Digital Currencies: Principles, Trends, Opportunities, and Risks

Paolo Tasca

Deutsche Bundesbank and ECUREX Research

Summary:

The report describes the ongoing innovations in the financial sector brought about by digital currencies from a multi-level perspective: systemic, technical, legal, and industrial. The report extensively covers the current trends in the domain, in order to give the reader a quantitative understanding of the potential opportunities and risks arising from the global adoption of digital currencies.

With the support of:

James B. Glattfelder

ECUREX Research and University of Zurich, Department of Banking & Finance

Nicolas Perony

ECUREX Research and Tamedia Digital

Correspondence to: Paolo Tasca.

Current Affiliations:

(1) **Deutsche Bundesbank**, Frankfurt am Main, Germany.
E-Mail: paolo.tasca@bundesbank.de

(2) **ECUREX Research**, Zurich, Switzerland.
E-Mail: tasca@ecurex.com

ECUREX Research Working Paper, 7th of September 2015 (version: October 2015)

Contents

1 EXECUTIVE SUMMARY

1.1 BLOCKCHAIN TECHNOLOGIES

In the last century, global business and trade have been facilitated by successive technological revolutions that brought down manyfold the costs of transportation, manufacturing, and, more recently, communication on a global scale. The next frontier on the journey to a truly globalised economy lies in overcoming the difficulty and costs of developing, maintaining and securing financial relationships between agents on a global scale. While the solution to this problem has traditionally relied on central authorities, the advent of distributed-consensus ledgers on peer-to-peer networks has brought a new, reliable way to handle any interaction requiring trust, proof and contract enforceability. These technologies are often referred to as "blockchain technologies". Advances in cryptography, global connectivity, and computing power have led to infrastructures that allow for the creation of such trust-less disintermediated and decentralised markets. These advances represent a significant forward leap for economics, as they have the potential to significantly reduce the architectures that traditionally oversee the correct and smooth operation of those markets. Generally, blockchain technologies can simplify the operation of markets relying on at least one of the following mechanisms: 1) intermediation; 2) clearing and settlement; 3) recording systems; 4) rating or voting systems; 5) database systems; 6) distributed storage, authentication, anonymisation of private information; 7) rewarding and punishing incentive schemes; 8) transaction traceability schemes; 9) refereeing, arbitration or notarisation. To this day, the most popular application of blockchain technologies has been Bitcoin, the first decentralised digital currency, which provides a solution to the problem of trust in a currency system. In this report, we explore in detail the current innovations brought about by Bitcoin and other digital currencies, and discuss the ongoing and future effects of these innovations.

1.2 MOTIVATION FOR THIS REPORT

Since the introduction of Bitcoin in 2009, an enormous amount of information has been produced about digital currencies, often in the form of short articles, which suffer from a lack of investigative depth and technical knowledge. This report is the first comprehensive study on digital currencies that provides **a joint, deep quantitative analysis of their technological, entrepreneurial, economic, and legal aspects**.

It is the result of over 2 years of work, including an extensive monitoring of the digital currency markets, involving the collection and analysis of **data from over 30 different sources**.

Our analysis is summarised in **over 60 different descriptive statistics** and exposes original results on the (in)efficiency and dynamics of digital currency markets. The report is primarily intended for readers with some preliminary knowledge of Bitcoin technology; however, through the introduction of many fundamental notions and the support of a large number of self-explanatory charts and tables, anyone will be able to appreciate the breadth and depth of the analysis presented here. Due to its interdisciplinarity, the report is relevant to different readerships: (1) *technologists*, who wish to know more about the legal nature of digital currencies and their market dynamics; (2) *economists*, who wish to deeply explore the digital currency ecosystem and acquire, at the same time, some technical and legal understanding; (3) *legal practitioners*, who want to have an overview of the regulatory issues relevant to digital currencies, in addition to understanding market threats and opportunities.

1.3 KEY FINDINGS

The most important key findings are summarised here. For the original research and details on the data sources, see the corresponding sections in the main text.

- **The average amount transferred per Bitcoin transaction is larger than in any other major payment network.** During the period 2011–2015, the average amount (in USD equivalent) per transaction constantly increased, and since 2013 it remained larger than in the major payment networks such as Visa, Mastercard, Discover, or Western Union. Although the Bitcoin payment network is getting closer in total transaction volume to these large networks, its daily transaction volume of ca. USD 50 million (about one quarter of Western Union's) is still the lowest one.

- **The relative capitalisation of Bitcoin with regard to other digital currencies is receding in favour of Ripple's.** Until mid-2014, Bitcoin dominated the digital currency market by covering up to 95% of its total volume. Since then, its dominant position has been eroded by Ripple, which now covers about 10% of the total market capitalisation. On average, the relative currency strength of Bitcoin has decreased compared to that of the other (almost) existing 500 digital currencies, even though Bitcoin remains dominant on the digital currency market.

- **China is the largest country in the world** per: (1) number of active Bitcoin clients; (2) mining capacity (since the end of 2014, Chinese mining pools cover 50% of the total market share); (3) volume of Bitcoins exchanged via electronic trading platforms (since 2014,

the traded CNY/BTC volume in is about 3 times larger than the USD/BTC volume, with peaks at BTC 4 million per week).

- **Bitcoin startups raised almost USD 1 billion in three years with an annual investment growth rate of about 150%.** Capital investments in Bitcoin-related startups is a recent trend that started in the first quarter of 2012. Since then, the Bitcoin industry raised almost USD 1 billion and it represents the fastest growing sector for capital investment. Within the Bitcoin sector, the Mining and Payment & Remittance industries drove the funding race. 21 Inc alone covered over half of the capital raised by the Mining industry, and Coinbase one third of the capital raised by the whole Payment & Remittance industry.

- **In January 2015 the Bitcoin volume exchanged on electronic trading platforms reached 50% of the total number of Bitcoins ever mined at that time.** At two points in mid-2014 and January 2015n the volume of Bitcoins exchanged via electronic trading platforms reached a historical high equivalent to over half of the number of Bitcoins that had been mined at that time. Since then, the volume of Bitcoins traded on electronic exchanges has remained stable at a higher value than the volume of transactions between users, recorded in the public Bitcoin blockchain.

- **During the year 2014, the transaction costs in digital currencies dropped significantly**. Throughout 2014, the average fee per Bitcoin (Litecoin) transaction decreased from about USD 20 (7) cents to USD 10 (1) cents.

- **The year 2014 saw fewer incidences and less arbitrage opportunities than the previous years. In effect, the digital currency market is becoming more efficient.** Since 2011, Bitcoin's volatility has been constantly decreasing. In addition, the likelihood and intensity of arbitrage opportunities dramatically dropped to less than 1%, signalling that the digital currency exchange markets are becoming more efficient.

- **The wealth distribution in the Bitcoin ecosystem is highly unequal, and this inequality is growing**. The inequality of the distribution of Bitcoins amongst addresses, summarised by the Gini coefficient (higher is more unequal), grew from 0.09 in 2010 to 0.99 in 2015: from quasi-perfect equality to quasi-perfect inequality. However, this is not a "rich get richer" phenomenon. During the period 2009–2015, the top 100 richest addresses kept a constant relative wealth, totalling about 20% of the total value of the Bitcoin economy. The increase in the inequality is the result of: (1) a socio-economic phenomenon, due to the growing popularity of Bitcoin, and (2) wallet fragmentation due to security practices such as single-use addresses and new addresses generated for change transactions.

- **The Mining industry is consolidating as an oligopoly.** The Bitcoin mining market is currently under control by 5 to 7 major mining pools. During the period 2013-2015, the cumulative market share of the largest 10 pools relative to the total market hovered in the 70%–80% range.

