicability to adjacent potential use cases, such as employee fraud prevention and dispute mitigation.

The collective importance of blockchain application research is two fold. Initially, it is due to increasing doubts regarding the value of blockchain. These doubts are valid, but we argue they are the result of misunderstandings around what blockchain does, its design choices, and its limits. This thesis contributes evidence of where blockchain is feasible and appropriate, and why it is often not appropriate. The follow on point is that only by better understanding the technology will it deliver the desired benefits and fully meet its potential. This research may in the future assist governments, regulators, companies and entrepreneurs in fully utilizing the ability to govern data in a new way. In particular, the research on a connection between a token and a project is relevant for financial regulators looking to adapt regulatory frameworks to digital tokens. It supports important regulatory actions such as SEC (2017, 2018a,b). Conversely the two application Chapters guide and support enterprises looking to improve completeness of markets and the integrity of their data.

Chapter 2

Literature review

2.1 Dissecting the hyper threaded topic of blockchain

This chapter reviews the economic literature, however many adjacent areas are housed in a separate Blockchain review (Chapter 3). Further, some topics of the literature review have been included in later chapters where appropriate. We summarize and relate the threads that connect them in this section. When reviewing the economic literature, it is tempting to jump straight into describing the rapidly growing field of blockchain economics (Section 2.6), or to start by referring to existing economic theories (Section 2.4). But this would be to do a disservice to the fact that blockchain is in fact multiple mechanisms; that entrepreneurs are trying to evolve into different mechanisms; each of which potentially justifies their own area of study. Broadly, it is possible to consider blockchain in three threads. The first is as a mechanism to enable decentralized record keeping (Section 2.5). A corollary of this would be the potential for decentralized decision making and organization - which minimizes the dependency on leaders and trust. Secondly are the tokens that can be created by such a system (Section 3.3). The censorship resistance of blockchain means that such tokens may be credible even when issued by a small group that a user does not trust or consider reliable. Censorship resistance can be used to break rules (Section 3.5). It is noted that both record keeping and tokens can be separately used to enable payments and the transfer of value. The third thread are blockchain synonymous technologies such as smart contracts (Section 3.4). Smart contracts are shared computer code used to create many tokens, but can also manipulate tokens, and behave predictably under alternative scenarios.

For each of these high level categories, it is justifiable to discuss how blockchain carries out each of these functions separately from the literature analyzing the related economic impacts. Unfortunately even this is insufficient to encapsulate the knowledge in the space. The term decentralization needs to be defined and contextualized (Section 2.7). Decentralization then has its own place in the economics of how blockchain works (Section 2.8). Bitcoin, the first and foremost blockchain token, spans both the first and second threads and deserves its own section as a particular application of blockchain - the payment token (Section 4.2.1). A key use case for non-payment blockchain tokens is the raising of finance, often referred to as Initial Coin Offerings (ICOs, Section 5.2.1), which encourages us to also then briefly venture into the capital structure literature (Section 5.2.2). Finance is not the limit of potential blockchain applications, there are others worth mentioning (Section 3.6). Finally there is a growing understanding of the limitations of blockchain (Section 3.8). And to set the scene for this gamut of academic research, we begin by touching on Adam Smith's concept of the invisible hand.

2.2 A note on perfect competition

McNulty (1967) explains how Smith (1776) is often cited as the father of the economic concept of competition, or more specifically the idea of the invisible hand. However references to the ability of buyers and sellers, via a mechanism of price, to eliminate excessive profits and unsatisfied demand was common in the literature prior to Smith's seminal work. Rather McNulty (1967) points out that Smith (1776)'s key contribution was to elevate a highly visible series of cause and effects to the level of general organizing principle of economic society. It would then be later mathematical economists such as Cournot that would transform this definition of competition to "that situation in which P does not vary with Q - in which the demand curve facing the firm is horizontal" Stigler (1957, p5). Later refinements and assumptions would include the need for perfect information and complete markets.

It should be clear that the economic concept of perfect competition is a polemic case designed to form a clear theoretical basis for further analysis. It should also be clear that blockchain, as well as intermediaries, are irrelevant and unnecessary under the assumptions of perfect information, negligible transaction costs and complete markets. Naturally in the real world these assumptions do not hold.

2.3 The role of intermediaries

Coase (1937) showed how the existence of transaction costs is an incentive for individuals to bind their efforts together under the auspices of a firm. Repeated purchases, in particular of services of small nominal value, becomes poor value if the cost of a service is a function of the act of transacting, rather than based solely on the cost of the task. Firms - and by implication intermediaries - may act as economic structures that pool activity to eliminate transaction costs. Shaw (1912) analyzed a variety of purposes for intermediaries, including: risk sharing; transportation; financing; selling; assembling and assorting. Shaw's research highlighted the importance of advertising in differentiation and distribution, without quite explaining why. Stigler (1961) would later identify advertising as an information producing industry, in an economy that faces potentially significant search costs in the acquisition of any good where price and quality is not homogeneous. In this environment intermediaries have a natural role in pooling information and reducing search costs borne by consumers and employers. Building on this work with a particularly memorable turn of phrase, Akerlof (1970) highlighted how asymmetric information, between buyers and sellers of used cars, is likely to squeeze out high quality used cars. This leaves the market containing only "lemons" trading at a single, justifiably low price. Akerlof notes that this is a good outcome compared to continuous distributions of quality where markets fail to form completely. It is at this point that blockchain becomes sharply relevant to the field of economics. It is a technology that enables multiple writers to agree a single record of fact. From this, a private permissioned blockchain implies a consensus of symmetric information between writers, while a public blockchain would denote symmetric information between insiders and outsiders. In Akerlof's example, this might be instituted as the history of a vehicle's ownership and servicing immutably recorded, and accessible to all. It also leads to one vector of how blockchain might impact transaction costs, in line with the related hypothetical activity of an intermediary.

Building on the work of Coase, Williamson (1975, 1985) developed a separate resource based view of the firm, that concentrated on the resources that generate competitive advantage for firms.

One dimension of this argued that market intermediaries can reduce the cost of acquiring information, and the transaction costs of negotiating and enforcing contracts. Bessy and Chauvin (2013) focuses on the role of intermediaries in valuation, but also spends considerable time on the informational aspects that are first order relevant to blockchain. Once assumptions of complete markets and symmetric information are loosened, it is possible for agents to take advantage of market features for gain, including via strategic actions. Information becomes valuable in multiple ways, as its absence implies a cost that is a barrier to transact. For example the cost of finding partners for exchange, costs related to evaluation of product quality, and costs in establishing pricing. The last of these can easily veer to price fixing, e.g. a headhunter groups a strong conventional candidate with unconventional candidates, in order to imply a scarcity of desirable employees. Spulber (1996) explained how intermediaries might delineate a market's microstructure via pricing, clearing, providing liquidity, matching buyers and sellers, searching, offering guarantees and by monitoring transactions.

2.4 Locating blockchain in the economic literature

Placing the phenomena of blockchain in the context of existing economic theory is nuanced, partly because its real world application remains circumscribed. However, it is also because blockchain technology addresses the failure of a core assumption of classical economics, notably perfect information. This backdrop means that blockchain has no natural home in classical economics and yet also has a complex relationship to the literature on imperfect information and intermediaries. Merton (1995) identifies six core functions of a financial system. These include (1) payments system; (2) pooling of funds; (3) transferring economic resources across time / regions / industries; (4) managing uncertainty and risk; (5) generating price information; and (6) addressing asymmetric information and incentive problems. Different bundles of these functions are carried out by the institutions of a financial system, such as its banks, insurers and investment funds. Blockchain can substitute some services performed by a centralized intermediary, but might not deliver as much value as the intermediary it is trying to replace. A number of blockchains, including Bitcoin, are able to function as a stand alone payments system. Decentralized Finance (DeFi) has made progress in a number of other functional categories. Platforms like Aave can pool deposit like liquidity and transfer it via loans.[1] DEXs such as Uniswap match buyers and sellers of tokens and generate price information (Chapter 6). Ventures such as these open up the possibility of creating alternative financial products that are decentralized rather than issued by a financial institution. This gives consumers the opportunity to choose the features and context of the financial service that best suits their requirements. Despite this, blockchain is yet to truly prove itself as an intermediary killer of any kind - despite an increasing number of impressive alternatives. This is because these alternatives are still circumscribed, with most lending on an over-collateralized basis with limited risk transformation. Flash loans are a DeFi innovation requiring no collateral, with risk minimized by having the borrow and repayment transactions confirmed in the same block.[2] New use cases such as these bring excitement, but economics seeks explanatory theory connected to statistically significant evidence.

Three economic theories are relatively straightforward to juxtapose with blockchain. The first comes from the seminal paper of Bresnahan and Trajtenberg (1995) and uses the examples of the steam engine and semiconductors to illustrate General Purpose Technologies (GPT) that contributed to sustained periods of technical progress and economic growth. In a Schumpeterian sense, it is possible to characterize blockchain as a GPT that is disrupting existing economic rents related to patterns of production and exchange (Schumpeter, 1934). Such a framework might view blockchain as factor (labor and capital) augmenting - in other words a superior technology for a specific task. For example, the production cost of transportation may be historically elevated due to poor industry record keeping and record sharing. Daniel Wilson of TradeLens, a supply chain platform, argues that applying blockchain might mean "small amounts of value can be created across the entire supply chain ecosystem because people no longer have to wait for information or actionable instructions".[3]

The second and third perspectives (both partly touched upon with respect to intermediaries in Section 2.3) are Transaction Cost Economics (TCE) and Resource Based View (RBV) of the Firm, related to the work of Coase (1937) and Williamson (1975, 1985) respectively. Coase makes the case that firms are preferred to markets in the presence of transaction costs. Williamson's work develops this by acknowledging that with full rationality, complete information and costless transactions, all

[1] aave.com/

[2] blog.zerion.io/lets-talk-about-aave-defi-s-biggest-liquidity-protocol-6b633b7ca07

[3] blog.tradelens.com/news/how-to-talk-blockchain-to-skeptics

agents can make complete contracts with no need for trust. Therefore in the converse, real world scenario of bounded rationality and incomplete information, an ability to exploit trust arises that is referred to as opportunism. One example of opportunism is in the presence of asset specificity i.e. assets are specialized to the task and difficult to repurpose. Therefore once a party invests in such assets, they become sunk costs that can be exploited ex-post by the other party in a transaction. Within RBV, hierarchical organization and relational contracting become ways to control for opportunism. Blockchain can fit into the TCE and RBV literature by enabling symmetry of information, and via smart contracts expand the contract space and clarify part of the long tail of unlikely outcomes (Cong and He, 2019). Together these could result in lower transaction costs, and therefore represent a new technology that might support markets over firms.

A thorough overview of GPT, TCE and RBV are laid out at the beginning of Davidson, De Filippi, and Potts (2018). This paper then uses this context to argue that both (1) blockchain lowering production costs and (2) blockchain lowering transaction costs might be distracting us from blockchain as a new form of institutional technology. Economic institutions of capitalism have consisted of firms, markets, commons, clubs, relational contracts and governments that furnish society with money, law, property rights, contracts and finance. Instead of supporting markets over firms, Davidson, De Filippi, and Potts (2018) posits that perhaps blockchain is adding a new entry to the list of possible economic institutions. Although a fascinating paper in its own right, Davidson, De Filippi, and Potts (2018)'s argument is somewhat too black and white in its categorization of alternate theories. For instance their example of lower transaction cost in the literature Catalini and Gans (2016) is the leading paper arguing that blockchain is a General Purpose Technology, and makes little distinction between production and transaction costs. In addition, it ignores the dependence of blockchains on others to enforce a digital record on real world outcomes (Abadi and Brunnermeier, 2018). As will be explored further down, blockchains may not have the breadth of applicability consistent with an institutional technology, except in digital spaces where digital enforcement is sufficient.

Taking a more philosophical approach Reijers and Coeckelbergh (2018), introduces the concept of blockchain as a narrative technology. The existing financial system has the power to determine whether a transaction is good or bad. Bitcoin does not do this and therefore changes our view of finance. Reijers and Coeckelbergh (2018) argues that at its heart Bitcoin is a way to enable censorship resistance, reducing the ability of existing systems to decide if an agent is allowed to use a platform, and if their transactions are valid. Despite this, their paper questions whether institutional power will be decentralized or merely abstracted. Kewell, Adams, and Parry (2017) uses affordance theory to explore how distributed ledger technologies might become a force for good, and contribute to the sustainability and development agenda.

Although formulated as a supply chain research framework, Treiblmaier (2019) provides an extremely clear spring board for examining blockchain via four related theories of management and innovation. Beginning with an overview of Principal Agent Theory (Jensen and Meckling, 1976), Transaction Cost Economics (Coase, 1937), Resource Based View (Williamson, 1985) and Network Theory (multi-disciplinary and multifaceted e.g Castells (2011) and Rinehart et al. (2004)), Treiblmaier (2019) puts forward an interesting set of research questions related to what changes might be heralded by the arrival of blockchain technology. These include how does blockchain impact contract efficiency? How does blockchain change transaction costs? What blockchain related resources generate competitive advantage? To what extent does blockchain replace personal trust? Can blockchain eliminate agency problems? Given the answers to these other questions, does it change the competencies and optimal scope of firms?

Overall, a key blemish with mapping blockchain within the sphere of transaction costs and intermediaries via Transaction Cost Economics and the Resource Based View of the firm is that these impacts become solely evolutionary. This thesis argues that blockchain contains revolutionary impacts where markets may form in areas where they currently do not exist as markets or as firms. For example this may apply in privacy, in cultural heritage, and in responsibilities. We have already seen the creation of tradable utility tokens (Howell, Niessner, and Yermack, 2018), that reflect a right to consume a quantity of a platform service. Another less developed area is how shareholder equity is a financing mechanism that involves the trading of a bundle of ownership rights and benefit rights. Perhaps blockchain tokenization can unbundle these functions. It is novel yet broad applications such as these that create grounds to hope that blockchain can influence the nature of economic human interaction sufficiently to justify its own sub-field of economics.

2.5 Contextualizing blockchain as an authentic record

Taking a step back in time, humans have been recording trades since ancient Mesopotamia - perhaps beginning with beads in a clay “wallet” (Jasim and Oates, 1986). With the invention of writing and spreadsheets, the cost of making records has fallen considerably. Yet simply because it is recorded, does not ensure that any economic value is associated with these records. That has required either (1) a degree of trust between the two parties, or (2) an authoritative third party that can stand between, or above, the two. In an exploration of the multi faceted and multi dimensional nature of trust (the definition of which often differs between academic disciplines), Nooteboom (2007) explains how institutions create trust by being a source of reliability. In this framework trust between individuals is typically based on intrinsic motives such as morality, whereas institutional trust is usually more extrinsic and based on tangible rewards and punishments.

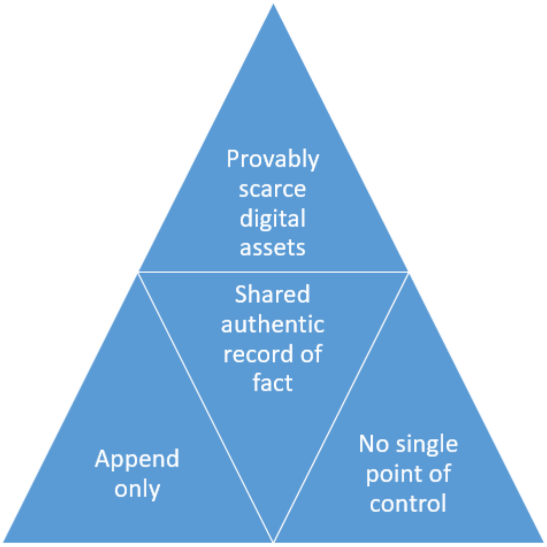

Provably scarce digital assets
Shared authentic record of fact
Append only
No single point of control

Figure 2.1: Two features that improve on integrity of a record - and enable multiple new functions

Blockchain has opened up the possibility of a middle way. One feature that has always been available is public openness - for example in contested elections where vote counts are written on boards outside voting stations. Blockchains adds two uncommon features to this type of transparency. (Nakamoto, 2009) laid out a technical framework that makes records public, append only and with no single point of control. Simplistically they constitute a system that promises to be an authentic publicly accessible record of fact (Figure 2.1 shows this with one possible new capability at the apex). This shared public record, or consensus, with its mathematically quantifiable trust model of record authenticity, is the first breakthrough of blockchain that enables other breakthroughs. Catalini and Gans (2016) makes the case that the power of a blockchain record is its reduction in verification cost of shared facts. That the technology enables both parties involved in a transaction and third parties to cheaply check and verify any records held on a blockchain. "[Blockchain] allows for the verification of transaction attributes in a privacy-preserving way", Catalini and Gans (2016, Page 7). Trust, intermediaries and blockchain are all ways that we can justify relying on a piece of information to be true. Lemieux (2016) separates authenticity - that the record is what it claims to be and is free from tampering or corruption - from the concept of reliability. The latter is the record's trustworthiness as a statement of fact, based on the competence of the author, completeness and controls on creation. Lemieux (2016) observes that paper records can be better than electronic blockchain records where reliability is particularly important. For example, perhaps a government issuing hard copy certificates is the least worst option for constructing a ledger of citizenship. Another way to consider this is that nation states often have the power to censor records separate from whether or not they maintain the record, so are well placed to out compete blockchain where not only authenticity, but also reliability of the record, is critical.

The second breakthrough, as evidenced by the Bitcoin blockchain, is to leverage its decentralized secure ledger to create a digital payment system. Narayanan and Clark (2017) observes the simplicity of transferring value given a secure ledger two parties consider authentic. The payment system underpinning Bitcoin is fundamentally different than existing systems. One way to illustrate this is to identify who stands behind alternative ways of transferring value. A physical note of fiat currency is backed by a country's issuing authority, typically part of the state's central bank. An electronic bank deposit is backed by the financial institution offering the depository service. A cash balance on a smartphone based loyalty application, such as Starbucks, is backed by the firm managing the scheme. A cryptoasset is not backed by any person or any organization.

It is important to understand that a blockchain based payment system does not necessarily require its own native cryptoasset. Although Ripple[4] the company does have a cryptoasset, the latter is not required to make payments on their platform. Therefore we separate out a third breakthrough, which is a class of entity that did not exist previously: provably scarce digital assets (Figure 2.1). At its heart, the features of (1) a tamper resistant record of history, (2) the absence

[4] ripple.com/company

of political authority, and (3) third party verification, provides guarantees of authenticity at the same time as minimizing the risk of censorship. A new literature is emerging to better understand economics of this new decentralized record keeping technology and what activities it makes newly feasible.

2.6 The economics of what blockchain does

As discussed in Section 2.3 and 2.5, blockchain can substitute for intermediaries, or solve for gaps where intermediaries or markets have not formed. Section 2.4 lists out a variety of economic costs, such as opportunism, and how a reduction in verification costs has the potential to address them. However, given the various caveats to blockchain's prospects of replacing powerful intermediaries, and the difficulties so far in moving blockchain from theoretical use cases to applications, it is fortunate that the benefits of blockchain are wider than this. Catalini and Gans (2016) builds on verification costs and argues that blockchain's largest benefit, for new use cases, could arise from reductions in networking costs. Networking costs relate to the lowered barriers to creating provably scare tokens - and what is then possible with said tokens. This group of benefits is sometimes referred to in the concept of tokenomics. Catalini and Gans (2016) divides this networking cost into two separate aspects, or phases. The first phase is at start up, where issuing a token to crowdfunders in an ICO finances the project, and offering the token to partners and employees is a form of early employee equity. These uses of a token help bootstrap the launch of a new venture. The second phase is the operation and scaling of the project. Tokens can be used to reward miners to process transactions (Bitcoin, Ethereum), pay infrastructure providers to offer storage (Filecoin, Storj), or incentivize individuals to generate content (Steemit). Blockchain "allows open source projects and startups to directly compete with entrenched incumbents through the design of platforms where rents from direct and indirect network effects are shared more widely among participants" Catalini and Gans (2016, page 21). Previously, issuing an economic token to govern a small community was prohibitively expensive. The lower verification costs of shared facts by blockchain enables tokens and micro-economies at dramatically smaller scale. These micro-economies open up new ways of sharing the benefits of a community - and have lowered the cost of tokenization - where the token is a economic or sociological moderator that changes the relationship between two or more agents.

The smart contracts (that can be used to implement tokens on a blockchain) have additional non-token related benefits. In an important paper connecting the technology to the economics of blockchain, Cong and He (2019) provides a formal proof of how a blockchain based consensus, that includes smart contract based prices contingent on delivery, can support new entrants. In their framework, new entrants signal quality by trustlessly guaranteeing buyers compensation if the product fails, explicitly enlarging the contract space. This would address a second major assumption in economics (after perfect information) of complete markets.

2.7 Defining decentralization

The above subsection 2.6 can be thought of as an overview of two things (credible tokens and contingent contracts) that were difficult previously but are conceivable and practical with blockchain. It forms part of the basis of the research thesis, its research questions and its component papers. But it is only one corner of the literature on blockchain. Another putative benefit of blockchain is decentralization. This is only indirectly addressed via a discussion of lower verification cost of shared facts (which is one output of a decentralized system of many writers who can straightforwardly verify each other's contributions). However decentralization is not merely a benefit but also part of blockchain's structural design, and therefore extends into the economics of how blockchain works. Delving more deeply is complicated by the fact that the term decentralization is poorly defined, and definitions of decentralization often contradict between disciplines, and between users of the phrase. Schneider (2019) explores the word decentralization by surveying its usage across politics, economics and blockchain. In his seminal text on American democracy, Tocqueville (1838) analyzes centralization, and decentralization, of political authority. In economics the term first appears in English directly imported from Bastiat (1846)'s use of décentralisation in the treatise *Popular Fallacies Regarding General Interests.* Compared to the broader social sciences, blockchain and cryptoassets can delineate decentralization in a relatively specialized way. In a blog posting,[5] Vitalik Buterin, the founder of Ethereum, splits the term into (1) Architectural decentralization 'How many physical computers is a system made up of?' (2) Political decentralization 'How many individuals / organizations ultimately control these computers?' and (3) Logical decentralization

[5] medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

‘Is it possible to split the interfaces and data structures and have both halves operate independently?’ Jamie Burke, CEO of Outlier Ventures, an investor in blockchain tokens, puts forward a typology almost completely technology specific - offering five aspects of a blockchain as metrics of decentralization.[6]

- Consensus formation - who controls the nodes determining consensus?
- Protocol value - how decentralized and distributed is the value capture in the network
- Protocol improvements - who controls the product road map?
- Conflict resolution - how are disputes resolved and enforced?
- Platform development - how many people / organizations are building on a network?

Based on their wide ranging survey, Schneider (2019) argues that periods of decentralization - and typical follow on periods of recentralization, are an illusion - with an underlying shift of power and control simply becoming visible over time. A key example of this is how the decentralizing technology of the Internet has led to large centralized Internet monopolies such as Google, Facebook and Amazon. If we somewhat inappropriately apply Outlier Ventures’ criteria to two platform Internet businesses, Airbnb would be centralized on all these dimensions, while Google’s Android would be centralized on the first four and decentralized on platform development.[7] This line of reasoning also has some validity in blockchain, as although cryptoassets offer decentralization across many measures, typically they are then held and traded on centralized exchanges with the risks that imply (Brandvold et al., 2015; Gandal et al., 2018). Irrespective of this, it should be noted that there is a leap of logic between a technology that is decentralized on one or more dimensions, and the conclusion that centralized groups will inevitably capture the majority of the value creation. Path dependence is far from forming a theory with explanatory power, with a literature that often confuses the process of history unfolding in a self-reinforcing manner, with an outcome of a persistent state of affairs with specific properties (Vergne and Durand, 2010). At the time of the creation of the Internet there was no technology that enabled decentralized third party verified record keeping. This is the technology of blockchain. Analysis of blockchain enabled

[6] outlierventures.io/research/pathway-to-decentralisation

[7] airbnb.com and android.com

decentralization is the hub of many of the most important questions in blockchain. Aste, Tasca, and Di Matteo (2017) highlights a few of these, for example: is a peer-to-peer disintermediated market more reliable than a traditional one? Does it have more or less protection for participants? Does it have a greater ability to deal with stress?

Another way to consider decentralization relates to who is allowed to use a platform. Raskin, Saleh, and Yermack (2019) defines centralization depending on if a party is not prevented to participate or there does not exist someone who can act in such a way. In other words free entry of users determines if a digital currency is decentralized. For our purposes we focus on the architectural and political decentralization discussed by Vitalik Buterin. The measure of these become the number of points of failure and the number of points of control respectively. A centralized system has one or more points where a technical problem could bring down the entire system, and an ultimate single point of control. In such a system a failure of 1% of the network can eliminate 100% of network performance. A perfectly architecturally decentralized system contains no points in the network where a failure could bring down the entire system - network activity is correlated with network performance. A perfectly politically decentralized system has no points of control. Blockchains and distributed ledgers sit somewhere on a continuum between these poles, a position likely determined on the Bitcoin blockchain by the number of mining pools, but also by the objectives of key developers. Gencer et al. (2018) use a longitudinal measurement study, and find that 90% of mining power (hashpower) is controlled by 16 entities on the Bitcoin network and 11 entities on the Ethereum network. However the identity of these entities are dynamic and varies with investments in computation, mining pool organization and the price of both tokens. Stepping away from the conundrum of grading levels of decentralization, outputs of even relative forms of decentralization offers potential benefits such as fault tolerance, mitigation of vulnerability to attack, censorship resistance, limits on collusion and increased competition. Overall, although the direct economic benefits of decentralization are hard to scope, these benefits form an important area for future research. In addition to this, another vector would be the value of nodes on a Proof of Work blockchain that do not contribute to consensus. In Section 1.3 we emphasize the centrality of political decentralization, and de-emphasize architectural decentralization because cloud providers like Amazon AWS possesses the latter but not the former. The focus research should be on what blockchain changes, not what it repeats.

2.8 The economic cost of blockchain decentralization

This section drills deeper into the authentic record thread of blockchain research by delving into the economics of how blockchain works and the associated cost of implementing decentralization. Ma, Gans, and Tourky (2018) maps the Bitcoin protocol to a game between miners, and highlights the role of competition and free entry in determining system costs. These costs are likely to be wasteful, at the same time as driving miners' equilibrium profits to zero. Their work notes that regulation, for example dynamically deciding the number of miners, as one way to reduce system costs. It also sets a different tone to much research on resource consumption in calling for further analysis of what benefits are being derived from decentralization. Abadi and Brunnermeier (2018) discusses how blockchain splits a centralized ledger into separate proposer of rules (e.g. developers) and record writers (e.g. miners). Both blockchains and centralized ledgers control a valuable set of user data. This user data, which can be a straightforwardly financial balance of currency or as intangible as an individual's social media account, is a stake in the network, that enables a centralized ledger keeper to charge an economic rent. Users' stakes embed value in an incumbent ledger relative to any new competitor. However blockchain forks enable users to take their ledger data with them, increasing competition as user stake no longer locks them into a given platform. Furthermore, free entry of record keepers plays a crucial role as it makes record keeper profits zero at equilibrium, ameliorating their opportunity to bribe and collude in such a state. Abadi and Brunnermeier (2018) also explains how blockchain forks that roll back history are powerful defense mechanisms against attacks, and how real world enforcement requirements may favor a centralized ledger.

One aspect of this decentralization is explored by Huberman, Leshno, and Moallemi (2019), who compare a stylized Bitcoin payment system (BPS) with a monopolistic payments firm. The latter charges higher willingness to pay users and processes transactions without delay, the corollary of which is to exclude low value users. The BPS serves everyone with a delay, generating strictly positive economic surpluses for all users with charges based on platform congestion. The trade off is a costly set of infrastructure that ensures competitive pricing (as small miners enter freely), versus private monopolist dead weight losses due to price discrimination. This paper is the clearest so far in arguing that decentralized blockchain based payment tokens are welfare enhancing.

Considerable research is now focused on reducing the cost component associated with no single point of control under proof of work (Bentov, Gabizon, and Mizrahi, 2017; Eyal et al., 2015; Li et al., 2017; Rocket, 2018). Budish (2018) explores this cost via a series of equations. Under a condition of repurposable mining technology, at equilibrium such a blockchain system would have (1) zero-profit miners and (2) incentive compatibility such that the computational costs of majority attack exceed the benefit to the attacker. These two points imply a third condition: that the recurring "flow" payments to miners are large relative to the one off "stock" benefits of attacking this blockchain i.e. the system is fundamentally expensive. Under the alternative assumption of non-repurposable mining technology, which is the case with specialized Bitcoin ASIC miners, then an attacker also risks the value of its sunk investments in equipment. This mitigates the original system cost conditions, at the same time as raising a fresh critique. The higher the value of Bitcoin in aggregate, the higher the potential vulnerability to a sabotage attack that wishes to profit from a collapse in value. Budish (2018) suggests this may ultimately lead to a ceiling on Bitcoin's value. Collectively the literature on the expense of proof of work blockchains catalogs the high price of using such a mechanism to ensure there are many record keepers and their profits at equilibrium are zero. The papers above put forward a host of approaches that do indeed reduce this expense, but so far it has been difficult for their authors to prove that users are willing to pay for the extra complexity and reduced censorship resistance. This is actually surprising as the benefits they promise are clear, while the costs introduced are ambiguous. Reasons as to why a higher cost payment token continues to dominate the blockchain ecosystem are easy to put forward e.g. first mover advantage and the importance of coordination, but hard to prove. Note that the inevitable success of a single blockchain fork is critiqued by Biais et al. (2019).

Chapter 3

Blockchain review

3.1 The bounded capabilities of Blockchain

What is now possible with the liberation of data governance and data ownership alluded to in Section 1.3? Despite the success of blockchain in a number of related areas, strong narratives in this field results in numerous category errors and explanations that distract from important points. Identifying these errors and limitations is a key part of answering the primary question in 1.4: can blockchain solve real world problems? As discussed, using Bitcoin to illustrate blockchain (which we do in Chapter 4) often leads to confusion between the technology and its use case of tokenization. We use the future launch of a Chinese CBDC[1] to illustrate how a cryptoasset payment system is arguably the first capability showcased by a blockchain. The creation of digital tokens like Bitcoin can then be considered the second capability.

A CBDC is a good way to explore this intuition as such a new electronic currency would be a close substitute with bank deposits. This highlights how the point is not the payment token but the payment system. The United States and its allies control the SWIFT international payments system and the clearance of dollars - used to both cut off Iran (Majd, 2018), and to sanction Russian banks.[2] Critically, a blockchain based Chinese digital currency would bootstrap a new payments system that can operate largely separate from the SWIFT international payments system. We observe how a ledger we collectively agree on is a natural value transfer system. Building on this

[1] scmp.com/economy/china-economy/article/3043134/chinas-new-digital-currency-isnt-bitcoin-and-not-speculation

[2] dw.com/en/eu-us-uk-to-exclude-some-russian-banks-from-swift/a-60931401

point, BOE (2020) discusses the potential resiliency benefit of a core payment network that sits outside the commercial banking system. Note that both blockchain based payments and tokens compete with centralized competitors that are deployed today e.g. SWIFT and the Starbucks loyalty app respectively. The benefits of a new payment system are separate from the benefits of a token. One of the latter would be Catalini and Gans (2016)'s reduction in networking cost - the ability to incentivize communities and accelerate ventures. Offering and even giving away tokens raises the possibility of a novel asset and liability in the capital structure (See Chapter 5).

A separate misunderstanding is the idea that blockchain creates trust - The Economist describing it as a Trust Machine.[3] Yet this confuses a human feeling with the academic definition of trust. Hawlitschek, Notheisen, and Teubner (2018) observes how different disciplines define trust differently, but broadly share a core concept of accepting vulnerability on the basis of positive expectations. Blockchain does not increase the acceptance of vulnerability, but minimizes the need to be vulnerable. Journalists may be trying to assert that blockchain can manufacture reliability, not trust. For example, imagine a situation where a woman lends a friend her apartment. In this circumstance, the transaction can plausibly occur based solely on trust. As this expands to a transaction with friends of friends, or to strangers in the same city - trust is no longer sustainable. Three things together can take the place of trust: a record, the ability to verify that record, and enforcement of rights consistent with this record. This describes a contract with legal redress. For large numbers of transactions, individual contracts with these functions are less scalable. Instead large sets of records, or ledgers, of this type have utilized a centralized third party, such as a government, a bank, or in our example a firm such as AirBnB.[4]. Nooteboom (2007) notes how centralized institutions can substitute for trust via consistency and reliability. Historically, in the gap between trust and centralization, where trust is inadequate yet the cost of a centralized counterparty is too great, markets and trades struggle to form (Catalini and Gans, 2016). This gap is one of the contexts where trustless blockchain systems can help. Intuitively this can be thought of as the unmediated risks (or trust vacuums) that exist in society, for example where a restaurant's lamb stew is in fact horse - and in this situation might be addressed by blockchain provenance solutions. Catalini and Gans (2016) argues blockchain does this by lowering the cost of verification. If the

[3] economist.com/leaders/2015/10/31/the-trust-machine

[4] airbnb.com

meat provider and the restaurant utilize such a solution, then provenance is vouched for. This does inject another caveat, blockchain does not prevent the slaughterhouse from deceit (the writer of the data), it only reduces the ability of the restaurant to deceive (the relayer of the data).

Abadi and Brunnermeier (2018) explores the trade offs at the intermediary layer by proving a blockchain trilemma: that it is impossible for a digital ledger to be rent-free, trustless and resource efficient. The options under this are contextualized as either a centralized ledger that charges an economic rent; a Proof of Work ledger that is resource intensive; or other types of ledgers that require trust or safeguards external to the system. Another way to think of this is that Centralized ledgers and Proof of Work blockchains are incentive compatible - and that you do not need to trust a system that is being paid to be honest or that requires electricity to participate.

The above blockchain trilemma clarifies how blockchain systems are not strictly superior to existing centralized systems. On top of this there is the enforcement gap, with blockchain able to enforce digital records but not physical reality. Ergo, enforcement may be an important activity provided by an intermediary. Two hard edges to the capabilities of blockchain should now be becoming visible. The benefit of blockchain begins subsequent to the data creator, and ends prior to any need for enforcement in the physical world. Only when the property and rules at stake are digital, can blockchain offer enforcement. Expanding from enforcement issues, arguments in favor of blockchain disintermediation often ignores other activities performed by intermediaries. This can relate to core purposes, largely unaddressed by blockchain, such as the transformation of risk and maturity by banks. Despite these caveats, blockchain is a powerful mechanism for creating and holding facts, and provides a novel alternative where arguably either an intermediary charged an economic rent, or where no alternative existed before. The thrust of the argument becomes the need to be more astute regarding its application.

Finally, blockchain is not merely about shared facts, smart contracts on blockchain infrastructure can also create shared rules. Smart contracts are better described as shared computer code that can manipulate state. They are first mentioned in Szabo (1994), who imagined that “They react on events, have a specific state, are executed on a distributed ledger, and are able to interact with assets stored on the ledger”. The idea is that shared computer code can now be verified and relied upon. Again, agents can then act on them in confidence, not merely with respect to information about the past, but on their future behavior based on future events. With smart contracts the potential use cases of blockchains widen dramatically, including for the Decentralized Exchange in Chapter 6. On that note, we move on to discussing various mechanics, features and applications of blockchain.

3.2 Blockchain as a mechanism

A large number of research papers have mapped out the state of the literature on blockchain, from computer science to economics. Bohme et al. (2015) is an introduction to the Bitcoin ecosystem and its economics. Zheng et al. (2018) provides a concise survey of the blockchain. Yli-Huuomo et al. (2016) is a computer science orientated literature review of blockchain. Xu, Chen, and Kou (2019) is a systematic review of 119 business and economic academic articles selected from a sample of 756 research papers on the topic of blockchain. Collectively they suggest that blockchain is well beyond the status of "new" technology. One caveat to any discussion of a technology's (past and future) relationship with society must also observe that society has endogenously created that technology. A sequence of self-reinforcing path dependent decisions may have begun with an uncorrelated human decision - in other words it is important to be wary of technological determinism. Narayanan and Clark (2017) connects a panoply of historical research relevant to the invention of Bitcoin, and then to recent attempts to adapt the underlying technology. Although attempts at applying blockchain to new areas often gives the sense of a solution looking for a problem, Bitcoin is very much an engineered solution to avoiding the use of a financial institution when making a payment - as noted in the abstract of Nakamoto (2009). The first question that arises in creating a ledger with distributed control is: how to measure or justify the importance of individual participants? A corollary of this is how to defend against Sybil attacks, which is where fake identities are created in order to manipulate the system. PoW is the Bitcoin blockchain's answer to this.

In the rest of this section, we address the operation of the Bitcoin blockchain. Narayanan et al. (2016) provides a summary of the technical framework of blockchain, a sketch of which follows. The information layer of the Bitcoin blockchain consists of blocks of transaction data linked together, such that an attempt to change one transaction, requires changing all those chained after it. A simpler way to describe this immutability is that the data is append only. Many writers are involved in the writing of records. Any processor (referred to as a miner), authentic or adversarial, can compete for the right to add a block to the chain, and garner a reward of cryptoasset, by solving a compute intensive cryptographic puzzle referred to as Proof of Work (PoW).