2 INTRODUCTION

People familiar with technology often refer to the 1965 prediction of exponential growth by Intel co-founder Gordon Moore, who envisioned that the power of central processing units in our computers would double every two years. Many predicted this would be a short-term phenomenon. Yet exactly 50 years later, this prediction still holds. Every couple of years the world witnesses a technological revolution, aiming at improving the quality of life in our society. There has truly been an explosion in the adoption of personal computers, smartphones, tablets, and, in parallel, the widespread dissemination of the Internet with cloud computing, and other disruptive technologies. The latest such innovation seems to be the arrival of peer-to-peer (P2P) network-based technologies. These technologies are dramatically transforming our economic systems, and our society in general, into something very different from what we were used to thinking about over the last few decades. This technology shift is enabling a rapid transition towards what is known as the economy of *Collaborative Commons*, (CC): a digital space where providers and users share goods and services at close to zero marginal cost. According to Jeremy Rifkin [1], CC are transforming the way we organise our economic life with the potential of dramatically narrowing the income divide, democratising the global economy, and creating a more ecologically sustainable society. Indeed, CC already disrupted the "information goods" industries (e.g., recording industry, film and television, newspapers and magazines, and book publishing) as consumers turned into prosumers[1] and started to produce and share their own content for free as CC on the Internet: from music, videos, news, to knowledge. At the same time, consumers already started some years ago to share services and products for free. All over the world, younger generations share bikes, automobiles, homes, clothes, and countless other items, preferring access over ownership. The financial system is not immune to this abrupt impact of Information and Communication Technology (ICT) on consumer behaviour. Crowdfunding, peer-to-peer lending, *e*wallets, digital currencies or interoperable payment infrastructures are some of the new disruptive forms of finance that are influencing

[1] The term was coined by futurologist Alvin Toffler in 1980 in his book "The Third Wave" [2]. A portmanteau of "proactive consumer", a prosumer is a common consumer who would become active in the production process and personally help to improve or design the goods and services of the marketplace.

our everyday lives and are transforming the way we, as a society, interact and conduct business. More broadly, we are leaving the era of what has been called e-finance[2] and are entering into the era of peer-to-peer (P2P) finance. Allen et al. [3] define e-finance as: "The provision of financial services and markets using electronic communication and computation." The term e-finance includes mobile and digital financial services (online banking, Internet transactions, online trading). P2P finance can instead be understood as:

> *"The provision of financial services directly by end-users to end-users using computer-based and network-based information and communication technologies."*

P2P finance is indeed based on information communication technologies, cryptography, open source computing methods, time-stamped ledgers, and peer-to-peer distributed networks that allow end-users direct anonymous, disintermediated and secure access to assets, payments and financial services. By observing the current trend in financial innovation, in the near future we envision a landscape where disruptive technology will create more agile and disintermediated financial systems. The evolution towards P2P financial markets will gradually remove costly intermediation layers fostering financial inclusion and will also reduce the dependence on cash.[3] However, P2P financial markets will also pose new challenges for current legal systems, issues related to the safety and soundness of regulation, next to competition policy, consumer and investor protection, and global public policy. Specific issues include: (1) the emergence of new forms of fraud and cybercrimes; (2) uncontrolled herding behaviour and excessive firm concentration, thereby creating market distortions with potentially disastrous repercussions on the real economy; (3) bubble dynamics; (4) preferential use by terrorists and criminals to conduct untraceable transactions. Among the different P2P financial instruments, this report will focus on *digital currencies*. Despite its name, a digital currency, (also known as electronic currency, cryptocurrency, or virtual currency) is not only a digital medium of exchange (a token) that acts as money, but also a decentralised payment system. The seminal white paper by the anonymous writer(s) under the pseudonym of Satoshi Nakamoto [9] explains how the technology works. Basically digital currencies are founded on: (1) decentralised peer-validated time-stamped ledgers (instead of trust-based centralised ledgers); (2) crypto-

[2] This is a concept introduced at the beginning of the new millennium by Allen at al. [3] and Shahrokhi [4].

[3] Indeed, the idea of dispensing with cash in favour of alternative, more efficient means of payments is not new. Pre-1900 utopian thinkers devoted a lot of effort to finding a way to allow people to get rid of what Robert Owen called the "insane money-mystery" [5]. In more recent years, economists have also begun to study the implications of living in cashless societies, especially referring to the role of central banks and to the conduct of monetary policy, [6] [7] [8].

graphic hash function message encryptions;[4] and (3) proof-of-concept principles. These features allow for: (1) anonymous and trust-less peer-to-peer network transactions; (2) authenticity verification of the network transactions and automatic bookkeeping of the public ledgers; (3) expansion of the total amount of coins (i.e., monetary base) at a constant (or controlled) pace. The first of these digital currencies, and still the most prominent at the time of writing, is Bitcoin. In the next sections we will describe key technical, economic and legal innovations that characterise digital currencies in general and Bitcoin in particular by supporting our analysis with descriptive statistics in order to provide the reader with a global picture of the current market situation and with the sense of the possible future market trends.

3 DIGITAL CURRENCIES: WHAT THEY ARE AND HOW THEY WORK

This section provides a description of the key technical and economic features characterising digital currency as both money and payment systems. Money and payment systems are intrinsically connected because the former provide the accounting unit needed to update the ledgers of both senders and receivers; the later instead provide the plumbing infrastructures that allow for a secure transfer of money. Modern payment systems are supported by data servers connected by encrypted interface data processing centres where money practically exists only as digital records on commercial bank accounts.[5] For the first time in history, digital currency schemes combine the features of payment systems and currencies. This novelty is brought about by the introduction of distributed ledger technology and a cryptographic protocol. As we will explain below, this innovation allows money to be moved around as *information* within payment systems that operate in a decentralised way, i.e., without the need for any intermediary third party or central authority.

Digital currencies are money expressed as a string of bits sent as a message in a network that verifies the authenticity of the message via different mechanisms, such as proof-of-work (PoW) or proof-of-stake (PoS) that we briefly explain here below. Most digital currencies exhibit a publicly visible distributed ledger which is shared across a computing network. What distinguishes each digital currency is the process by which its users agree on changes to its ledger (in other words, which transactions to accept as valid) and the mechanism according to which the validation process is rewarded. The first ever invented time-stamping scheme is

[4] Indeed, there currently exist some digital currencies that do not rely on cryptographic techniques (such as Ripple), however, all cryptocurrencies are digital currencies.

[5] For example, only about 10% of the US broad money supply (M2) consists of physical coins and paper money.

the PoW scheme by Satoshi [9].[6] This is the first credible decentralised file-to-system solution that solves an old problem in computer science, called the Byzantine Generals' Problem, of ordering transactions in a decentralised network.[7] The most widely used PoW schemes (also called protocols or functions) are based on the *SHA-256* hash function, which was introduced by Bitcoin, and *scrypt*, which is used by currencies such as Litecoin. Indeed, the latter currently dominates the world of digital currencies, with about 500 confirmed implementations [12].

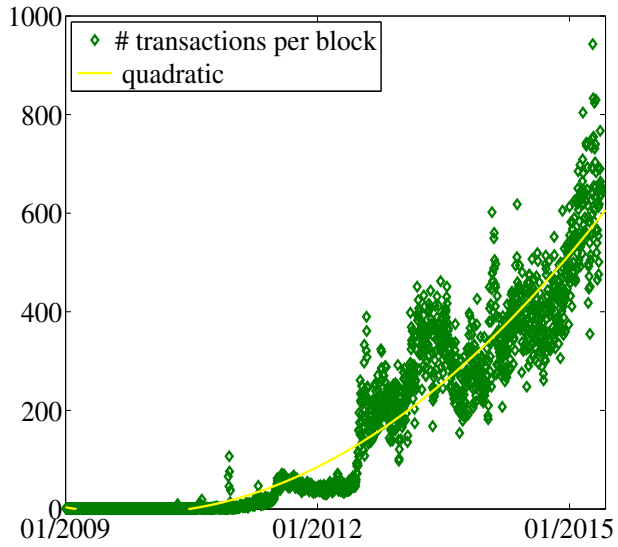

FIGURE 1: Number of average Bitcoin transactions in a single block. Data source: Blockchain.info. Internal calculation.

Some currencies support the PoW and PoS schemes in parallel. In general, a PoW scheme is used to deter denial of service attacks and other abuses such as spam on a network by requiring some "work" to be done by the user (or requester, if different from the user) of the service. The "work" usually consists of the user's computer expending processing power. A key characteristic of such schemes lies in their asymmetry: the work must be appropriately challenging but still feasible on the user side but very easy to check for the service provider. Applied to digital currencies, PoW is the combination of two ideas: (1) to (deliberately) make it computationally costly for network users to validate transactions; and (2) to reward them for their work trying to help validate transactions. The PoS protocol is a method of securing the network (also used to validate transactions) and it is based on the concept of "coin age" (the product of the currency

[6] Following Satoshi Nakamoto's seminal paper on Bitcoin [9], technologists have been extensively writing on the digital currency cryptographic protocols and their technical aspects. For example we refer the reader to the book by [10].

[7] A reliable network-based system must be able to cope with the failure of one or more of its components. A failed/corrupted component may exhibit a behaviour that may be overlooked, i.e., it may send conflicting information to different parts of the system. The problem of coping with such failure is formalised as the Byzantine Generals Problem. In this problem, Byzantine army generals can communicate only by messenger. By observing the enemy, they must choose a common plan of action. In effect, all generals must devise an algorithm to guarantee that: (1) the loyal generals decide upon the same plan of action; (2) a small number of traitors cannot cause the loyal generals to adopt a bad plan [11]. Indeed, Bitcoin doesn't solve this problem in the general case, but only under the simplifying assumption that the attackers are computationally limited (i.e., they have less than 51% of hash-power).

amount which is held and the length of time it has been held for). When generating a PoS block, the users send some money to themselves, consuming their coin age in exchange for a preset reward as a percentage of the "staked" coins.[8] How transactions of digital currencies for fiat money or services and goods occur via registrations on the public ledgers is explained here [10]. However, the basic process is as follows. Let us imagine that Alice (A) wants to give Bob (B) a digital currency, for example one Bitcoin. Since digital currencies are based on money-as-information concept, the transfer of one Bitcoin from A to B is similar to a string of bits where A writes the message "I, A, am giving B one Bitcoin with serial number 123456". To this message, A attaches a code that will act as a signature: A takes the hash of the message and encrypts the message with a private key (k). Therefore, the signature depends on the content of the message and on k and it is generated via a signing algorithm.

Finally, A will send to B the message together with the signature and the public key (K).[9] To practically send the message to B, A needs to know B's Bitcoin address.[10] Through the presentation of the message, the signature and K, B (upon verification by other members in the Bitcoin network who must confirm that A indeed owns the Bitcoin at the time of the transfer) can accept the transaction as valid.[11] B hashes the original message, and with the help of K, unencrypts the originally signed data. If the two hashes are equivalent the signature is valid and message authentication, non-repudiation and integrity will be granted. Before moving on to explain how the transaction from A to B happens, we will describe in general terms how the public ledger works. Every node in the network collectively composes a "decentralised" bank that book keeps a unique public ledger called the *blockchain*. Each node provides serial numbers for Bitcoins, keeps track of who has which Bitcoins, verifies that transactions are legitimate and registers in the ledger the passage of messages between users. The blockchain is a decentralised ledger that allows the current balance of each address to be recovered according to a *cash-flow* approach because the blockchain contains all the transactions ever to occur in the Bitcoin network. Then, to continue with the description of the transaction from A to B,

[8] Block rewarding from mining will drop near zero in the long run, at least for Bitcoin. Therefore, some see the PoS as a remedy to the *tragedy of the commons* in which very few honest miners are willing to mine [13].

[9] By elliptic curve multiplication (a one-way cryptographic function), public keys can be generated from private keys.

[10] A Bitcoin address is simply a string of digits and characters that can be shared with anyone and used to send Bitcoins to. Addresses are produced from public keys by using one-way cryptographic hash functions.

[11] Ownership of Bitcoins is established through the possession of k that is automatically generated (also offline and independently from the Bitcoin protocol) and stored in a file called a wallet via software called a Bitcoin client. A must keep k secret at all times, as revealing it to third parties is equivalent to giving them control over the Bitcoins secured by k. Any accidental loss of k must also be prevented, otherwise funds linked and secured by it are lost as well.

in the next step we describe the verification process. B, who keeps a copy of the block chain, does a sanity check that the Bitcoin with serial number 123456 belongs indeed to A. If this is the case, B will broadcast the signed string of bits to the entire network and other nodes in the network will collectively verify whether A holds one Bitcoin with serial number 123456. Now imagine that David (D) is one of the users in the Bitcoin network receiving the message "I, A, am giving B one Bitcoin with serial number 123456" and queuing it together with other messages recently received that must be digested (pending transactions of the last 10 minutes not yet approved by the network). Together, all these transactions form a so-called "transaction block". To give the reader an idea of the the effort devoted by the miners to validate the Bitcoin transaction blocks, we analyse and plot the data provided by [14] on the number of Bitcoin transactions over the past few years.

As one may directly observe from Figure 1, the number of transactions has increased vastly by three orders of magnitude since 2010. At this point it is worth mentioning that there are in fact no "Bitcoin-specific serial numbers". So, formally it is not correct to say "I, A, am giving B one Bitcoin with serial number 123456". Instead, there are transactions that reference other previous specific transactions. Thus, the serial number 123456 actually contains references to previous transactions (inputs) with which A received at least one Bitcoin that is now being transferred to B. The verification process now checks if the inputs are sufficient in order for A to transfer one Bitcoin to B. With his copy of the blockchain and the public keys, D can verify that each transaction in his block is valid. However, D must solve an NP-hard computational puzzle before broadcasting to the network the validity of the transactions. This is the so-called PoW principle explained above that is at the heart of the mining process: mining is indeed a competition among users to approve transactions.[12] D needs to compute new hash values based on the combination of the

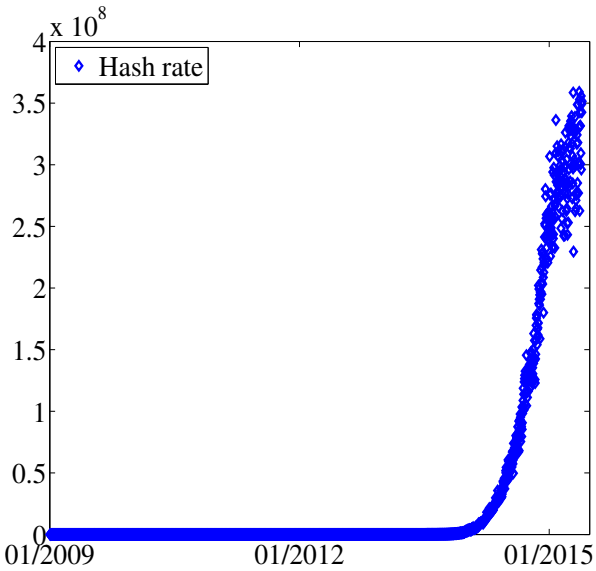

FIGURE 2: Estimated number of giga hashes per second (billions of hashes per second) the Bitcoin network is performing. Data source: Blockchain.info. Internal calculation.