PoW is the mechanism behind the system decentralization, firstly by protecting against Sybil attacks. PoW makes the number of identities irrelevant by making computational power the key measure of significance within the system. PoW empowers a rule that the longest chain of proofs determines consensus regarding the state of the world. The longest chain rule is the consensus mechanism, but PoW makes it stable in the presence of multiple writers. Public keys, known as addresses, link transactions with pseudonymous address owners. Together, this web of computer science, game theory and cryptography, delivers the provably scare, measurably secure, and highly fungible digital asset of Bitcoin (Nakamoto, 2009). It produces a ledger that contains valuable information without use of a single point of control e.g. government department or bank. The corollary of immutability plus architectural decentralization plus political decentralization is censorship resistance. Immutability makes changing the data difficult, while the two types of decentralization means no single party has the power to break the rule of immutability without meeting a quantifiable level of opposition.

Two specific vulnerabilities of PoW blockchains relate to 51% attacks and selfish mining. Nakamoto (2009) explained the risk to a PoW blockchain of an attacker with greater than half of the computational power of the network. Such a party would have a high probability of determining the longest chain, and then be able to engage in double spend attacks that issue and rewrite payments, repeatedly spending the same payment tokens. Sayeed and Marco-Gisbert (2019) provides considerable detail on previous 51% attacks. It notes the largest loss from a series of these attacks as USD 18 million of Bitcoin Gold extracted from cryptoasset exchanges. Eyal and Sirer (2014) lowered the bar for malicious behavior to 25% of network computation power. Under these circumstances it becomes possible for a large miner or writer of blocks to engage in selfish mining, whereby keeping blocks temporarily private can trick competitors into wasting effort on orphan blocks that are ultimately excluded from the true chain (i.e. is determined to not be canonical with the respect to the state of the world).

Each distributed ledger mechanism for achieving consensus among nodes has two parts. For example PoW protects against Sybil attacks, and longest chain finds consensus regarding the true chain. Permissioning and PoS are the main alternatives to PoW, but are not on their own substitutes for longest chain. All of these frameworks produce architecturally decentralized distributed ledgers with no single point of failure. As explained above, Nakamoto consensus (Bitcoin) blockchains with PoW and unpermissioned free entry of writers, adds no single point of control to architectural decentralization - even if the actual level of political decentralization is up for debate (Gencer et al., 2018). On the other hand, permissioning is where writers must be authorized by a rule making authority. This addresses Sybil attacks but as explained in Section 1.3, permissioning reflects a clear creep back towards single point of control. It weakens any claim of political decentralization. A distributed ledger combining append only with merely no single point of failure can in practice end up delivering a narrower form of tamper resistance than a blockchain (See Figure 3.1).

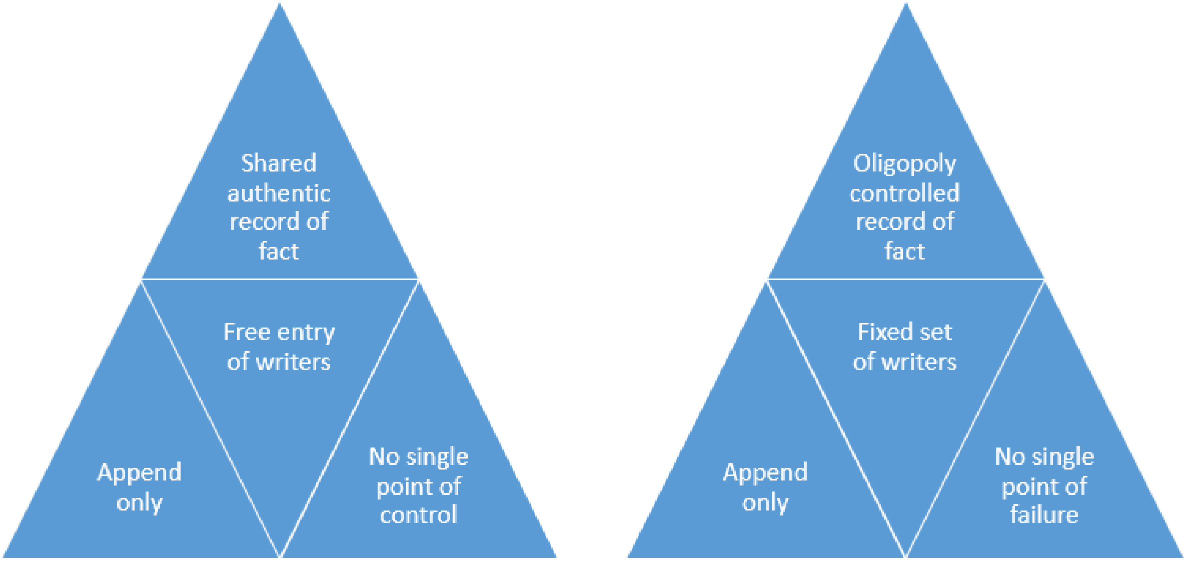

Shared authentic record of fact
Free entry of writers
Append only
No single point of control
Oligopoly controlled record of fact
Fixed set of writers
Append only
No single point of failure

Figure 3.1: Single point of control (left) and single point of failure create different types of records

Moving on, PoS replaces the hashing competition of PoW with a leader election correlated to stake size. The proportion of tokens held and staked determines an agent's probability of being elected leader and given the right to append the next block of data. (Li et al., 2017). As one block is added to a sole canonical blockchain, the conundrum is no longer how to determine which chain is correct. Instead it is how to validate the writer of the latest block. Both permissioned distributed ledgers and PoS uses Byzantine Fault Tolerance (BFT) mechanisms to create consensus (Vukolić, 2016). BFT is a decades old messaging based consensus protocol that resolves disagreements in the presence of malicious agents. It has in the past required permissioned data writers, and is rarely used commercially (Chondros, Korkordelis, and Roussopoulos, 2012). A set of upgrades referred to as Ethereum 2.0, addresses the potential need for permissioning by allowing any stake of 32 Ether to be sufficient to qualify as a validator node.[5] PoS can reflect no single point of control, which justifies its inclusion within the blockchain category. This does not however change the trust critique of Abadi and Brunnermeier (2018), and the increased overlap between rule makers and data writers (Chapter 1.3). The dominance of Bitcoin and Ethereum 1.0, on many measures such as market capitalization, suggests that PoW and the longest chain rule continues to be the leading way to implement ledgers with no single point of control.

3.3 Provably scarce digital tokens

The functionality of tokens issued on a blockchain is one axis of this thesis. A logical starting point for investigating this is to ask: what is a digital token? Unfortunately, the dictionary is little help, Merriam-Webster having simply added “a unit of cryptocurrency” to its definition of token.[6] Additionally, we decline to use commercially centric conceptualizations of a token such as a “unit of value that an organization uses to self-govern its business model”.[7] Instead we put forward our own definition: digital tokens are scarce entities that embody rights and / or responsibilities and act as a moderator on economic behavior. Rights are a useful term as it includes purchasing power, but also non-fungible tokens (NFTs) that reference digital art and goods. Such a formulation arguably ends up including electronic bank balances as tokens. However pure blockchain tokens are provably scarce digital entities (by third parties using public information), whereas bank deposits are merely credibly scarce. Conversely, it is observed that the ability to include a responsibility is far removed from what is expressed by tokens presently. Although it is outside of the scope of this thesis, we expect the tokenization of non-financial items such as responsibilities to gain traction.

What is the difference between a blockchain token and a centrally issued token? The literature review above has illustrated that the technological rails formulated by blockchain are novel, not simply relative to technology in production (for example a centralized mainframe or centrally managed cloud computing network), but also relative to decentralized products rigorously developed by academia e.g. BFT systems such as PBFT and Paxos. The technology of blockchain has changed

[5] blog.sfox.com/ethereum-2-0-what-the-next-three-years-of-ethereum-will-look-like-b366a46f9704

[6] www.merriam-webster.com/dictionary/token

[7] William Mougyar, author of The Business Blockchain

the production possibilities frontier for records, contracts, and tokens - and therefore the role of ledger based points of control (Section 2.8). Blockchain creates decentralized systems with no single point of control. From this it follows that the blockchain tokens that run on these rails will share some of this novelty, but to what extent and in what way?

A simple observation to make is that the usefulness of a token and its level of political decentralization are separate phenomena - large, credible firms can issue similar tokens without using blockchain. For example Starbucks allows customers to make cash payments into a centrally hosted loyalty scheme - and act as a form of private non bank money denominated in fiat (Brainard, 2020). In practice once payment is made into Starbucks' smartphone application, individuals have exchanged money for digital coffee tokens denominated in US dollars - in a way that helps fund Starbucks' operations.

In spite of this, the relationship between a token holder and a token is different, whether it is centrally issued, or issued on a blockchain. The holders of the former take on a tail risk of the institutional backer defaulting on its liabilities, but if this does not happen, not only are they able to contact the institution's customer service department, they may also have recourse to dispute mechanisms such as the Courts of Law. The holders of a blockchain token do not have to be concerned about the issuer entering bankruptcy proceedings, but they have limited recourse outside of what is programmatically coded in the token. Superficially this does not put blockchain tokens in a favorable light - until they are compared with past corporate token programs. In a survey of airline frequent flyer programs, Boer and Gudmundsson (2012) observes that by 2005 frequent flyer points accruals exceeded capacity growth by a multiple of ten. Ultimately both accrual mechanisms, and rates of exchange into reward flights, were made less generous until reward programs had positive net present value for the airline. Returning to the Starbucks example, the firm reserves the right to change and terminate both the program and a user's account at any time.[8]

Because of this, the second key change (other than changing the role of issuers and intermediaries) of a blockchain token is that small, non-credible firms and groups can now issue tokens that are as reliable and credible as those that have been issued in the past by large organizations. In other words, a craft coffee shop can issue a digital cappuccino token almost as valid as the Starbucks loyalty scheme. This is the reduced barriers to issuing a token. Certainly the craft coffee

[8] starbucks.com/rewards/terms

shop does not have the financial balance sheet of a large multinational corporation, but the token itself potentially offers a set of guarantees regarding quantity issued and verification of ownership stronger than available from a centralized issuer.

Issuer defined claims and promises can be attached to a token at two levels: those that are made in associated documentation, and those that are written in the software code. Cohney et al. (2019) surveys the 50 largest token issues of 2017, and compares marketing promises with smart contract code. They find that most promise a token supply cap, and two thirds deliver this in code. However they also find that a quarter (12/45) enabled code modification - for example by referencing another smart contract that can be easily replaced. Their survey highlights the opportunity to use technology to address agency costs, at the same time as revealing major issues in implementation.

In terms of the capabilities of tokens, we hew to Catalini and Gans (2016), that introduced two umbrella benefits from issuing tokens under the term network costs: (1) venture bootstrapping; and (2) platform scaling. Credible tokens have value and that value can help reward staff and future users, persuading them to perhaps risk the benefits they were receiving from their prior employer or from a token-less competitor platform. In Chapter 5 we examine token functionality and venture financing. In Chapter 6 we look at a DEX created to exchange blockchain tokens without the use of a centralized exchange with its profit margins and customer services.

3.4 Smart contracts

A useful, but not necessary, step from payment tokens to the use case of financing a venture, is the development of smart contracts. The latter meant that novel digital tokens no longer required their own separate blockchain - in other words it made it easier to build applications and blockchain infrastructure separately. Smart contracts can be described as shared computer code that can manipulate state, and are first mentioned in Szabo (1994), who imagined that “They react on events, have a specific state, are executed on a distributed ledger, and are able to interact with assets stored on the ledger”. These computing objects on the blockchain work transparently, can be verified by third parties, and are tamper resistant - therefore making their actions credible to outsiders (Cong and He, 2019). Smart contracts are not a core feature of Bitcoin. Buterin (2013) describes how payment token systems like Bitcoin are databases with one operation: subtract X from A and give X to B; on the proviso that (i) A has > X units prior to transaction and that (ii) A approves of the transaction. Smart contracts on the Bitcoin blockchain are therefore purposefully limited to the same set of actions, in order to minimize the attack surface available to malicious agents.

Vitalik Buterin did not believe the benefits of this decision outweighed its costs. Instead the Ethereum platform he founded created two step changes in smart contract performance, first by enabling programmatic flexibility (a Turing complete computer language), and then implementing the ERC-20 tokenization standards. Smart contracts on the Ethereum platform metamorphosed blockchain tokens from payment assets related to a specific blockchain protocol, into anything the human mind could conceive, from as mundane as a US dollar proxy,[9] to as lighthearted as cryptographic cats.[10] Bartoletti and Pompianu (2017) surveys various smart contract blockchain platforms, applications and design patterns. They highlight the diminished barriers to issuing tradeable digital tokens.

The name smart contract is a category error as they are neither smart nor contracts. They are able to predefine certain contract like actions, such as contingent payments, but they cannot address unexpected events. Including smart contracts on a blockchain imbues these programming objects with the authentic record of fact and action of the underlying blockchain. But they do more than this. Referring back to Lemieux (2016)'s work discussed in Section 2.5, although facts on the blockchain are authentic (are more likely to be free of tampering than alternatives), smart contracts sit higher than this and are arguably reliable - because their action is visible and verifiable the changes they make are potentially more legitimate than if made by a human. They come with controls with respect to their authorship of facts and state changes that a human would find difficult to match. This does not make smart contracts infallible, merely that the room for human error is triangulated to their initial coding. A separate risk is that smart contracts may be coded to accrue benefits to their owners dishonestly. Harz and Boman (2018) puts forward a trust model for detecting misbehaving smart contracts in permissionless blockchains, based on deposits, reputation and incentives for review agents.

Conversely Molina-Jimenez et al. (2019) notes that it is unproven that smart contracts neces-

[9] media.consensys.net/the-state-of-stablecoins-2018-79ccb9988e63

[10] medium.com/loom-network/how-to-code-your-own-cryptokitties-style-game-on-ethereum-7c8ac86a4eb3

sarily belong on the blockchain. The authors speculate that in the future it may be optimal for computation to occur off blockchain, with solely verification of the behavior of the computation recorded on the blockchain. The company nChain have created a software solution that enables the creation of applications whose actions can then be verified on the BitcoinSV blockchain.[11]

The study of smart contracts is an emerging area and their risks continue to be only loosely delineated. Perez and Livshits (2019) surveys smart contract vulnerabilities and finds that only 504 out of 21,270 contracts have been exploited. A critical reason is that most funds are kept in a small number of smart contracts that are developed to a higher standard. DAO re-entry and Parity multisig locked Ether are two notable exceptions. McCorry, Hicks, and Meiklejohn (2019) presents 3 smart contracts that can be used to exchange mining bribes for activities favorable to the miner. These incentivize actions such as mining uncle blocks away from the main chain, mining a fork rather than the longest current chain facilitating a double spend attack, or pay for the mining of empty blocks on another blockchain. A discussion of the benefits of smart contracts continues in subsection 5.1.

3.5 Decentralization as a method to subvert rules

The Internet is a distributed network, that is architecturally decentralized as defined in Section 2.7. It developed out of the United States of America's Arpanet, the first operational packet-switched network. Lukasik (2011) explains why the US Department of Defense invested in this system. "The goal was to exploit new computer technologies to meet the needs of military command and control against nuclear threats, achieve survivable control of US nuclear forces" (Lukasik, 2011, Page 1). System hardening is an accepted use case for decentralization. But there is another use case that we summarize as the ability to break rules. In order to understand how this relates to blockchain tokenization, it is necessary to touch on another historical chapter of technologically enabled decentralization. Napster and Bittorrent, shared computer resources without centralized intermediation or support (Androutsellis-Theotokis and Spinellis, 2004), and facilitated the peer-to-peer movement of media files. The sharing of music, video and software via these platforms broke long standing rules regarding content copyright, but the owners of this content had little ability to

[11] coingeek.com/kensei-by-nchain-is-the-gateway-to-definitive-blockchain/

prevent such sharing, other than by increasing the attractiveness of legal digital downloading and reducing prices (Vernik, Purohit, and Desai, 2011). BitTorrent in particular, prevented traditional copyright models migrating from offline to online. Decentralization was used to break a rule, ultimately so much so that the rule became untenable.

Despite being technically completely different, blockchain applied a superficially similar decentralization to the task of moving money without a bank. The payment token Bitcoin, which facilitates this movement of value, circumvents the traditional banking system (or more accurately the payment system they jointly administer), with its Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements. In these two areas, technological decentralization is again being used as a methodology to bypass rules and regulations. Foley, Karlsen, and Putnins (2019) uses a variety of network analyses, such as transactions with known dark web market wallets, to estimate that during their sample period, one quarter of Bitcoin users were involved with illegal activities, equating to USD 76 billion in transactions. “Cryptocurrencies are transforming...black markets by enabling black e-commerce”, Foley, Karlsen, and Putnins (2019, Page 1798).

It is worth highlighting though that Napster and BitTorrent led to the rise of private companies such as YouTube and Netflix, whereas Bitcoin remains largely outside the scope of government regulators, except via service providers such as exchanges and wallets (Vandezande, 2017). Banking rules, such as KYC and AML, will likely put up a much stronger fight than copyright - conversely hinting that perhaps Bitcoin will prove more durable than the first movers in the peer to peer media space. This would have been tested by the proposed launch of the purported cryptocurrency Libra by the social media firm Facebook (Libra, 2019). Libra would have tested the possibility that it is not AML and KYC rules that are driving the use case for digital currencies, but simply the banking industry and its multiple layers of margin - though it effectively shelved for now.

Moving away from payment tokens, initial coin offerings (ICOs) - where tokens are sold to potential future platform users and third party investors - is a major use case for blockchain that has perhaps already come to a close. ICOs are less a desire to avoid the banking system than a need to access financing without being subject to onerous securities regulation. Again the breaking of rules is an important component of their emergence. “Crypto-tokens have turned out to be a successful way for startups to raise early financing” Conley (2017, Page 1). Both payment tokens, and fund raising, are use cases enabled by the straightforwardness of issuing and transacting in provably scarce tokens on a blockchain. However in cases such as Airfox, the regulator has begun to pursue and punish issuers (SEC, 2018a). The next three subsections explores the the overlapping fields of blockchain applications, token applications and barriers to adoption.

3.6 Proposed blockchain applications

The digital tokenization of existing securities, discussed above, is not the only use case for blockchain in financial services. Federal Reserve governor Brainard (2016) notes that distributed ledgers could be revolutionary, specifically with respect to transparency and settlement within financial markets, and also through smart contract automation of tasks currently provided by intermediaries such as the payment of dividends. However, Abadi and Brunnermeier (2018) points out that these often cited benefits of blockchain (transparency and fast settlement), are incidental to blockchain as they are implementable under other technologies. Irrespective of this, given the successful deployment of these features under Bitcoin, blockchain could still be the most practicable way to deploy transparency in other ledgers as the code is readily available. With respect to corporate governance and incentives, Kaal (2019) explores the problems and opportunities arising from blockchain and potential decentralized autonomous organizations (DAOs). Considerable discussion of how DAOs might replace firms is placed in a broader context of how blockchain based agency constructs might supplement existing business forms, increasing accountability and incentive-compatibility.

Zhao, Fan, and Yan (2016) provides an early introduction to a number of research opportunities in blockchain. Gatteschi et al. (2018) discusses the potential implementation of blockchain in the insurance industry. It is focused on possible applications rather than appropriateness. Fanning and Centers (2016) is a high level scan for opportunities across financial services for the implementation of blockchain. Sun, Yan, and Zhang (2016) connects blockchain to the trending concepts of smart cities and the sharing economy. Nowinski and Kozma (2017) tries to link blockchain to the literature on business models. Maull et al. (2017) takes the blockchain and business model discussion further towards implications, with a series of workshops and interviews with individuals at incumbent firms and start ups. Hughes et al. (2019) approaches the subject from the perspective of firms, analyzing applications within a series of industry verticals.

Many of the use cases discussed can be characterized as solutions looking for problems. This can be seen when trying to use blockchain to replace an intermediary without considering deeply whether it is empirically superior to the use of an intermediary. Blockchain in financial services is a focus of much effort, yet blockchain is unsuited to high frequency markets such as equities because of both (1) the issue of transaction capacity and (2) the benefits of existing delayed settlement mechanisms e.g. daily netting of trades and subsequent reduction in capital required (Mainelli and Milne, 2015). This inferiority with respect to high frequency trading use cases is evidenced by the dominance of centralized exchanges for the trading of cryptoassets. Mainelli and Milne (2015) puts forward an alternative use case: a permissioned distributed ledger could address anti-money laundering (AML) and know your customer requirements (KYC) - a large and repeated cost for financial intermediaries that could be assisted by an authentic, verifiable record.

When examining the literature on proposed blockchain applications, two preliminary fields stand out. Firstly supply chains, which are an economy wide industry, with multiple agents, that must work with partners up and down the logistic network. Ganne (2019) notes how the shipping industry has seen relatively little innovation since Malcolm McLean invented the intermodal sea container in the 1950s. They provide an example of shipping a container of roses and avocados traveling from Mombasa to Rotterdam, and state that such a shipment might produce a 25 centimeter high pile of paperwork. The administrative cost of this may end up exceeding the associated transportation cost. The process itself may involve 100 individuals and 200 information exchanges. Furthermore, each agent has some incentive to hide any mistakes.

Using blockchain in supply chains, complemented by other technologies such as radio frequency identification (RFID) tags and GPS location tracking, is a clear opportunity that Maersk and IBM are currently attempting to address with TradeLens (Jensen, Hedman, and Henningsson, 2019). Montecchi, Plangger, and Etter (2019) discusses how blockchain can provide four capabilities (traceability, certifiability, trackability and verifiability) that enable the four assurances of (1) origin, (2) authenticity, (3) custody, and (4) integrity. Azzi, Chamoun, and Sokhn (2019) includes two case studies of commercial blockchain based supply chain systems, that integrate such systems with RFID and GPS tags. George et al. (2019) observes that Walmart has introduced blockchain systems with respect to the tracing of pork and mangoes in their supply chain, and propose their own variant to track food quality. They use an example of use by dates on pork, and lay out a blockchain system that records and indexes the age of food in the supply chain, or location, relative to its final use by date. This is an interesting exploitation of the transparency possible in any database system, but that is inherent in an appropriately configured blockchain system, and raises the possibility of new vectors of competition between restaurants and retailers. Pearson et al. (2019) focuses on using distributed ledgers to enhance food traceability. Current standards revolve around the concept of "one up, one down", where agents in the supply chain are expected to record the the sources of their purchases and sales. Blockchain could bring all these parties and their disparate data into a single record of fact, improving traceability at the same time as addressing the complexity of multi-step, vertical and horizontal branching of supply chains e.g. where products are blended, dissected or mixed. If such a system recorded weights or volumes, it might even enable preemptive identification and discouragement of adulteration. However distributed ledger technology "helps secure the evidence chain, it does not replace any of the industry and regulatory standard procedures required...to control fraud" Pearson et al. (2019, page 147). A major limit of blockchain continues to be the line between the digital and the physical, a problem that is often reflected in discussions regarding the gap between expectations and reality.

Hofmann, Strewe, and Bosia (2019) focuses on the opportunity for blockchain in supply chain finance. Large amounts of capital are tied up in cargoes of goods moving great distances. Supply chain finance processes are often manual e.g. compliance checks comparing different paper based trade finance documents. Blockchain can visualize the physical flow of goods, digitize administration, and therefore identify where cash and liquidity is being held up in the supply chain. Marrying this with fast settlement would not be a unique improvement, but would enable greater efficiency and lower risk in the financing of trade flows.

Healthcare data also presents a problem that could be improved. Each individual has a healthcare record written by many parties. The two most common state of affairs is either that this record is not accessible by a specific doctor at the point of treatment, and / or that the data is held outside the individual's control. Kuo, Kim, and Ohno-Machado (2019) compares a blockchain system with a distributed traditional database management system (DDBMS), within the healthcare industry. They highlight five key advantages. The first is decentralized database management whereby cooperation can occur without any party ceding control to an intermediary. Secondly, blockchain comes with an immutable audit trail, as such systems only support create and read functions, largely extirpating the ability to update and delete. Third, the ownership of a digital asset, such as an individual's data, can only be changed by the asset owner, rather than solely by the system administrator. This also means such assets are traceable and suitable for reuse, for example for insurance purposes. Forth, it would be costly for DDBMS to match blockchain's level of data redundancy and therefore its anti-fragility. Fifth, security and privacy is enhanced by the use of cryptographic algorithms by default.

Engelhardt (2017) contrasts the current industrial mentality of health care, where data is hoarded and patients are assumed to be ignorant, with a new paradigm that puts the patient at the center. This includes making sure the information held is complete and that privacy and access are implemented appropriately. Such a paradigm would help address the major problem of cost inflation as populations age by reducing mistakes and increasing effectiveness. The author discusses the use of blockchain to track public health, centralize research data, organize patient data, lower overheads and monitor and fill prescriptions. Kuo, Kim, and Ohno-Machado (2019) notes that Health Information Exchange (HIE) related to patient records is the most discussed use case, followed by insurance claims and secondary use of data in research e.g. genomic studies. Problems to be addressed includes confidentiality, scalability, and the threat of 51% attacks. Given these factors, a permissioned blockchain may be the type most suited to being applied in a healthcare setting.

Both healthcare and supply chain are areas where valuable data is held in multiple locations without any system of reconciliation. Both areas have a business case for a central authority yet past industry structure has prevented one from coalescing. Both areas are ripe for improvement. Unlike in finance where incumbents create resistance to disintermediation, the primary barrier in healthcare and supply chains to adopting blockchain is the required level of cooperation.

In the unconstrained speculative application space, Laabs and Dukanovic (2018) links blockchain with the possible fourth industrial revolution of self organizing production lines / supply chains that coordinate across devices and firms with ease. They provide two case studies, briefly explaining the opportunity for blockchain in autonomous problem solving and commercial machine to machine (M2M) services. Dai and Vasarhelyi (2017) sketches out a new blockchain based accounting ecosystem based on improved data integrity, sharing of necessary information and programmable control of processes. The paper places blockchain as the third record into a triple entry bookkeeping system, such that accounts can be matched across firms. Smart contracts are proposed for a variety of mechanisms, including invoicing and accounting rule compliance. Within this framework, the assurance of financial information becomes a continuous process (as opposed to summary statistics organized by time) and is shared appropriately with the relevant stakeholders. An obligation token is put forward as one way for accounts payable and accounts receivable to be digitized. Both Laabs and Dukanovic (2018) and Dai and Vasarhelyi (2017) lay out an ecosystem of emerging tech including blockchain, machine learning, internet of things, robotics and crowdsourcing that could completely revolutionize the way that business is carried out. However many smaller steps can be and must be operationalized prior to the actualization of their end goals.

3.7 Proposed token applications

The usefulness, and therefore application, of blockchain tokens is not easy to determine. They are novel in implementation, but are conceptually not a new phenomena - with an emerging definition that has similarities to currencies, food stamps and gift cards. What has changed is the required deployment scale, the transparency of supply, and its ability to be credibly customized (Section 3.3). An alternative to a centralized ledger, that requires a large upfront investment, is a decentralized verifiable record that can be bootstrapped user by user. This is how a system that is costly by design has led to lower barriers to deployment of tokenization (Section 2.6). We argue that the surface has barely been scratched regarding what is possible with straightforward to deploy, verifiably scarce digital tokens built on blockchain. Smaller organizations, down to a single individual, can now issue a tradable token to govern and distribute the benefits of a specific platform or project. The benefits of this include raising finance for the project, rewarding employees for their contribution, and sharing value with users for growing the platform. A good example of the last advantage is the Brave browser.[12] It enables a faster experience of the internet, primarily by blocking adverts. It includes an option for users to accept adverts, but then sharing 70% of revenues with the user. This revenue share is paid in Brave blockchain tokens. In other words advertisers pay Brave in US dollars and Euros, and it then rewards users with a contingent expense, that is only real if the project succeeds. The positive feedback loop becomes rewards attracting new users, which increases the value of the rewards. At launch these rewards were difficult to change into US dollars

[12] brave.com

and Euros, but is now carried out by the firm's wallet partner. Overall, many of the benefits of tokens fall under Catalini and Gans (2016)'s reduction in networking costs, even if considerable detail on implementation exists below that level.

Arguably the academic literature lags real world token deployments, perhaps because of the frenetic pace of innovation by blockchain start ups. Nevertheless, multiple token applications have been proposed by the literature. Ferraro, King, and Shorten (2018) pairs a useful overview of the directed acyclic graph in IOTA's Tangle consensus algorithm, with a proposal to use a token to enforce rule compliance in a traffic management setting. Mohan (2019) proposes using a blockchain mechanism to address academic misconduct, based on token rewards and agent reputation. O'Dair and Owen (2019) discusses the use of blockchain tokens to fund creative industries, in particular recorded music. Burer et al. (2019) provides a broad survey of incumbent and start up efforts to introduce blockchain and tokens across the energy sector.

Baum (2020) explores tokenization in commercial real estate, focusing on the fractionalisation of large properties, and the fractionalisation of funds invested in property. Examples of this includes the St Regis Aspen Resort in Colorado (USA), which was tokenized and sold through a Security Token Offering (STO) in 2018. Outside of real estate, the Masterworks platform securitizes art. Masterworks registered 99,825 shares in Andy Warhol's artwork 'Colored Marilyn' with the United States SEC in 2018, and sold them to investors. The shares / tokens are stored on the Ethereum blockchain. At the heart of these projects, and others from different asset classes, is the use of tokens to digitize ownership of an underlying item of value, and the use blockchains as a custody layer that eliminates one or more middle man (Micheler and Heyde, 2016).

Shafagh et al. (2017) puts forward a blockchain based access control layer designed for Internet of Things (IoT) storage use cases. Although it does not utilize a token, storage is an area a number of ventures are attempting to address. Both Filecoin and Storj[13] have raised capital via ICOs and intend to use the tokens issued to govern their decentralized storage platforms. These types of tokens would fit into William Mougyar's definition of a token as a unit of value to self govern a business model. Because they transact in something of clear value (storage) where markets already exist, such use cases must explain why a platform specific token is appropriate from a

[13] filecoin.io and storj.io

users perspective. Note that this point does not detract from the benefit to the venture of reduced bootstrapping and platform scaling costs.

The number of projects funded by ICOs have fallen significantly following the tighter regulation discussed in Section 5.2.1. Fortunately innovation has continued unabated. A number of blockchain applications have waxed and waned in popularity. Here we separate out certain categories of projects, depending on where they sit in the software stack. Bitcoin is a payment token integrated with its own infrastructure - it is the entire software stack. Payment tokens are discussed in Section 4.2.1. Ether is a payment and utility token on the Ethereum platform. It differs from Bitcoin in the suitability of its smart contract infrastructure to hosting third party applications. Ethereum has multiple competitors including Solana and Binance Smart Chain.[14] Our discussion seeks to focus on tokens as opposed to infrastructure (and the tokens that mediate that infrastructure). Projects built on these platforms are often referred to as Dapps or decentralized applications. They are typically a web or mobile front end application connected to smart contracts running on blockchain infrastructure. As of 8 October 2021, the top 10 Ethereum applications listed on DappRadar.com included: one NFT marketplace, five DeFi projects, two collectibles and two games. 24 hour user counts varied from 31,000 to 1,300. Some of these projects have a token - which is used primarily for platform scaling - and some do not. This snapshot does not reflect the periods of intense popularity and activity that has occurred historically with respect to both DeFi and non-fungible tokens.

Which tokens, that do not currently have many users, have innovated what is possible with blockchain tokens? One worth mentioning would be the game application cryptokitties,[15] which utilizes Ethereum's ERC-721 standards for NFTs. Effectively 'kitties' (1) have DNA linked to their cryptographic private key, (2) are encapsulated by unique tokens, and (3) pairs of 'kitties' can be 'bred' to create new 'kitties'. The ERC-721 standards are well suited to tracking ownership of digital collectibles, such as in game items, that are one of a kind unique. Other token capabilities that have been added to Ethereum include tokens that can own other tokens (ERC-998 composable non-fungible tokens), and used in the game Caesar's Triumph to enable to consolidation of land.[16] An additional direction Ethereum has studied are tokens designed for regulated use cases. ERC-1400 enables tokens to have restrictions on who they are sent to, how they are split, identification

[14] solana.com and binance.org/en/smartChain

[15] medium.com/loom-network/how-to-code-your-own-cryptokitties-style-game-on-ethereum-7c8ac86a4eb3

[16] guide.caesarstriumph.com/land/land-composer

requirements etc. This has proven a controversial set of standards given the ethos of the blockchain community.

Relative to the token applications above, we put forward an even more speculative application of tokens: the adoption or responsibility token, whereby token holders are contributing to philanthropic projects or social goods (Medda et al., 2019). As part of the EU 2020 Horizon project Circular models Leveraging Investments in Cultural Heritage (CLIC), a proposal has been provided to a charitable organization in Amsterdam which would see the crowdfunding of an adoption token to finance an adaptive reuse project. The token would transfer no financial rights and have no intrinsic value. This project would digitize existing forms of philanthropy, potentially create a new recurring stream of financing, and could be tested for its impact on adopter and the underlying item of cultural heritage. The concept of an adoption token leverages the fund raising visible during the ICO bubble of 2017, but at the same time attempts to avoid the regulatory investment contract issues that brought this period to a close (for example SEC (2018a)). The academic significance of such a use case could be large as such an effort would be tokenizing a relationship. To our knowledge this would be the first such project to digitize a connection between a person and a cause, and open up a large space for innovation and further research related to whether or not a token can moderate economic behavior. Research on adoption tokens is a work in progress.

3.8 Barriers to wider adoption

Multiple researchers are focused on improving blockchain to drive adoption. Meiklejohn (2018) lists a set of computer science related conundrums related to distributed ledgers in order to shine a light on current and future avenues for research and development. Saito and Iwamura (2019) attempts to address the high volatility of cryptoassets, and proposes a number of ongoing supply adjustment mechanisms, namely difficulty adjustment mechanisms and negative interest rates on unspent (UTXO) balances. However these discussions are focused on the areas where blockchain has proven itself as a viable concept, notably Bitcoin and ICOs.

Moving beyond this, the slow adoption of blockchain outside of payments but within the financial sector is for our purposes more relevant. Wadsworth (2018) uses an 8 part criteria to compare distributed ledgers to existing payment systems. This criteria included (1) national boundaries, (2) speed, (3) cost, (4) transparency, (5) liquidity, (6) scalability, and (8) finality. Existing systems have low domestic fees, high cross border fees, at the same time as being fast, scalable and private. The paper identifies single point of failure as the key risk, and ignores the topic of single point of control. In comparison, the Bitcoin blockchain has high domestic fees, relatively low cross border fees, high energy use, public transaction data, and poor scalability. A point that emerges from their analysis is that merging clearing and settlement into a single validation stage increases liquidity requirements as payments cannot be batched and offset on a daily basis. Wadsworth (2018) then summarizes two tests of distributed ledger technology: Project Jasper by the Central Bank of Canada and Project Ubin by the Monetary Authority of Singapore. The first phase of both projects used permissioned PoW blockchains. This phase was viewed particularly negatively as degradations in energy use, scalability and privacy would have been somewhat offset by reduced single point of failure risk, except that the latter had been reintroduced by efforts to implement permissioning and better privacy. The second phase utilized hierarchy via a central node that validated transactions and replaced PoW. Although this eliminated many of the problems with blockchain based systems, the resulting system had more similarities to existing payment rails than blockchain. Kuhn and Yaga (2019) takes a different tack and observes that many financial applications require the ability to delete erroneous data and transactions. They put forward the use of a verified time protocol as an alternative consensus algorithm, and the use of a data block matrix. The latter uses hashes at the column and row level, such that deletion of one table entry leaves other entries verifiable by the remaining column and row hashes.

Outside of the financial sector, it is necessary to contextualize the lack of implementation of blockchain by asking does a use case even need to be on a distributed ledger. Wust and Gervais (2018) formulates a process for judging whether or not a blockchain may be appropriate for a specific application. This framework suggests the following necessary conditions for the applicability of a blockchain: (1) a need to store state, (2) multiple writers and (3) a reason that mitigates the benefits of using a trusted third party . The criteria of whether or not all agents are known and / or trusted determines a preference for permissioned or unpermissioned distributed ledgers. A key problem is the interface between the real world and the digital world mapped out by a blockchain. If a trusted third party is required to enforce the blockchain, then a trusted third party is likely the dominant option. From this one requirement, it becomes clear that many speculated use cases never made any sense. Many aspects of government are simply ledgers, from citizenship to home ownership. However, if the government or its agency is removed from process, who enforces these ledgers and who has the right to write to them? Until this issue is resolved, the applicability of a blockchain will be relatively more appropriate for digital goods and services. Conversely, the financial aspects of government such as tax obligations can make more sense. Tax liabilities arise from multiple vectors, and blockchain, as a payment protocol, can enforce changes of state and the movement of funds. Tucker and Catalini (2018) delves further into how blockchain does not solve the "last mile" verification of the existence or location of something physical. They use the example of the location of a baby, or that a viewer of an advertisement is human rather than a programmatic bot, where it should be clear that a blockchain can provide a digital record but not physical proof.