[12] A miner's chance of winning the competition is roughly equal to the proportion of the total computing power controlled by the competing other miners. Therefore, specific hardwares and new production mechanisms have

previous hash values contained in the message, the new transaction block and a *nonce* (an arbitrary number used only once), such that the new hash value will start with a given number of zeros that is less than or equal to the *target*. The target number is automatically adjusted by the Bitcoin protocol to ensure that a Bitcoin block takes an average of about ten minutes to validate.[13] Thus, a larger computing power (i.e, network hashing rate) generates a higher mining difficulty rate, seen in Figure 2. If D finds the suitable nonce, he will broadcast the message "*Yes, A owns one Bitcoin with serial number 123456 and it can be transferred to B*" together with the other transactions in the transaction block and the nonce (so that the network can verify the validity). D will be rewarded for the mining activity because each transaction block contains a *coinbase transaction*[14] that pays (currently) 25 BTC to the winning miner to a newly created address in D's name. Finally, everyone updates their copy of the blockchain to show that one Bitcoin having the serial number 123456 now belongs to B, and the transaction is complete. Notice that, although BTC does not comply with the ISO 4217 currency code standards, in the following we borrow the practice in use within the Bitcoin community which continues using BTC as a unit name and code currency [15]. The same rule applies also for other coins (for example the currency code for Litecoin is LTC).

4 SECURE, FAST, TRACEABLE AND LOW-COST PAYMENT NETWORK

The evolution of the means of payment has continually been addressing broader business needs. Prior to the advent of the Internet, payments were simpler than what they are now. They were also not so fundamental to personal finance and people made significantly fewer transactions than nowadays. The majority of payments were proxies for cash transactions. Alternatively, simple instruments like cheques or traveller's cheques were used. Those instruments were the prevalent means of payment and people did not travel enough or did not buy enough products or transfer enough money from one country or jurisdiction to another to justify global, systemic, fast and costless payment infrastructures. The Internet opened the doors to new ways of transferring goods (i.e., e-commerce) and new ways of downloading or accessing services

been introduced during the last years in order to speed-up the puzzle-solving capacity of the miners, see Section 11.

[13] The target is a 256-bit number that all Bitcoin clients share. Each hash simply returns a random number between 0 and the maximum value of a 256-bit number. If D finds a hash below the target, then he/she wins. If not, he/she needs to increment the nonce (thus completely changing the hash) and try again.

[14] A unique transaction with no inputs that can only be created by a miner.

in a rapid and global scale. The result was an increase of the frequency of the number of international transfers and an increase of international transactions per user. Since the 1980s, credit cards and international wire transfer systems like SWIFT have been the primary methods for initiating and receiving electronic cross-border payments. However, within individual countries, payers and payees used different electronic payment systems. For example in the US, there exists the Automated Clearing House (ACH) system[15] and in EU there is the direct debit system [17]. Direct debits are made under each country's rules. They usually restricted to domestic transactions in those countries. An exception since 2010 is the implementation of the Single Euro Payments Area (SEPA) which allows for Euro-denominated cross-border (and domestic) direct debits [18]. With the expansion of Internet-based activities and trades, it became necessary to provide new methodologies to connect a disparate group of international payment systems. Thus, Payment as a Service (PaaS) solutions like Paypal have been developed. These solutions represent a layer – or overlay – that resides on top of the various systems and allows the two-way communication between the payment system and the PaaS. Communication is governed by standard APIs created by the PaaS provider. However, these solutions are built on the bedrock of banks and come with cost and legacy problems. Under this framework, banks lost the front-end but continued to be central by providing back-end infrastructure in the form of accounts, security and compliance. Thus, alternative blockchain-based payment networks have been recently developed in order to provide a worldwide settlement framework which grants faster, cheaper and secured cross-border payments. These methods have back-ends relying only on decentralised consensus protocols like Bitcoin or Ripple which will be explained in Section 12.4.[16] These solutions allow for domestic and international payments, in any combination of currencies, which can then be settled directly between the parties without the need for credit cards, central clearing houses or correspondent banks. Their socio-economic impact is even better understood if we recall that recent studies show that cross-border shopping and remittances will continue to grow at a fast pace during the next

[15] ACH is a clearing and settlement system which processes the exchange of electronic transactions between participating US depository institutions [16].

[16] For example, BitPesa is an international remittance system based on the Bitcoin protocol. BitPesa allows users to send money to and from Kenya and Tanzania. It accepts Bitcoin from nearly anywhere in the world and exchanges it for Kenyan and Tanzanian Shillings into a Kenyan or Tanzanian mobile money wallet (M-Pesa, Tigo, Orange, Airtel, or Yu) [19].

years.[17]

4.1 FAST AND CHEAP TRANSACTIONS

Transactions in the blockchain-based networks take place at almost zero cost (independently from the amount transferred) and are confirmed within seconds or maximum few minutes (independently from the distance between sender and receiver and independently from their jurisdiction of residence). Unlike the traditional payment infrastructure supporting credit cards, money transmitters or international bank wire transfers (e.g., via SWIFT), digital currencies are not bound by rules or legal status of any one government's currency.[18] Digital currency transfers can therefore be costless because transactions are not subject to middle-man activity, exchange rates, interest rates, and specific country-to-country transaction fees. To give an idea, in the Bitcoin network a typical transaction size is 500 bytes and the corresponding transaction fee for a low-priority transaction is 0.1 mBTC (i.e., 0.0001 BTC), irrespective of the number of coins sent [22]. The left plot in Figure 3 represents the average confirmation time in minutes for a transaction from one user to another in both the Bitcoin and Litecoin networks. We also compute the average cost per transaction during 2014 for both the Bitcoin and Litecoin networks, see Figure 3 (right). The formula is:

$$\text{Average cost per transaction} = \frac{\text{Daily transaction fee in coins earned by miners}}{\text{Nr. of unique daily transactions}} \times Ex \quad (1)$$

where Ex is the average exchange rate (BTC/USD and LTC/USD) taken from different trading platforms (OKCoin, BTC-e, Bitfinex, Cex.io, Hitbtc, The Rock trading, Cryptsy, Crypto-Trade, Bter, Kraken, EXMO, Bitkonan, Indacoin, Vircurex, emeBTC, LiteTree, CCEDK, UseCryptos, Prelude, Comfort, C-Cex, upBit, Cryptonit).

4.2 SECURE AND IRREVERSIBLE TRANSACTIONS

What also distinguish blockchain-based payment methods from many others like Paypal or credit/debit cards (and even bank wires up to a certain limit) is the irreversibility (undoing) of transactions. On this aspect, we refer the reader to the May Scale of money hardness [23]. This means that a transaction of a digital currency from A to B cannot be undone. Instead, a new

[17] According to Paypal, in 2018 we will spend over USD 307 billion in cross-border shopping. In 2013 we spent USD 105 billion [20]. Moreover, the remittance industry is a global business that despite the current global economic slump has continued to grow. From USD 234 billion in 2004 to USD 534 billion in 2012 and is expected to grow to USD 685 billion by 2015 [21].

[18] Also financial settlement systems adopted by central banks (e.g., CHAPS, TARGET2 and Fedwire) are relatively expensive and suffer from high legacy and stagnant costs.