Many of the barriers discussed in the literature are being addressed. Proof of Stake consensus mechanisms such as the Ethereum upgrades, previously referred to as Ethereum 2.0, have reduced energy consumption and will increase transaction processing capacity.[17] PoW blockchains can now even enforce court orders at the miner level [18]. An under discussed topic is that many blocks on Ethereum are censored.[19]. This is because most validators on Ethereum are paid to outsource their block production duties to Miner Extractable Value (MEV) boost relays These firms make money from ordering transactions. 4 out of 7 of the major relays are compliant with the USA's Office of Foreign Assets Control (OFAC) sanctions list and will prevent transactions involving these addresses and assets. Overall the major barriers to adoption continue to be real world enforcement of blockchain records, and the related point regarding the value added by intermediaries that are targets for replacement. One major aspect of this is the higher profitability available to a venture if it organizes itself in a centralized way relative to decentralized organization. Coinbase and Binance continue to enjoy higher and more consistent volumes than their decentralized competitors.[20] To an extent, the point on profitability is a corollary of Abadi and Brunnermeier (2018)'s blockchain trilemma. In a world where it is impossible for a ledger to be rent-free, resource efficient and trustless, the high rent option will inevitably be the most profitable.

[17] ethereum.org/en/upgrades/

[18] bitcoinsv.io/digital-asset-recovery

[19] mevwatch.info/

[20] coinmarketcap.com/rankings/exchanges/

Chapter 4

Bitcoin mining: converting computing power into cashflow

4.1 Introduction

The Bitcoin mining industry processes 300,000 transactions, and generates \$15 million dollars worth of Bitcoins and \$500k of fees daily (Figure 4.1). Prior to 2017, Bitcoin scaled efficiently with transactions. It offset transaction growth with higher transactions per block. Blocks processed per day - and consequently Bitcoin mining prize games - have been stable since 2011 (Table 4.1). More recently divergences occurred as Bitcoin reached its block size limit, which specifies how much data may be contained in each block.

These divergences include a peak in transactions, higher transaction fees and a rise in mining revenues. The latter two are a user cost and a system cost respectively. Mining revenues reached \$50 million per day during December 2017. These divergences are now moderating with the adoption of SegWit, which reorganizes the location of any unlocking signatures and counting them at a quarter of their prior weight.[1].

Bitcoin utilizes cryptographic digital signatures and proof of work computing tasks (Nakamoto, 2009). These form a pseudo public database, that transfers value without relying on a trusted central party. Iansiti and Lakhani (2017) describes Bitcoin as a narrow use case of blockchain, or distributed ledger technology, in an area with low coordination requirements.

[1] medium.com/@jimmysong/understanding-segwit-block-size-fd901b87c9d4

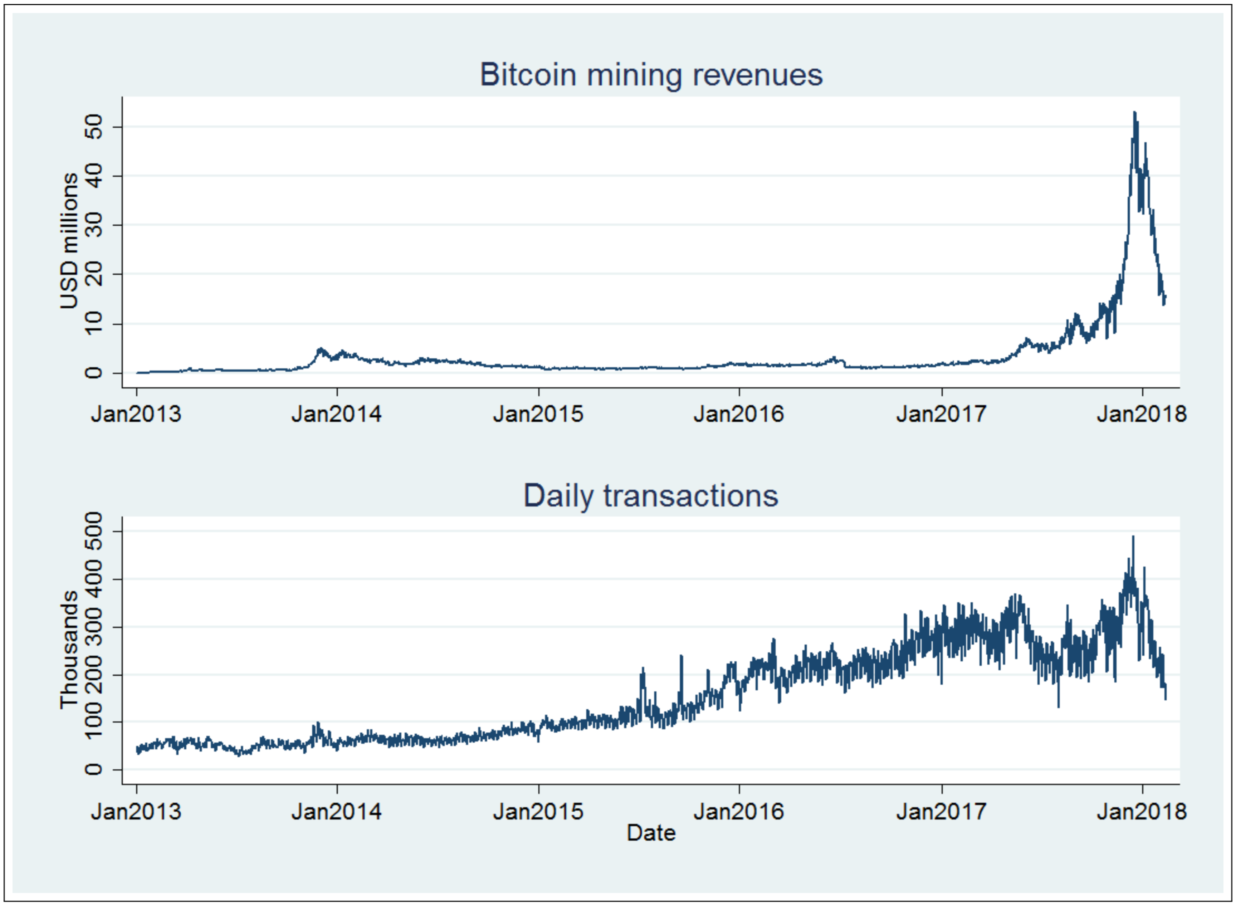


Figure 4.1: Daily Bitcoin mining revenues $m, and transactions '000s

Parties move Bitcoins, a unique digital asset, between electronic addresses via transactions. Transactions are submitted to the mempool (temporary storage). Most processing is carried out by collective mining pools, that reduce individual reward variance, and divides in two the task of transferring transactions from the mempool to the blockchain (Gervais et al., 2014). The pool administrator checks, selects and orders transactions. Pool participants contribute computing to the resource intensive proof of work required to validate blocks. Blocks must contain a solution to a cryptographic puzzle related to its transactions and its place in the chain (Nakamoto, 2009). Block processing earns miners Bitcoin rewards and fees. Buterin (2013) describes this as a first-to-file system: transactions are ordered by when they are processed. Bitcoin mining converts computing power into cash flow, and incentivizes participation. To be successful, malicious actors need to control over a quarter of this computing power (Eyal and Sirer, 2014). Nakamoto (2009) and Kroll, Davey, and Felten (2013) consider spending on Bitcoin mining as an attacker's cost function.

	N	Mean	Standard Dev	Min	Max
Bitcoin mining rev inc fees USD '000s	2,737	2,387	(5,887)	0.34	53,191
Bitcoin mining rev exc fees USD '000s	2,737	2,097	(4,626)	0.34	42,863
Transactions, '000s	2,737	109	(104)	0.27	491
Bitcoin US Dollar (BTCUSD) price	2,737	924	(2,411)	0.06	19,498
Transaction fees, USD '000s	2,737	291	(1,418)	0.00	22,724
Blocks processed	2,737	166.1	(82.54)	6.5	2,941.5
Difference in log mining rev exc fees	2,736	0.0038	(.1439)	-1.03	0.9678
Difference in log Transactions	2,736	0.0022	(.1966)	-3.27	2.8799
Difference in log BTCUSD	2,736	0.0042	(.0646)	-1.04	1.0043

Table 4.1: Descriptive statistics for Bitcoin Mining industry and daily difference logs, 17 August 2010 to 12 February 2018

Although Vukolić (2016) suggests directions for addressing blockchain's limitations, most Bitcoin mining literature focuses on game theory and incentives. Eyal and Sirer (2014) outlines Bitcoin's vulnerability to selfish mining strategies. Schrijvers et al. (2017) models mining pool reward functions. Other work compares Bitcoin transaction costs, borne by users, when exchanging international currencies (Kim, 2017).

This paper adds to the literature an empirical analysis of the financial components of Bitcoin mining revenues: their contribution to daily changes, how this has been varying, and their contribution to its variance. We find that the Bitcoin USD price, and transactions, are statistically significant drivers of revenues. The higher the Bitcoin price, the greater the computing used in hashing, and the higher the system security. Rolling regressions examine these coefficients over time, and hint that despite SegWit, scaling remains an issue. The coefficient on Transactions appears to rise as transaction numbers peak and churn (Figure 4.2), i.e. volumes are relatively less important to miner revenues until capacity is exceeded. The results adds color to the mechanics of Bitcoin and its throughput cap related to the block size limit. Our results support continued research into blockchain scaling, for example the Lightning Network or Ethereum 2.0's move to Proof of Stake (Buterin and Griffith, 2013). We use these results to highlight the connection between scalability and nodes.

4.2 Literature review

4.2.1 Cryptocurrency payment tokens

Brainard (2020) explains how the existing payments infrastructure utilizes central bank money (cash, plus deposits at the Fed), commercial bank money (deposits at banks) and certain kinds of non-bank private money (e.g. Paypal and Starbucks account balances). Each provides a medium of exchange based on the US dollar as a unit of account, and is as reliable and resilient as their institutional backer (although Grinberg (2012) identifies the Iraqi Swiss Dinar as an example of a paper money operated in the absence of any state authority). Financial institutions collectively own parts of the infrastructure traditionally used to make payments within the United States. Conversely, cryptocurrencies are distinctly non-institutional. They use variations of the decentralized ledger mechanism of blockchain for their payments infrastructure, and consequently can put themselves forward as verifiably scarce and natively digital. Whether they are assets with any value is a decision for users. We favor the term payment tokens rather than cryptocurrencies, inline with the Swiss financial regulator FINMA (2018), but consider the terms interchangeable. It is observed that the traditional payments system is built around widely accepted forms of money, whereas cryptoassets (all non-payment crypto tokens) are often differentiated and defined by their associated infrastructure. The two digital tokens with the highest aggregate value, implied by market price, are Bitcoin and Ether, native to the Bitcoin blockchain and the Ethereum blockchain respectively. They operate as two separate payments systems, with different features. Buterin (2013)'s Ethereum platform formalized smart contracts on a blockchain. Smart contracts are shared, immutable computer code that can manipulate state, for example token balances. Smart contracts enable many contingent actions, including the issuance and trading of non-native tokens by third parties on blockchains such as Ethereum, in under 30 minutes.[2] Smart contracts are discussed further in Section 3.4.

Bitcoin in particular, has become a highly effective way to make payments outside of traditional bank controlled payment systems (Dwyer, 2015). The illicit component of this is well analyzed, with Foley, Karlsen, and Putnins (2019) estimating that approximately one quarter of Bitcoin users are involved in illegal activities. However Raskin, Saleh, and Yermack (2019) argues that cryptocurrencies may act as a check on fiscal and regulatory policy in less developed economies,

[2] news.bitcoin.com/launching-an-ico-token-on-ethereum-in-less-than-thirty-minutes

and therefore enhance citizen welfare. Although forcing all citizens on to a single highly censored payments system limits many illegal actions, it also creates costs. Kim (2017) provides evidence that when converted via Bitcoin, effective exchange rates between a sample of currencies are on average 5% superior to retail foreign exchange rates. Although most users are not ready to be their own bank, there are many potential benefits to cutting out middle men.

Where does Bitcoin and other payment tokens fit into the wider discussion around digital money? Schreft (1997) notes that US dollars in physical cash and US dollars deposited at a bank are not perfect substitutes. In the modern era where these deposits exist primarily electronically, the author observes that the key point is not that one form is physical while the other is electronic, but that the bank deposit in this instance is privately issued. This could be addressed by the full backing of each deposit by US treasury bills and bonds, but this is rarely the case. Instead each bank engages in, for profit, risk and maturity transformation characteristic of fractional reserve banking, potentially securitizing liabilities in a way where these risks do not even appear on its balance sheet (Merton, 1995). Therefore each holder of a bank deposit is exposed to mismanagement and default risk, that can be thought of as a tail risk of differences in exchange (Schreft, 1997).

Blockchain tokens designed to work as a currency differ from legal tender in ways that do not fit on a substitution scale from perfect to imperfect. They are worse than bank deposits in not sharing a name, approximate value and unit of account with a form of state money such as the US dollar. At this time they cannot be used directly to discharge debt-contracts, the definition of money put forward by Keynes (1930). However they have an advantage over bank deposits in that although they are privately issued, they are not privately backed. Previous digital assets required trusted counterparties and custodians to maintain a ledger, who are a counterparty risk and often monopolistic price makers. Importantly, the latter are able to censor behavior (Aste, Tasca, and Di Matteo, 2017). Blockchain based payments tokens are provably scare digital assets that are absent traditional forms of counterparty risk. This type of risk even extends to state issuers. Mazumdar (2017) examines empirically the benefit to real GDP of allowing a rise in trend inflation (decline in purchasing power of money) by one percentage point, an incentive that does not apply in the same way for blockchain token systems with transparent issuance schedules.

Awkwardly, that does not change the fact that early blockchain based payment assets have no intrinsic value. This statement is often used as a critique, ignoring that "State monopoly currencies, such as the U.S. dollar, the euro, and the Swiss franc, have no intrinsic value either", (Berentsen and Schar, 2018, Page 9). This paper, from researchers at the St Louis Federal Reserve, highlights characteristics that Bitcoin shares with physical cash, e.g. anonymity and decentralization. In contrast, digital cash facilitated by the banking network, which resolved physical cash's requirement that the buyer and seller be physically proximate, is centralized and easily traced to an identity. Kahn, McAndrews, and Roberds (2004) makes the case in favor of anonymous money. A model is devised where public information regarding the identity of a buyer increases the chance of theft. The theft is socially wasteful and inhibits trading. The paper argues that money has social value in situations where parties cannot trust each other not to take subsequent opportunistic actions. Cryptocurrencies are characterized as a costly and low capacity version of bank digital cash. The reality is that digital bank money is a convenient but circumscribed version of physical cash, and cryptocurrencies plausibly a closer approximation of the money in your wallet. Raskin, Saleh, and Yermack (2019) develops a model of digital currencies in an emerging market, and shows that diversification and restraint on monetary policy benefits can lead to higher consumer welfare in an incentive compatible way for governments.

Despite the benefits described above, a full understanding of payment tokens requires the acceptance of their many flaws. These can include low throughput, multiple prices (Pieters and Vivanco, 2017), and regular exposure to centralized trading venue risks (Brandvold et al., 2015; Gandal et al., 2018). Although Athey et al. (2016) searches for fundamental drivers of the price of Bitcoin (steady state, non-investor, transaction levels and beliefs regarding the survival of Bitcoin), it is easy to argue that tokens designed for payments have become synonymous with speculation. Cocco, Concas, and Marchesi (2017) models cryptocurrency markets with an agent based model, and finds that momentum traders using limits can generate the non-stationarity, fat tails and volatility clustering seen in the price history of Bitcoin. Even privacy benefits should not be assumed to be valuable. Athey, Catalini, and Tucker (2017) uses data from a behavioral economics experiment that gave Bitcoin to a group of students to find evidence of the privacy paradox: revealed preference for privacy typically ran much lower than stated preferences. However these should not distract from the breakthrough of a differentiated class of assets, the prices of which could even be an adoption signal for a technological prototype (Lo, 2017). Payment tokens also have attractively uncorrelated returns. Using hourly Bitcoin and foreign exchange prices, Urquhart and Zhang (2019) finds that

Bitcoin can be an intraday hedge for movements in the Swiss Franc, Euro and Sterling. Ciaian, Rajcaniova, and Kancs (2017) finds a variety of relationships between Bitcoin and various altcoins (1st and 2nd generation blockchain tokens). Additionally, their paper finds 15 statistically significant long run relationships between 19 digital assets or indices, and 6 macro variables. This is out of a possible 114 relationships, adding empirical evidence to the building argument that cryptoasset prices are relatively unconnected to macroeconomics and other asset classes (See also Briere, Oosterlinck, and Szafarz (2015) and Bouri et al. (2017)).

4.3 Data

We source our Bitcoin mining data from blockchain.info via the Quandl platform. Effectively this outsources the creation of a single composite Bitcoin price index to the former, and the selection of time of day to the latter, which eases replication of our results. We note that blockchain.info is now blockchain.com and Quandl is now owned by Nasdaq. As a check of robustness, we also utilize daily pricing data from the Bitstamp exchange. Bitstamp's Bitcoin market is indirectly regulated by the United States CFTC via being referenced by the CME Bitcoin Future. This check highlights the data quality issues in the field: most exchanges are unregulated, the period available (beginning 28 November 2014) is shorter than for the blockchain.info index, and the time of data acquisition impacts sample values. We download our Bitstamp data at 9:50am EST on the 12 February 2018. These discrepancies can be particularly problematic when using live API data feeds. The high and low intraday prices are provided by Cryptocompare, a data aggregator. Blockchain.info calculates mining revenues by tracking the number of blocks processed and the daily transaction fees. Table 4.1 shows a variety of descriptive statistics. The time period of the primary analysis covers 17 August 2010 to 12 February 2018.

4.4 Empirical Model & Methodology

The blockchain algorithm ensures that less than 21 million Bitcoins (BTC) are issued. As part of this, mining rewards halved to 25 BTC per block on 28 November 2012 and to 12.5 BTC on 9 July 2016. Estimated total daily compensation in dollars, or Bitcoin mining revenues, takes the following mathematical form.

$$E(RI_t) = \frac{T_t}{B_t} \times C_t \times U_t + F_t \tag{4.1}$$

Under this notation, RI_t is the Bitcoin mining revenue for a given day, including fees. T_t is the number of the transactions. B_t is the average number of transactions per block. C_t is the block reward rate, which does not have to be collected by the miner. U_t is blockchain.info's benchmark exchange rate of US dollars per Bitcoin. F_t is the daily total of an optional transaction fee. The most prominent reason for the equation not holding would be intraday and intra-exchange differences between actual Bitcoin prices and the daily benchmark price.

Our analysis is focused on Bitcoin mining revenue RX_t excluding transaction fees. The contribution of fees F_t, blocks and transactions per block are difficult to address empirically as they are statistically collinear with other variables, particularly on a day to day basis. Fees are specified individually for every transaction on the blockchain. We exclude C_t as it changes infrequently and is effectively discrete. We assume that miners collect coin rewards. Note that actual Bitcoin mining revenues follow an identity numbered in Bitcoins. For our estimated revenue figure we assume that miners convert the Bitcoins they mine into USD the same day. It is likely that all but a minority of miners monetize their rewards, due to the cost of electricity and processing equipment.

We transform our ex-fees nonlinear equation into a linear equation by taking logarithms. We take first differences, which reject the null of non-stationarity at the 99% significance level. We define a spread variable of the intraday $High/Low = S_t$. Baek and Elbeck (2015) found a monthly spread variable to be a statistically significant factor in monthly price changes. We follow the literature and incorporate S_t.

$$\Delta(lnRX_t) = \alpha + \beta_1\Delta(lnT_t) + \beta_2\Delta(lnU_t) + \beta_3\Delta(lnS_t) + \epsilon \tag{4.2}$$

In addition to an analysis for the complete period, we calculate 365 day rolling regressions, with overlapping time periods, to chart the coefficients on daily difference in log BTCUSD, and daily difference in log Transactions, over time. This provides insights on the time varying mechanics of on chain Bitcoin transaction processing costs.

We carry out two separate checks of our analysis. We perform a winsorization of the variables of the empirical model (Dixon, 1960). This compacts the top and bottom 5% of each series, replacing them with the 95th and 5th percentile value respectively. We also carry out the analysis with an alternate data source for the Bitcoin price (Bitstamp). Besides being a check of robustness, we use this to highlight problems with gathering data on Bitcoin, and channels of financial regulation. Most Bitcoin markets are unregulated and therefore more vulnerable than usual to activities such as spoofing (fake bids and offers) and wash trading (false trading in order to create false information).

4.5 Results & Discussion

First difference log	Mining revenues	
	β_i	VIF_i
Transactions	0.0905***	1.00
	(7.31)	
Bitcoin USD index	0.996***	1.01
	(26.39)	
Spread	0.000717	1.00
	(0.03)	
Constant	-0.000675	
	(-0.28)	
N	2735	
Adjusted R^2	0.220	
Breusch-Pagan test statistic	0.569	
BP(p)	0.451	
Ramsay RESET test statistic	2.569	
RR(p)	0.0527	

The variance inflation factor is calculated as $VIF_i = \frac{1}{1-R_i^2}$ where the independent variable i is regressed against the other independent variables

*** indicates statistical significance at the 0.001 level

Table 4.2: Empirical model

As we have taken logs of both sides, based on the empirical model the coefficients β_n are elasticities. Consequently a 100% change in Transactions implies a 9% change in mining revenues. In comparison, our regression implies a one for one elasticity (almost 100%) between changes in the BTCUSD exchange rate and Bitcoin mining revenues. We did not find significance for the other variables from the expected Bitcoin mining revenue identity (not shown).

The VIFs in Table 4.2 indicate that the independent variables are unlikely to be collinear. At the 95% significance level, the Breusch-Pagan test result does not reject the null hypothesis of constant variance; and the Ramsay RESET test result does not reject the null hypothesis of no omitted variables, but does reject the null at the 90% significance level. When we regress the residuals of the model against lagged residuals, at the 99% significance level the F-test and t-test results reject the null of zero on the lagged residual coefficient. We find negative serial correlation (-0.389) is present even after first differencing logs of the variables. Standard errors are overstated.

First difference logs	Partial sum of squares	DF	Mean sum of squares	$Prob > F$
Empirical model	12.510	3	4.170	0.0000
Transactions	0.863	1	0.863	0.0000
BTCUSD	11.256	1	11.256	0.0000
Spread	0.000014	1	0.000014	0.9761
Residual	44.129	2,731	0.0162	
Total	56.639	2,734	0.0207	

Independent variables are specified as continuous

Table 4.3: Bitcoin mining: variance decomposition

We present an analysis of model variance in Table 4.3. The R^2 for the empirical model is 22%, which is primarily explained by the Bitcoin USD price (20%).

Moving to the rolling regressions, we find that the coefficient on the Bitcoin USD price varies from a low of 0.47 to a high of 1.15 (Table 4.4 and 4.2). The rolling coefficient on the log daily change in Transactions varies from a low of -0.01 to a high of 0.58.

	N	Mean	Standard Dev	Min	Max
Coefficient on BTCUSD	2,373	0.8537	(.12223)	0.47	1.149641
Coefficient on Transactions	2,373	0.1732	(.119209)	-0.01	.578560

Table 4.4: Summary statistics of rolling 365 day coefficients

In the most recent 365 day period, a 100% change in BTCUSD or Transactions, implies a closer to 90% and 58% change in Bitcoin mining revenues respectively. This compares to 100% and 9% for the 2,737 day period encapsulated in our empirical model. The upturn in the coefficient on Transactions is coincident with the peak and subsequent churn in daily transactions from Spring 2017 (Figure 4.1). Note that although the throughput capacity of Bitcoin is often given as 7 transactions per second (600k transactions a day), this is with unusually small transaction sizes. Half this level is more plausible (Croman et al., 2016), and is supported by the results of our rolling regression. The second peak in transactions around December 2017 relates to the initial adoption

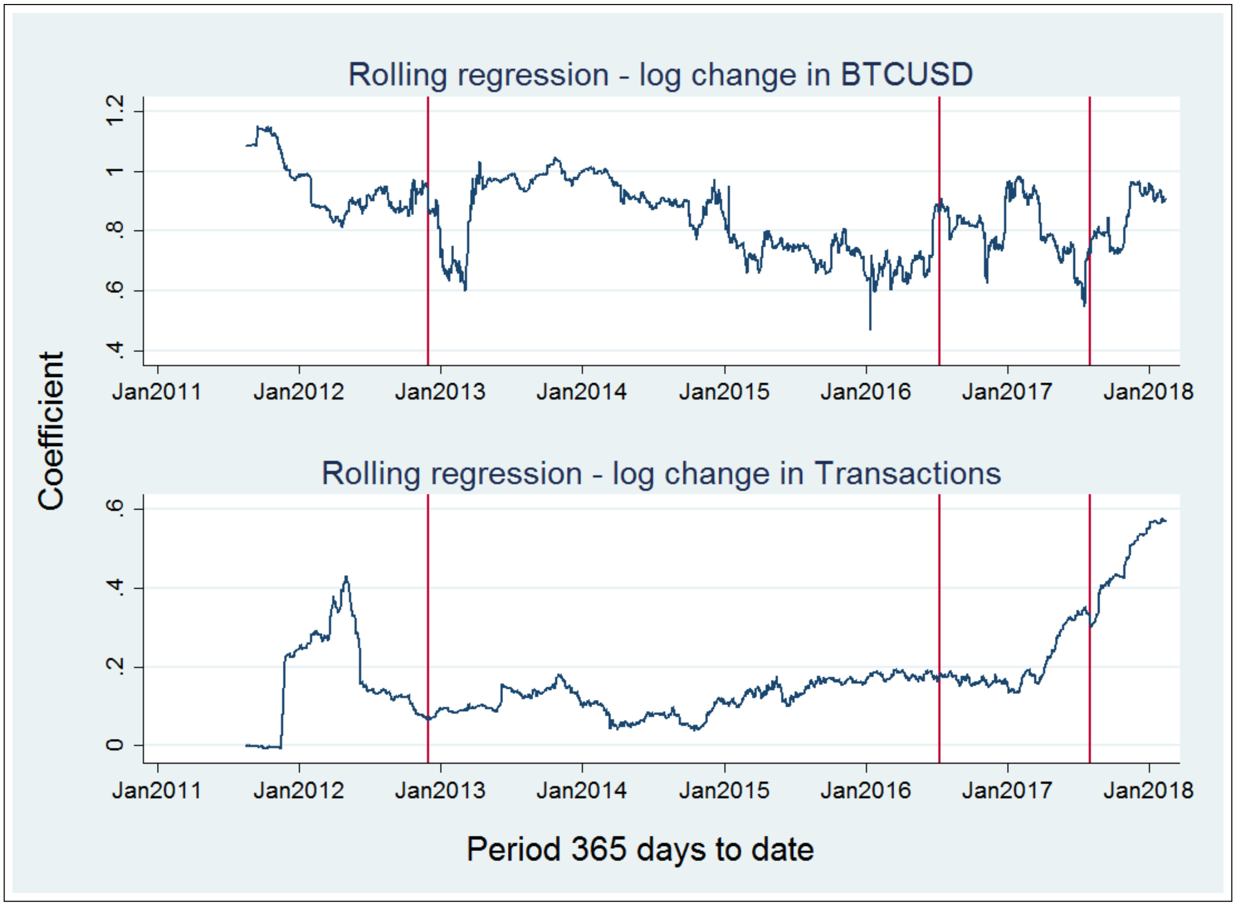


Figure 4.2: Rolling 365 day coefficient on log daily change in BTCUSD and Transactions. First and second vertical lines from the left are reductions to coinbase reward rate. Third vertical line is the Bitcoin Cash hard fork

of SegWit, the peak in the Bitcoin price and the coincident introduction of futures derivatives contracts on Bitcoin.

With respect to the winsorization of our extreme observations in 4.5, we find no change in statistical significance, and modestly higher coefficients on Transactions and the Bitcoin price. Conversely when using Bitstamp price data, the statistical significance of Transactions remains above 99.9% while that on price declines to the 95% level. That the coefficient on Transactions rises is unsurprising given the removal of the early part of the time series where Transactions were less important. However, as discussed in the data section, the decline in the coefficient on price to 0.226 from 0.996 highlights issues with using data from one Bitcoin exchange. The results from using other alternative Bitcoin price indices were similar to the original empirical model (not shown).

4.6 Summary - Bitcoin mining

A major beneficiary of Bitcoin's volatile appreciation in price is the Bitcoin mining industry. Average revenues over 2010-2018 exceed $2m US Dollars per day. Our analysis confirms that the dominant driver of daily differences in Bitcoin mining revenues is the Bitcoin USD price.

The importance of transactions appears to be changing. Unfortunately for proponents of Bitcoin, there are clear signs of growing pains, with a peak in transactions, higher fees being offered to gain processing priority, and higher Bitcoin mining cost per transaction. This is now being partly addressed by the SegWit update, but will likely require longer term solutions that are currently being explored. A corollary from this analysis is that transaction volumes are relatively unimportant, in terms of miner revenues and the cost of transactions, when block size is not binding. This follows trivially from the supply of capacity exceeding demand for capacity. Furthermore, it should not be controversial to state that capacity constraints are not an inherent feature of blockchain, but is simply a trade off with another feature e.g. number of nodes. A more controversial discussion might be the value of such nodes. If the value of many nodes is unproven (or that some subjective number of nodes defines a blockchain), then the scaling issues of blockchain are no longer inherent, but reflect design decisions. The impact that these scaling issues are having on the Bitcoin price, and any subsequent correction, should be borne in mind by economists and policy makers.

First differenced logs	Model	Winsorized	Bitstamp Bitcoin price
Transactions	0.0905^{***}		0.348^{***}
	(7.31)		(12.47)
Bitcoin USD index	0.996^{***}		
	(26.39)		
Spread	0.000717		-0.0621
	(0.03)		(-0.76)
Winsorized Transactions		0.217^{***}	
		(12.64)	
Winsorized Bitcoin USD index		1.071^{***}	
		(18.44)	
Winsorized Spread		-0.0102	
		(-0.22)	
Bitstamp Bitcoin USD price			0.226^{*}
			(2.49)
Constant	-0.000675	-0.000610	0.00114
	(-0.28)	(-0.29)	(0.31)
N	2735	2735	1171
Adjusted R^2	0.220	0.166	0.121

t statistics in parentheses. * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 4.5: Comparison of empirical model dataset against winsorised dataset and Bitstamp Bitcoin USD variable

Chapter 5

Assets on the blockchain: an empirical study of token functionality and price

5.1 Introduction

As discussed in Section 2.1, we place the creation of tokens in the second level of blockchain's capabilities. Payment activities can be executed via the authentic record functionality or with a token. However, the raising of financing from third parties is a function that has grown primarily from the ability to issue tradable tokens, and falls under Catalini and Gans (2016)'s lower networking costs related to venture bootstrapping. It should be clear that this thesis believes additional use cases for tokens can be developed.

Bitcoin is the leading payment token, and is mined into existence as processors are rewarded for carrying out tasks. In contrast, ICOs involve a crowdfunding to third parties. It is possible for payment tokens to be an ICO, by engaging in what is termed a premine, and then selling these tokens. However the subtlety is that for most ICOs, a change in how the tokens are made available is paralleled by a change in the underlying claim. The creation of Bitcoin did not fund anything and third party capital flows acquired a portion of the Bitcoin medium of exchange (Grinberg, 2012). Conversely ICO tokens can be sold for capital or distributed to potential users. The claim that ICO holders acquire can be anything the ICO issuer promises it to be. However, that they can be anything, does not mean they are something. With the issuance of venture backed tokens for financing, what are entrepreneurs and platforms giving up - and investors receiving in exchange?

The Spanish Bank BBVA quotes William Mougayar, author of The Business Blockchain, to define a token as a “unit of value that an organization uses to self-govern its business model”. We concur that any token, including payment tokens, can be used to govern and distribute the economic value of a platform or community. But we argue that the token doing this can be a bundle of many different things, and that it can be unrelated to business. There are multiple ways to define blockchains, and their tokens, for example Tasca, Thanabalasingham, and Tessone (2017), but one of the most intuitive will be by their function.

One functional category is the utility token, which is a token exchangeable for a service on a platform. Catalini and Gans (2018) use economic proofs to show how such a utility token, limited in quantity, and the sole medium of exchange, can appropriate the returns to a given platform. Under these conditions, the token price can appreciate in proportion to a rise in demand for the service on the platform. They note how these platforms are typically open source software protocols that equate to shared infrastructure among ecosystem participants. They use this framework to contrast token fund raising and venture capital. Importantly, equity investment offers the returns on all current and future projects of a firm, whereas token investment is solely in the current platform. These tokens therefore represent a more circumscribed package of entrepreneurship, value creation and value capture than an equity. Malinova and Park (2019) compares the use of stylized revenue share and output presale tokens relative to the equity financing of a project. The equity offering is simplified to share of project profits. A revenue share token promises a fraction of future project revenues and would likely count as a security offering under FINMA, 2018. It leads to under production as the entrepreneur sets output to where the retained fraction of marginal revenue is equal to total marginal cost. An output presale token fixes the token to output exchange rate and would likely count as a utility token under FINMA, 2018. It leads to over production as future issuance does not take into account the interests of existing token holders. Malinova and Park (2019) puts forward a hybrid token, which is an output presale token that includes a share of the value of future token issuance. They then provide an example where this form of token finances a project that includes entrepreneur effort as a variable (moral hazard), but would not have been financed by an equity offering at equilibrium. Canidio (2018) addresses the possibility of exit scams, where an issuer steals the funds raised, with retained token holdings and mixed strategies. In Chod and Lyandres (2018), retained token holdings are one way for issuers to align the interests of insiders and outside investors, and address the problem of information asymmetry.

Describing a single functional grouping of tokens over simplifies what is possible, and over determines what has been transferred. Despite the scope and scale of cryptoassets, there is limited understanding of what a token holder has acquired. This is partly because unregulated blockchain based tokens rarely include any legal obligations. As users are being asked to fund a business, a follow on question becomes: what they are receiving relative to what they are promised? Cohney et al. (2019) explores this by comparing marketing promises with smart contract code. Parallel to this, most empirical work on blockchain tokens to date have been focused on their associated prices (Bouri et al., 2017; Brandvold et al., 2015; Briere, Oosterlinck, and Szafarz, 2015; Lo, 2017; Pieters and Vivanco, 2017) or ICO success and size (Adhami, Giudici, and Martinazzi, 2018; Amsden and Schweizer, 2018; Benedetti and Kostovetsky, 2018; Howell, Niessner, and Yermack, 2018). Overall the academic literature is responding to this new capital structure of a venture, yet so far lacks evidence that its newest components authentically link project and token. In this chapter, we examine the relationship between various token functions and the market price of the corresponding token. We consider 86 venture related blockchain tokens, and develop the analysis through a stepwise testing of four hypotheses using panel ordinary least squares with cluster-robust standard errors. We find that token functions are statistically significant in relation to token prices. In the absence of an established legal framework, we argue that our results complement recent regulatory actions identifying tokens to be investment contracts in a common venture.

5.2 Literature review

5.2.1 Issuer perspective of initial coin offerings

The benefits to the issuers of ICOs are comparatively straightforward - token offerings have a clear use case as a new way to raise capital. Howell, Niessner, and Yermack (2018) provides a thorough discussion of the similarities and differences between ICOs and equity initial public offerings (IPOs). In addition to this, Li and Mann (2018) draws attention to the coordination problems in building a platform - where a lack of users can torpedo a socially valuable concept. Their work shows how it is possible to move this coordination problem to the sale of tokens at the time of ICO. If tokens are purchased, forward induction makes user adoption the logical choice. Their solution to the ICO coordination problem, extending the time period of the ICO, is unsatisfying. However it hints at how financial speculation might improve the probability of a socially positive equilibrium. Cong, Li, and Wang (2018) uses network effects to formulate a dynamic model of a tokenized economy, providing a wider lens to the why go Crypto question. Kampakis (2018) presents three case studies on token issuers focusing on the modeling of their micro-economies, and ways to incentivize the holding of their specific tokens. This work points out how important, and how easy, it is to customize a blockchain token. This customizability contrasts with how many early projects were copycat payment tokens that differed little relative to Bitcoin. Tu and Xue (2018) tests for Granger causality between the price of Bitcoin and the price of Litecoin, and the impact of a structural break related to the Bitcoin Cash hard fork. It notes that the creation of Litecoin only saw minor algorithmic changes compared to Bitcoin. Bitcoin Cash saw even fewer changes - hard forks do not merely replicate the application software, but the actual state (i.e. the addresses and balances of all prior users) of a payment token.

As the blockchain token space has matured, the amount of variation has increased, and in particular where that variation is occurring in the technology stack. Bitcoin is a vertically integrated infrastructure blockchain, native payments protocol application and payment token. Conversely, Fenu et al. (2018) examines 1388 initial coin offerings, adumbrates the importance of the Ethereum platform in the space, and discusses the mechanics of ERC-20. These standards consists of a set of rules for the issuance of a token on the Ethereum platform, including six mandatory functions such as how tokens are moved between addresses. These rules means anyone with Internet access can issue a token. Furthermore, smart contract enabled platforms like Ethereum have made it simple to have many different tokens share the same blockchain infrastructure. The relationship between a token and an application is determined by the issuer. These relationships are non-standardized in ways that gives rise to the unique economics of each token. This is based not on their legal claims, but on their promises and abilities, and the consequent relationships that extend from the underlying business. In contrast, a share in IBM and a share in Coca Cola are the same legal and financial claim upon different businesses. As it stands there is no effective class of attributes that groups all ICO tokens (though this persisting is another matter). Blockchain tokens have in the past taken the form of a profit share, a utility token, or simply a non-legally binding promise to develop. This variation begs the question of whether or not such attributes impact price, and is only starting to be explored e.g. Catalini and Gans (2018).