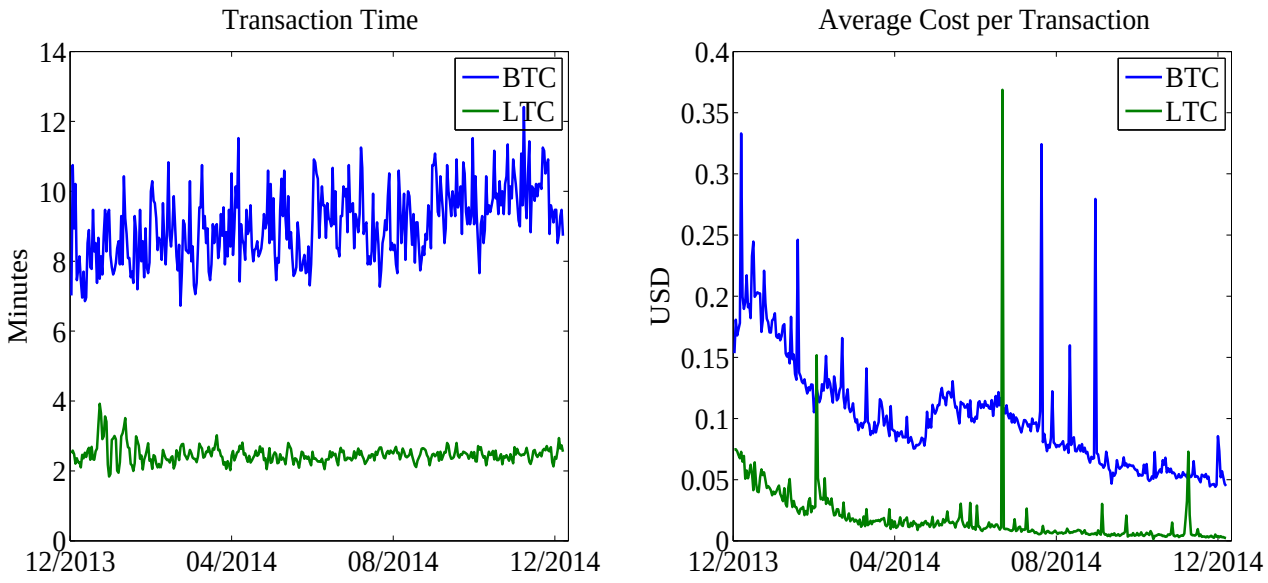

FIGURE 3: Average confirmation time in minutes and average transaction cost in USD. Data source: Bitinfocharts, Cryptocoincharts. Internal calculation.

transaction from B to A has to be generated. It is indeed debatable if this is a good or bad feature. On the one hand, irreversibility may be a good feature if considered from the side of the seller who is expecting to be paid for his service or product without exceptions. On the other hand, if seen from the side of the buyer, irreversibility may be considered a bad feature because the purchase may be unwanted or mistaken. Although buyers and sellers can always voluntarily agree to correct errors, generally blockchain-based payment networks like Bitcoin do not offer built-in mechanisms to undo errors. Moreover, another major characteristic that puts blockchain-based payment networks on a different level compared to traditional networks is the use of time-stamped concatenated blocks of transactions. The PoW and PoS principles, combined with block time-stamping, prevent the so-called double-spending[19] by allowing all users to eventually impose a global ordering on transactions, and by maintaining a list of unspent transaction outputs and validating a transaction only if its input addresses appear in that list.

4.3 TRACEABILITY AND ACCOUNTABILITY

All transactions in Bitcoin-like networks are digitally signed to ensure non-repudiation (verifiability). However, each transaction also needs to be transparent (for accountability). At the outset these two objectives may seem contradictory to each other. However, these features

[19] Double-spending occurs when a dishonest user tries to execute rapid multiple transactions before the blockchain is updated, see Section 3.

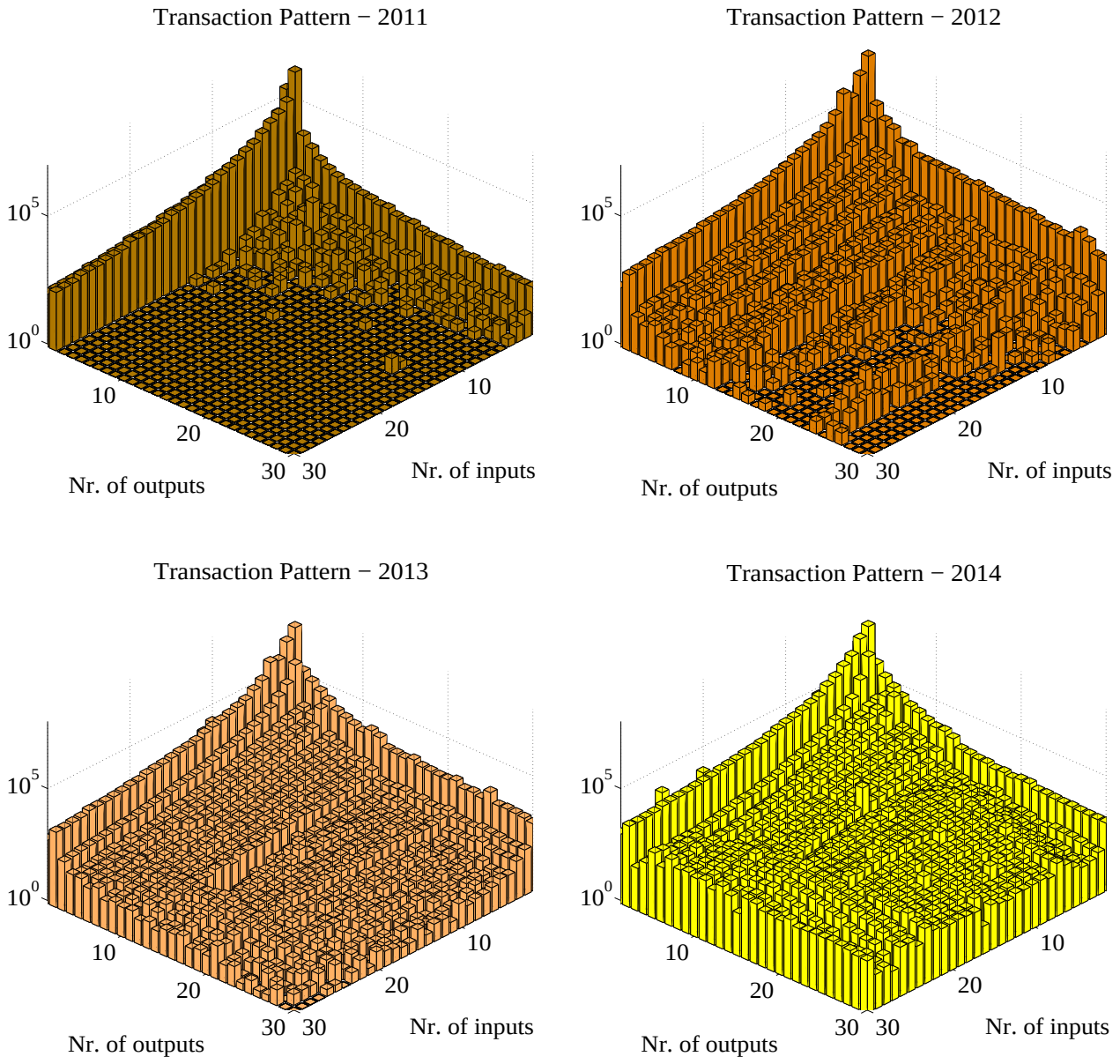

FIGURE 4: Log-scale distribution of Bitcoin transactions per number of inputs and number of outputs. Data Source: Bitcoin blockchain. Internal calculation.

are attainable using strong public-key encryption algorithms, see Section 3. Thus, anonymity is preserved but all transactions are also fully traceable because they are recorded in the public ledger. This means that, for each address one could do a cash-flow analysis and observed its balance at each point in time by verifying the historical transactions that involved that specific address as either input or output. For example, given an address A one can verify from which other addresses B, C, etc. it got the coins from and to which other addresses D,E, etc. it sent the coins to. Alone, this information cannot be used to identify a person because the addresses are

simply random numbers. However, if somebody knows who owned address B (because for example it is a public address), they could be able to pressure this person into disclosing to them who owns the address A. This second user might then be forced to reveal the owner of address D and so on. Note that, differently from addresses, any specific coin is just a record and does not have any identifiable number in the system.

The traceability of transactions is a sensible topic for the digital currency community, that's why the officially encouraged practice of using a new address for every transaction is designed to make any identity attack more difficult. Moreover, already back in 2013 the community developed the so-called principle of "coinjoin" transactions. According to this method, people pool together their transactions and agree to form a single transaction. This method mixes the addresses in both inputs and outputs in a way that makes tracking the exact input-output relations between specific addresses impossible. One characteristic of coinjoin transactions is that they have at least nine inputs and at least nine outputs. However, the number of inputs and outputs may also be drastically different between them [24]. We know from Section 3 that each input has a distinct signature (scriptsig) which is created in accordance with the rules specified in the past-output that it is consuming (scriptpubkey). In the case of coinjoin transactions, the signatures, one for each input, inside a transaction are completely independent from each other. Thus, users can agree on a set of inputs to spend, and a set of outputs to pay to. Later, individually and separately they sign the transaction and merge their signatures. The transaction is not valid and will not be accepted by the network until all signatures are provided, and no one will sign a transaction which is not to their liking. From outside it is therefore impossible to verify if one of the addresses in the output, for example A, received digital currencies from either B, C or any other address in the input list. Differently from other mixing services[20] with the coinjoin method a user's coins will always stay under their control and therefore it is impossible for them to be stolen or confiscated [27]. For more information on coinjoin transactions we refer the reader to [28]. Figure 4 shows how the practise of using coinjoin transactions increased in 2013 and 2014.

4.4 NETWORK EXPANSION

Although developments in the blockchain-based payment systems merit ongoing attention, to date, the only prominent network is still Bitcoin. Thus, we use data from Bitcoin to compare its expansion with other competitive payment networks like VISA, Mastercard, Western Union

[20] These services accept payments from customers, deduct significant commissions (4.555%) and then forward the balance to the address designate by the users [25], [26].

and Discover.[21]

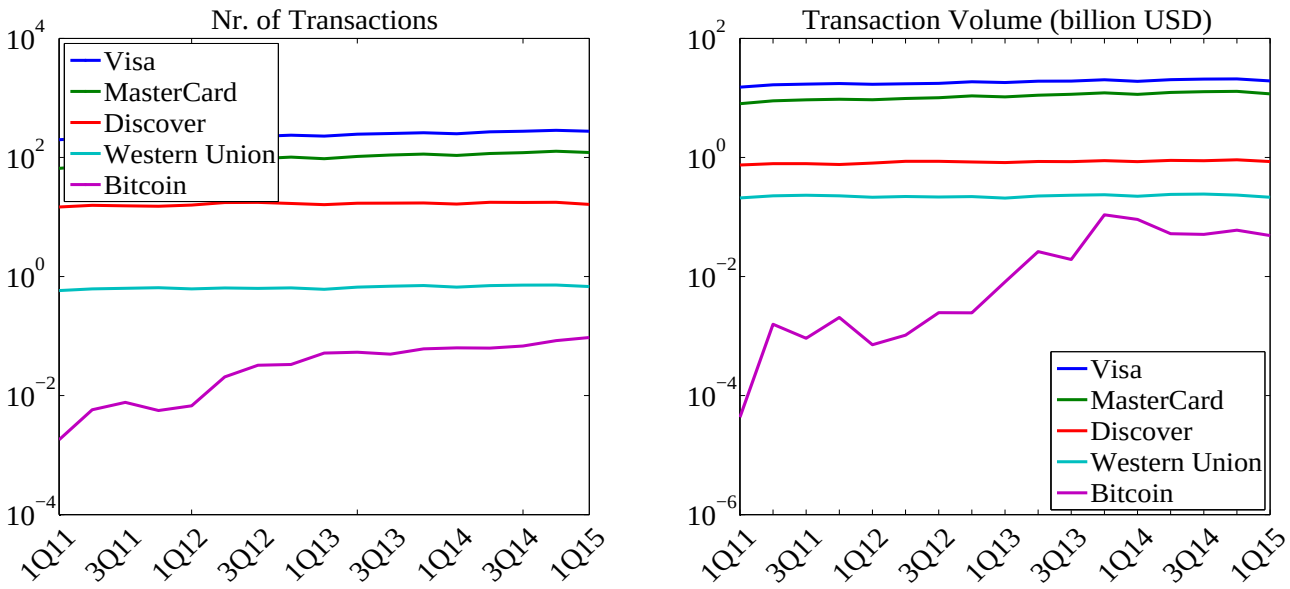

FIGURE 5: Comparison between different payment networks. Left: Average (log) number of daily transactions. Right: Average (log) amount of daily transactions in USD. Data source: Bitcoin blockchain, VISA, MasterCard, Discover, Western Union performance reports. Period: from 1Q2011 to 1Q2015. Internal calculation.

We rank them with respect to the (average) number of daily transactions and the (average) total daily volume in USD, see Table 1. Our analysis shows that from 2011 to 2015 the prominently payment networks, in order of importance, are VISA, Mastercard, Discover, Western Union and Bitcoin, see Figure 5. At the end of 2014 and beginning of 2015, the US Dollar value of daily Bitcoin transactions oscillates around USD 50 million. This value includes all transactions on the Bitcoin network, meaning they do not include trades via online exchanges, which are generally off-chain transactions that hence do not show up on the network. This volume is still pale in comparison to oldest and more mainstream remittance and payment networks. However, it is just one fourth of the exchange of the 2-century-old Western Union, which amounts to USD 210 million per day. Moreover, the Bitcoin network has kept growing during the period of the analysis. This expansion is confirmed by Figure 6 which compares the average amount of US Dollars transferred in each transaction by the payment networks un-

[21] We average quarterly data provided by VISA, Mastercard, Discover, Western Union performance reports [29], [30], [31] and [32]. Bitcoin data is provided daily by [14]. Since "Total Output Volume" statistics, which represents the total value of all transaction outputs per day in the Bitcoin network, includes coins that are returned to the sender as change, we replace it with "Estimated Transaction Volume". This statistic is comparable to the total output volume, where an algorithm attempts to remove change from the total value. This may be a more accurate reflection of the true transaction volume. We use BTC/USD exchange rate from the statistics "Market Price (USD)".

Year	VISA		MasterCard		Discover		Western Union		Bitcoin	
	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)
1Q11	15,153.8	198.3	8,011.0	65.6	746.5	14.7	208.8	0.6	0.04	0.002
2Q11	16,604.4	213.2	8,934.1	72.5	787.0	15.7	226.4	0.62	1.6	0.006
3Q11	17,033.0	217.7	9,285.7	77.1	787.0	15.4	231.9	0.63	0.92	0.008
4Q11	17,450.5	223.6	9,505.5	84.4	761.3	15.1	226.4	0.65	2.1	0.006
1Q12	16,934.1	215.7	9,329.7	84.8	804.3	15.8	214.3	0.62	0.7	0.007
2Q12	17,252.7	218.7	9,780.2	93.8	861.1	17.5	220.9	0.64	1.04	0.021
3Q12	17,582.4	225.3	10,087.9	95.4	860.9	17.6	216.5	0.63	2.47	0.032
4Q12	18,648.4	236.8	10,835.2	101.3	840.1	16.8	219.8	0.64	2.45	0.033
1Q13	18,120.9	227.9	10,406.6	95.1	819.2	16.1	207.7	0.61	8.12	0.052
2Q13	19,109.9	245.6	11,087.9	104.1	856.1	17.0	225.3	0.66	26.2	0.053
3Q13	19,175.8	252.1	11,494.5	109.9	850.5	17.1	231.9	0.69	19.3	0.050
4Q13	20,197.8	259.9	12,142.9	114.0	883.8	17.2	236.3	0.71	108.65	0.061
1Q14	19,011.0	249.9	11,483.5	108.2	850.4	16.5	223.1	0.66	91.01	0.063
2Q14	20,274.7	269.6	12,351.6	116.6	892.2	17.6	239.6	0.70	52.35	0.063
3Q14	20,703.3	275.9	12,714.3	120.5	881.0	17.5	242.9	0.72	51.07	0.068
4Q14	20,879.1	285.4	12,879.1	127.1	912.0	17.7	233.0	0.72	60.1	0.084
1Q15	19,263.74	275.6	11,681.32	121.3	852.32	16.3	214.29	0.68	48.80	0.094

TABLE 1: Volume in million USD (Vol.) and millions of transactions (Tx.) via major international payment networks. Data source: Bitcoin blockchain, VISA, MasterCard, Discover, and Western Union performance reports. Period: from 1Q2011 to 1Q2015. Internal calculation.