The use case of blockchain tokens for raising finance raises many questions regarding regulation and oversight. In the United States, ICOs that possess the characteristics of a security offering likely breach existing financial regulations designed to protect investors. In SEC (2017), the Securities and Exchange Commission determined that DAO tokens were securities under the Securities Act of 1933. It used the Howey test to determine whether or not an offering is a security, with the dimensions: (1) investment of money, (2) a common venture, (3) expectation of profits and (4) the efforts of others. A year later, SEC (2018a) found against two token issues, Paragon Coin and Carrier-EQ (AirFox). These were American registered corporations that raised funds from American citizens, and made marketing claims implying future profits. Both firms agreed to refund investors and register their tokens as securities. Additionally AirFox agreed to pay a fine of $250k, which equates to 1.67% of original funds raised, below the yield at the time on 10yr treasuries.[1] In Chapter 5, we use token function dummies to provide empirical evidence that blockchain token structure does impact token price. This suggests that projects with a value are being successfully connected to tokens that have a market price, and is supportive of the SEC's claim that they are investment contracts in a common venture. The pace of ICOs have slowed following these regulatory moves, although some now categorize themselves as Initial Exchange Offerings (IEOs), where the venture offering a token works closely with an established cryptocurrency exchange. Going forward ICOs are likely to either avoid US exposure or register as securities. Empirical papers in the field includes Benedetti and Kostovetsky (2018)'s survey of the price performance of a sample of 4,003 ICOs; Amsden and Schweizer (2018) that looks at 1,009 tokens and attempts to define determinants of crowdfunding success (e.g. quantity of raised funds), a topic that Howell, Niessner, and Yermack (2018), Ante, Sandner, and Fiedler (2018) and Adhami, Giudici, and Martinazzi (2018) also address. The choice of dependent and independent variables can be important in dealing with potential endogeneity of the supposedly independent variables. Variables such as team size and social media metrics will change if a fund raising gains momentum before closing.

[1] bloomberg.com/quote/USGG10YR:IND

5.2.2 Equity, debt and crowd funding within a capital structure

Given the use of blockchain tokens to raise finance, it is logical to connect them to the fecund literature on capital structure. Jensen and Meckling (1976) lays the foundations of the links between asymmetric information, the separation of control caused by the issuance of equity, and the Principal-Agent problem this leads to. Myers (2000) defines a pecking order for funding a business, from preferable to least preferable: internal cash flow, external debt, and external equity. Myers usefully highlights the primitive rights encapsulated by debt and equity. Lenders have a call option on a firms' assets, contingent on failure to pay interest and principal on debt. Equity investors can withdraw assets from insiders at any time. The clear contrast with ICO tokens is that blockchain tokens have no primitive rights. Ritter and Welch (2002) and Robb and Robinson (2014) study the empirical data on initial public offerings and on newly founded firms respectively, to better understand firm actions and decision making.

Financial instruments from cash to equity shares to financial bonds, are well established fungible items with frequent pricing. They are valuable enough so as to warrant representation in paper and more recently in digital form at a custodian. In theory it is possible to represent each of them with a blockchain token, and immediately save on custody costs. Eliminating intermediaries enables the elimination of custodians (Micheler and Heyde, 2016). It is logical that these prized markets have been targeted for blockchain implementation, but to the extent that high aggregate price is correlated to high transaction levels, these markets may not be the most suitable for low transaction capacity blockchains. Conversely there are potential use cases of blockchain where transaction velocity will not become a binding constraint. Such use cases may require a higher level of coordination (Iansiti and Lakhani, 2017), but if implemented could reduce costs, particularly where oligopolistic rents are being extracted, and increase trust in the truth recorded.

A bridge between existing financial securities and blockchain tokens is crowdfunding. Belleflamme, Lambert, and Schwienbacher (2014) examines two models of crowdfunding: pre-ordering and profit share. They discuss pre-ordering as a form of price discrimination, with examples where the pre-order price is higher than the later full availability price. This contrasts with ICOs where typically early funders receive purchase discounts or bonus tokens. Belleflamme, Lambert, and Schwienbacher (2014) notes that profit share is increasingly preferred as the amount of capital required increases. Ahlers et al., 2015 utilizes a dataset of 104 offerings on an Australian crowdfunding platform to examine this phenomena empirically. In some ways ICOs are a tradable crowdfunding asset (and even we adhere to the phrase that ICOs crowdfund), however token models offer greater flexibility around technical features, business models and economics. Clearly one of these flexibilities is that blockchain tokens are liquid and easily traded, a key driver and benefit of blockchain tokenization. These tokens leverage the features and network of the underlying blockchain infrastructure, and use it as a custody or notarization data layer.

5.3 Hypothesis development

We look to add empirical evidence to the emerging field of tokenomics. Utilizing a sample of 86 venture related blockchain tokens, we first parse out the relationships between our sample and two major cryptocurrencies. We then isolate the effect of different token functions, token features and token distribution characteristics highlighted in the literature (Figure 5.1). We develop our paper through a four step approach based on four hypotheses which aim to investigate the link between the token asset and its market price.

The cryptoasset space is dominated by two specific cryptocurrencies. Bitcoin is the primary means of buying and selling tokens, while Ethereum smart contracts are often the technological basis of many of these tokens, and sometimes a transactional cost of the application business an ICO is building. Bitcoin and Ether are also the main currencies used in funding ICOs. Both underpin distribution of tokens following a token generation event. For example, ERC-20 is the technical standard for issuing third party tokens on the Ethereum platform. Therefore buying an ERC-20 token with Ether occurs on a single blockchain platform, and is the easiest way to engage in such a transaction. Buying an ERC-20 token with other cryptocurrencies requires additional steps or coding, because the transaction crosses between two blockchains. Our first hypothesis emerges from the importance of these two cryptocurrencies.

- H1: "Price changes in Bitcoin and Ether cause statistically significant price changes in ICO tokens in the same direction."

In our analysis we assume a direct relationship between Bitcoin, Ether and ICO prices. We

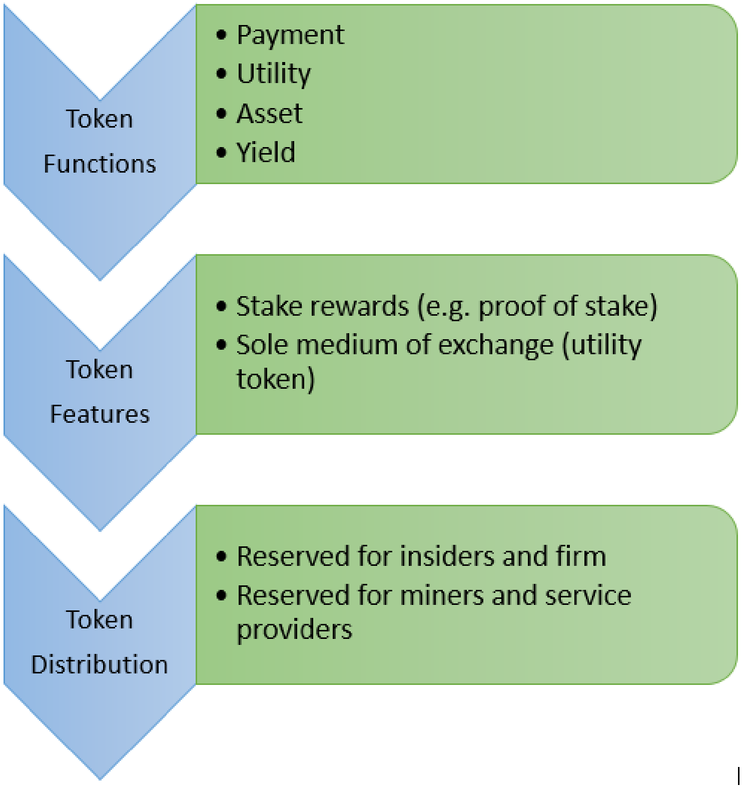

Token
Functions
• Payment
• Utility
• Asset
• Yield
Token
Features
• Stake rewards (e.g. proof of stake)
• Sole medium of exchange (utility token)
Token
Distribution
• Reserved for insiders and firm
• Reserved for miners and service providers

Figure 5.1: Token characteristics addressed in the analysis

then move on to our core hypothesis, that the functions that constitute a token create an economic link between a project that has a value, with a token that has a price. The idea that price and value can be separate is commonplace in the finance literature, though the definition of intrinsic value varies with the object of study (Froot and Ramadorai, 2005; Lee, Myers, and Swaminathan, 1999).

- H2: "Token function has a statistically significant impact on the issuing business value and its market price e.g., one or more token functions will trade at a higher price than the rest."

Our paper classifies the sample of tokens according to the token's functionality. We look specifically for the influence of functional dummies on a token's trading price. The four key functions we study are: (1) payment, (2) utility, (3) asset and (4) yield. We distinguish between share of profits type yields, and proof of stake blockchain type rewards (that distribute tokens to nodes that participate in consensus generation). One difference between the two is that the former is paid in a separate currency out of platform income (e.g. a dividend in Ether), while staking is in the token currently held, and numerically dilutive. Because of this, we consider share of profits to be a function and staking to be a feature. For reference, yield only tokens do exist in the dataset, but staking is typically associated with other functionalities as it reflects an underlying technical choice e.g. a proof of stake blockchain variant. There are other ways to interpret the promise of staking, including the potential elimination of platform mining costs and lower electricity consumption. However we are wary of categorizing a promise of stake rewards as usage of proof of stake technology (versus proof of work), because sampled project tokens typically begin trading on a proof of work blockchain platform such as Ethereum.

With respect to a token being the sole medium of exchange on a platform, in theory it is necessary for a utility token to adhere to this in order to appropriate the benefits of the platform (Catalini and Gans, 2018). We collect data on whether or not a utility token is intended as the sole medium of exchange for the related platform and test for any relationship between this factor and the token's trading price. The features of staking and sole medium of exchange are bundled together in our third hypothesis.

- H3: "Tokens promising the characteristics of stake rewards and sole medium of exchange on a platform, trade at a statistically significant higher price."

Designating a token as the sole medium of exchange does not always resonate with investors. A prominent example of this is how Basic Attention Token (BAT) has faced calls to make payments in US Dollars or Bitcoin instead of BAT tokens [2]. Sole medium of exchange requirements may slow wider adoption, as changing in and out of the utility coin becomes a barrier to use.

Our final hypothesis revolves around the criticality of token distribution at the time of ICO. This focuses on the split in economics between investors, relative to insiders and future service providers. These token distribution decisions are likely endogenous, and operate in two contrasting ways. It is plausible that the better the project, the higher the share of tokens reserved for insiders - and therefore signals quality to outsiders. Conversely, an increase in either of these reserved token categories decrease the share of platform economics received by funders. Our framework enables us to test for which of these effects dominate in terms of price.

- H4: "ICOs with a higher proportion of outstanding tokens reserved for the token issuer, or

[2] https://blog.goodaudience.com/basic-attention-token-bat-fails-to-live-up-to-its-claims-7b1a91d46b01

> a lower proportion of tokens reserved for mining, trade at a statistically significant higher price."

We use the proportion of tokens reserved for founders / team members / company controlled foundation, or reserved for mining, future marketing or future partnership building.

5.4 Token classification

Blockchain token structures are non-standardized. The potentially unique economics of each token are not based on legal rights, but on their promises (e.g. claims and features) and abilities (functions). Consequently these features and functions may create economic relationships extending from the underlying business to the digital token. In contrast, a share in IBM and a share in Coca Cola are the same legal and financial claim upon different businesses, and contain legally enforceable primitive financial and managerial rights (Myers, 2000). As it stands there is no comparable class of attributes that groups all ICO tokens.

The Bitcoin blockchain is a payment protocol, a set of rules and conventions for the movement of value between network addresses. Narayanan and Clark (2017) observe the simplicity of leveraging a secure ledger to create a digital payment system. But tokens can have other uses. For this paper, our starting point is the Swiss financial regulator FINMA (2018)'s identification of financial blockchain tokens into three functional categories: payment tokens, utility tokens, and asset tokens. These categories are not mutually exclusive - a token can be designed to perform all three functions.

Payment tokens are a means of value trans-

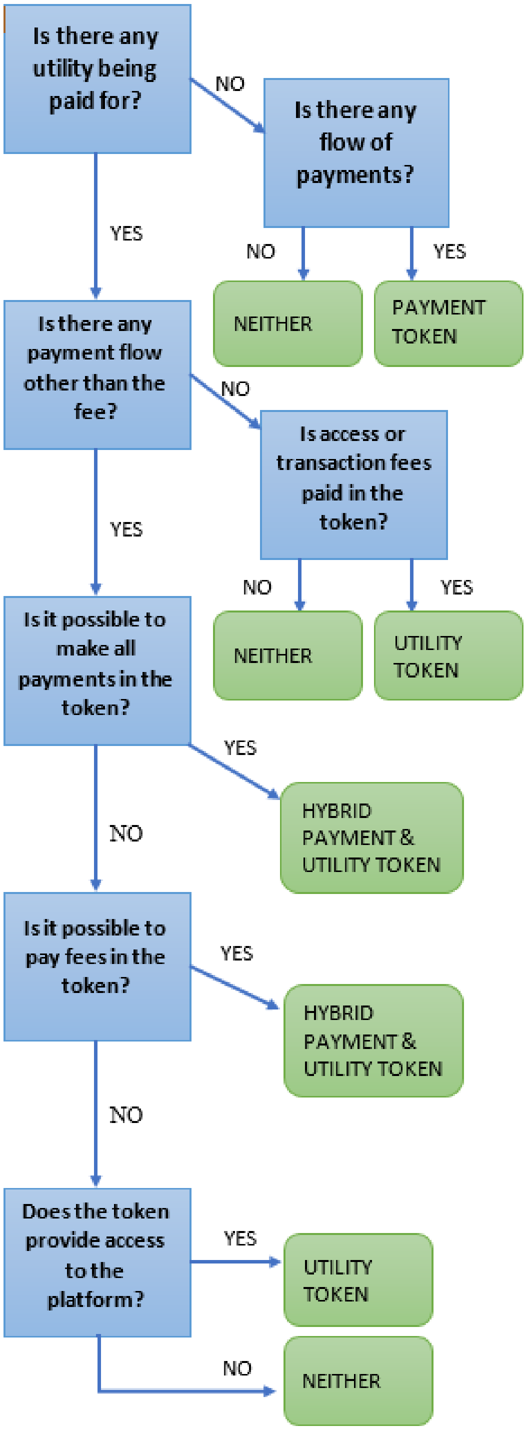

Is there any utility being paid for?
NO
Is there any flow of payments?
NO
YES
NEITHER
PAYMENT TOKEN
YES
Is there any payment flow other than the fee?
NO
Is access or transaction fees paid in the token?
NO
YES
NEITHER
UTILITY TOKEN
YES
Is it possible to make all payments in the token?
YES
HYBRID PAYMENT & UTILITY TOKEN
NO
Is it possible to pay fees in the token?
YES
HYBRID PAYMENT & UTILITY TOKEN
NO
Does the token provide access to the platform?
YES
UTILITY TOKEN
NO
NEITHER

Figure 5.2: Characterization of token as payment or utility

fer, spanning cryptocurrencies like Bitcoin, to industry specific ICO tokens e.g. DragonChain that seeks to reduce frictions within the casino industry. FINMA (2018) defines a utility token as intended to provide access digitally to an application or service, by means of a blockchain-based infrastructure. This may include the ability to exchange the token for the service. The Ethereum blockchain's utility is its smart contracts, that enable the distributed processing of permissionless computer code in a predictable way. Consequently, we define Ether as a payment and utility token, with smart contract execution, network fees, and the ability to transfer value outside of fees. The sample of blockchain token prices that we test, as a dependent variable, includes three cryptocurrency like payment and utility tokens (Tezos, Viacoin, and Wanchain). We note that we do not make the distinction, sometimes seen in computer science, that a blockchain Coin is one that trades on its own infrastructure, and that a blockchain Token is one that trades on third party infrastructure.

FINMA's definition of an asset token includes attempts to bind physical or digital assets to a digital blockchain token, and promises to share profits. Our framework differs from FINMA's model, in that we separate the asset category into two functions: (1) tokens linked to a physical or digital asset e.g. silver or collective Crypto investment funds, and (2) tokens that promise to pay a share of profit or revenue. We refer to the former as the functionality of asset, and the latter as the functionality of yield.

Both asset and yield functions are binary in nature, and therefore straightforward to categorize. However it is necessary to formalize the identification of payment and utility functionality. This is illustrated in the flow diagram in Figure 5.2. The key criteria within the proposed framework for definition as a payment token is the presence of a payment flow other than the fee, and the ability to use the token to address either the flow or the fee. The flow diagram divides the payment ability of the token into (1) transacting the payment flow and (2) paying the fee, not because the result is different, but to highlight that many tokens make this distinction in usage. A payment flow opportunity addressed by a platform, but not payable in the associated token, might not be designated a payment token. Our sample does not include any payment only cryptocurrencies like Bitcoin, rather they are primarily industry or purpose specific payment tokens.

In our sample, the most common reason that a token is neither a payment nor utility token is because it is an asset token, linked either to a portfolio of cryptoassets, some off-chain real world asset like silver, or a share of platform profits. For example, Crypto20's token C20 is a tokenized Crypto investment fund. An example of a utility token with no payment flow is the WePower WPR token. Its objective is to streamline the presale of renewable energy (facilitate project funding), with WPR receiving a share of "donated" power. WPR is not considered a payment token as separate energy tokens are sold by plant or projects on the WePower platform. This is in contrast to another energy platform token, Suncontract SNC, which does not use a secondary token in this way. Each SNC token is intended to be associated with a quantity of electricity.

Our framework categorizes non-platform businesses as a utility token. For example Hedge Token HDG was a Crypto financial services provider, selling its own products and services via its token. HDG has now migrated to the Blocktrade token BTT, which is a Crypto exchange, and therefore within our framework it is now a hybrid payment and utility token, with a payment flow between buyers and sellers of other tokens on their exchange. Other variables are covered under the Data section.

5.5 Data

	N	mean	sd	min	p25	p50	p75	max
Token price at close, USD	979	1.7	6.4	0.0	0.0	0.2	0.9	104.6
Ave token market cap, USD mil	979	701	12,638	0.0	2.9	20.8	113	390,000
BTC price at close, USD	979	6,788	3,766	223	4,403	6,835	9,114	19,065
Ave Bitcoin price, mth USD	979	6,945	3,865	228	4,096	7,772	9,003	15,312
ETH price at close, USD	947	490	290	0.7	289	452	670	1279
Ave Ether price, mth USD	951	498	282	1.0	305	519	629	1,137
Diff in log Token price at close	893	-0.07	0.8	-4.1	-0.5	-0.1	0.3	7.0
Diff in log Bitcoin price at close	893	0.03	0.3	-0.6	-0.2	0.1	0.3	0.6
Diff in log Ether price at close	861	0.06	0.4	-0.8	-0.2	-0.0	0.5	1.3
Major deployment dummy	979	0.41	0.5	0.0	0.0	0.0	1.0	1.0
Pct tokens allocated to insiders	979	25.4	22.4	0.0	10.0	20.0	33.0	92.0
Pct tokens allocated to mining	979	17.4	28.7	0.0	0.0	0.0	28.0	99.0

Table 5.1: Descriptive statistics for sample of 86 blockchain tokens (N=monthly)

The primary source of our data is the Cryptocompare.com API, which is used by over 500 companies across the blockchain space, and media platforms such as Yahoo Finance.[3] On 18 July 2018, we downloaded data on 86 blockchain tokens, or ICOs. This data includes the daily closing

[3] https://min-api.cryptocompare.com/

token price in Bitcoin, the daily closing US dollar exchange rate of Bitcoin / Ethereum / Litecoin and Ethereum Classic, data on cryptocurrencies raised by each ICO, estimated total US dollars raised, and total supply of each token. Where appropriate we convert a token price denominated in Bitcoin into a US dollar price. For our robustness check, we form monthly averages (mean value for the month) from daily time series. Observe how the peak value of BTC declines from USD 19,065 to USD 15,312 when moving from closing prices to monthly average. It is notable that more token prices ("cross rates") are available in Bitcoin than in US dollars. We calculate token market capitalization by multiplying token price by the total supply of tokens. These values are charted in Figure 5.3. Market capitalization is the least worst way to visualize the importance of each token, but is prone to many issues including inconsistent ability to exchange, locked tokens and tokens that are no longer accessible. The data on invested capital is declared by the issuer and can come in two forms: (1) a disclosed quantity of cryptocurrencies, or (2) a US dollar equivalent. Using the last closing cryptocurrency price prior to the official end of the ICO period, we estimate the parallel figure when one is absent. This may assume a token raised funds in Bitcoin because it was launched prior to the launch of Ethereum. This may assume a token raised funds in Ether because it began life as an ERC-20 token that operated on the Ethereum platform. The data is unbalanced and covers the period between 2 December 2014 to 17 July 2018, part of which is summarized in Table 5.1.

We use the frameworks defined in section 5.4 in order to classify our tokens. The four key functional designations of the token framework are: (1) payment, (2) utility, (3) asset and (4) yield. We note that 4 functionalities enable $2^4 = 16$ potential functional combinations, and that not all combinations are present in the sample. Each included token has at least one of these functionalities. All the functional token specifications are identified through the dummy variables in Table 5.2. The number of tokens with payment functionality is $43 + 8 = 51$, and the number with utility functionality is $43 + 26 = 69$. When all the dummies are equal to zero, this is the reference state which corresponds to a hybrid payment and utility token - the most common token type in the sample. Delineating this reference category, and explicitly excluding it from all regressions, is necessary to prevent multicollinearity. There are 11 tokens linked to off chain assets and 14 tokens promising a dividend like yield.

In particular, TPAY is equal to 1 when the token has a payment functionality but no utility

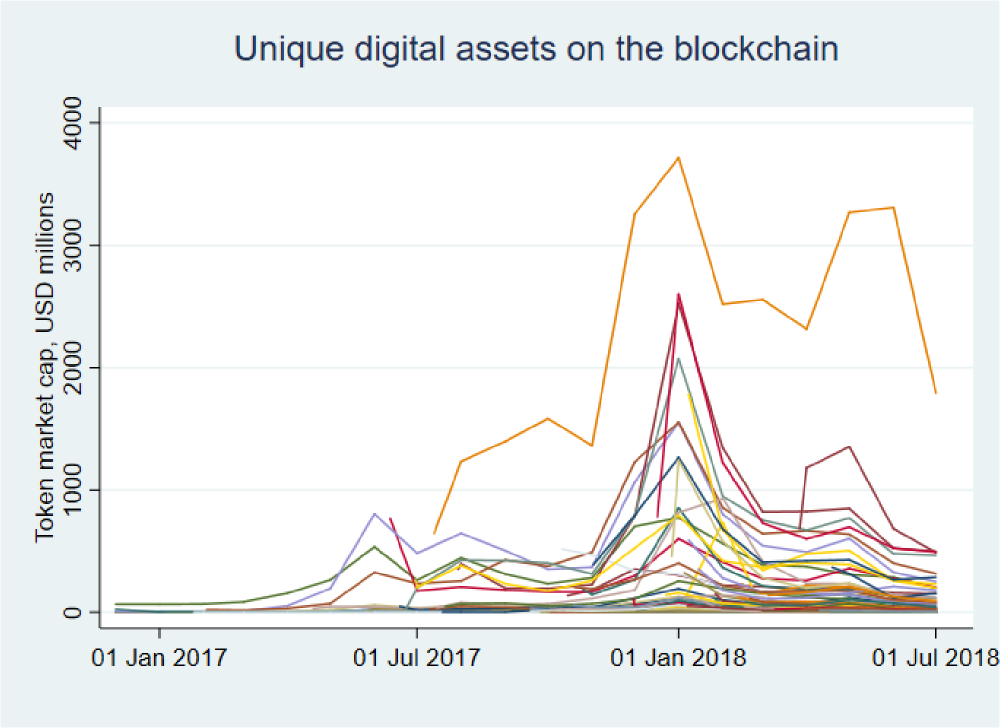


Figure 5.3: Market capitalization of study sample of blockchain tokens

functionality. TUTE is 1 when the token has utility functionality but no payment functionality. TASSET is 1 when the token is linked to an off-chain asset. TYIELD is 1 when the token promises to pay a dividend in a token other than itself. The functional dummies (plus reference category) are considered together as a set of groups that span the sample. The other dummies are Boolean in nature, and reflect a default state where they do not apply. If TSTAKE is 1, then the issuer envisions its token within a proof of stake style platform that pays out a reward in itself. The reference category when TSTAKE is 0 is that the token is expected to indefinitely exist on a blockchain without stake rewards (e.g. proof of work). If the white paper, or the platform website, of a token claims that its token will be the sole medium of exchange, or the sole means of payment of the platform fee, then the TSOLE dummy is equal to 1. The reference state where TSOLE equals 0 is that either the platform contains alternative media of exchange, or that it does not possess a utility functionality. Calculating interaction terms, such as TASSET * TYIELD (which would estimate the additional mean difference between this type of hybrid token relative to a hybrid payment and utility token), is not appropriate as these would be small sub-samples of four or less tokens.

	Description	Number	Share
Counter	Total number of tokens	86	1.00
Counter	Hybrid payment / utility functionality	43	0.50
TPAY	Payment functionality (No utility)	8	0.09
TUTE	Utility functionality (No payment)	26	0.30
TASSET	Asset functionality	11	0.13
TYIELD	Yield functionality	14	0.16
TSTAKE	Stake rewards	8	0.09
TSOLE	Sole medium of exchange	35	0.41
TDEAD	No longer trading	9	0.10

Hybrid, payment and utility are mutually exclusive token designations, however other dummy types are not mutually exclusive. 10% of tokens have neither payment nor utility functions.

Table 5.2: Token dummy statistics

Many tokens are issued prior to the implementation of their product. In order to control for this, we include a deployment dummy. If a significant element of its product road map is deployed, then from that month, its TDEPLOY dummy is coded as 1. If this is coded 0 then the project has no significant products ready for use. Additionally, we track trading activity at the time of data download. If a token has not traded on an exchange within the week prior to the data download, then the TDEAD dummy is coded as 1. If this dummy is coded 0, then the token continued to trade on an exchange that provides data to Cryptocompare at the time of data download.

The variable RINSIDER is the proposed proportion of tokens reserved for founders, employees, company vehicles, trusts and advisors. This is distinct from tokens that are sold during the token generation event and the raised funds specified for payment or transfer to insiders (cash out). This category does not include early investors. RINSIDER can be thought of as retained interest in the future success of a project. RINSIDER does not adjust for ex post changes in how tokens are distributed e.g. when tokens reserved for insiders are later airdropped to users. RMINE is the proposed proportion of tokens that will either be released in the future for mining (e.g. transaction processing services similar to Bitcoin), or for future partnerships and marketing. When less tokens are sold to investors than intended, these proportions end up higher, irrespective of whether such tokens are then held by the issuer e.g Ripple, or are burnt (permanently eliminated). Both of these variables are ratio scaled.

In figure 5.4, we chart the selection bias of our sample of 86 blockchain tokens, by plotting

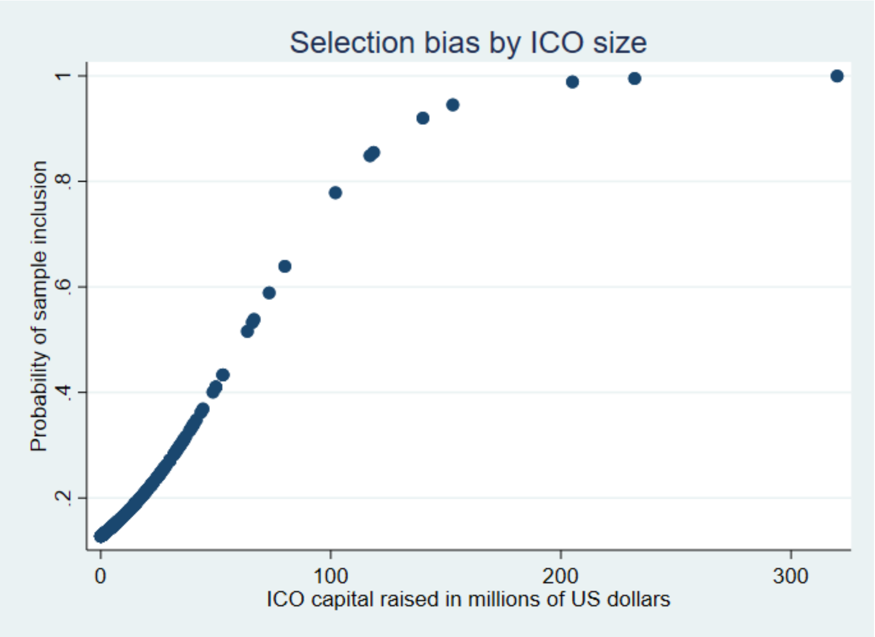


Figure 5.4: Blockchain token selection bias

probability of inclusion versus US dollars raised at ICO. At the time of download, 2700 coins and tokens were identified on the Cryptocompare platform. 465 (17%) of these were designated as ICOs i.e. that they had raised capital from third parties. Our sample of 86 tokens are 18% of this group. The probability of sampling is correlated to ICO size in dollars. This is primarily driven by the data relationship between Cryptocompare and the trading exchange providing the underlying time series. A token must be listed on an exchange, and a formal agreement exist between Cryptocompare and an exchange, that enables this data to be provided via Cryptocompare's API. Criteria on inclusion includes data on amount of capital raised and at least two periods of price data. A plausible justification of the size bias to this relationship is that the listing of cryptotokens on exchanges is often facilitated by monetary payments from a token team to an exchange.[4] Unfortunately, it is not possible to utilize a Heckman correction to adjust our empirical results for these selection biases, as we cannot identify all the missing time series observations such a procedure requires.

[4] http://uk.businessinsider.com/cryptocurrency-exchanges-listing-tokens-cost-fees-ico-2018-3

5.6 Methodology

To test our four hypotheses we perform an ordinary least squares regression. An advantage to this approach arises from the data being formed in unbalanced panels - which are outside the scope of some alternative methods. Feasible GLS modeling for example, which allows direct specification of auto-correlation and heteroskedasticity across panels, is ruled out as modeling for auto-correlated errors requires equally spaced data, while modeling for cross-sectional errors requires balanced panels. We begin by examining the non-stationarity of our data by carrying out Augmented Dickey Fuller (ADF) tests on the price of Bitcoin and Ether, using Akaike Information criteria (AIC) to choose the number of lags, and do not reject the null of a unit root. ADF tests on the first difference of the log of monthly closing Bitcoin and Ether prices do reject the null. These results suggest that Bitcoin and Ether are integrated of order 1 and justify the use of first difference of logs to ensure stationarity.

The token time series are less straightforward. We use Fisher-type tests for panel unit roots (Choi, 2001), that apply ADF tests to each panel. These are four statistical tests under the null hypothesis that all panels contain a unit root, versus the alternative hypothesis that at least one panel has a unit root. For one and two lags, the Fisher-type tests reject the null that all panels include a unit root. This implies that some (or all) of the panels are stationary. We note that significant price declines such as that seen in 2018, consistent with the bursting of a financial bubble (Brunnermeier and Oehmke, 2012), may cause pseudo-stationarity. The Fisher-type tests do not reject the null under 3 lags, but may be over specified. When testing monthly average market capitalization (rather than monthly closing price), the Fisher type tests do not reject the null under 2 lags, but reject the null when the first differences are taken. Overall we choose to use first differences of logs to ensure symmetric distributions of the price variables. The correlation coefficient matrix for before and after these transformations are shown at the end in Table 5.7 and 5.8. Serial correlation within panels is addressed with cluster robust standard errors (discussed below).

Therefore we formulate a linear model, for our panel ordinary least squares regression tests, using the first difference of price at monthly close. The daily token closing price observations in Bitcoin are converted into US dollars, and we select the last observation for each month. This forms the basis for the key dependent variable of our model DLPX, the first difference of the log of monthly closing ICO token prices, in US dollars, for 86 separate blockchain tokens. Independent variables include DLBTC, the first difference of the log of monthly closing price of Bitcoin, and DLETH the first difference of the log of monthly closing price of Ether. A summary of our linear empirical model is given in equation 5.1.

$$\Delta(ln\mathbf{y}_t) = \alpha + \beta\Delta(ln\mathbf{x}_t) + \gamma\mathbf{z} + \epsilon_t \tag{5.1}$$

Where:

$\Delta(ln\mathbf{y}_t)$ = first difference of the log of monthly closing ICO token prices in US dollars at time t.

$\Delta(ln\mathbf{x}_t) = k \times 1$ vector of the first difference of log of monthly closing benchmark crypto prices at time t.

$\mathbf{z} = p \times 1$ vector of token dummies and token distribution ratios.

ϵ = error term with mean zero and unit variance.

α = constant.

$\beta = k \times 1$ coefficient vector.

$\gamma = p \times 1$ coefficient vector.

We conduct multiple regressions to test the significance of the set of Bitcoin and Ether price variables, token function, feature, and distribution dummies. For clarity, our panel OLS methodology stacks each change in price for each of the 86 blockchain tokens, regresses them on the related independent variable observations, and estimates a single coefficient and standard error for each independent variable across the entire sample. It is sometimes referred to as a pooled OLS model. The intercept (results not shown) ensures that the mean of the error term is zero. This can be written in matrix notation (equation 5.2), where the first difference in logs is folded into the variables where appropriate, and subscript *it* reflects the value of the variable for blockchain token *i* at time *t*.

$$\mathbf{y}_{it} = \alpha + \boldsymbol{\beta}^T\mathbf{x}_{it} + \boldsymbol{\gamma}^T\mathbf{z}_i + \epsilon_{it} \tag{5.2}$$

Given that we are formulating and testing a linear regression model, standard OLS assumptions apply with respect to linearity, spherical error terms, and exogeneity. It is not possible to run a fixed effects panel model with token dummies given the fact that many of the dummies are non-varying within our ICO token panels i.e. any such dummy effect would be incorporated in the panel fixed effect. We use cluster robust standard errors (Cameron and Miller, 2015) as it is likely that regression model errors are correlated within clusters (visible when graphing residuals - not shown). Cluster robust adjustments requires the additional assumption that the number of clusters goes to infinity. Moulton (1986) notes how the effect of within cluster correlation can be particularly pronounced when analyzing a policy variable, or aggregated regressor, that takes the same value for all observations within a cluster - which applies to almost all our token dummies. Cluster-robust standard errors also helps address the heteroskedasticity identified in the data. For a final robustness check we also calculate the implied market capitalization by multiplying daily token prices by total token supply - and rerun the analysis with this data.

5.7 Results and Discussion

	[A]	[B]	[C]
DLBTC	0.221	0.222	0.222
DLETH	0.733***	0.733***	0.732***
TPAY	-0.106*	-0.104*	-0.108*
TUTE	-0.017	-0.020	-0.019
TASSET	-0.017	-0.019	-0.020
TYIELD	-0.065	-0.066	-0.068
TSTAKE	-0.006		
TDEPLOY	-0.053	-0.051	-0.053
TSOLE	0.012	0.014	
RINSIDER	-0.000	-0.000	
RMINE	0.000		
aic	1791.917	1787.959	1784.120
bic	1849.015	1835.540	1822.184
Adjusted R^2	0.223	0.224	0.226
n tokens	86	86	86
N observations	861	861	861

All models refer to POLS using cluster-robust standard errors.

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 5.3: Determinants of token price change

As discussed above, the dependent variable DLPX is the first difference of log token price at close, which given a monthly data set approximates the monthly percentage change in price.

Column [A] of Table 5.3 is a general specification containing all the explanatory variables. The reference state when all the dummies take the value 0 is that the token is a hybrid payment and utility token with no asset or yield function. In Table 5.3 column [B] and [C] we reduce the number of independent variables. Column [B] is focused on two aspects raised by the prior literature (and the testable hypotheses), sole media of exchange and tokens reserved for insiders. Note that none of the core functionality dummies can be removed without impacting the meaning of the reference state. All three specifications find 99.9% statistical significance on the first difference in log price of Ether. As the dependent variable and the independent price variables are logs, the coefficients β_k are elasticities (where k is the related independent variable). Therefore our results indicate that a 100% change in the price of Ether leads to a 73% change in the price of our sample of blockchain tokens. The coefficient on the first difference in log price of Bitcoin is not statistically significant. Together these findings reject the null of no relationship in favor of Hypothesis H1, that Ether is a driver of the price of other tokens in the same direction. In terms of our token function dummies, the majority are negative and not significant, with two exceptions. The payment dummy TPAY is negative and statistically significant at the 95% level. This result rejects the null of no relationship in favor of Hypothesis H2, that token function is impactful. Within our sample, payment protocols without associated utilities are predicted to have more negative percentage changes in value. The TSOLE dummy has a positive coefficient, however this result is not statistically significant at the 95% level. Adding in the lack of evidence of statistical significance on TSTAKE, these results do not reject the null of no relationship between these token features and token price, with respect to Hypothesis H3. In terms of Hypothesis H4, we are unable to reject the null that tokens distributed to insiders or future service providers do not impact token price. Column [C] is designated the empirical model based on the Akaike (AIC) and Bayesian Schwarz Information Criteria (BIC). The lower the AIC and BIC, the more appropriately specified the model.