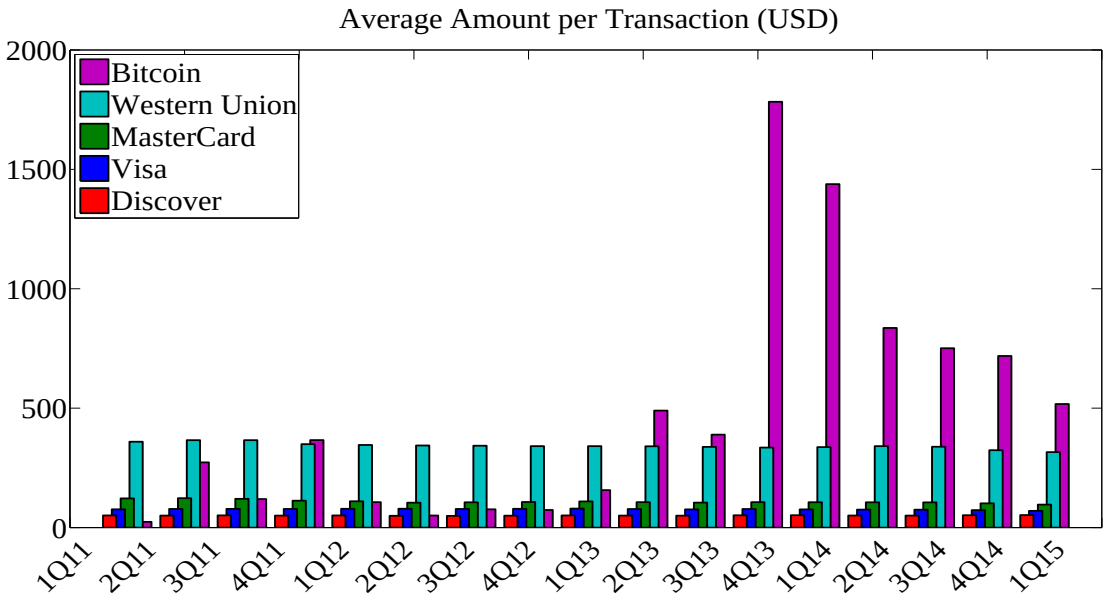

FIGURE 6: Comparison between different payment networks. Average daily USD amount per transaction from 1Q2011 to 1Q2015. Data source: annual/quarter report of listed company Data source: Bitcoin blockchain, VISA, MasterCard, Discover, Western Union performance reports. Period: from 1Q2011 to 1Q2015. Internal calculation.

der analysis. Due to high volatility of the BTC/USD exchange rate (see Figure 27), the average volume in US Dollars per Bitcoin transaction fluctuated remarkably during the period of the analysis but since 2013 it has remained larger than that of the other payment networks.

5 NON-STATE , DECENTRALISED AND HYBRID ASSET-BACKED MONEY?

Currencies can be classified according to the nature of the issuing entity and to the underlying backing of the currency value. Along this line of reasoning, in Table 2 we show that currencies may be either public/state or non-state and either fiat or asset-backed:

- Public currencies, known as "tax-driven money", are issued by central authorities in monopoly and recognised as the unique valid means of payment that cannot be legally refused by a creditor in satisfaction of a private but mostly public debt.[22]
- non-state currencies are issued by a private centralised or *decentralised* community-based organisation. They are not backed by any government, central bank or sovereign note.
- Fiat currency is intrinsically valueless money. It derives its value from government regulation or law.
- Asset-backed currencies are commodity currencies whose value is based on a good, often a precious metal such as gold or silver.

	Non-state Currency	**Public/State Currency**
Fiat Currency	Ithaca Hours (special type of labour voucher) Time Dollars	USD, GBP, EUR, etc.
Asset-backed Currency	Liberty Dollar (1998–2009) Digital Currencies (?)	U.S. paper currency (1863–1933)

TABLE 2: Types of currencies.

Although the debate on whether digital currencies like Bitcoin can be considered as real money is ongoing [33], in the following we explain why, according to us, (some) digital currencies could, to certain extent, be considered non-state asset-backed currencies. We first start by considering why digital currencies are non-state money. The explanation is straightforward if we consider that the trust given to digital currencies is not related to the reputation of one single entity like a central bank but to all the users and miners that sustain the network. It has been estimated that today there are over 4,000 private currencies issued in more than 35

[22] This definition is related to the concept of legal tender introduced in the 17th Century.

countries [34]. Among these currencies we include private gold and silver exchanges, local paper money (e.g., Ithaca Hours, BerkShares), computerised systems of credit and debit, electronic currencies (e.g., digital gold currency), and digital currencies (e.g., Bitcoin, Litecoin). At the time of writing there are over 500 young digital currencies [35] circulating in online markets and mostly based on the Bitcoin protocol. Despite the rapid growth of the ecosystem, in Figure 7 we show that Bitcoin is the strongest currency in terms of relative market capitalisation.[23] However, other alternative currencies may gain popularity in the near future and could also take over Bitcoin as dominant currency.

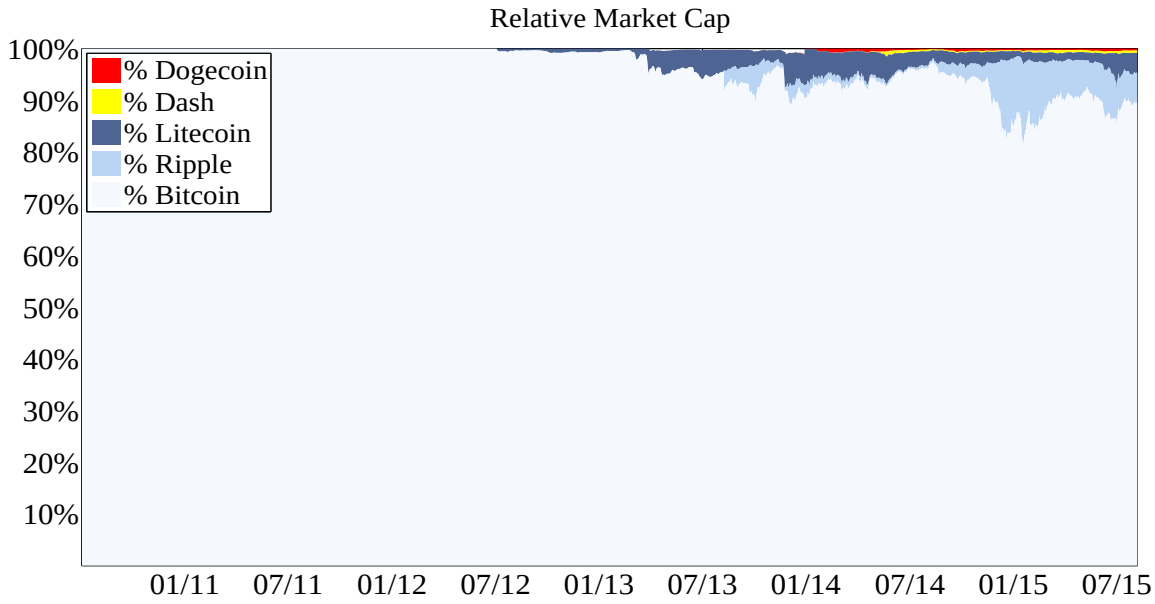

FIGURE 7: Relative market capitalisation of Bitcoin, Ripple, Litecoin, Dash, Dogecoin. Data source : Coinmarketcap. Internal calculation.