In Table 5.4 we explore the influence of ICO funding type. Column [C] is identical between Table 5.3 and 5.4. In column [D] we form a sub-sample of tokens that disclosed raising Ether at the time of ICO, or are ERC-20 tokens. In column [E] we include tokens that raised Bitcoin at time of ICO. All of this latter set of tokens will have either disclosed the Bitcoin raised or launched prior to the launch of Ethereum. These two groups are not mutually exclusive as some will have raised funds in both Bitcoin and Ether. Column [D] of Ether fund raisers see an increased correlation with

	[C]	[D]	[E]
DLBTC	0.222	-0.089	0.478***
DLETH	0.732***	0.996***	0.511***
TPAY	-0.108*	-0.101*	-0.071
TUTE	-0.019	-0.031	0.023
TASSET	-0.020	-0.066	-0.054
TYIELD	-0.068	-0.091	0.014
TDEPLOY	-0.053	-0.052	-0.088
aic	1784.120	1237.312	621.377
bic	1822.184	1271.358	653.349
Adjusted R^2	0.226	0.205	0.281
n tokens	86	66	26
N observations	861	521	402

All models refer to POLS using cluster-robust standard errors.

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 5.4: Differences arising from fund raising

Ether. A 100% change in the price of Ether leads to a 99.6% change in the price of the blockchain token, and the TPAY dummy remains negative and statistically significant. The TPAY dummy in column [D] relates to 5 payment functionality only tokens. The coefficient on Bitcoin price changes becomes negative. Column [E] of Bitcoin fund raisers see a decline in correlation with Ether, but the Bitcoin price coefficient becomes statistically significant. This model suggests that a 100% change in the price of Bitcoin and Ether leads to a 48% and 51% change in the price of the sub-sample of blockchain tokens respectively. The TPAY dummy loses statistical significance. This result suggests that the form of fund raising, or underlying platform, is important to the performance of a token, and that it is Payment tokens raising Ether that have statistically significant changes in price. We advise caution regarding the interpretation of the token dummies under the Bitcoin funded sub-sample [E] due to the decreased sample size of 26 tokens.

In Table 5.5 we perform two robustness tests on the empirical model. Column [C] is identical between Table 5.3 and 5.5. In column [Y] we drop the not statistically significant Bitcoin price variable. In column [Z] we control for the tokens that have not traded recently using the TDEAD dummy. We note that both models have hardly any impact on our results, but do lead to an undesirable increase in the AIC and BIC ratios.

In Table 5.6 we review robustness by rerunning the modeling from Table 5.3 with token market capitalization and monthly averages of our price data. The dependent variable becomes the first

	[C]	[Y]	[Z]
DLBTC	0.222		0.222
DLETH	0.732***	0.826***	0.732***
TPAY	-0.108*	-0.107*	-0.108*
TUTE	-0.019	-0.019	-0.020
TASSET	-0.020	-0.018	-0.024
TYIELD	-0.068	-0.068	-0.070
TDEPLOY	-0.053	-0.054	-0.051
TDEAD			0.010
aic	1784.120	1787.267	1786.102
bic	1822.184	1820.574	1828.924
Adjusted R^2	0.226	0.222	0.225
N observations	861	861	861

All models refer to POLS using cluster-robust standard errors.

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 5.5: Robustness check - Bitcoin variable and no longer trading

difference of log monthly average market cap (DLMMC) for each of our tokens. This moderates the impact of outliers and checks if token supply impact our results. The correlation coefficient matrix for before and after these transformations are shown at the end in Table 5.8. The Bitcoin variable is DLMBTC first difference in log monthly average of the Bitcoin price, and the Ether variable is DLMETH first difference in log monthly average of the Ether price. All the other variables are unchanged. We observe that the statistical significance on the Ether and TPAY dummy coefficients remain. The adjusted R^2 is lower and that the AIC and BIC criteria are higher when compared to Table 5.3.

Given the results of our analysis, we can now examine our hypothesis in order.

- H1: "Price changes in Bitcoin and Ether cause statistically significant price changes in ICO tokens in the same direction."

We find strong evidence of a positive relationship between the price of Ether and price of the blockchain tokens contained in our sample, at the 99.9% statistical significance level. We find weaker evidence that the price of Bitcoin impacts these tokens. For the full dataset in Table 5.3 there is no finding of statistical significance on the Bitcoin price coefficient. However for the subset of tokens that raise funds in Bitcoin, Table 5.5 puts forward evidence that Bitcoin does have a positive relationship at the 99.9% statistical significance level. Our results are consistent with

	[A2]	[B2]	[C2]
DLMBTC	0.126	0.127	0.128
DLMETH	0.949***	0.949***	0.947***
TPAY	-0.090*	-0.085*	-0.090*
TUTE	-0.025	-0.029	-0.027
TASSET	-0.030	-0.031	-0.032
TYIELD	-0.060	-0.059	-0.061
TSTAKE	-0.032		
TDEPLOY	-0.034	-0.029	-0.031
TSOLE	0.016	0.018	
RINSIDER	-0.000	-0.000	
RMINE	0.000		
aic	2249.128	2245.240	2241.396
bic	2306.281	2292.868	2279.498
Adjusted R^2	0.130	0.132	0.134
n tokens	86	86	86
N observations	865	865	865

All models refer to POLS using cluster-robust standard errors.
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 5.6: Robustness check using first difference of log market capitalization (DLMMC) as the dependent variable, and monthly average prices

Ciaian, Rajcaniova, and Kancs (2017), which performed a ARDL analysis on Bitcoin and a sample of altcoins, and detected a selection of cointegration relationships particularly over shorter time periods. Specifically, Ciaian, Rajcaniova, and Kancs (2017) find a negative relationship between Bitcoin and an index of altcoins, which they ascribe to competition effects across a given menu of investment options. We note that a Vector Auto Regressive or Vector Error Correction Model would provide more information on the direction of causality, but for our dataset would be over specified. Our work provides additional evidence that ICO tokens, which represent an underlying business or platform, are a separate asset class from Bitcoin.

- H2: ”Token function has a statistically significant impact on the issuing business value and its market price e.g., one or more token functions will trade at a higher price than the rest.”

We confirm a negative and statistically significant coefficient at the 95% level, on our payment only token function dummy, under multiple different specifications. The utility only dummy has a negative coefficient, but no statistical significance. Our results suggest that either industry specific frictions may not justify a new method of payment, or that payment and utility may be an optimal combination in terms of driving value. We argue that it is rational to discount the idea that these payment only tokens are competing with Bitcoin (and losing), as the tokens in the sample are proposed businesses, not merely potential stores of value. The yield dummy, which some might argue would add value to a token consistent with a dividend discount stock valuation model (Gordon, 1959), did not lead to any statistically significant result, and had a negative coefficient.

- H3: "Tokens promising the characteristics of stake rewards and sole medium of exchange on a platform, trade at a statistically significant higher price."

The stake reward dummy was not statistically significant. For the purposes of discussion, we juxtapose this feature with the function of yield, because yield and staking token characteristics promise either: (1) a monetary dividend in another currency e.g. Ether; or (2) a scrip-like dividend in the same token (more shares of the token's aggregate value). There are three plausible reasons for their lack of statistical significance. The first is that token value may accrete from these features from the date they are implemented, and for the majority of our sample, they have not been instituted yet. Another point is that these features or rights can exist at two levels: those that are made in associated documentation, and those that are written in the software code (Cohney et al., 2019), and these reward promises are still marketing promises rather than hard coded. A final reason might be that it is in fact very difficult to pay such rewards. Large quantities of tokens are held in aggregated wallets at exchanges where they are bought or sold. This creates problems with the identification of ownership and payment of any rewards.

Although we find a positive coefficient on the TSOLE dummy, suggesting that definition as the sole medium of exchange is a value increasing utility token feature, we are unable to find sufficient statistical evidence to reject a null hypothesis that being the sole medium of exchange has no impact on blockchain token prices. Therefore we fail to present empirical evidence in line with the work of Catalini and Gans (2018).

- H4: "ICOs with a higher proportion of outstanding tokens reserved for the token issuer, or a lower proportion of tokens reserved for mining, trade at a statistically significant higher price."

Our study is unable to reject the null hypothesis that tokens reserved for insiders and tokens earmarked for mining have no impact on blockchain token price. We note that in theory payments for mining and future partnerships should be made at the expected value of services rendered. The effect of insider ownership on the other hand reflects two alternative perspectives: (1) that a high stake reflects skin in the game and inside information about the quality of the business (Chod and Lyandres, 2018), and (2) that the investor's share of platform economics is being circumscribed. These factors may become more tractable to economic analysis once an increasing proportion of these platforms are deployed and achieve scale.

5.8 Summary - Assets on the blockchain

One way to introduce the phenomena of cryptoassets and blockchain is to say that they have raised great expectations among technologists and financial professionals. This salience is highlighted by the sizable market cap of Bitcoin, a digital token that is the leading medium of exchange for a plethora of imitators and extensions. Given the prices of two major cryptocurrencies and a set of dummies related to token function, token features and token distributions, we tested four hypotheses in order to explore the broad topic of token value and price. We show that the designed functional connection can be effective, thus linking a project that has a value, with a blockchain token that has a price. This is in the absence of a legal connection or claim.

This paper is a step towards illuminating the question "What can a blockchain token embody and connect?" The public blockchains on which the sampled tokens operate, are systems where no higher authority is necessary to create trust between distrusting agents. This decentralization equates to no single point of control, and a reduction in establishment costs. Without system critical gatekeepers, such as governments or banks, blockchain is dramatically reducing the barriers to create provably scarce tradable tokens. These tokens are being used to raise crowdfunding and digitize real world assets. From here it is only a short step to trustlessly digitizing rights and responsibilities.

Our results complements regulatory actions such as SEC (2018a), which posits that tokens may be an investment contract in a common venture. It supports both FINMA (2018) and FCA (2019) in distinguishing tokens by function. Additionally these findings respond to the prima facie argument that blockchain is not significant. To date, cryptoassets are "a minority sport with few users", while blockchain has seen limited wider application and adoption (Roubini, 2018). However, the logic of slow adoption becomes clear once we accept that blockchain is not a revolution in higher performance services (Croman et al., 2016). Capacity constraints is a feature of blockchain's decentralization functionality (Lo and Medda, 2018). This lower relative capacity handicaps blockchain's ability to displace centralized financial systems, at the same time as its decentralization feature enables new types of competitors, new economic structures, and new methods of value discovery.

We argue going forward that the opportunity in blockchain may be in creating novel digital tokens for abstract assets and liabilities that have never traded before, rather than tokenizing existing assets such as equity shares. Future research directions may include how tokens could be used to delineate responsibilities digitally, or solve problems of externalities by expressing currently unobserved social costs as digital blockchain tokens. Such research would provide evidence that blockchain can change the economic behavior of agents, as opposed to changing the distribution of economics and control.

	(1)					
	TOKENUSD	BTCUSD	ETHUSD	DLPX	DLBTC	DLETH
TOKENUSD	1					
BTCUSD	0.105^{**}	1				
ETHUSD	0.116^{***}	0.839^{***}	1			
DLPX				1		
DLBTC				0.347^{***}	1	
DLETH				0.474^{***}	0.621^{***}	1

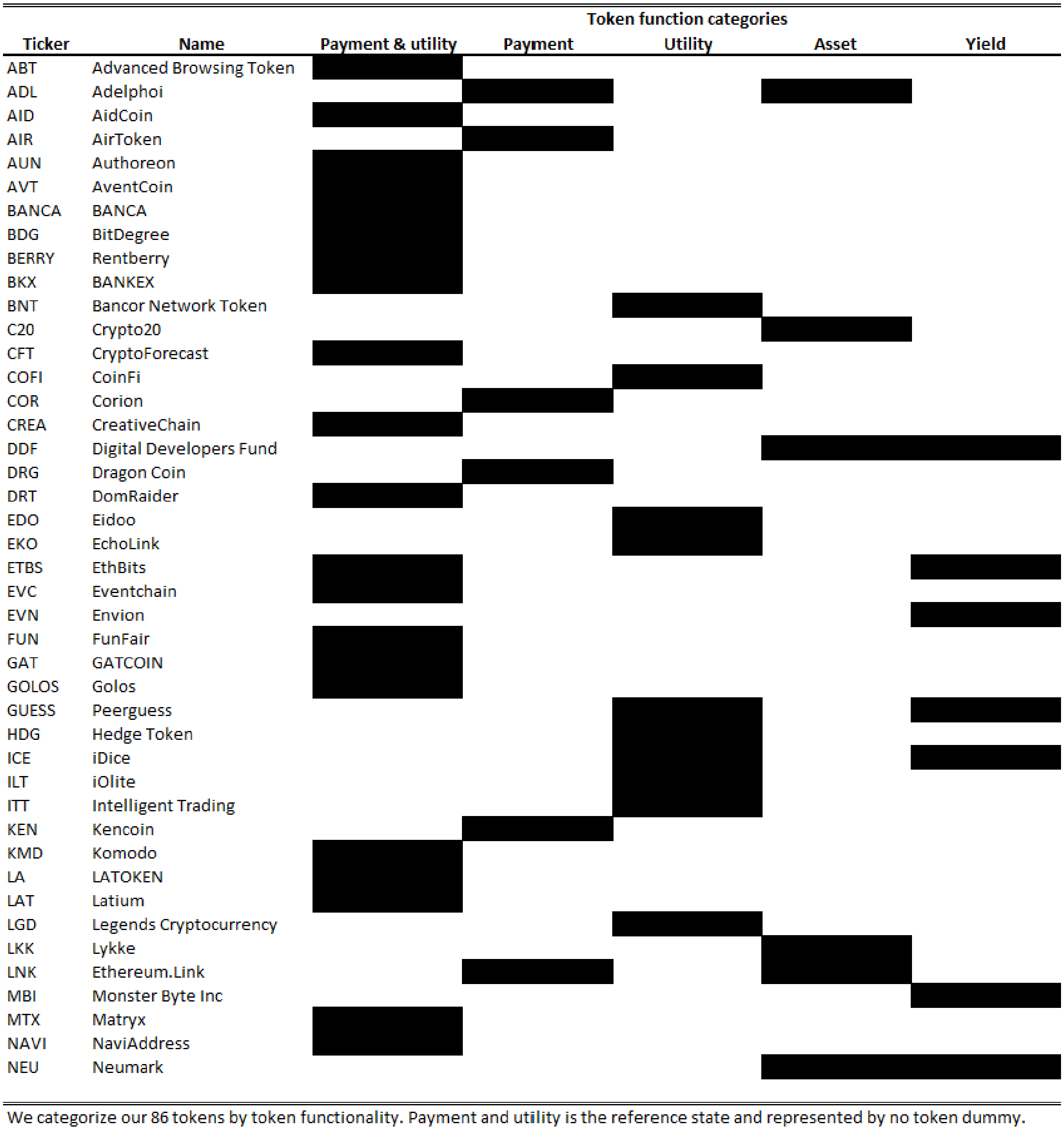
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 5.7: Correlation coefficient matrix - primary model

	(1)					
	MKTCAP	BMTH	EMTH	DLMMC	DLMBTC	DLMETH
MKTCAP	1					
BMTH	0.0595	1				
EMTH	0.0804^{*}	0.862^{***}	1			
DLMMC				1		
DLMBTC				0.232^{***}	1	
DLMETH				0.372^{***}	0.563^{***}	1

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 5.8: Correlation coefficient matrix - secondary model



		Token function categories				
Ticker	Name	Payment & utility	Payment	Utility	Asset	Yield
ABT	Advanced Browsing Token	■				
ADL	Adelphoi		■		■	
AID	AidCoin	■				
AIR	AirToken		■			
AUN	Authoreon	■				
AVT	AventCoin	■				
BANCA	BANCA	■				
BDG	BitDegree	■				
BERRY	Rentberry	■				
BKX	BANKEX	■				
BNT	Bancor Network Token			■		
C20	Crypto20				■	
CFT	CryptoForecast	■				
COFI	CoinFi			■		
COR	Corion		■			
CREA	CreativeChain	■				
DDF	Digital Developers Fund				■	■
DRG	Dragon Coin		■			
DRT	DomRaider	■				
EDO	Eidoo			■		
EKO	EchoLink			■		
ETBS	EthBits	■				■
EVC	Eventchain	■				
EVN	Envion					■
FUN	FunFair	■				
GAT	GATCOIN	■				
GOLOS	Golos	■				
GUESS	Peerguess			■		■
HDG	Hedge Token			■		
ICE	iDice			■		■
ILT	iOlite			■		
ITT	Intelligent Trading			■		
KEN	Kencoin		■			
KMD	Komodo	■				
LA	LATOKEN	■				
LAT	Latium	■				
LGD	Legends Cryptocurrency			■		
LKK	Lykke				■	
LNK	Ethereum.Link		■		■	
MBI	Monster Byte Inc					■
MTX	Matryx	■				
NAVI	NaviAddress	■				
NEU	Neumark				■	■

We categorize our 86 tokens by token functionality. Payment and utility is the reference state and represented by no token dummy.

Figure 5.5: List of sampled ICO tokens - part 1

		Token function categories				
Ticker	Name	Payment & utility	Payment	Utility	Asset	Yield
NGC	NagaCoin	■				
ORI	Origami	■				
OTX	Octanox	■				
PART	Particl	■				
PGL	Prospectors			■		
PIX	Lampix			■		
PLR	Pillar			■		
POWR	Power Ledger			■		■
PRIX	Privatix	■				
RCC	Reality Clash			■		
REN	Republic Token			■		
RIYA	Etheriya	■				
RKC	Royal Kingdom Coin		■		■	■
SETH	Sether			■		
SJCX	StorjCoin	■				
SNC	SunContract	■				
SND	Sandcoin			■	■	
SNM	SONM	■				
SNOV	Snovio	■				
STORJ	Storj	■				
STRAT	Stratis			■		
STU	BitJob	■				
SWARM	SwarmCoin				■	■
TFD	TE-FOOD			■		
TIO	Trade.io			■		
UMC	Umbrella Coin	■				
UNITY	SuperNET				■	■
VEE	BLOCKv			■		
VIA	ViaCoin	■				
VOISE	Voise	■				
VSL	vSlice					■
WINGS	Wings DAO			■		
WPR	WePower			■		■
WRC	Worldcore	■				■
XTZ	Tezos	■				
ZRC	ZiftrCoin		■			
FIL	FileCoin	■				
SRN	Sirin Labs			■		
SNT	Status Network Token			■		
WAX	Worldwide Asset eXchange	■				
NTK	Neurotoken	■				
WAN	Wanchain	■				

We categorize our 86 tokens by token functionality. Payment and utility is the reference state and represented by no token dummy.

Figure 5.6: List of sampled ICO tokens - part 2

Chapter 6

Uniswap and the rise of the decentralized exchange

6.1 Introduction

This paper is focused on a growing application of blockchain - the decentralized exchange (DEX). On 17 May 2021, USD 1.7 billion worth of digital tokens traded on the Uniswap V2 DEX in a single day. These trades utilized almost USD 9 billion of committed liquidity.[1] In the prior year the platform's volumes have at times exceeded that of the largest centralized cryptoasset exchange Coinbase.[2]

Despite this progress, the majority of cryptoasset trading takes place on centralized exchanges owned by a firm. This is ironic as the record keeping functionality of blockchain makes them natural payment and token transfer mechanisms. Blockchains such as Bitcoin are payment systems (Huberman, Leshno, and Moallemi, 2019). In comparison, centralized exchanges offer consistent transaction costs, fast settlement and optimized user interfaces. The negative of such venues are the regular hacks, and collapses, that jeopardize the assets they custody. Gandal et al. (2018) examines the fall of the Mt Gox exchange as well as the increasing price manipulation leading up to the actual event. Only recently have DEXs gained significant share of cryptoasset volumes relative to centralized exchanges.

[1] v2.info.uniswap.org/home

[2] cryptobriefing.com/uniswaps-daily-volume-overtook-coinbase-more-80-million/

Lin (2019) identifies four dimensions across which exchanges can be decentralized, including (1) the blockchain platform, (2) the mechanism for discovering a counterparty, (3) the order matching algorithm and (4) transaction settlement. Choices regarding these functions impact an exchange's trade off between performance, privacy and capital intensity. Uniswap V2 is decentralized across all four dimensions. Lin (2019) enumerates the benefits of DEXs as lower counterparty risk, potentially lower fees, and more trading pairs. Trends favoring a switch towards DEXs include (1) increasing quantity of distinct cryptoassets, (2) the regulatory risk of listing a cryptoasset on a centralized exchange, and (3) user preferences to avoid Know Your Customer and Anti Money Laundering (KYC/AML) regulations required by a centralized exchange.

Connecting to the last point, centralized exchanges are a focus of regulatory actions, with the CFTC and SEC charging the derivatives platform Bitmex with providing US based customers access to unregulated financial derivatives, and not following AML requirements CFTC (2020). In the UK, FCA (2020b) banned the sale of derivatives that reference cryptoassets to retail investors. Importantly, the FCA has not banned the trading of cryptoassets. Uniswap and other DEXs are not yet offering derivatives, but it is clear that both regulation and cryptoasset infrastructure continue to evolve at speed. Alexander and Heck (2020) details the problems arising from inconsistent regulation of cryptoasset markets. The increasing significance of DEXs will make financial regulation more difficult.

Research into DEXs connects to the literature on financial market infrastructure and microstructure. Lees (2012) provides an overview of conventional capital markets. All financial markets seek to optimize price or transactions by bringing multiple parties to a single exchange. That electronic exchanges can be distributed geographically is not new. Biais, Glosten, and Spatt (2005) reviews the microstructure literature including transaction costs and bid ask spreads. Both centralized exchanges and early DEXs utilize order books of bids and asks. The bid consists of prices and volumes participants are openly willing to buy at. The ask consists of prices participants are willing to sell at. If the same party engages on the bid and the ask at the same time, they are a specialist or market maker, looking to profit on the spread. Comerton-Forde et al. (2010) find that market maker balance sheet and income statement variables impact time variation in liquidity - in other words spreads widen when specialist participants have large positions or lose money - and the benefits of market makers become negatives during times of stress. However an alternative to a bid-ask based financial market is a disintermediated reserve based model that holds pools of assets that traders can access. Uniswap V2 is such a model.

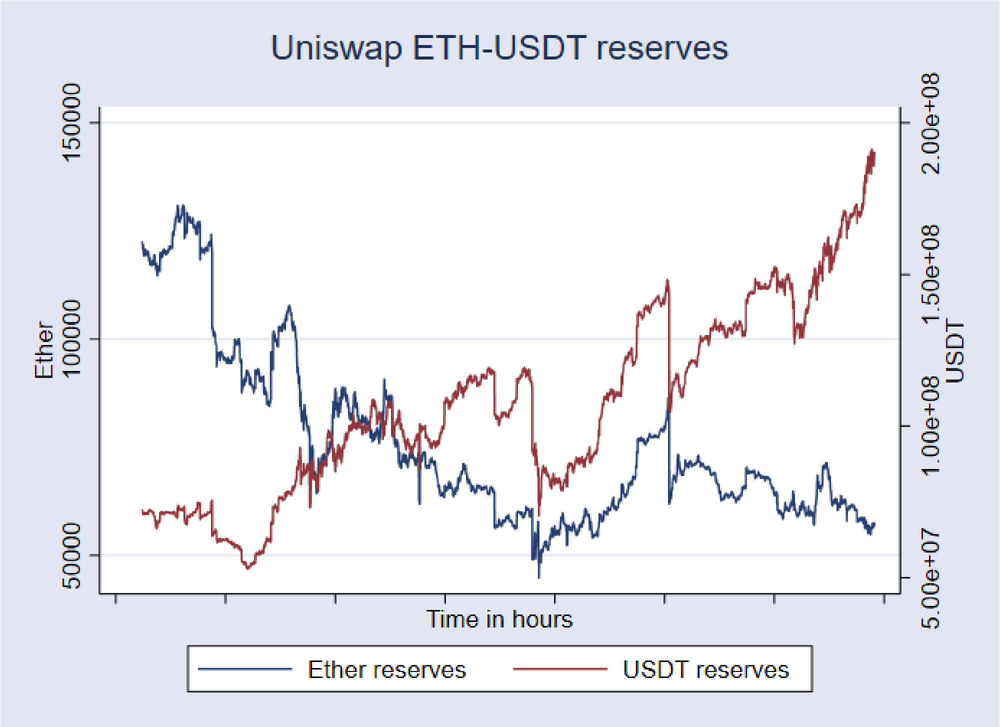


Figure 6.1: Ether and Tether reserves for the ETHUSDT pair on Uniswap

Liquidity providers (LPs) commit proportionate quantities of two cryptoassets to form the basis of a trading pair (Figure 6.1 shows the Ether and Tether reserves for the ETHUSDT pair). In return LPs receive 0.3% of the value of trades. Angeris and Chitra (2020) notes how Uniswap applies a constant product rule to these reserves to map them to a marginal price. Further detail on these mechanics are provided in subsection 6.2.2. We utilize an hourly dataset of 154 days of cryptoasset reserves for the ETHUSDT pair from Uniswap, and explore the research question: are DEXs, in particular Uniswap, an effective cryptoasset exchange? If that is the case, then they improve market completeness in two ways. As DEXs replace non-linear-liquidity providing agents with continuous pricing curves (1) prices are available at any volume, and (2) are less influenced by agent profit and loss. We examine this question with three testable hypotheses.

- H1: The price of the ETHUSDT Uniswap pair is cointegrated with its exchange rate off Uniswap.

In a centralized exchange, market makers and participants ensure varying degrees of the Efficient

Market Hypothesis (Fama, 1970). Uniswap uses passive liquidity pools instead of active market makers, and therefore it is logical to test the connection between prices on and off Uniswap. Cointegration of the ratio of reserves and non-Uniswap pricing is a necessary, though not sufficient, condition of the effectiveness of Uniswap. It is where the pricing curve of Uniswap's constant product market maker equates to the price off platform. A series of equilibrium correction Auto Regressive Distributed Lag (ARDL) models are formulated to test this hypothesis. We use a Vector Error Correction Model (VECM) as a robustness test. We note that the selection of this pair is based on its sizable liquidity. Griffin and Shams (2020) highlights some of the suspicious activity associated with the minting of Tether.

- H2: The price of Ether, Bitcoin and the volume of transactions are statistically significant predictors of changes in Uniswap reserves.

Here we examine which independent variables assist in predicting changes in reserve balances. Additionally, ARDL requires that there is at most one cointegrating relationship with the dependent variable, which testing this hypothesis can also check for.

- H3: Changes in one reserve balance, of a pair, Granger causes changes in the other reserve balance in the opposite direction.

ARDL does not prove causality. Therefore we apply a VAR model, and its test of Granger causality, to see if changes in one reserve balance, of a pair, influences the other reserve balance. We expect a move in the opposite direction as we expect the arbitrage to parity to be the follow on trade i.e., a reversal.

Our results contribute empirical evidence that liquidity pools on Uniswap V2 can be an effective cryptoasset exchange. It complements Angeris, Evans, and Chitra (2020) that analyses the mathematical implications of different constant function market maker curves. Both our ARDL and VECM methodologies find in favor of the existence of a cointegrating vector between the derived ETHUSDT price on Uniswap and its price elsewhere. This cointegration is a necessary but not sufficient condition of effectiveness. We find a statistically significant relationship between the Ether and Tether reserves of the pool and the price of Bitcoin. This may indicate a connection between the liquidity pool and the wider cryptoasset space. Our VAR analysis suggests that over the study period, changes in Tether reserves Granger causes changes in Ether reserves. This would be consistent with a specific type of arbitrage behavior that supports price cointegration.

The effectiveness of DEXs impacts both market completeness and cryptoasset regulation. Although blockchain promised the ability to digitally trade anything, in practice the liquidity may not have existed. Reserve based markets imply that trades can now be carried out at any volume, enhancing the completeness of financial markets. Furthermore, decentralized marketplaces will challenge the objectives and enforcement capabilities of regulators. In particular, as highlighted by Zetzsche, Arner, and Buckley (2020), decentralizing the institution eliminates the venture's need for a registered address and permanently located infrastructure, and therefore reduces the surface it exposes to the authorities. The next section provides background to decentralized finance and Uniswap's pricing mechanism. Following that are sections on Data, Methodology, Results and Discussion. The research closes with a short Conclusion.

6.2 Background

6.2.1 Blockchain, speculation and decentralized finance

Blockchain has become synonymous with digital tokens like those traded on Uniswap. However there is more to the technology than this. We highlight five threads. The first is as a mechanism to enable decentralized record keeping - and exemplified by Maersk and IBM's TradeLens project that records the movement of 60% of the world's shipping containers (Jensen, Hedman, and Henningsson, 2019). A record agreed by all is by definition accepted as "true". This reduces the need for trust, and at a minimum accelerates dispute resolution. In the future this may enable decentralized decision making. Secondly are the smart contracts coded on the blockchain, that are commonly used to issue and manipulate third party tokens. Shared code, that all agree to be "true", can be thought of as shared rules. This may later open up new types of automation and agent relationships. Cong and He (2019) provides a formal proof of how a blockchain based consensus, using smart contract based prices contingent on delivery, can support new entrants. In their paper, new entrants signal quality by trustlessly guaranteeing buyers compensation if the product fails, explicitly increasing the completeness of the contract space. The shared computer code referred to as smart contracts do not come with guarantees. Rather any consequences are public prior to interaction. The third thread are digital tokens. It is noted that both record keeping and tokens can be separately used to enable payments and the transfer of value. However it is with tokens that we enter the field of tokenomics, and their ability to reduce project networking costs. Catalini and Gans (2016) implicitly divide these cost reductions into venture bootstrapping, where tokens are sold to investors or incentivize employees; and platform scaling where tokens are offered to miners to process transactions, or to evangelize users.

The fourth thread is distributed ledger as a payment infrastructure. There is limited need for a new electronic currency to substitute for bank deposits. However there is demand for a novel payments infrastructure. Internationally, the USA are a pivotal part of the SWIFT payments system used to cut off Iran and sanction multinational companies (Majd, 2018). Critically, a blockchain based Chinese Central Bank Digital Currency (CBDC) would bootstrap a new payments system that can operate separately from existing infrastructures. Furthermore, BOE (2020) discusses the domestic resiliency benefit of a core payment network that sits outside the commercial banking system. But it only touches on why this facilitates features such as negative interest rates: a blockchain based CBDC hands the payment system, user balances and its data to a single system owner. Kahn, Rivadeneyra, and Wong (2020) argues that distributed ledgers do not change the trade-offs of retail central bank accounts, but they do change the trade-offs of offering a token based system.

The fifth thread is conversely the ability to use decentralization to break rules and disrupt existing systems. The rise of blockchain tokens have facilitated online crime and money laundering. Foley, Karlsen, and Putnins (2019) use a variety of network analyses, such as transactions with known dark web wallets, to estimate that one quarter of Bitcoin users were involved with illegal activities, equating to USD 76 billion in transactions. "Cryptocurrencies are transforming...black markets by enabling black e-commerce", Foley, Karlsen, and Putnins (2019, Page 1798). Nevertheless, the evolution and use of digital tokens suggest that illicit activities are not the primary use case of digital tokens. Firstly, Brainard (2020) observes that the money-like use cases of (1) means of exchange, (2) store of value and (3) unit of account, have increasingly been taken over by stablecoins. Dwyer (2015) argues these were never well addressed by Bitcoin. BOE (2020) defines cryptoassets as "a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of their perceived or inherent value", and stablecoins as a type of cryptoasset “whose value is linked to another asset”, i.e. the US dollar. The most popular stablecoin is the Tether digital token (USDT). It is 5% of the value of all cryptoassets, compared to 60% for Bitcoin, but manages double the daily transaction value.[3] Such stablecoins are unsuited to illicit activities as they are typically centralized and easily frozen by their issuers.[4]

Despite stablecoins and cryptoassets evolving what is possible with payments, plausibly the leading use case for digital tokens is speculation. This is difficult to address empirically. Lo (2017) provides evidence that the price action of Bitcoin is consistent with it being traded as a proxy for the prototyping phase of a new technology. Ciaian, Rajcaniova, and Kancs (2017) use an ARDL methodology to find a variety of relationships between Bitcoin, altcoins and a set of macroeconomic variables. These intriguing papers reveal relatively little consistency or connection between any of these digital assets. Other than Bitcoin, Ether and stablecoins, few cryptoassets have retained share of value of the space. Cumulatively, all this speaks to the speculative context of trading such vehicles. Arthur, Williams, and Delfabbro (2016) review the differences between gambling, speculation and investing. The key distinctions are expected value (EV) and variability of returns. Speculation involves a higher EV than gambling (where negative EV is the norm), and higher variability than investing. This is not to deride the importance of speculation. Both venture capital and oil drilling (especially prior to seismic surveys and shale drilling) observe a high number of project failures. In particular in the crypto space, these flows of funds have been critical to the creation of decentralized building blocks, known as primitives.

Uniswap is one of the primitives of the wider space known as Decentralized Finance (DeFi). The fund manager Kyle Samani defines DeFi as “Enforcing financial contracts through code running on censorship resistant and permissionless public blockchain”.[5] Other large players in DeFi include Compound in the lending and borrowing of cryptoassets, and Synthetix in cryptoasset derivatives.[6] The DeFi space has become popular for liquidity mining or yield farming, where ether, stablecoins and other assets are committed and rewarded. Part of these rewards are payments such as Uniswap’s 0.3% fee for liquidity providers, but the majority are tokens handed out by the venture for platform scaling. Yearn.finance[7] is an example of how primitives are building blocks. Smart contracts manage

[3] en.ethereumworldnews.com/tethers-usdt-daily-trade-vol-eclipses-btcs-marketcap-hits-13b/

[4] trustnodes.com/2020/09/26/tether-freezes-30-million-usdt-after-kucoin-hack

[5] twitter.com/KyleSamani/status/1308280047984242688

[6] compound.finance and synthetix.io

[7] yearn.finance/dashboard

deposits on its platform, minting assets on Synthetix and trading on DEXs as required, to maximize potential rewards.

6.2.2 Uniswap's constant product automated market maker

By construction, a constant product automated market maker (AMM) ensures that the reserves before and after the trade (assuming no fees) adhere to the function:

$$R_\alpha R_\beta = k \tag{6.1}$$

k is a constant, R_α is the quantity of reserves of asset α, and R_β is the quantity of reserves of asset β. Equation 6.1 is plotted in Figure 6.2. If we differentiate both sides of $k = R_\alpha R_\beta = F(R_\alpha, R_\beta)$ to $0 = F_{R\alpha} dR_\alpha + F_{R\beta} dR_\beta$, we can rearrange to show the price for any given ratio of reserves (Equation 6.2). $F_{R\alpha}$ is the partial derivative of the function F in terms of $R\alpha$.

$$p_{\alpha\beta} = \frac{F_{R\alpha}}{F_{R\beta}} = -\frac{dR_\beta}{dR_\alpha} \tag{6.2}$$

This price is only available where trades do not change the ratio of reserves (i.e., small). Otherwise the marginal price of a transaction is the relative change in quantity of the two reserves $p'_{\alpha\beta} = -\Delta R_\beta / \Delta R_\alpha$. This is the slope of the line joining the before and after points on the curve. The slippage (difference between the realized price $-\Delta R_\beta / \Delta R_\alpha$ and the original price $-dR_\beta / dR_\alpha$) of a trade is positively correlated with trade size and inversely correlated to the size of reserves.

Angeris and Chitra (2020) generalizes the mathematics of constant product market makers, and argues that they provide a tractable optimization problem for arbitrageurs to synchronize on and off chain prices. On a traditional exchange, the price of an asset lies between the bid and the ask, but this does not apply on DEXs. Market makers contribute to price discovery, but liquidity providers are price takers. LPs have no price protection other than the constant product function, which treats price as an output. Because arbitragers capture some of the value of price changes, the assets of an LP excluding fees will underperform a fixed portfolio of the original assets, unless price reverts. This is deceptively referred to as impermanent loss - yet even if price reverts, LPs underperform a portfolio that actively rebalances.[8] The CEO of Uniswap Hayden Adams has

[8] medium.com/coinmonks/uniswap-a-graphical-exposition-part-ii-ba440b3fc522

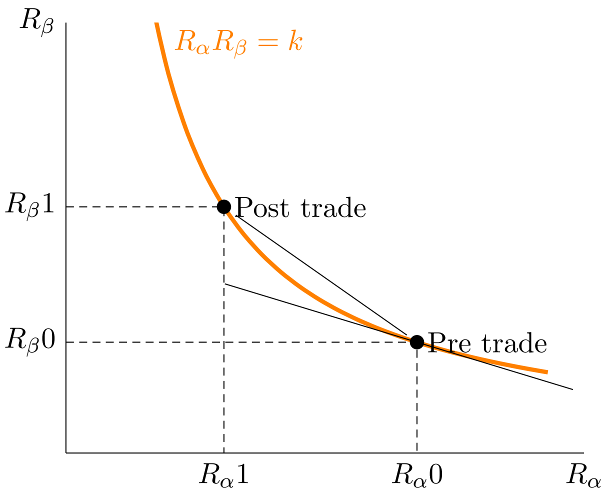


Figure 6.2: Uniswap constant product automated market maker

referred to LPs as "Long fees/volatility and short volatility/fees"[9] In other words LPs benefit from fees which are a function of volatility, but suffer from price change volatility. Separately, traders can specify a maximum deviation relative to an external price oracle, to protect themselves from short term reserve fluctuations. Notably, large trades on Uniswap are vulnerable to front running, where bots watch Ethereum's mempool of unprocessed trades, and buy and sell around market moving transactions.[10]

6.3 Data

This study is based on closing hourly Uniswap data for the period 2 December 2020 to 5 May 2021, via multiple queries of the Uniswap V2 subgraph.[11] Subgraphs are a way of storing public data, and accessible via Graph Query Language (GQL). The 3,705 hours captured equates to 154 days. We note that on 5 May Uniswap V3 launched with its concentrated liquidity product, so later data is not comparable. We acquire via API the closing ETHUSDT and BTCUSDT price from the Cryptocompare.com data aggregator, used by firms including Refinitiv and Quandl. The integration of the two datasets is based on the hourly unix timestamps native to both. We do not know the exchange weights or methodology used by Cryptocompare's benchmark exchange

[9] twitter.com/haydenzadams/status/1309176877869826048?s=20

[10] medium.com/token-flow-insights/how-to-munch-on-pickles-from-a-whale-dinner-edb5628cc769

[11] thegraph.com/explorer/subgraph/uniswap/uniswap-v2

ETHUSDT rate. Descriptive statistics for a selection of dataset variables are shown in Table 6.1. Total reserves for the pair in USD are charted against trading volumes in Figure 6.3.

	N	Mean	St dev	Min	p50	Max
Ether reserves, tokens	3,705	75,754	19,562	44,800	69,271	130,929
USDT reserves, tokens	3,705	107,042,548	30,741,537	52,994,920	103,405,152	191,274,496
Total reserves, USD mil	3,705	214	61.5	106	207	383
Ether tx volume, ETH/hr	3,705	2,630	3,824	573	2,010	194,929
USDT tx volume, USDT/hr	3,705	3,840,317	3,285,136	405,076	3,116,107	50,567,096
ETH reserves * USDT reserves	3,705	7.76e+12	1.74e+12	3.16e+12	7.89e+12	1.26e+13
Ratio of reserves USDT/ETH	3,705	1,542	631	538	1,629	3,473
ETHUSDT close price, USD	3,705	1,542	632	539	1,627	3,484
BTCUSDT close price, USD	3,705	43,210	13,800	17,649	47,455	64,568
Diff in log Ether reserves	3,704	-.000207	.0131	-.319	-.000137	.14
Diff in log USDT reserves	3,704	.00026	.0127	-.311	.000495	.142

Table 6.1: Descriptive statistics - 154 day snapshot of Uniswap ETH-USDT pair

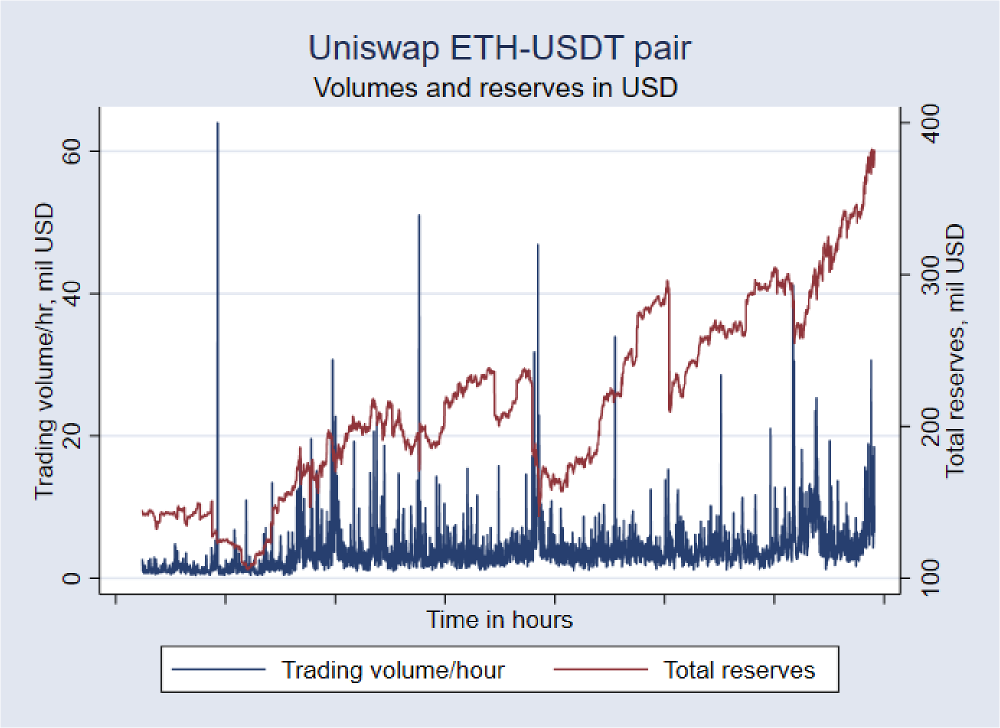


Figure 6.3: Total reserves and trading volumes for the ETHUSDT pair on Uniswap

6.4 Methodology

Hypothesis H1 requires us to test for cointegration between price and the ratio of reserves. This cointegration is central to the effective trading of cryptoassets on Uniswap, and can be thought of as a common stochastic trend. Within equilibrium correction ARDL, the test of cointegration is referred to as the Bounds test. We proceed there via (1) categorizing the variables by their order of integration; (2) discussing the framework of the ARDL model; and (3) laying out the equilibrium correction ARDL to which the Bounds test is applied. Although Pesaran, Shin, and Smith (2001) commented that ascertaining the order of integration was unnecessary prior to testing for cointegration under ARDL, this was asserted in a bounded fashion: the framework does not extend directly to variables that are integrated of order two I(2). Therefore we test for unit roots using Augmented Dickey-Fuller (ADF), Phillips-Perron (PP) and Dickey-Fuller GLS (DFGLS) tests. We use the Akaike Information Criteria (AIC) to determine the appropriate number of lags.

	ADF		PP		DF-GLS	
	level	1st diff.	level	1st diff.	level	1st diff.
Ether reserves	NS	S	NS	S	NS	S
USDT reserves	NS	S	NS	S	NS	S
Ether volumes	S	S	S	S	S	S @ <18 lags
USDT volumes	S	S	S	S	S	S @ <21 lags
ETHUSDT price	NS	S	NS	S	NS	S
BTCUSDT price	NS	S	NS	S	NS	S
Ratio of reserves	NS	S	NS	S	NS	S

3 tests of stationarity applied to 7 time series, on levels and first differences.
NS = non-stationary, S = stationary, at the 5% statistical significance level.

Table 6.2: Stationarity test results

The results shown in Table 6.2 indicate that our sample contains a mix of integration orders. Reserves, ratio of reserves and prices are stationary in the first differences I(1), while volumes are likely to be stationary in levels I(0). The DF-GLS test applies a generalized least squares (GLS) detrending on the series prior to running an ADF test, which can improve the power of the test (Elliott, Stock, and Rothenberg, 1996). Although both OLS and GLS based tests see declining power in the presence of level or trend breaks, the risk is in misidentifying a stationary time series with a structural break as non-stationary i.e. that the order of integration is over estimated (Cook and Manning, 2004). Therefore ARDL is appropriate and can be represented thus:

$$y_t = c_0 + c_1 t + \sum_{i=1}^{p} \phi_i y_{t-i} + \sum_{j=0}^{q} \beta_j x_{t-j} + u_t \tag{6.3}$$

y_t is the dependent variable at time t, with up to p lags included in the model.

x_t is the k x 1 vector of independent variables. For simplicity we display here lag order q as the same for all the independent variables - this does not have to be the case.

u_t is a random error term.

c_0 and c_1 are deterministic intercept and time trend coefficients.

An extension of the model in Equation 5.1 estimates the long run relationships as an equilibrium correction process (Pesaran, Shin, and Smith, 2001). It frames the independent variables as long run forcing of the dependent variable (Kripfganz and Schneider, 2020). This assumes the independent variables are weakly exogenous, and models should consider the directionality of effects during formulation e.g. it may be plausible for transactions to drive changes in reserves, but it is less likely that reserves force transactions. With respect to hypothesis H1, y_t becomes the ratio of reserves R_t; while x_t are the exchange rates of ETH and BTC with Tether. This is shown in Equation 6.4.

$$\begin{aligned}\Delta R_t =& c_0 + c_1 t + \alpha(R_{t-1} - \theta_1 ETHUSDT_{t-1} - \theta_2 BTCUSDT_{t-1}) + \sum_{i=1}^{p-1} \varphi_{Ri} \Delta R_{t-i} + \omega_1 \Delta ETHUSDT_t + \\ & \omega_2 \Delta BTCUSDT_t + \sum_{j=1}^{q-1} \varphi_{ETHj} \Delta ETHUSDT_{t-j} + \sum_{k=1}^{r-1} \varphi_{BTCk} \Delta BTCUSDT_{t-k} + u_t\end{aligned} \tag{6.4}$$

α is the adjustment coefficient.

θ are the long run coefficients on first lags of $ETHUSDT_t$ and $BTCUSDT_t$.

ω are the short run coefficients on the first differences of $ETHUSDT_t$ and $BTCUSDT_t$.

φ are the short run coefficients on the lagged differences of R_t, $ETHUSDT_t$ and $BTCUSDT_t$.

This choice of methodology benefits from its ability to estimate both short run and long run parameters at the same time. Furthermore, Pesaran and Shin (1999) observes that an appropriate estimation of the orders of the extended ARDL(p,m) model is sufficient to both correct for the residual serial correlation, and the problem of endogenous regressors. The ARDL models and coefficients are estimated in Stata utilizing the ARDL package, which is based on Kripfganz and

Schneider (2020). These models are subjected to two parts of the ARDL Bounds test. Note that if there is no cointegration, then the ARDL model in Equation 5.1 is used to estimate relationships between variables and their lags. Hypothesis H1 is investigated via a variety of specifications that look for cointegration between the ratio of Ether and USDT reserves and the exchange rate of ETHUSDT. Hypothesis H2 utilizes the same methodology and searches for the presence of cointegrating and auto regressive relationships between reserves, transactions and price.

Cointegration implies that there are stationary equilibrium relationships between separate non-stationary variables. A corollary of this is that when these variables diverge, at least one of the cointegrated variables converges back to return the system to a long run equilibrium. In Equation 6.4 the rate of this is estimated by the coefficient α. The Bounds test begins with a Wald test (F-statistic) of the joint hypothesis H_0^F that $\alpha = 0$ and $\sum_{i=0}^{q} \varphi_{xi} = 0$, versus the alternative hypothesis H_1^F that $\alpha \neq 0$ and $\sum_{i=0}^{q} \varphi_{xi} \neq 0$. If the null hypothesis is rejected, then the t-statistic is used to test the second H_0^t of $\alpha = 0$ versus H_1^t of $\alpha \neq 0$. The distributions of these test statistics are nonstandard and depend on the integration order of the independent variables. Kripfganz and Schneider (2020) extend the set of available critical values for the bounds test via estimating response surface models, with each significance level showing four critical values based on I(0) and I(1) for the F-test and t-tests. There can be at most one cointegrating relationship between the independent variables and the dependent variable (although there may be additional cointegrating relationships between the independent variables). The validity of the Bounds test depends on normally distributed error terms that are homoskedastic and serially uncorrelated. For the equilibrium correction ARDL model for the ratio of ETH/USDT reserves to ETHUSDT price, we carry out the Breusch-Godfrey LM test for autocorrelation, and the Breusch-Pagan test for heteroskedasticity. Kripfganz and Schneider (2020) notes that Bounds testing with higher lag order can be useful for addressing remaining serial error correlation, with a more parsimonious model applied after testing for forecasting purposes. Across our analysis AIC, which indicates the optimality of a model, is used to select the set of variables and the number of lags. AIC is less parsimonious than Schwarz's Bayesian Information Criteria (BIC), but in ARDL lowers the risk of serial correlation.

Our study uses a Vector Error Correction Model (VECM) as a robustness check of our hypothesis H1. VECM models are an extension of Vector Auto Regressive (VAR) model we use to test for

Granger causality as part of hypothesis H3. We explain how VAR models address directional changes in cryptoasset reserves before moving on to discussing VECM. VAR modeling specifies as many models as dependent variables (Enders, 1995). We use first difference of logs, to ensure the linearity of changes in the two rapidly increasing reserve balances. In a basic form of two variables with a single lag, VAR modeling would define two equations thus.

$$\Delta(lnETH_t) = \alpha_u + \beta_{u1}\Delta(lnUSDT_{t-1}) + \epsilon_u \tag{6.5}$$

$$\Delta(lnUSDT_t) = \alpha_e + \beta_{e1}\Delta(lnETH_{t-1}) + \epsilon_e \tag{6.6}$$

Variables are considered endogenous. Although it is possible to use lags selectively, typically each model repeats the same lagged explanatory variables symmetrically. The Granger causality tests within the VAR model examine if prior period first difference of log of one cryptoasset reserve provides information about the value of current period first difference of log of the other cryptoasset reserve. Tests of Granger causality exploits the directionality of time to imply the directionality of the relationship. Changes in reserve balances are a corollary of trades on the Uniswap platform, and following such trades, the mechanism by which arbitrageurs cointegrate the reserve ratio and price.

VAR models require stationary time series. Earlier, we used first difference of logs of the original I(1) time series to ensure this. VECM models add back some of the information of the undifferenced time series. First it estimates the long-run equilibrium using ordinary least squares. Note that the VAR model is applied to changes in reserves, but hypothesis H1 and this VECM is on the ratio of reserves and the ETHUSDT price. If they are cointegrated, residuals are stationary and estimators super consistent (Enders, 1995).

$$R_t = \alpha + \beta' ETHUSDT_t + \epsilon \tag{6.7}$$

The differences between actual observations and modeled observations are then included in the VECM. These residuals are the deviation from the long run equilibrium. One form of this is shown below, with one lag and no deterministic trend.

$$\Delta R_t = \alpha + \lambda(R_{t-1} - \beta' ETHUSDT_{t-1}) + \beta_1 \Delta ETHUSDT_{t-1} + \epsilon_1 \qquad (6.8)$$

Note that in multivariate notation typically a cointegration matrix $\prod$ is used to represent the potentially complex nature of the cointegrating relationship, whereas here it is written out explicitly. λ is the error correction term, which estimates how changes in R_t varies when one of the variables deviates from the common stochastic trend. As with VAR modeling, VECM is symmetric and $\Delta ETHUSDT_t$ is also estimated as a function of R_t. In the next section we examine the results.

6.5 Results and discussion

	[A]	[B]
Adjustment factor		
L. (Diff from equilibrium)	-0.900***	-0.904***
Long run effects		
L. (ETHUSDT price)	1.000***	1.000***
L. (BTCUSDT price)		0.000
Short run effects		
LD. (Ratio of reserves)	-0.063***	-0.063***
D. (ETHUSDT price)	0.951***	0.937***
LD. (ETHUSDT price)	0.069***	0.063***
D. (BTCUSDT price)		0.001***
LD. (BTCUSDT price)		0.000
aic	20387.975	20376.652
bic	20425.273	20432.599
N	3701	3701
Bounds test results		
F-statistic	798.271	536.459
t-statistic	-39.956	-40.116
F-test p-value I(1)	0.000	0.000
t-test p-value I(1)	0.000	0.000

Bounds test rejects H0 no level relationship at 5% significance level

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 6.3: ARDL - Ratio of reserves and ETHUSDT price

The results of applying ARDL to our dependent variable, the ratio of Ether to USDT reserves, with the exchange rate of Ether and the exchange rate of Bitcoin (both priced in USDT) are shown in Table 6.3. As all three variables in this model are I(1), the bounds test statistics are compared to the I(1) critical values. The F-statistic and the t-statistic are more extreme than the related critical values (p-value = 0.000), which rejects the null hypothesis of no level relationship. This provides evidence in favor of the first of our testable hypothesis.

- H1: The price of the ETHUSDT Uniswap pair is cointegrated with its exchange rate off Uniswap.

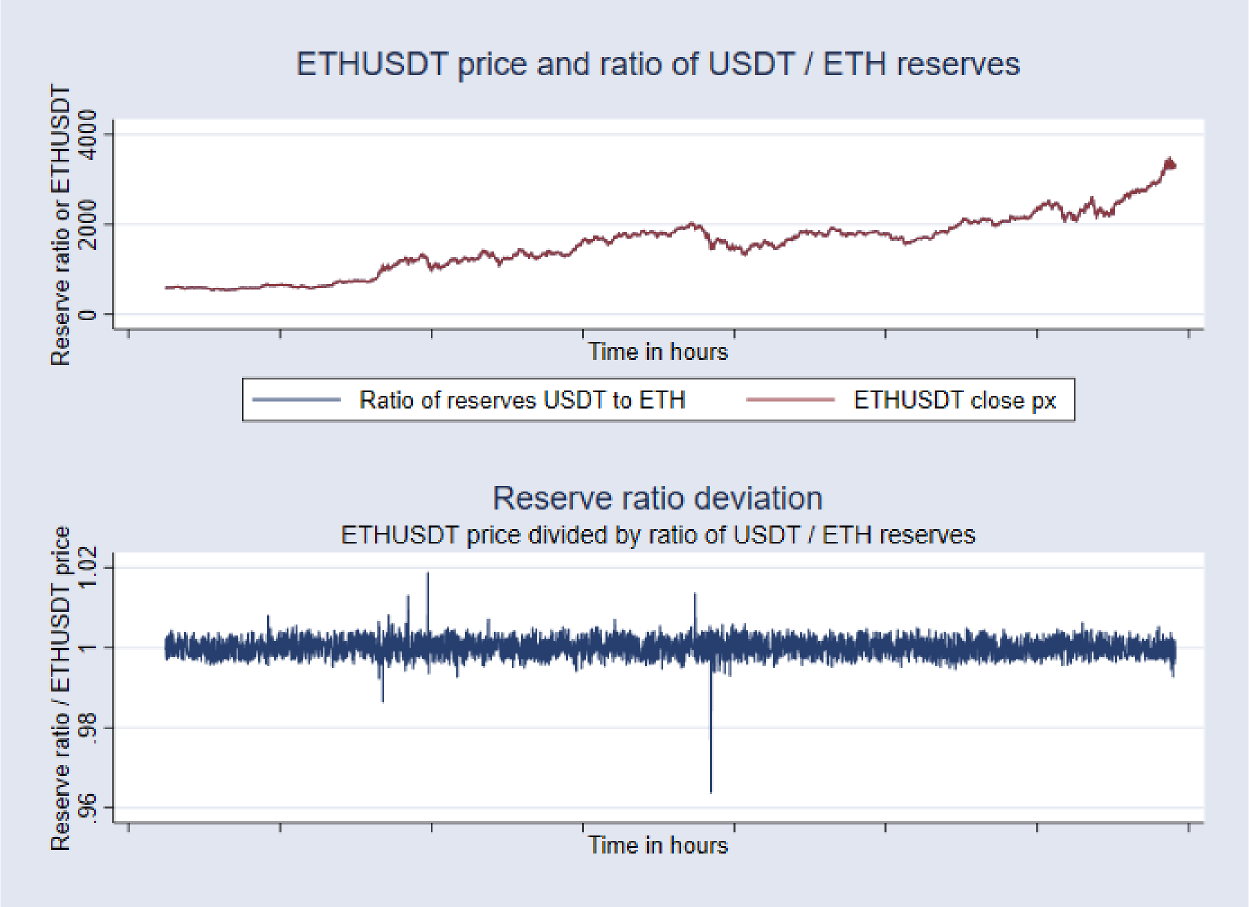


Figure 6.4: The ratio of Ether and Tether reserves (on the ETHUSDT pair on Uniswap) versus the ETHUSDT price

This result confirms empirically the effectiveness of Uniswap's reserve balance based Ether and USDT exchange pair on an hourly time frame. These results are supported graphically in Figure 6.4. The lower part of this figure indicates that some of the arbitrage opportunity is visible in the data, but over the sample period exceeds 1% only 5 times. We note that because of fees, arbitrage is unlikely to take place when the difference between on and off Uniswap prices are less than 0.3%.

Returning to Table 6.3, during the study time period, the adjustment factor α is 0.9. This suggests that 90% of the difference between the ratio of reserves and the ETHUSDT price is adjusted back to long run equilibrium over the course of the subsequent hour. The long run effects are the coefficients θ on the lagged exchange rates of ETHUSDT and BTCUSDT. In both specifications, the coefficient on the lagged ETHUSDT price is 1. Of the long run coefficients, only ETHUSDT is statistically significant. The short run effects are φ and ω from equation 6.4, which are the coefficients on the first and lagged differences of our variables. All of the short run effects are statistically significant except for the lagged difference of BTCUSDT. The lower AIC value and the statistical significance of the first difference of BTCUSDT suggests the Bitcoin price does contain information in predicting changes in the ratio of reserves. This may be because of Bitcoin's importance in the cryptoasset space; its impact on trader wealth; or some residual use as a unit of account. We run a Breusch-Godfrey LM test for autocorrelation, which does not reject the null of no serial correlation for 1 to 10 lags at the 5% significance level. The Breusch-Pagan test for heteroskedasticity has a χ^2 test statistic of 0.24 and a p-value of 0.6269. Therefore we do not reject the null of constant variance at the 5% significance levels.

	[C]	[D]
D. (Ratio of reserves)		
L. (Error correction coefficient)	-0.893***	-0.853***
LD. (Ratio of reserves)		-0.023
LD. (ETHUSDT price)		0.038
D. (ETHUSDT price)		
L. (Error correction coefficient)	0.079	0.049
LD. (Ratio of reserves)		0.043
LD. (ETHUSDT price)		-0.033
aic	52822.888	52798.676
bic	52847.757	52848.411
N	3704	3703

Models ordered by AIC descending

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 6.4: Robustness check - Vector error correction model

As a robustness check, we execute a VECM model to complement our ARDL model. It is an alternative way to examine our two time series, the ratio of reserves between Ether and USDT, and the ETHUSDT price. As required, both are integrated of order 1. The first differences are taken and regressed on zero or one lagged difference, as suggested by selection order information criteria. The error correction coefficient is the critical output - and indicates whether and how the two time series converge. The results in Table 6.4 indicate that the reserve ratio moves towards the model equilibrium, in both specifications, at the 99.9% statistical significance level. We do not find evidence that the ETHUSDT price moves towards the ratio of reserves. This supports the case that the two time series are cointegrated using a second methodology - and offers evidence that Uniswap pricing moves to match the price elsewhere.

We note that a finding of cointegration is a necessary, but not sufficient, condition for the effectiveness of Uniswap and its automated market maker. If they are not cointegrated then one of these prices is wrong for a prolonged period, and an arbitrage opportunity for risk free profits would be sustained. Drilling further into the efficiency of the ETHUSDT pair is a vector for future research as more data becomes available. Additionally, analyzing the effectiveness and efficiency of other markets on Uniswap is a open problem. The issue of the 0.3% trading fee is universal. But the plethora of rarely traded token pairs on Uniswap results in variations in data available. This paper has focused on a token pair where off DEX pricing is liquid and high frequency. Yet for many token pairs this is not the case and we highlight the difficulty in empirical analysis of illiquid markets that may exist solely because of a LP based platform such as Uniswap e.g. where there is no off Uniswap benchmark price. However we observe that this is a opportunity as well as a constraint. Anecdotally, it is now possible to observe changes in liquidity as prices changes, which opens up a largely unexplored space for empirical researchers.

- H2: The price of Ether, Bitcoin and the volume of transactions are statistically significant predictors of changes in Uniswap reserves.

In order to explore our second hypothesis H2, we put the ratio of reserves to one side, and run ARDL models with Ether reserves and USDT reserves as our dependent variables. The Bounds tests on these equilibrium correction models (not shown) do not reject the null hypothesis of no level relationship - we find no evidence of cointegration. Because of this, the equilibrium correction models are not appropriate, and the results of the standard ARDL model are presented in Table 6.5 and 6.6. For both dependent variables, we execute 3 models with different independent variables, from specific to general. The lower the AIC the more appropriately specified the model. For both Ether reserves and USDT reserves the most general models with the most variables appear to be preferred in predicting changes in the dependent variables. That the price of Ether impacts reserves makes sense as reserves are a function of (1) liquidity provision in a ratio set by price and (2) trades

	[E]	[F]	[G]
L. (ETH reserves)	0.903***	0.903***	0.899***
L2. (ETH reserves)	0.095***	0.095***	0.099***
(USDT reserves)	0.001***	0.001***	0.001***
L. (USDT reserves)	-0.001***	-0.001***	-0.001***
L2. (USDT reserves)	-0.000***	-0.000***	-0.000***
L3. (USDT reserves)	0.000*	0.000*	0.000*
(ETH price)	-38.534***	-38.519***	-35.147***
L. (ETH price)	32.288***	32.243***	28.683***
L2. (ETH price)	6.746***	6.663***	6.420***
L3. (ETH price)	-1.266*	-1.208*	
L4. (ETH price)	0.731	0.790	
(ETH volume)		-0.001	-0.000
(USDT volume)		0.000	0.000
L. (USDT volume)		-0.000*	-0.000*
(BTCUSDT price)			-0.203***
L. (BTCUSDT price)			0.201***
aic	56105.509	56106.529	56058.911
bic	56180.105	56199.775	56152.157
N	3701	3701	3701

Models ordered by AIC descending

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 6.5: Short run ARDL model of Ether reserves within ETHUSDT Uniswap pair

	[H]	[I]	[J]
L. (USDT reserves)	0.862***	0.865***	0.862***
L2. (USDT reserves)	0.160***	0.161***	0.163***
L3. (USDT reserves)	-0.025**	-0.029***	-0.029***
(ETH reserves)	1138.738***	1135.284***	1140.416***
L. (ETH reserves)	-983.720***	-982.353***	-984.978***
L2. (ETH reserves)	-153.029***	-150.898***	-152.422***
(ETH price)	52473.761***	52261.263***	48944.982***
L. (ETH price)	-4.27e+04***	-4.26e+04***	-3.91e+04***
L2. (ETH price)	-9620.627***	-9504.396***	-9637.803***
(ETH volume)		0.947	0.899
(USDT volume)		-0.011*	-0.010*
L. (USDT volume)		0.016***	0.016***
L2. (USDT volume)		-0.004	-0.003
L3. (USDT volume)		0.008	0.008
L4. (USDT volume)		-0.009*	-0.009*
(BTCUSDT price)			208.153***
L.(BTCUSDT price)			-206.205***
aic	1.09e+05	1.09e+05	1.09e+05
bic	1.10e+05	1.10e+05	1.10e+05
N	3701	3701	3701

Models ordered by AIC descending

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 6.6: Short run ARDL model of USDT reserves within ETHUSDT Uniswap pair

that exchange one reserve for another at a price dependent on impact. The statistical significance on volumes is somewhat weaker. Notably, the statistical significance of Bitcoin is unexpected. Together these results find in favor of our hypothesis H2. We test the other variables to ensure no additional cointegrating relationships that may impact our earlier analysis. Mostly there is no logic for such directionality, and we do not find such evidence. Over the study time period we also do not find cointegration between the price of Ether and the price of Bitcoin (not shown). The result of this may be different over longer time periods.

Our third hypothesis examines how the Uniswap ETHUSDT reserves returns to equilibrium.

- H3: Changes in one reserve balance, of a pair, Granger causes changes in the other reserve balance in the opposite direction.

We investigate this with a VAR model. We begin by reviewing the order selection statistics for our two variables. The lag order selection information criteria suggest 1 and 4 lags. We run two

	[K]	[L]
First difference of log Ether reserves		
LD. (log ETH reserves)	-0.008	-0.013
L2D. (log ETH reserves)	-0.018	
L3D. (log ETH reserves)	0.033	
L4D. (log ETH reserves)	-0.079***	
LD. (log USDT reserves)	-0.045*	-0.047*
L2D. (log USDT reserves)	0.066**	
L3D. (log USDT reserves)	-0.077***	
L4D. (log USDT reserves)	0.019	
First difference of log USDT reserves		
LD. (log ETH reserves)	-0.026	-0.030
L2D. (log ETH reserves)	-0.004	
L3D. (log ETH reserves)	0.043*	
L4D. (log ETH reserves)	-0.002	
LD. (log USDT reserves)	-0.023	-0.022
L2D. (log USDT reserves)	0.044*	
L3D. (log USDT reserves)	-0.090***	
L4D. (log USDT reserves)	-0.045*	
aic	-4.50e+04	-4.50e+04
bic	-4.49e+04	-4.49e+04
N	3700	3703

Models ordered by AIC descending

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 6.7: VAR model of Ether and USDT reserves

models, one with 1 lag and the second with 4 lags. The results of this are shown in Table 6.7. Tests of model stability suggest that the Eigenvalues are appropriately within the unit circle.

When the dependent variable is the first difference in log of Ether reserves, the lagged first difference in log of USDT reserves are statistically significant under both specifications. Although the 4 lag model identifies a number of other statistically significant autoregressive relationships, the AIC and BIC are very slightly higher, so do not appear to boost predictiveness.

At the 5% statistical significance level, we reject the null that the first differences of the log of USDT reserves does not Granger-cause changes in the first differences in the log of Ether reserves. For 1 lag the χ^2 test statistic is 5.14 with a p-value of 0.023. For 4 lags the χ^2 test statistic is 29.24 with a p-value of 0.00. However we do not reject the null that the first differences of the log of Ether reserves does not Granger-cause changes in the first differences in the log of USDT reserves (p=0.125 and p=0.154 for 1 and 4 lags respectively). Overall we find evidence in favor of H3 that changes in one reserve balance (USDT), of a pair, Granger causes negative changes in the other reserve balance (Ether). It is hard to explain definitively why this would be the case. However, we can make inferences because on Uniswap every trade has a price impact. Ceteris paribus, arbitrage trades following off Uniswap price changes should not have next period impacts. Only arbitrage trades following trading induced reserve changes should link two time periods. Arguably arbitrage should lead to bidirectional Granger causality. As this is not the case, it may simply be that non-arbitrage trades are tending to be purchases of Ether. Because of the nature of the automated market maker, that is when the USDT balance changes by more. In other words, our Granger causality results are consistent with a reserve ratio at equilibrium impacted by a first trade of buying Ether that pushes USDT reserves out of balance. Afterwards, an arbitrage trade sells Ether (buys USDT) to bring the reserve ratio back into equilibrium with benchmark pricing. This sequence sees a change in USDT reserves leading a change in Ether reserves.

Bringing together the various findings, the error correction ARDL and VECM results support the case that ETHUSDT prices on and off Uniswap V2 are cointegrated. The VECM results suggest that the on Uniswap reserve ratio and price move towards the off Uniswap price, hinting that price discovery for ETHUSDT occurs on centralized exchanges. Hasbrouck (1995)'s Information Share would be a suitable method for analyzing this further. The VAR results delve further into the equilibrium process, finding that changes in the USDT reserves Granger causes changes in the Ether reserve balances.

6.6 Summary - the decentralized exchange Uniswap

This research provides empirical evidence regarding the effectiveness of reserve based asset exchanges. We find that for the sample period, the ratio of Ether and USDT reserves on the ETHUSDT pair is cointegrated with a third party ETHUSDT exchange rate benchmark. For a constant product automated market maker, this cointegration is a necessary condition of the exchange rate on platform approximating the exchange rate off platform. The success of Uniswap is a rare example of a financial market operating without the classic features of bids and asks, market makers or auctioneers. It is a clarion call to regulators, governments and financial market participants that the innovation and decentralization promised by blockchain based systems is starting to gain traction. It is easy to discount the long term impact of new highly speculative trading instruments, but less easy to deride new financial infrastructure that improves market completeness. DEX structures may be able to complement traditional bid ask based capital markets. An argument made by this thesis in Chapter 2 and 5 is that blockchain does not build strictly superior systems, but alternative systems that are attractive along uncommon dimensions, e.g. no single point of control (political decentralization) and censorship resistance. Yet improved market completeness would constitute a quantitative benefit of blockchain. Further, DEXs have important implications for regulation, as decentralized exchanges do not require a legal form or fixed geographical infrastructure. This begs the question of how should regulators and governments respond to a marketplace that does not need a registered address and geographically fixed physical infrastructure? To date, rule makers have focused on regulating the institutions of the emerging cryptoasset space (Blandin et al., 2019). This may no longer be possible.

Directions for future research include the potential to add an uncorrelated LP asset to investor portfolios; whether decentralized exchanges are more or less risky than centralized exchanges; and if decentralized exchanges can exist without centralized exchanges providing price discovery.

Chapter 7

Regulatory compliance: a case study in data integrity

7.1 The costs of poor anti-money-laundering process

In 2020, the UK Financial Conduct Authority (FCA) fined Commerzbank £37 million ($47m) for inadequate anti-money laundering (AML) controls and risk management systems (FCA, 2020a). It observed 1,700 corporate clients overdue updated due diligence checks. A few years prior to this, Commerzbank had failed to add 40 high risk countries and 1,110 high risk clients to its transaction monitoring tool. Despite these failures, it got off lightly – earning a 30% discount on its fine for settling early in the investigation.

Although this figure is small relative to the $1.9 billion in forfeitures and fines paid by HSBC when it admitted laundering funds for Mexican drug cartels (DoJ, 2012), the Commerzbank case is noteworthy as it relates to processes to comply, not to actual money laundering. Regulatory compliance capability as opposed to regulatory compliance. Both types of fines highlight how good systems are a risk management tool – versus the risk of regulatory action and the risk of engaging with fraudulent clients. However, these systems and processes have value outside of risk and regulation. As business know your customer (KYB/KYC) checks are required prior to onboarding, they are a core component of time to first revenue. An automated and effective anti-money laundering process accelerates revenue generation, increases the ability to adjust risk appetite, and becomes a competitive advantage versus other firms.

As indicated by the K in KYB, the heart of an AML system is data on all the parties involved. This is not as easy to acquire as it may sound. As part of its response to Covid-19, the UK Government implemented a Bounce Back Loan scheme that extended £47 billion ($62bn) via 1.5m loans to registered and unregistered companies. The UK Department for Business, Energy and Industrial Strategy's central estimate of fraud losses on this portfolio is £4.9 billion, or 11% (BEIS, 2021). Although this is related to the aggressive launch of the program, it also highlights how difficult it is to be fully cognizant of a set of companies that are organized and pay taxes in a single jurisdiction. Financial services customer onboarding must extend this data problem to hundreds of jurisdictions, their board members and who can sign or represent these firms. In addition to this, there is the issue of ultimate beneficial owner. Nitsche (2021) notes how 150,000 UK companies are owned by overseas companies, so checks on one company becomes a check on a chain of them across multiple borders. This data requirement is not static, which was one of the problems Commerzbank struggled to address. Each time a board member, key executive or primary shareholder changes, a company's KYB check does so too and must be updated.

To address these linked conundrums, in house compliance teams and third parties such as Kompany[1], which is part of the credit ratings agency Moody's, aggregate the data required for comprehensive KYB checks. Kompany's platform connects to systems in two hundred jurisdictions, half in real time, to bring together data on 110 million companies. Kompany argues that using its platform can reduce the cost of KYB checks for a small or medium sized enterprise from Euro 800 to Euro 50, and the time to process checks from 6 weeks to same day.[2] Schneider et al. (2016) at Goldman Sachs estimates industry wide AML compliance costs at $10 billion a year. This figure rises to $18 billion in 2014 when including regulatory fines.

Where might blockchain engage with the AML problem and existing KYB solutions on the market? The first point is that data quality is often poor. Data can be defined straightforwardly as information used to help decision making.[3] Using standardized data assessments sampled across 75 primarily technology, healthcare and financial firms, Nagle, Redman, and Sammon (2020) found

[1] kompany.co.uk

[2] paymentandbanking.com/en/kompany-the-principle-of-the-data-platform-for-kyc-kyb-data

[3] dictionary.cambridge.org/dictionary/english/data

that a median of 44% of data rows checked contained errors. Although many might expect customer data to be incomplete, the sample included staff, sales and operational records – some of which would end up in national databases. This research noted the potential to use data improvement policies to boost operational standards, for example where unsatisfactory hospital records reflect a prioritization of patient flow over quality of care. Their conclusion highlights the second point: the importance of process.

Therefore blockchain can enhance KYB as a data and process improvement technique. Leading edge KYB data platforms improve the probability that the input data is up to date, but blockchain may be able to timestamp the date and time of each stage of the KYB process. In the next section we provide a case study on Kompany's Business Know Your Customer tool, KYC onchain. Kompany argue that notarizing this process on a public blockchain, with its tamper resistance and rapid audit capability, is superior to existing processes. Arguably it is equivalent to best-in-class existing systems – with the benefit for the client revolving around the reduction in cost due to automation and accelerated auditing. Furthermore, the guarantees of tamper resistance cross the boundaries between Kompany and their clients. In Section 7.3 we add color to the complexity of adopting new technology for regulatory purposes (RegTech). Importantly for the regulator, it eliminates the need for them to trust that a firm's processes are best-in-class. We observe that it may have been existing regulations that have delayed the adoption of blockchain based RegTech, and that as these barriers are resolved, the time may be ripe for wider adoption.

In Section 7.4 we contextualize the use of blockchain to notarize data and process in the field of data integrity – in particular that the data is certified and processed correctly. In Section 7.5 we explore two adjacent blockchain data integrity use cases in dispute mitigation and occupational fraud. We close with a short conclusion.

7.2 Applying blockchain to business Know Your Customer

Kompany are a leader in KYB. The problem Kompany addresses for its clients is straightforward: monthly database searches and record keeping, using email or internal systems, does not meet the many regulatory requirements a company is subject to when accepting clients. The EU's 6th Anti-Money Laundering Directive (6AMLD), the UK's Proceeds of Crime Act, and the USA's National

Defense Authorization Act all demand rigorous collection of data and customer due diligence. With respect to the EU's AML regulations, this could be punished by 4 years in prison, fines and the cessation of business activities. Kompany's core product helps by providing a dynamic data check, and a third-party record of the check. In July 2021, Kompany began notarizing KYB checks on to a public blockchain. Notarizing here is defined as the immutable time stamping of a hash of useful data – a digital attestation. Kompany partners with nChain, a blockchain innovator, to write data to BitcoinSV, a distinct implementation of the original Bitcoin protocol.

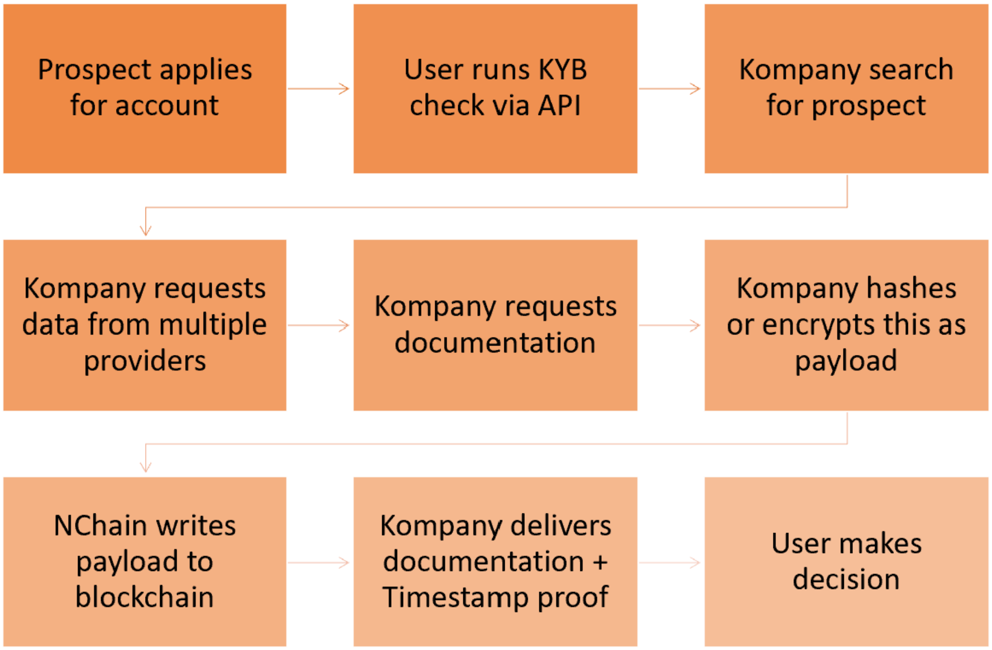

Prospect applies for account
User runs KYB check via API
Kompany search for prospect
Kompany requests data from multiple providers
Kompany requests documentation
Kompany hashes or encrypts this as payload
NChain writes payload to blockchain
Kompany delivers documentation + Timestamp proof
User makes decision

Figure 7.1: Kompany KYC onchain process flow

The CTO and Founder of Kompany Bainbridge-Clayton explains how the three key elements of business verification are (1) Who the check is about, (2) What the check found, and (3) When the check occurred.[4] In the past, this would consist of account history records, gathered into a paper trail that is organized by the dates on a series of PDFs. Kompany's new model is to have requests and responses to their Application Programming Interface (API) recorded to the blockchain (Figure 7.1) Entire documents can be encrypted and written to the blockchain, but the standard model is to store the data package elsewhere (referred to as the pre-image) and a hash of the data notarized. The Who, What and When is now in the form of a single hexadecimal text. The pre-image can be stored on Kompany's server and on the client's network. Furthermore, the notarization is done in

[4] coingeek.com/coingeek-zurich-know-your-business-on-bsv-blockchain/

a way that can link it to all prior and future KYB checks for that client. Every transaction on a Bitcoin blockchain consists of inputs and outputs (the cash and coins of a digital cash system), and the linking of data transactions can be as simple as using an output from one transaction record as the input to the next.

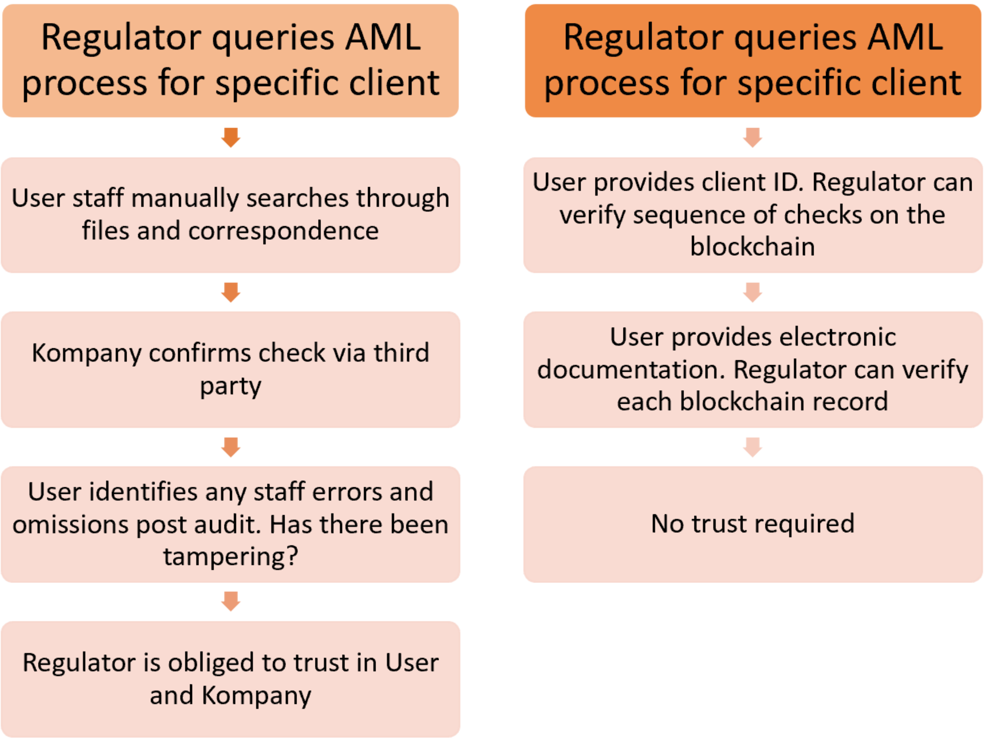

Regulator queries AML process for specific client
User staff manually searches through files and correspondence
Kompany confirms check via third party
User identifies any staff errors and omissions post audit. Has there been tampering?
Regulator is obliged to trust in User and Kompany
Regulator queries AML process for specific client
User provides client ID. Regulator can verify sequence of checks on the blockchain
User provides electronic documentation. Regulator can verify each blockchain record
No trust required

Figure 7.2: Regulator query process comparison

The result is immutable proof of the request and the response, locked in time and sequence, and easy to locate. As noted above, presently only a hash of any documentation is on the blockchain. However, it is also possible, at the user's discretion, for all this information to be encrypted and directly stored on the blockchain. The use of a public blockchain with encryption opens up the possibility of not merely selective sharing of encryption keys (plus the data they encrypt) with the regulator, but also between firms running checks. This duplicated effort is a key pain point noted by Schneider et al. (2016). Secure sharing in the literature is most advanced in healthcare records. Huang et al. (2020) explores a blockchain based solution that uses zero knowledge proofs to address GDPR and privacy issues. Irrespective, Kompany's methodology collapses the time required to perform the onboarding, transacting, monitoring, and offboarding elements of customer KYB for the entire life cycle of a customer. Audits which may have previously taken staff days to scour through emails and archives now takes minutes. The results of such audits are evidential in quality and hard to critique in a court of law. If documents are provided (e.g., to a regulator or auditor) and a hash of those documents is present on the blockchain, then those documents existed on or before the timestamp on that block. An audit package provided by a non-blockchain KYB process includes a risk that all the records were created the day after the regulator enquiry. It includes a risk that the original records have been tampered with. Figure 7.2 indicates how blockchain notarization eliminates the need for the regulator to trust in the evidence provided by the regulated firm and Kompany, because the blockchain guarantees the hashed data of the process, the order that they happened in, and that any tampering is immediately visible. In contrast to Zikratov et al. (2017), which proposes a theoretical, dedicated variation on an existing blockchain for establishing a data integrity system, nChain's solution consists of a readily deployable software code that makes calls on their API. Enterprises can integrate the code and / or the API with their existing software to notarize high value data. Any series or network of data within a firm can now be notarized immutably and thus have a mathematically defined level of authenticity. The underlying BitcoinSV blockchain use large block sizes to offer over 5,000 transactions per second (TPS),[5] though this is reciprocal with a decline in the number of distinct systems running node software (200 compared to 8,000 on Bitcoin BTC as of May 2021)[6]. We note that BTC's desire for users to run their own record keeping nodes is based on the ability to personally verify transactions, and therefore appropriate for digital gold use cases, but less important for storing data. In terms of the cost of the data integrity guarantee, nChain offers its services at rates as low as Euro 0.01 per write transaction. Another alternative to a blockchain is to use a permissioned distributed ledger such as Hyperledger[7]. A complete comparison of these ledger technologies is outside the scope of this chapter, however we note three points. One is that permissioned ledgers have centralized sponsors that are effectively rule makers (Section 1.3). The existence of a rule maker, that likely also writes data, means that any promise of tamper resistance is commensurately weaker. Although such systems have no single point of failure, they often have a critical single point of control. The second point is that the permissioned ledger's owner must fund the development of both the infrastructure and the application, whereas on a public blockchain only the application must be funded by the

[5] bitcoinassociation.net/bsv-proves-that-bitcoin-scaling-works-surpasses-btc-blockchain-in-accumulated-data-size

[6] blockchair.com/bitcoin-sv

[7] hyperledger.org

sponsor. The final point is that cloud computing is both cheap, secure and promises no single point of failure. In choosing a permissioned distributed ledger, has anything been proposed that is not already provided by a cloud provider?

7.3 Regulatory perspective on blockchain

Given the arguments and benefits laid out above, and in papers such as Treleaven and Batrinca (2017), it is worth asking why regulatory use cases have not been deployed before on blockchain. Interestingly, regulators are enthusiastic adopters of SupTech, technologies which help them improve their supervisory capabilities. Financial Stability Board (2020) surveys 41 regulatory organizations in 25 countries and finds that over two thirds have adopted SupTech. Their research provides multiple case studies, for example detailing the application of machine learning to data submitted by firms. However hardly any of the survey group admit to using blockchain. In terms of RegTech, technologies which help firms meet their regulatory requirements, almost all regulators surveyed claim that regulated firms have adopted some form of it. Critically, less than half of the surveyed regulators are encouraging the adoption of RegTech.

There are several reasons the adoption of blockchain based KYB is emerging now. The first reason is that many existing products, for example Kompany's suite of non-blockchain software offerings, are rigorous and effective. Kompany offers a dynamic multiple source checking service with a third-party guarantee. They complement sophisticated financial services compliance teams, that include layered technologies that check new customers and their transactions. Once a customer or transaction is flagged, documented manual checks are carried out. As mentioned already, where these checks fail or are irreparably delayed, regulators have imposed large fines. The dynamics of existing systems highlights one dialectic important to the evolution of regulatory compliance. Although enterprises would like to reduce the cost of these systems, arguably the regulator cares more on increasing effectiveness. Another way of phrasing this is that companies want to reduce the false positive flagging of customers and transactions, whereas the regulator is focused on decreasing the rate of false negatives – catching more money launderers and money laundering. Arguably, if regulators believed that RegTech achieved the latter, more of them would be encouraging its adoption.

The European Commission's Digital Finance Strategy (EC, 2020) lay out further reasons for slow adoption. Many existing regulations did not envisage the present step change in what is possible. For example, EU regulations exist that specify the use of an intermediary such as a clearing house in a process – disincentivizing investment in any technology that might result in disintermediation. In addition, implementing changes to these regulations are laborious. Consequently, only now are proposals published to either adapt regulation to new technical capabilities or, more typically, to provide regulatory waivers.

Nevertheless, that leaves a more traditional set of problems for adopters of RegTech to overcome. One highlighted by the European Commission is that regulators seek to future proof any changes by being technology neutral. There is no wish to specify the use of any one technology, which might create dependencies on a single provider or crowd out other initiatives. A corollary of technology neutral regulation is that regulators require market participants to lead the way on prototyping and deploying new technology. Market participants, looking to regulators for rules that might reduce their deployment risk, are given limited guidance. Furthermore, there is unlikely to be a willingness on the part of the regulator to allow regulated firms to pass responsibility for compliance to technology. This means that until regulated firms show that a system is as good or better than existing systems, they may be required to run both systems with both sets of costs.

Based on the EU's Digital Finance Strategy, we observe that in Europe at least, the time is right for blockchain based RegTech. Both the development risk and potentially delayed cost benefits are not commercially unusual. Perhaps more controversially, we argue that blockchain based RegTech can both reduce long run compliance cost and improve the effectiveness of compliance processes. In addition to the blockchain benefits discussed in the sections above, we add three more. One is that encrypted networked registries on a public blockchain can be used to give regulators fine grained insight into the activities of agents within the financial system i.e., improved surveillance. In terms of dynamic process, Kompany's system already stipulates a fresh KYB check not only when opening a new account, but also whenever key data changes. However blockchain can add to this the proactive and automated withdrawal of linked permissions related to KYB (Tartan et al., 2021). Thirdly, if so desired, regulators can drive towards any level of manual checking it wishes to accompany the deployment of blockchain based RegTech. These points indicate how public blockchain can provide improved supervision and programmable regulatory implementation.

Instead of substituting regulatory responsibility for technology, technology can empower regulation – at the same time as saving costs. We contrast this with machine learning, where SupTech and RegTech use cases are arguably separate and distinct. Conversely, blockchain contains the potential to merge meeting regulatory requirements with improving supervisory capability.

7.4 Placing blockchain within the data integrity literature

In this section, we anchor the case study on Kompany in the field of data integrity. Data integrity has a variety of definitions. Ruthberg and Polk (1989) contextualizes the term wider than the data itself. Although it incorporates quality (i.e. accuracy, precision, timeliness), it juxtaposes this with its objective - data integrity is where the relative quality of the data is appropriate for its practical purpose. Having different purposes in mind may explain why different authors emphasize different aspects of data integrity. Motro (1989) describes two dimensions of integrity: validity where all false information is excluded, and completeness where all true information is included. Although insightful, in practice this is somewhat idealistic with two measures that strain peer reviewed content. Many papers focus on states and state changes (Clark and Wilson, 1987; Moerkotte and Lockemann, 1991), and argue that a system can reflect data integrity if the initial data and any transformative processes meet specific conditions. In other words that they have been certified and the rules have been followed. Process, checks and controls are critical to making data trustworthy. Might the processes and controls of blockchain meet this requirement of data integrity? Lemieux (2016) describes the archival science perspective and splits the trustworthiness of a record into two parts. Firstly, Reliability is the record's trustworthiness as a statement of fact, as in a measure of the competence of its author, its completeness, and any controls on its creation. Secondly, Authenticity is what a record is compared to what it claims to be – that it is free from tampering and corruption.

All ledgers suffer from issues of reliability regarding the creation of records, even when the relevant authority and ledger owner is the same e.g., government. None can eliminate human error. However, centralized ledgers like those run by banks are particularly vulnerable to accidental corruption and adversarial tampering, and this has been exacerbated by digitization. Lemieux

(2016) notes how paper records are in many ways more resilient than electronic records. Neither correcting fluid nor a freshly printed certificate are stealthy in action.

This inability to make undetectable changes is a key reason why PoW blockchain is tamper resistant. Any changes, whether by stakeholders or outsiders, is immediately evident. Each block of data is linked to all others by a technique referred to as hashing. Hashing takes any data, scrambles it and returns a unique fixed length result (Narayanan and Clark, 2017). Its effect is one way math. A record of a hash is an easily verified proof that an item of data is unchanged since the hash was computed. When used to formulate a ledger of sequential elements, it is easily verified evidence that the ledger sequence and its contents are unchanged. When used as a puzzle, there are no short cuts, only actual computation will solve the puzzle. Separately, the public by default nature of blockchains adds another layer of transparency. Centralized ledgers can be public but have in the past rarely chosen to be so. Opaqueness can hide mistakes. Further, with respect to blockchains, honest miners and users have an option to respond when tampering becomes clear. They can increase their hashing capacity and fork away if necessary. Another facet of this tamper resistance is that blockchains are append only – a rule regarding data transformation that private permissioned distributed ledgers like Hyperledger also share.

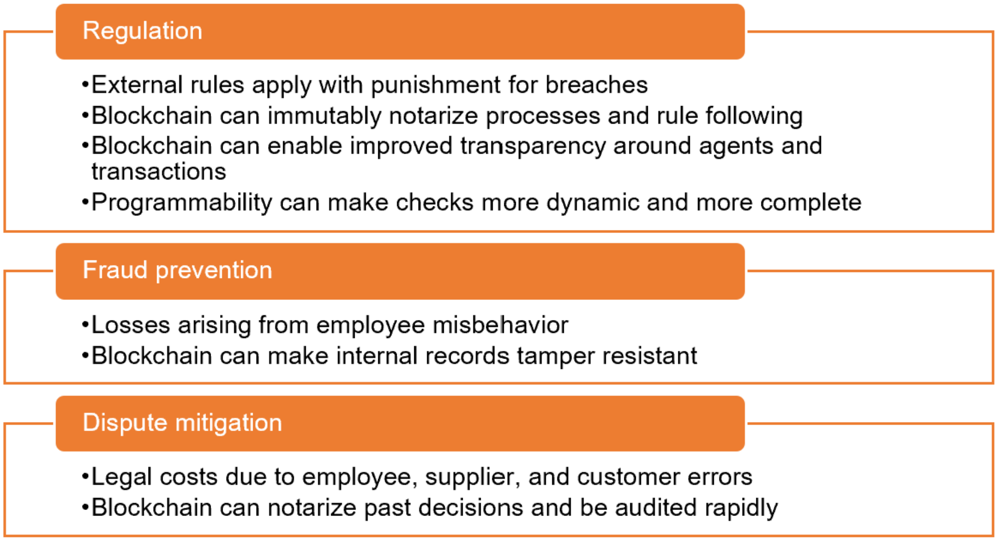
Juxtaposing blockchains and the data integrity technique Remote Data Auditing (RDA), we see that hashing and replication are two of the core features of both. Sookhak et al. (2015) describes RDA as a way to ensure that data in cloud computing environments matches the data originally uploaded. Replication improves resiliency, while hashing is used to check two sets of data are identical without resending all the data. Dividing data into traceable units, at the same time as replicating and hashing, helps triangulate missing or corrupted data quickly. Much of this work and process is now standard in cloud deployments. ISO (2021) defines message authentication codes (MAC) that are hash algorithms used to ensure data integrity in the cloud. In addition to tamper resistance, Narayanan and Clark (2017) discusses how Spam, Denial of Service, and Sybil attacks (where adversaries manufacture additional voting identities) are all attempts to magnify one user's importance over others – and that PoW can mitigate against all three. Bringing this all together, it should not be surprising that distributed ledgers reflect the RDA framework and share the same techniques. PoW blockchains are designed to have adversaries on the network and yet be correct. The surprise is that blockchain data integrity use cases have taken so long to arrive, even as financial market use cases such as decentralized exchanges have started to emerge (Chapter 6).

The connection between the data integrity literature and secure sharing most often goes via medical data or the risk of data breaches. A critical feature of data worth sharing is that it is authentic. Jin et al. (2019) surveys secure sharing in the field of healthcare. It observes that separate data silos may hold multiple copies of purportedly the same data in many places, leading to errors, under use and inconsistent security. Their paper categorizes research to improve this by three methods: cryptographic, anonymity and blockchain. Interoperability is noted as the primary constraint to cryptographic solutions, while balancing utility versus privacy has often led to data leakage under anonymity solutions. Blockchain is highlighted as a potential connective layer, that uses smart contracts to join, update and access multiple separate data silos held by organizations such as clinics or hospitals. The differences of this to the discussions on data integrity above are largely a matter of nuance and emphasis. Jin et al. (2019) concludes that a lack of on chain blockchain capacity suggests that off chain storage is most likely for the secure sharing of data. This is a conclusion we disagree with, and propose as an area for future research and development. We expand on both data integrity and secure sharing use cases in the next section.

7.5 Creating business value from data integrity

Identifying blockchain data integrity use cases can be framed by a number of questions. What data in an organization is valuable enough to being raised to evidential quality? Further, which records generate risks that justify the stronger security model of blockchain? Finally, when does the sharing of these records mitigate these risks? This paper provides some guidance to practitioners by expanding the discussion to three sets of use cases shown in Figure 7.3, (1) regulatory, (2) fraud prevention, and (3) dispute mitigation.

The potential of the first is addressed by Kompany's KYC onchain; Cai (2021)'s triple entry accounting; and ties in with Auer (2019) on embedded regulation. The last example uses blockchain ledgers to securely share with regulators real time information on bank balance sheets, which are subject to strict regulatory capital requirements. Arguably, additional obligations on regulated institutions to publicize certain data points daily, or even down to every ten minutes, on public



Regulation

- External rules apply with punishment for breaches
- Blockchain can immutably notarize processes and rule following
- Blockchain can enable improved transparency around agents and transactions
- Programmability can make checks more dynamic and more complete

Fraud prevention

- Losses arising from employee misbehavior
- Blockchain can make internal records tamper resistant

Dispute mitigation

- Legal costs due to employee, supplier, and customer errors
- Blockchain can notarize past decisions and be audited rapidly

Figure 7.3: Three enterprise data integrity risk reduction use cases

blockchains may discourage risky behavior, for example the activities that proceeded the collapse of Lehman brothers in 2008. If a bank is obliged to publicize the mark to market on its trading book daily, would internal risk limits be higher or lower? Note that by publicizing we do not necessarily mean to the general public. The data might be encrypted with cryptographic keys jointly held by the firm and its regulators. Within KYB and compliance, another key pain point is false positives (Schneider et al., 2016). Potentially these could be reduced if blockchain improves the completeness of data transmitted, provides enhanced clarity around sender and receiver, and if automated checks included prior transactions, rather than being made solely on the merits of individual transactions. A separate regulatory use case is in healthcare records, both of patients and clinical trials (Engelhardt, 2017).

A fraud prevention use case can be demonstrated with a financial industry example. Jennings (2011) discusses the similarities between the unauthorized trading losses of Kweku Adoboli, Jerome Kerviel and Nick Leeson, that incurred significant losses at UBS, Société Générale and Barings Bank respectively. Each of them involved a trader circumventing internal controls. For example, Adoboli used phantom trades that appeared to offset the losses and risk exposures of his real trades. The impact of all three rogue traders could have been minimized by more rigorous and regular compliance checks. Another alternative to costly and intrusive trader surveillance would be to publicize each of their daily profit and losses on a blockchain. Then any tampering of internal records would have been limited to a single day and if attempted be obvious within 24 hours. ACFE (2020) reviewed 2,500 cases of occupational fraud between 2018-2019 and estimated that they caused USD 3.6 billion in losses. The organization's members posit that perhaps 5% of corporate revenues are subject to fraud, which could extrapolate to over USD 4.5 trillion a year. Firms can use blockchain to significantly reduce the attack surface of occupational fraud.

The examples provided show how public blockchain can document data and the time of its existence immutably. This difficult to tamper with record is then appropriate for the most rigorous use case possible, a legal or regulatory dispute. In this way, we can begin to see how data integrity via blockchain can become a dispute mitigation device – the easy to recover evidence that negates the need for further investigation and discourages legal escalation. Resilience Partners[8], a UK based start-up, are working with real estate project managers and investors to write construction and environmental data to the Polkadot blockchain. Data integrity is particularly important to the former. If all the elements of contract negotiation, planning and construction are appropriately and immutably recorded, then when disputes arise evidence can be produced in minutes and forestall further delay or legal escalation. HKA Global analyzes 1,100 construction projects from 88 countries between 2018-2020, to estimate that they were subject to USD 48 billion in claimed disputes (Axten et al., 2020). In this use case, blockchain does not prevent mistakes, but is intended to generate savings on related legal expenses.

7.6 Summary - regulatory compliance and data integrity

Data integrity has both broad and narrow definitions. Blockchain can be used to address some facets of data integrity: the potential for tampering, errors and omissions after the data has been created. We argue that PoW blockchains combine a new form of ledger that has no single point of control, with techniques seen in the field of Remote Data Auditing, to make tampering difficult to execute and easy to identify. In a case study of Kompany, who are writing KYB checks to the blockchain, we present a data integrity use case in deployment today. In a discussion of the regulator's perspective on RegTech, we draw out reasons why now may be the time for blockchain based RegTech. Regulation, internal fraud prevention and dispute mitigation are high value, enterprise

[8] resilience-partners.co.uk

level, data integrity blockchain use cases. We simplify our selection of value-added blockchain data integrity applications by using examples where the beneficiary is also the implementor, thereby avoiding the coordination issues that may be delaying other superficially similar projects. This reduces the need for the risk sharing strategies discussed by Malhotra, O'Neill, and Stowell (2021). When blockchain notarization is of a regulatory process, it is improving the compliance of the firm and its ability to avoid regulatory failures. When blockchain notarization is upgrading an existing internal corporate control, then it is improving the firm's ability to follow its strategy and fine tune its risk appetite. When blockchain notarization can forestall the escalation of a dispute, it reduces a firm's operational risk and reduces legal expenses.

Chapter 8

Thesis conclusion

8.1 Objectives

The objective of this thesis is to address the question: does blockchain solve real world economic problems. We observe that there is space for analysis and case studies that explore blockchain adoption. In other words, there is a need for more evidence of the impact of blockchain on economic processes. This thesis approaches the central objective via four sub questions.

- What are the drivers of Bitcoin mining revenues? How does this relate to transaction processing capacity?
- Do blockchain tokens, and the project that issues them, have an observable economic connection?
- Can blockchain improve the completeness of a financial market?
- Can blockchain improve data integrity?

The answers to these four sub-questions (1) analyzes the core mechanism of the original PoW blockchain, (2) investigates a key assumption of the blockchain token literature, and (3) explores two in production use cases that attempt to solve real world problems.

8.2 Main findings

This thesis provides evidence that blockchain can solve real world economic problems. In Chapter 4, we analyze the mechanics of the first application of blockchain: Bitcoin. In a study of Bitcoin mining revenues, we map out the relative importance of the two key drivers of this, changes in the price of the token and changes in transaction volume. We find that transaction volumes have a proportionately small impact on mining revenues until the system becomes capacity constrained. We use this finding to argue the importance of design and developer choices on a key constraint of PoW blockchains - the low transaction throughput. Although this may have been contentious at the time of publication, this point has now been made elsewhere with the upgrade of Ethereum to PoS and the commerciality of other high throughput blockchains such as BitcoinSV, Tezos and Solana.

In Chapter 5, we present evidence that a key assumption in the blockchain token literature, that tokens are linked to the underlying issuing project, is plausible. This is despite the lack of any legal connection. We do this empirically by showing that the function of a token has a statistically significant impact on the trading price of the token. We note that we assume that the function of the token is chosen by the venture in order to carry out the objectives and purpose of the project.

In Chapter 6 on Uniswap the decentralized exchange, we find that the exchange rate between Ethereum and Tether is cointegrated between its price on Uniswap and an index of its price on centralized venues. This confirms that decentralized exchanges can be effective.

In Chapter 7, we use a case study methodology to explore the use of blockchain for data integrity. The Know Your Customer (KYC) service provider Kompany, that is now part of the ratings agency Moody, is notarizing all its customer API calls to the blockchain to provide a new level of data reliability and auditability. These benefits are core goals of the data integrity literature.

This thesis and the evidence it puts forward, complements the idea that blockchain is a record keeping technology with reduced cost of verification. It makes a nuanced argument that a key change wrought by blockchain is in the governance of data. In other words that it can constitute definitive repositories of shared facts with no single point of control. We use a political analogy to provide a new intuition on this: centralized ledgers are ‘monarchic’ in nature, which blockchain can substitute for with a ‘competitive’ model of data governance. Use cases of blockchain such as disintermediation, payments, and self sovereign identity (with enhanced privacy) emerge from this new capability. For example, a user can only own their data if no one else controls it.

8.3 Contribution

We focus on three contributions of this thesis. Firstly is the evidence of a connection between a token and its project. There are many papers such as Catalini and Gans (2016) that build theory and evidence regarding the benefits of tokens. Many token markets are visibly driving economic behavior. All of this research and activity is based on the assumption that tokens are connected to the underlying project despite the lack of a legal connection. In contrast, all prior elements of a firm's capital structure, such as bonds and shares, do not assume this - they have their connection comprehensively laid out in contract law.

The second contribution relates to decentralized exchanges. Unlike with payments and price discovery, this application of blockchain was not commercialized previously. Although it directly competes with centralized exchanges, never before had we seen liquidity pool based markets which react passively to the behavior of other traders. This passivity means they do not withdraw from markets at times of stress - as seen with financial market makers (Comerton-Forde et al., 2010). Decentralized exchanges, such as Uniswap V2 enable the ability to trade at any volume and any price, filling gaps that may exist elsewhere. Chapter 6 contributes evidence that they can be effective, and therefore that such decentralized exchanges can improve market completeness. The latter is a tangible real world problem and a major assumption across economic research.

The third contribution relates to the field of data integrity. This thesis adds a case study of a real world, revenue generating application of blockchain to the literature, that is not dependent on tokens or price. The case study explores the use of blockchain for Know Your Customer / Anti Money Laundering purposes, which improves process and auditability. It then discusses the applicability of adjacent potential use cases, such as employee fraud and dispute mitigation.

8.4 Limitations

The existence of applications outside of payments and price discovery has particular importance to this topic, as being implemented in multiple sectors and verticals is a necessary condition of blockchain constituting a General Purpose Technology (Bresnahan and Trajtenberg, 1995). We add Chapter 7 on Kompany to Jensen, Hedman, and Henningsson (2019)'s work on TradeLens, for supply chain, as examples of this non-financial usage. We note however that more applications and more evidence is required to answer the question implied by Catalini and Gans (2016): Is blockchain a General Purpose Technology? Both Kompany's KYC onchain and TradeLens are early with respect to adoption.

In terms of Chapter 6 on decentralized exchange, there are two limitations. The first is that cointegration of the price on and off the DEX only proves that the DEX is effective. More research is required to show that a DEX is sufficient in its role as a marketplace. This might involve analysis of DEX pairs where there are no centralized competitors. The second limitation is that subsequent to the time period tested in the thesis, Uniswap introduced its V3 implementation, with concentrated liquidity. This improved capital efficiency - liquidity providers can specify ranges where their assets are deployed - at the same time as reducing market completeness, the key point of our work. We note however that Uniswap V2, and that other DEXs such as Sushiswap, continues to match trades in the way explored in the thesis. Uniswap V2 and V3 are complements.

8.5 Future research

We observe that the key question of the thesis - Can blockchain solve real world problems? - is an open ended question. We have added evidence to the literature, but more solutions and examples are required. The first area that we highlight as an avenue for future research is the secure selective sharing touched on in Chapter 7. We have argued that blockchain is a new data governance technology. Conversely, valuable data often has no single source of truth, or definitive repository. Can we use blockchain to finally introduce a definitive repository that resolves the existence of multiple data silos that contain contradictory information?

Related to this is the emerging commercial excitement around self-sovereign identity and personal data. Advancements in this area may be able to offer a solution to Tucker and Catalini (2018)'s research question: can individuals have property rights over their own data? A user cannot own their data if that data is owned by a company. Blockchain can remove the latter via its political decentralization, and potentially enable user ownership and control of data. It is plausible that financial applications will continue to dominate the blockchain space, but we observe that perhaps opportunities in data offers more revolutionary potential.

8.6 Policy implications

This thesis contains a number of implications for policy makers, practitioners and academics. Chapter 4 highlights the importance of design decisions in the features of a blockchain, it supports regulation that is technology neutral (EC, 2020). It argues against those that would reject blockchain solutions based on historical limitations. Chapter 5 provides evidence of the connection between a token and a project in the absence of a legal basis. Such a link is critical if tokens are to impact economic processes outside of speculation, and are often assumed to exist. It is supportive of regulatory efforts related to digital tokens and crypto assets. American securities law uses the Howey test, a check of an investment contract, to determine whether or not something is a financial security. Although the Howey test is much broader than merely a connection, our work is consistent with their arguments. Chapter 6 highlights how regulators and market participants might exploit the features of decentralized exchanges to improve market completeness. Most financial markets are based on quotes made by buyers and sellers, leading to gaps between supply and demand. Automated market makers, such as Uniswap V2 based on liquidity pools, have no such gaps. There is some volume available at every given price, and there is some price available at any given volume. Market completeness is a common assumption in the economic literature that often does not hold in practice. As the most practical work of the thesis, Chapter 7 provides multiple suggestions to regulators and practitioners. These span the importance of process and data integrity to regulation, as well as the ability to improve and harden the data within an organization in order to tackle compliance, employee fraud and dispute mitigation. Cumulatively, the applications examined show how firms and society are gradually traversing the hype cycle, deploying blockchain, creating value and solving real world economic problems.

Bibliography

Abadi, J. and Brunnermeier, M. (2018). *Blockchain economics.* Working paper 25407. National Bureau of Economic Research. DOI: 10.3386/w25407.

Acemoglu, D., Robinson, J. A., and Torvik, R. (2013). "Why do voters dismantle checks and balances?" In: *The Review of Economic Studies* 80.3, pp. 845–875. DOI: 10.1093/restud/rdt007.

ACFE (2020). *Report to the nations. Global study on occupational fraud and abuse.* Tech. rep. Association of Certified Fraud Examiners. URL: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf.

Adhami, S., Giudici, G., and Martinazzi, S. (2018). "Why do businesses go crypto? An empirical analysis of coin offerings". In: *Journal of Economics and Business* 100, pp. 64–75. ISSN: 0148-6195. DOI: 10.1016/j.jeconbus.2018.04.001.

Ahlers, G. K. C. et al. (2015). "Signaling in equity crowdfunding". In: *Entrepreneurship Theory and Practice* 39.4, pp. 955–980.

Akerlof, G. A. (1970). "The market for lemons: quality uncertainty and the market mechanism". In: *The Quarterly Journal of Economics* 84.3, pp. 488–500. DOI: 10.1017/cbo9780511528248.007.

Alexander, C. and Heck, D. F. (2020). "Price discovery in Bitcoin: the impact of unregulated markets". In: *Journal of Financial Stability* 50, pp. 1–18. DOI: https://doi.org/10.1016/j.jfs.2020.100776.

Amsden, R. and Schweizer, D. (2018). "Are blockchain crowdsales the new 'gold rush'? Success determinants of initial coin offerings". In: *SSRN.*

Androutsellis-Theotokis, S. and Spinellis, D. (2004). "A survey of peer-to-peer content distribution technologies". In: *ACM Computing Surveys* 36.4, pp. 335–371.

Angeris, G. and Chitra, T. (2020). "Improved price oracles: constant function market makers". In: *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies.* AFT '20. Association for Computing Machinery, pp. 80–91. ISBN: 9781450381390. DOI: 10.1145/3419614.3423251.

Angeris, G., Evans, A., and Chitra, T. (2020). "When does the tail wag the dog? Curvature and market making". In: *arXiv.* DOI: 10.48550/arXiv.2012.08040.

Ante, L., Sandner, P., and Fiedler, I. (2018). "Blockchain based ICOs: pure hype or the dawn of a new era of startup financing?" In: *Journal of Risk and Financial Management* 11.4, pp. 80–99.

Arthur, J. N., Williams, R. J., and Delfabbro, P. H. (2016). "The conceptual and empirical relationship between gambling, investing, and speculation". In: *Journal of Behavioral Addictions* 5.4, pp. 580 –591. DOI: 10.1556/2006.5.2016.084.

Aste, T., Tasca, P., and Di Matteo, T. (2017). "Blockchain technologies: the foreseeable impact on society and industry". In: *Computer* 50.9, pp. 18–28.

Athey, S., Catalini, C., and Tucker, C. (2017). *The digital privacy paradox: small money, small costs, small talk.* Working paper 23488. National Bureau of Economic Research.

Athey, S. et al. (2016). "Bitcoin pricing, adoption, and usage: theory and evidence". In: *SSRN.*

Auer, R. (2019). *Embedded supervision: how to build regulation into blockchain finance.* Working paper 811. Bank of International Settlement. DOI: 10.24149/gwp371.

Axten, J. et al. (2020). *CRUX Insight 2020.* Tech. rep. HK Global. URL: https://www.hka.com/2020-crux-insight/.

Azzi, R., Chamoun, R. K., and Sokhn, M. (2019). "The power of a blockchain-based supply chain". In: *Computers and Industrial Engineering* 135, pp. 582–592.

Baek, C. and Elbeck, M. (2015). "Bitcoins as an investment or speculative vehicle? A first look". In: *Applied Economics Letters* 22.1, pp. 30–34.

Bartoletti, M. and Pompianu, L. (2017). "An empirical analysis of smart contracts: platforms, applications, and design patterns". In: *Financial Cryptography and Data Security.* Ed. by M. Brenner et al. Cham: Springer International Publishing, pp. 494–509. DOI: 10.1007/978-3-319-70278-0_31.

Bastiat, F. (1846). *Popular fallacies regarding general interests.* London: J Murray.

Baum, A. (2020). *Tokenisation - the future of real estate investment.* Technical report. Said Business School, University of Oxford.

BEIS (2021). *Annual report and accounts 2020-2021.* Tech. rep. Department for Business, Energy and Industrial Strategy UK. URL: `https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1036048/1210-APS-CCS0621807886-001_BEIS_ARA_20_21_Accessible.pdf`.

Belleflamme, P., Lambert, T., and Schwienbacher, A. (2014). "Crowdfunding: tapping the right crowd". In: *Journal of Business Venturing* 29, pp. 585–609.

Benedetti, H. and Kostovetsky, L. (2018). "Digital tulips? Returns to investors in initial coin offerings". In: *SSRN.*

Bentov, I., Gabizon, A., and Mizrahi, A. (2017). "Cryptocurrencies without Proof of Work". In: *International Conference on Financial Cryptography and Data Security.*

Berentsen, A. and Schar, F. (2018). "Short introduction to the world of cryptocurrencies". In: *Federal Reserve Bank of St Louis Review* 100.1, pp. 1–16.

Bessy, C. and Chauvin, P.-M. (2013). "The power of market intermediaries: from information to valuation processes". In: *Valuation Studies* 1.1, pp. 83–117.

Biais, B., Glosten, L., and Spatt, C. (2005). "Market microstructure: A survey of microfoundations, empirical results, and policy implications". In: *Journal of Financial Markets* 8.2, pp. 217–264. DOI: `10.1016/j.finmar.2004.11.001`.

Biais, B. et al. (2019). "The blockchain folk theorem". In: *The Review of Financial Studies* 32.5, pp. 1662–1715.

Blandin, A. et al. (2019). *Global cryptoasset regulatory landscape study.* Cambridge Centre for Alternative Finance, Cambridge Judge Business School. DOI: `10.2139/ssrn.3379219`.

BOE (2020). *Central bank digital currency. Opportunities, challenges and design.* Discussion paper. Bank of England.

Boer, E. R. d. and Gudmundsson, S. V. (2012). "30 years of frequent flyer programs". In: *Journal of Air Transport Management* 24, pp. 18–24.

Bohme, R. et al. (2015). "Bitcoin: economics, technology and governance". In: *Journal of Economic Perspectives* 29.2, pp. 213–238.

Bouri, E. et al. (2017). “On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier”. In: *Finance Research Letters* 20, pp. 192 –198. ISSN: 1544-6123.

Brainard, L. (2016). “Distributed ledger technology”. In: *Northwestern Financial Review* 201.12, p. 8.

— (2020). *The digitization of payments and currency: some issues for consideration.* Speech. Symposium on the Future of Payments.

Brandvold, M. et al. (2015). “Price discovery on Bitcoin exchanges”. In: *Journal of International Financial Markets, Institutions and Money* 36, pp. 18–35.

Bresnahan, T. F. and Trajtenberg, M. (1995). “General purpose technologies ‘Engines of growth’”. In: *Journal of Econometrics* 65.1, pp. 83–108.

Briere, M., Oosterlinck, K., and Szafarz, A. (2015). “Virtual currency, tangible return: portfolio diversification with Bitcoin”. In: *Journal of Asset Management* 16.6, pp. 365–373. ISSN: 1479-179X.

Brunnermeier, M. K. and Oehmke, M. (2012). *Bubbles, financial crises, and systemic risk.* Working paper 18398. National Bureau of Economic Research.

Budish, E. (2018). *The economic limits of Bitcoin and the blockchain.* Working paper 24717. National Bureau of Economic Research.

Burer, M. J. et al. (2019). “Use cases for blockchain in the energy industry opportunities of emerging business models and related risks”. In: *Computers and Industrial Engineering* 137, pp. 1–9.

Buterin, V. (2013). *A next generation smart contract and decentralized application platform.* White paper. Ethereum.org.

Buterin, V. and Griffith, V. (2013). *Casper the friendly finality gadget.* White paper. Ethereum.org. URL: `https://arxiv.org/abs/1710.09437`.

Cai, C. (2021). “Triple-entry accounting with blockchain: How far have we come?” In: *Accounting & Finance* 61.1, pp. 71–93. DOI: `10.1111/acfi.12556`.

Cameron, A. C. and Miller, D. L. (2015). “A practitioner’s guide to cluster-robust inference”. In: *Journal of Human Resources* 50, pp. 317–372.

Canidio, A. (2018). *Financial incentives for open source development: the case for Blockchain.* MPRA Paper 85352. Munich Personal RePEc Archive.

Castells, M. (2011). “A network theory of power”. In: *International Journal of Communication* 5, pp. 773–787.

Catalini, C. and Gans, J. S. (2016). *Some simple economics of the blockchain.* Working paper 22952. NBER. DOI: `10.3386/w22952`.

— (2018). *Initial coin offerings and the value of crypto tokens.* Working paper 24418. National Bureau of Economic Research. DOI: `10.3386/w24418`.

CFTC (2020). *Complaint for injunctive and other equitable relief and civil monetary penalties under the commodity exchange act and commission regulations.* Civil action 20-cv-8132. Chicago Futures Trading Commission.

Chod, J. and Lyandres, E. (2018). “A theory of ICOs: diversification, agency and information asymmetry”. In: *SSRN*. DOI: `10.2139/ssrn.3159528`.

Choi, I. (2001). “Unit root tests for panel data”. In: *Journal of International Money and Finance* 20, pp. 249–272.

Chondros, N., Korkordelis, K., and Roussopoulos, M. (2012). “On the practicality of practical Byzantine fault tolerance”. In: *Middleware 2012*. Ed. by P. Narasimhan and P. Triantafillou. Springer Berlin Heidelberg, pp. 436–455. ISBN: 978-3-642-35170-9.

Ciaian, P., Rajcaniova, M., and Kancs, d. (2017). “Virtual relationships: short- and long-run evidence from Bitcoin and altcoin markets”. In: *Journal of International Financial Markets, Institutions and Money* 52, pp. 173–195. DOI: `10.1016/j.intfin.2017.11.001`.

Clark, D. D. and Wilson, D. R. (1987). “A comparison of commercial and military computer security policies”. In: *IEEE Symposium on Security and Privacy*, pp. 184–184. DOI: `10.1109/SP.1987.10001`.

Coase, R. H. (1937). “The nature of the firm”. In: *Economica* 4.16, pp. 386–405.

Cocco, L., Concas, G., and Marchesi, M. (2017). “Using an artificial financial market for studying a cryptocurrency market”. In: *Journal of Economic Interaction and Coordination* 12, pp. 345–365.

Cohney, S. et al. (2019). “Coin-operated capitalism”. In: *Columbia Law Review* 119.3, pp. 591–676.

Comerton-Forde, C. et al. (2010). “Time variation in liquidity: the role of market-maker inventories and revenues”. In: *The Journal of Finance* 65.1, pp. 295–331. DOI: `10.1111/j.1540-6261.2009.01530.x`.

Cong, L. W. (2018). “Understanding blockchain and tokenomics”. In: *COJ Reviews and Research* 1.1, pp. 1–3.

Cong, L. W. and He, Z. (2019). “Blockchain disruption and smart contracts”. In: *The Review of Financial Studies* 32.5, pp. 1754–1797. DOI: 10.3386/w24399.

Cong, L. W., Li, Y., and Wang, N. (2018). *Tokenomics: dynamic adoption and valuation.* Working paper WP2018-13-015. Fisher College of Business.

Conley, J. P. (2017). *Blockchain and the economics of crypto-tokens and intial coin offerings.* Working paper VUEcon-17-00008. Vanderbilt University.

Cook, S. and Manning, N. (2004). “The disappointing properties of GLS-based unit root tests in the presence of structural breaks”. In: *Communications in Statistics - Simulation and Computation* 33.3, pp. 585–596. DOI: 10.1081/SAC-200033390.

Copeland, T. (2020). *Steem vs Tron: The rebellion against a cryptocurrency empire.* Internet article. URL: https://decrypt.co/38050/steem-steemit-tron-justin-sun-cryptocurrency-war.

Croman, K. et al. (2016). “On scaling decentralized blockchains”. In: *Financial Cryptography and Data Security.* Ed. by J. Clark et al. Vol. 9604. Springer Berlin Heidelberg, pp. 106–125. ISBN: 978-3-662-53357-4.

Dai, J. and Vasarhelyi, M. A. (2017). “Toward blockchain-based accounting and assurance”. In: *Journal of Information Systems* 31.3, pp. 5–21.

Dang, H. et al. (2019). “Towards scaling blockchain systems via sharding”. In: *Proceedings of the 2019 International Conference on Management of Data.* ACM. DOI: 10.1145/3299869.3319889.

Davidson, S., De Filippi, P., and Potts, J. (2018). “Blockchains and the economic institutions of capitalism”. In: *Journal of Institutional Economics* 14.4, pp. 639–658. DOI: 10.1017/s1744137417000200.

Dixon, W. J. (1960). “Simplified Estimation from Censored Normal Samples”. In: *The Annals of Mathematical Statistics.* Vol. 31. Institute of Mathematical Statistics, pp. 385–391.

DoJ (2012). *HSBC Holdings Plc and HSBC Bank USA admit to anti-money laundering and sanctions violations, forfeit 1.256 billion in deferred prosecution agreement.* Tech. rep. Department of Justice. URL: https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations.

Dwyer, G. P. (2015). “The economics of bitcoin and similar private digital currencies”. In: *Journal of financial stability* 17.C, pp. 81–91. DOI: 10.1016/j.jfs.2014.11.006.

EC (2020). *Digital finance strategy for the EU.* Tech. rep. 591. European Commission. URL: https://ec.europa.eu/info/publications/EC-Digital-Strategy_en.

Elliott, G., Stock, J., and Rothenberg, T. (1996). “Efficient Tests for an Autoregressive Unit Root”. In: *Econometrica* 64, pp. 813–36. DOI: 10.2307/2171846.

Enders, W. (1995). *Applied Econometric Time Series.* Hoboken, USA: John Wiley & Sons. DOI: 10.2307/2291367.

Engelhardt, M. A. (2017). “Hitching healthcare to the chain: an introduction to blockchain in the healthcare sector”. In: *Technology Innovation Management Review* 7.10, pp. 22–34. DOI: 10.22215/timreview/1111.

Eyal, I. and Sirer, E. G. (2014). “Majority Is Not Enough: Bitcoin Mining Is Vulnerable”. In: *Financial Cryptography and Data Security.* Ed. by N. Christin and R. Safavi-Naini. Berlin, Heidelberg: Springer, pp. 436–454. ISBN: 978-3-662-45472-5.

Eyal, I. et al. (2015). “Bitcoin-NG: a scalable blockchain protocol”. In: *CoRR.*

Fama, E. F. (1970). “Efficient capital markets: a review of theory and empirical work”. In: *The Journal of Finance* 25.2, pp. 383–417. DOI: 10.2307/2325486.

Fanning, K. and Centers, D. P. (2016). “Blockchain and its coming impact on financial services”. In: *Journal of Corporate Accounting and Finance* 27.5, pp. 53–57.

FCA (2019). *Guidance on cryptoassets CP19/3.* Consultation Paper. UK Financial Conduct Authority.

— (2020a). *FCA fines Commerzbank London £37,805,400 over anti-money laundering failures.* Tech. rep. Financial conduct authority. URL: https://www.fca.org.uk/news/press-releases/fca-fines-commerzbank-london-37805400-over-anti-money-laundering-failures.

— (2020b). *Prohibiting the sale to retail clients of investment products that reference cryptoassets.* Policy statement PS20/10. Financial Conduct Authority.

Fenu, G. et al. (2018). “The ICO phenomenon and its relationships with ethereum smart contract environment”. In: *2018 International Workshop on Blockchain Orientated Software Engineering (IWBOSE)*, pp. 26–32. DOI: 10.1109/IWBOSE.2018.8327568.

Ferraro, P., King, C, and Shorten, R. (2018). “Distributed ledger technology for smart cities, the sharing economy and social compliance”. In: *IEEE Access* 6, pp. 62728–62746.

Financial Stability Board (2020). *The use of supervisory and regulatory technology by authories and regulated institutions.* Tech. rep. FSB. URL: `https://www.fsb.org/wp-content/uploads/P091020.pdf`.

FINMA (2018). *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs).* Regulatory guidance. Swiss Financial Market Supervisory Authority.

Foley, S., Karlsen, J. R., and Putnins, T. J. (2019). “Sex, drugs, and Bitcoin: how much illegal activity is financed through cryptocurrencies”. In: *The Review of Financial Studies* 32.5, pp. 1798–1853. DOI: `10.1093/rfs/hhz015`.

Froot, K. A. and Ramadorai, T. (2005). “Currency returns, intrinsic value and institutional-investor flows”. In: *The Journal of Finance* 60.3, pp. 1535–1566.

Gandal, N. et al. (2018). “Price manipulation in the Bitcoin ecosystem”. In: *Journal of Monetary Economics* 95, pp. 86–96. DOI: `10.1016/j.jmoneco.2017.12.004`.

Ganne, E. (2019). “Why blockchain could become the new container of international trade”. In: *International Trade Forum* 1, pp. 16–17.

Gatteschi, V. et al. (2018). “To Blockchain or Not to Blockchain: That Is the Question”. In: *IT Professional* 20, pp. 62–74. DOI: `10.1109/MITP.2018.021921652`.

Gencer, A. E. et al. (2018). “Decentralization in Bitcoin and Ethereum Networks”. In: *2018 Financial Cryptography and Data Security Conference.*

George, R. V. et al. (2019). “Food quality traceability prototype for restaurants using blockchain and food quality data index”. In: *Journal of Cleaner Production* 240, pp. 1–8.

Gervais, A. et al. (2014). “Is Bitcoin a decentralized currency?” In: *IEEE Security and Privacy* 12.3, pp. 54–60.

Gordon, M. J. (1959). “Dividends, earnings, and stock prices”. In: *The Review of Economics and Statistics* 41.2, pp. 99–105.

Griffin, J. M. and Shams, A. (2020). “Is Bitcoin really untethered?” In: *The Journal of Finance* 75.4, pp. 1913–1964. DOI: `https://doi.org/10.1111/jofi.12903`.

Grinberg, R. (2012). “Bitcoin: An Innovative Alternative Digital Currency”. In: *Hastings Science and Technology Law Journal* 4.1, pp. 159–207.

Harz, D. and Boman, M. (2018). “The scalability of trustless trust”. In: *Financial Cryptography and Data Security 2018*, pp. 279–293.

Hasbrouck, J. (1995). “One Security, Many Markets: Determining the Contributions to Price Discovery”. In: *The Journal of Finance* 50.4, pp. 1175–1199. DOI: `10.1111/j.1540-6261.1995.tb04054.x`.

Hawlitschek, F., Notheisen, B., and Teubner, T. (2018). “A systematic review of blockchain”. In: *Electronic Commerce Research and Applications* 29, pp. 50–63.

Hofmann, E., Strewe, U. M., and Bosia, N. (2019). *Supply chain finance and blockchain technology: the case of reverse securitisation*. Springer International Publishing.

Howell, S. T., Niessner, M., and Yermack, D. (2018). *Initial coin offerings: financing growth with cryptocurrency token sales*. Working paper 24774. National Bureau of Economic Research.

Huang, H. et al. (2020). “A blockchain-based scheme for privacy-preserving and secure sharing of medical data”. In: *Computers and Security* 99, p. 102010. ISSN: 0167-4048. DOI: `10.1016/j.cose.2020.102010`.

Huberman, G., Leshno, J. D., and Moallemi, C. (2019). “An economist’s perspective on the Bitcoin payment system”. In: *AEA Papers and Proceedings*. Vol. 109. American Economic Association, pp. 93–96. DOI: `10.1257/pandp.20191019`.

Hughes, A. et al. (2019). “Beyond Bitcoin: what blockchain and distributed ledger technologies mean for firms”. In: *Business Horizons* 62, pp. 273–281.

Iansiti, M. and Lakhani, K. R. (2017). “The Truth About Blockchain”. In: *Harvard Business Review* 95.1, pp. 118–127.

ISO (2021). *Information security — Message authentication codes (MACs) - Part 2: Mechanisms using a dedicated hash-function*. Tech. rep. 9797-2:2021. ISO Standard. International Organization for Standardization. URL: `https://www.iso.org/standard/75296.html`.

Jasim, S. A. and Oates, J. (1986). “Early tokens and tablets in Mesopotamia: new information from Tell Abada and Tell Brak”. In: *World Archaeology* 17.3, pp. 348–362.

Jennings, M. M. (2011). “Yet another alleged rogue: there is no such thing as a rogue trader redux”. In: *Corporate Finance Review* 16.3, pp. 36–40.

Jensen, M. C. and Meckling, W. H. (1976). “Theory of the firm: Managerial behavior, agency costs and ownership structure”. In: *Journal of financial economics* 3.4, pp. 305–360. ISSN: 0304-405X.

Jensen, T., Hedman, J., and Henningsson, S. (2019). "How TradeLens delivers business value with blockchain technology". In: *Management Information Systems Technology Quarterly* 18.4, pp. 221–243. DOI: 10.17705/2msqe.00018.

Jin, H. et al. (2019). "A review of secure and privacy-preserving medical data sharing". In: *IEEE Access* 7, pp. 61656–61669. DOI: 10.1109/access.2019.2916503.

Joseph, D. et al. (2022). "Ledger comparative analysis". In: *Blockchain technology: advances in research and applications*. Ed. by E. R. Porras. Nova. Chap. 1. ISBN: 979-8-88697-162-0. DOI: 10.52305/RTZT8988.

Kaal, W. A. (2019). *Blockchain-based corporate governance*. Working paper 19-10. University of St Thomas (Minnesota) Legal Studies.

Kahn, C. M., McAndrews, J., and Roberds, W. (2004). *Money is privacy*. Working paper 2004-18. Federal Reserve Bank of Atlanta.

Kahn, C. M., Rivadeneyra, F., and Wong, T.-N. (2020). "Should the central bank issue e-money?" In: *Journal of financial market infrastructure* 8.4, pp. 1–22. DOI: 10.21314/jfmi.2019.117.

Kampakis, S. (2018). "Three case studies in tokenomics". In: *The Journal of the British Blockchain Association* 1.2, pp. 79–82.

Kewell, B., Adams, R., and Parry, G. (2017). "Blockchain for good?" In: *Strategic Change* 26.5, pp. 429–437.

Keynes, J. (1930). *A Treatise on Money*. Macmillan.

Kim, T. (2017). "On the transaction cost of Bitcoin". In: *Finance Research Letters* 23.C, pp. 300–305.

Kripfganz, S. and Schneider, D. C. (2020). "Response Surface Regressions for Critical Value Bounds and Approximate p-values in Equilibrium Correction Models". In: *Oxford Bulletin of Economics and Statistics*. in press, pp. 1–24. DOI: 10.1111/obes.12377.

Kroll, J, Davey, I, and Felten, E (2013). "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries". In: *Workshop on the Economics of Information Security 2013*.

Kuhn, R. and Yaga, D. (2019). "Rethinking distributed ledger technology". In: *Computer*, pp. 68–72.

Kuo, T.-T., Kim, H.-E., and Ohno-Machado, L. (2019). "Blockchain distributed ledger technologies for biomedical and health care applications". In: *Journal of the American Medical Informatics Association* 24.6, pp. 1211–1220.

Laabs, M. and Dukanovic, S. (2018). "Blockchain in industrie 4.0: beyond cryptocurrency". In: *Information Technology* 60.3, pp. 143–153.

Lee, C. M. C., Myers, J., and Swaminathan, B. (1999). "What is the intrinsic value of the Dow". In: *The Journal of Finance* 54.5, pp. 1693–1741.

Lees, F. A. (2012). *Financial Exchanges: A Comparative Approach*. London: Routledge. ISBN: 1136651497. DOI: 10.4324/9780203805893.

Lemieux, V. L. (2016). "Trusting records: is blockchain technology the answer?" In: *Records Management Journal* 26.2, pp. 110–139. DOI: 10.1108/rmj-12-2015-0042.

Li, J. and Mann, W. (2018). "Initial coin offering and platform building". In: *SSRN*.

Li, W. et al. (2017). "Securing proof-of-stake blockchain protocols". In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology ESORICS 2017, DPM 2017, CBT 2017*.

Libra (2019). *An introduction to Libra*. Tech. rep. Libra Association.

Lin, L. X. (2019). "Deconstructing Decentralized Exchanges". In: *Stanford Journal of Blockchain Law & Policy* 2.1. URL: https://stanford-jblp.pubpub.org/pub/deconstructing-dex.

Lipton, A. (2018). "Blockchains and distributed ledgers in retrospective and perspective". In: *The Journal of Risk Finance* 19.1, pp. 4–25. ISSN: 1526-5943. DOI: 10.1108/JRF-02-2017-0035.

Litan, A. and Leow, A. (2021). *Hype cycle for blockchain*. Tech. rep. Gartner.

Lo, Y. C. (2017). "Blockchain and Bitcoin: technological breakthrough or the latest tulip price bubble?" In: *SSRN Electronic Journal*. DOI: 10.2139/ssrn.3198530.

Lo, Y. C. and Medda, F. (2018). "Bitcoin mining: converting computing power into cash flow". In: *Applied Economics Letters* 26.14, pp. 1171–1176. DOI: 10.1080/13504851.2018.1540841.

Lo, Y. C. and Medda, F. (2020). "Assets on the blockchain: An empirical study of Tokenomics". In: *Information Economics and Policy* 53, p. 100881. ISSN: 0167-6245. DOI: 10.1016/j.infoecopol.2020.100881.

Lo, Y. C. and Medda, F. (2022). "Do DEXs work? Using Uniswap V2 to explore the effectiveness of decentralized exchanges". In: *Journal of Financial Market Infrastructures*. DOI: 10.21314/JFMI.2022.004.

Lukasik, S. (2011). “Why the Arpanet was built”. In: *IEEE Annals of the History of Computing* 33.3, pp. 4–21.

Ma, J., Gans, J. S., and Tourky, R. (2018). *Market structure in Bitcoin mining.* Working paper 24242. National Bureau of Economic Research.

Mainelli, M. and Milne, M. (2015). *The impact and potential of blockchain on the securities transction lifecycle.* Tech. rep. SWIFT Institute.

Majd, M. (2018). “The cost of a SWIFT kick: estimating the cost of financial sanctions on Iran”. In: *International Finance in an Age of Inequality.* Edward Elgar Publishing. Chap. 9, pp. 175–193. DOI: 10.4337/9781788972635.00017.

Malhotra, A., O’Neill, H., and Stowell, P. (2021). “Thinking strategically about blockchain adoption risks and risk mitigation”. In: *Business Horizons.* In press. ISSN: 0007-6813. DOI: 10.1016/j.bushor.2021.02.033.

Malinova, K. and Park, A. (2019). *Tokenomics: when tokens beat equity.* Report. Global Risks Institute.

Maull, R. et al. (2017). “Distributed ledger technology: applications and implications”. In: *Strategic Change* 26.5, pp. 481–489.

Mazumdar, S. (2017). “Output gains from accelerating core inflation”. In: *Journal of Macroeconomics* 51, pp. 63–74.

McCorry, P., Hicks, A., and Meiklejohn, S. (2019). “Smart contracts for bribing miners”. In: *Financial Cryptography Workshop 2018*, pp. 3–19.

McNulty, P. J. (1967). “A note on the history of perfect competition”. In: *Journal of Political Economy* 75.4, pp. 395–399.

Medda, F. et al. (2019). *Analysis of three levels of innovative financial models.* Tech. rep. Circular models Leveraging Investments in Cultural heritage adaptive reuse (CLIC). URL: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5cb8eaa85&appId=PPGMS.

Meiklejohn, S. (2018). “Top then obstacles along distributed ledgers’ path to adoption”. In: *IEEE Security and Privacy Magazine.*

Merton, R. C. (1995). “A Functional Perspective of Financial Intermediation”. In: *Financial Management* 24, pp. 23–41.

Micheler, E. and Heyde, L. v. d. (2016). “Holding, Clearing and Settling Securities Through Blockchain Technology Creating an Efficient System by Empowering Asset Owners”. In: *SSRN*.

Moerkotte, G. and Lockemann, P. C. (1991). “Reactive consistency control in deductive databases”. In: *ACM Trans. Database Syst.* 16.4, pp. 670–702. ISSN: 0362-5915. DOI: 10.1145/115302.115298.

Mohan, V. (2019). “On the use of blockchain-based mechanisms to tackle academic misconduct”. In: *Research Policy* 48, pp. 1–17.

Molina-Jimenez, C. et al. (2019). “On and off-blockchain enforcement of smart contracts”. In: *Euro-Par 2018: Parallel Processing Workshops.* Springer International Publishing, pp. 342–354.

Montecchi, M., Plangger, K., and Etter, M. (2019). “It’s real, trust me! Establishing supply chain provenance using blockchain”. In: *Business Horizons* 62, pp. 283–293.

Motro, A. (1989). “Integrity equals validity plus completeness”. In: *ACM Transactions on Database Systems* 14.4, pp. 480–502. ISSN: 0362-5915. DOI: 10.1145/76902.76904.

Moulton, B. R. (1986). “Random group effects and the precision of regression estimates”. In: *Journal of Econometrics* 32, pp. 385–397.

Myers, S. C. (2000). “Outside equity”. In: *The Journal of Finance* 43.3, pp. 1000–1037.

Nagle, T., Redman, T., and Sammon, D. (2020). “Assessing data quality: a managerial call to action”. In: *Business Horizons* 63.3, pp. 325–337. DOI: 10.1016/j.bushor.2020.01.006.

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* White paper. Bitcoin.org.

Narayanan, A. and Clark, J. (2017). “Bitcoin’s Academic Pedigree”. In: *Communications of the ACM* 60.12, pp. 36–45. ISSN: 0001-0782. DOI: 10.1145/3132259.

Narayanan, A. et al. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction.* Princeton and Oxford: Princeton University Press. ISBN: 9781400884155.

Nooteboom, B. (2007). “Social capital, institutions and trust”. In: *Review of Social Economy* 65.1, pp. 29–53.

Nowinski, W. and Kozma, M. (2017). “How can blockchain technology disrupt existing business models”. In: *Entrepreneurial Business and Economics Review* 5.3, pp. 173–188.

O’Dair, M. and Owen, R. (2019). “Financing new creative enterprise through blockchain technology: opportunities and policy implications”. In: *Strategic Change* 28, pp. 9–17.

Pearson, S. et al. (2019). “Are distributed ledger technologies the panacea for food traceability?” In: *Global Food Security* 20, pp. 145–149.

Perez, D. and Livshits, B. (2019). “Smart contract vulnerabilities: does anyone care?” In: *arXiv*.

Pesaran, M. H. and Shin, Y. (1999). “An Autoregressive Distributed Lag Modelling Approach to Cointegration Analysis”. In: *Econometrics and Economic Theory in the 20th century*. Cambridge University Press, pp. 371–413. DOI: 10.1017/CCOL521633230.011.

Pesaran, M. H., Shin, Y., and Smith, R. J. (2001). “Bounds testing approaches to the analysis of level relationships”. In: *Journal of Applied Econometrics* 16.3, pp. 289–326. DOI: 10.1002/jae.616.

Pieters, G. and Vivanco, S. (2017). “Financial regulations and price inconsistencies across Bitcoin markets”. In: *Information Economics and Policy* 39, pp. 85–96.

Raskin, M., Saleh, F., and Yermack, D. (2019). *How do private digital currencies affect government policy?* Working paper 26219. National Bureau of Economic Research.

Reijers, W. and Coeckelbergh, M. (2018). “The blockchain as a narrative technology: investigating the social ontology and normative configurations of cryptocurrencies”. In: *Philosophy and Technology* 3, pp. 103–130.

Rinehart, L. M. et al. (2004). “An assessment of supplier-customer relationships”. In: *Journal of Business Logistics* 25.1, pp. 25–62.

Ritter, J. R. and Welch, I. (2002). “A review of IPO activity, pricing and allocations”. In: *The Journal of Finance* 57.4, pp. 1795–1827.

Robb, A. M. and Robinson, D. T. (2014). “The capital structure decisions of new firms”. In: *Review of Financial Studes* 27.1, pp. 153–179.

Rocket, T. (2018). *Snowflake to avalanche: a novel metastable consensus protocol family for cryptocurrencies*. White paper. Avalanche.

Roubini, N. (2018). *Exploring the cyptocurrency and blockchain ecosystem*. Speech. Testimony for the Hearing of the US Senate Committee on Banking, Housing and Community Affairs.

Ruthberg, Z. G. and Polk, W. T. (1989). *Report on the invitational workshop on data integrity*. Tech. rep. National Institute of Standards and Technology. DOI: 10.6028/nist.sp.500-168.

Saito, K. and Iwamura, M. (2019). “How to make a digital currency on a blockchain stable”. In: *Future Generation Computer Systems* 100, pp. 58–59.

Sayeed, S. and Marco-Gisbert, H. (2019). “Assessing blockchain consensus and security mechanisms against the 51% attack”. In: *Applied Sciences* 9.9, p. 1788. DOI: 10.3390/app9091788.

Schneider, J. et al. (2016). *Blockchain. Putting theory into practice.* Tech. rep. Goldman Sachs. URL: https://perma.cc/YZ8U-2AKP.

Schneider, N. (2019). “Decentralization: an incomplete ambition”. In: *Journal of Cultural Economy* 12.4, pp. 265–285.

Schreft, S. (1997). “Looking forward: the role for government in regulating electronic cash”. In: *Economic Review* 82.4, pp. 59–84.

Schrijvers, O. et al. (2017). “Incentive Compatibility of Bitcoin Mining Pool Reward Functions”. In: *Financial Cryptography and Data Security.* Ed. by J. Grossklags and B. Preneel. Berlin, Heidelberg: Springer, pp. 477–498. ISBN: 978-3-662-54970-4.

Schumpeter, J. A. (1934). *The Theory of Economic Development: An Inquiry into Profits, Capital, Credit, Interest and the Business Cycle.* London: Transaction Publishers.

SEC (2017). *Report of investigation pursuant to section 21(a) of the securities exchange act of 1934: The DAO.* Release 81207. Securities and Exchange Commission.

— (2018a). *Order instituting cease-and-desist proceedings pursuant to section 8A of the Securities Act of 1933, making findings, and imposing penalties and a cease-and-desist order.* Release 10575. Securities and Exchange Commission.

— (2018b). *Order instituting cease-and-desist proceedings pursuant to section 8A of the Securities Act of 1933, making finds and imposing penalities and a cease-and-desist order.* Release 10574. Securities and Exchange Commission.

Shafagh, H. et al. (2017). “Towards blockchain-based auditable storage and sharing of IoT dat”. In: *Proceedings of the 2017 on Cloud Computing Security Workshop.* CSSW ’17. Association for Computing Machinery, pp. 45–50.

Shaw, A. W. (1912). “Problems in market distribution”. In: *The Quarterly Journal of Economics* 26.4, pp. 703–765.

Smith, A. (1776). *An Inquiry into the Nature and Causes of the Wealth of Nations.* London: Methuen and Co., Ltd.

Sookhak, M. et al. (2015). "Remote data auditing in cloud computing environments: a survey, taxonomy, and open issues". In: *ACM Comput. Surv.* 47.4, pp. 1–34. ISSN: 0360-0300. DOI: 10.1145/2764465.

Spulber, D. (1996). "Market microstructure and intermediation". In: *Journal of Economic Perspectives* 10.3, pp. 135–152.

Stigler, G. J. (1957). "Perfect competition, historicalyl contemplated". In: *Journal of Political Economy* 75.1, pp. 1–17.

— (1961). "The economics of information". In: *Journal of Political Economy* 69.3, pp. 213–225.

Sun, J., Yan, J., and Zhang, K. Z. K. (2016). "Blockchain-based sharing services: what blockchain can contribute to smart cities". In: *Financial Innovation* 2.26, pp. 1–9.

Szabo, N. (1994). *Smart contracts.* http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. Accessed: 2018-11-13.

Tartan, C. et al. (2021). "A scalable Bitcoin-based public key certificate management system". In: *Proceedings of the 18th International Conference on Security and Cryptography - SECRYPT.* INSTICC. SciTePress, pp. 548–559. ISBN: 978-989-758-524-1. DOI: 10.5220/0010556805480559.

Tasca, P., Thanabalasingham, T., and Tessone, C. J. (2017). "Ontology of Blockchain technologies. Principles of identification and classification". In: *arXiv.*

Tocqueville, A. d. (1838). *Democracy in America.* New York: G. Dearborn and Co.

Treiblmaier, H. (2019). "The impact of the blockchain on the supply chain: a theory-based research framework and a call for action". In: *Supply Chain Management: An International Journal* 23.6, pp. 545–559.

Treleaven, P. and Batrinca, B. (2017). "Algorithmic regulation: automating financial compliance monitoring and regulation using AI and blockchain". In: *Journal of financial transformation*, pp. 14–21.

Tu, Z. and Xue, C. (2018). "Effect of bifurcation on the interaction between Bitcoin and Litecoin". In: *Finance Research Letters* 31, pp. 382–385.

Tucker, C. and Catalini, C. (2018). "What blockchain can't do". In: *Harvard Business Review* hbr.org. URL: https://hbr.org/2018/06/what-blockchain-cant-do.

Urquhart, A. and Zhang, H. (2019). “Is Bitcoin a hedge or safe haven for currencies? An intraday analysis”. In: *International Review of Financial Analysis* 63, pp. 49–57. DOI: 10.1016/j.irfa.2019.02.009.

Vandezande, N. (2017). “Virtual currencies under EU anti-money laundering law”. In: *Computer Law and Security Review* 33, pp. 341–353.

Vergne, J.-P. and Durand, R. (2010). “The missing link between the theory and empirics of path dependence: conceptual clarification, testability issue, and methodological implications”. In: *Journal of Management Studies* 47.4, pp. 736–759.

Vernik, D. A., Purohit, D., and Desai, P. S. (2011). “Music downloads and the flip side of digital rights management”. In: *Marketing Science* 30.6, pp. 1011–1027.

Vukolić, M. (2016). “The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication”. In: *Open Problems in Network Security*. Ed. by J. Camenisch and D. Kesdoğan. Cham: Springer International Publishing, pp. 112–125. ISBN: 978-3-319-39028-4.

Wadsworth, A. (2018). *Decrypting the role of distributed ledger technology in payments processes*. Tech. rep. Reserve Bank of New Zealand.

Williamson, O. E. (1975). *Markets and hierarchies, analysis and antitrust implications: a study in the economics of internal organization*. Free Press.

— (1985). *The economic institutions of capitalism*. Simon and Schuster.

Wright, C. S. (2019). *Proof of (unregistered) security*. Internet blog. URL: https://medium.com/@craig_10243/proof-of-unregistered-security-798f4df2fbb9.

Wust, K. and Gervais, A. (2018). “Do you need a blockchain?” In: *Crypto Valley Conference on Blockchain technology*.

Xu, M., Chen, X., and Kou, G. (2019). “A systematic review of blockchain”. In: *Financial Innovation* 5, p. 27. ISSN: 2199-4730. DOI: 10.1186/s40854-019-0147-z. URL: https://doi.org/10.1186/s40854-019-0147-z.

Yli-Huuomo, J. et al. (2016). “Where is current research on blockchain technology? A systematic review”. In: *PLoS ONE* 11.10. Ed. by H. Song.

Zetzsche, D. A., Arner, D. W., and Buckley, R. P. (2020). “Decentralized finance”. In: *Journal of financial regulation* 6, pp. 172–203. DOI: 10.1093/jfr/fjaa010.

Zhao, J. L., Fan, S., and Yan, J. (2016). “Overview of business innovations and research opportunities in blockchain and introduction to the special issue”. In: *Financial Innovation* 2.1, pp. 1–7.

Zheng, Z et al. (2018). “Blockchain challenges and opportunities: a survey”. In: *International Journal Web and Grid Services* 14.4, pp. 352–375.

Zikratov, I. et al. (2017). “Ensuring data integrity using blockchain technology”. In: *20th Conference of Open Innovations Association (FRUCT)*. IEEE, pp. 534–539. DOI: 10.23919/fruct.2017.8071359.