Before moving to the reason why digital currencies belong to the category of asset-backed currencies let us briefly digress to the topic of currency competition. Our approach to monitoring currency competition is the use of currency strength indices. The digital currency indices give the strength of a currency in real-time, scaled with respect to the market's average strength. If in a given period a currency index is stronger than its competitors, it means that the underlying currency drives the market during that time window. Since Bitcoin, Litecoin and Ripple, altogether combined, account for about 90% of the global digital currency market capitalisation, we propose the Bitcoin Index (BTCX), the Litecoin Index (LTCX) and the Ripple Index (XRPX):

- BTCX represents the relative strength of Bitcoin with respect to both Litecoin and Rip-

[23] The rank includes also Ripple, although it is a particular digital currency with properties that make its usability very different from the others. See Section 12.4 for an explanation of the Ripple protocol.

ple exchange rates, weighted by: (1) their respective relative market capitalisation expressed in USD; (2) the inverse of the Bitcoin exchange rate volatility.

- LTCX represents the relative strength of Litecoin with respect to both Bitcoin and Ripple exchange rates, weighted by: (1) their respective relative market capitalisation expressed in USD; (2) the inverse of the Litecoin exchange rate volatility.
- XRPX represents the relative strength of Ripple with respect to both Bitcoin and Litecoin exchange rates, weighted by: (1) their respective relative market capitalisation expressed in USD; (2) the inverse of the Ripple exchange rate volatility.

Formally, they are expressed as follows:

$$BTCX := \Delta_{BTC} \times \text{Exp}\left\{\text{Log}\left[\frac{BTC/LTC}{\sigma\left(BTC/LTC\right)}\right](W_{BTC}) + \text{Log}\left[\frac{BTC/XRP}{\sigma\left(BTC/XRP\right)}\right](1 - W_{BTC})\right\}$$

$$LTCX := \Delta_{LTC} \times \text{Exp}\left\{\text{Log}\left[\frac{LTC/BTC}{\sigma\left(LTC/BTC\right)}\right](W_{LTC}) + \text{Log}\left[\frac{LTC/XRP}{\sigma\left(LTC/XRP\right)}\right](1 - W_{LTC})\right\}$$

$$XRPX := \Delta_{XRP} \times \text{Exp}\left\{\text{Log}\left[\frac{XRP/BTC}{\sigma\left(XRP/BTC\right)}\right](W_{XRP}) + \text{Log}\left[\frac{XRP/LTC}{\sigma\left(XRP/LTC\right)}\right](1 - W_{XRP})\right\}$$

where:

$$W_{BTC} = \left(\frac{\omega_{LTC}}{\omega_{LTC} + \omega_{XRP}}\right); \quad \omega_{BTC} : \text{market capitalisation of BTC expressed in USD};$$

$$W_{LTC} = \left(\frac{\omega_{BTC}}{\omega_{BTC} + \omega_{XRP}}\right); \quad \omega_{LTC} : \text{market capitalisation of LTC expressed in USD};$$

$$W_{XRP} = \left(\frac{\omega_{BTC}}{\omega_{BTC} + \omega_{LTC}}\right); \quad \omega_{XRP} : \text{ market capitalisation of XRP expressed in USD};$$

and Δ_{BTC}, Δ_{LTC} and Δ_{XRP} are normalisation factors. Figure 8 shows the trend of the indices over the period from January 2014 to July 2015. For a deeper Hayekian analysis of currency competition in the era of digital currencies, we refer the reader to [36] and [37]. Going back to the discussion on non-state currencies more in general, the reader must know that most of them are backed by an asset or commodity (e.g., Liberty Dollar, digital gold currency). In general terms, a currency is backed by something if it is redeemable for a specific amount of the good which backs it. In this respect, some digital currencies are examples of hybrid asset-backed currencies because their process of money creation is energy intensive. As seen in Section 3, in order to mine a coin (under the PoW scheme) users need to commit a lot of computational power (measured in the hash rate) that is sustainable only by adopting specialised hardware such as ASICs[24] and by incurring substantial energy costs. See also Section 11. A recent

[24] An acronym for application-specific integrated circuits, describing customised microchips aimed at solving a particular task with high efficiency.

study by [38] tried to estimate a lower bound for the fundamental value of one Bitcoin by computing the energy costs expressed in US Dollars of producing one Bitcoin and then by comparing the obtained value with the BTC/USD exchange rate for the period 2010–2013. Similarly, [39] established a theoretical micro-founded model to determine the production cost of one Bitcoin around which market prices tend to gravitate. The model uses as inputs the cost of electricity, the energy consumption per unit of mining power, the US Dollar price of Bitcoins, and the expected production of Bitcoins per day which is partially based on the mining difficulty.

To conclude, although digital currencies may require substantial mining costs, it is debatable whether they should be considered asset-backed currencies. First, digital currencies cannot be directly converted back to the equivalent amount of energy (measured for example in "joules of electricity") spent on mining. Second, also the mining of gold or other precious metals needs a substantial amount of investments and incurs energy costs, but gold (paper currency) is asset-backed because of the gold's inherent properties. Finally, some digital currencies, like Ripple, are not based on PoW or other energy-intensive mining schemes, see Section 12.4.

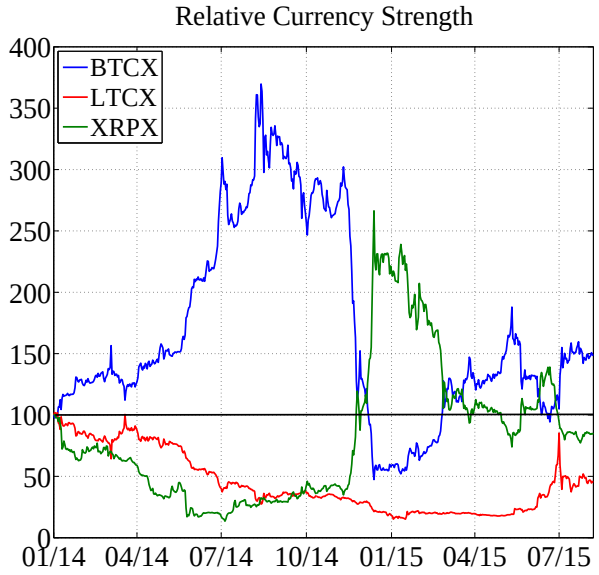

FIGURE 8: Comparison between relative index strengths. Ba= 100 on 01.01.2014 (BTCX, LTCX, XRPX). Internal calculation.

6 DIGITAL CURRENCIES ARE NOT LEGAL TENDER UNDER A STABILISING AUTHORITY

Digital currencies are not media of payment allowed by law or recognised by any legal system as valid for meeting financial obligations. The following features that are peculiar to any legal tender are not met by digital currencies: (1) mandatory acceptance, where the creditor of a payment obligation can in no way refuse the currency except if the parties have agreed on alternative means of payment; (2) acceptance at full face value, meaning the monetary value is simply equal to the indicated amount; and (3) the currency has the power to release debtors

from payment obligations. Historically, most of the countries have forbidden or restricted payments made by other means than by legal tender which is recognised within their jurisdiction.[25] With respect to digital currencies, more recently some countries have adopted a hostile attitude toward the propagation and adoption of Bitcoin specifically and digital currencies in general, especially to contain money laundering activities and combat the lack of banking supervision. Overall, the debate over how to deal with this new digital currency is still in its infancy. In China it is not explicitly illegal to own digital currencies. However, banks and financial companies have certain restrictions on their ability to transact or process digital currency payments. On the 3rd of December 2013 the People's Bank of China (together with the Ministry of Industry and Information Technology, China Banking Regulatory Commission, China Securities Regulatory Commission, and China Insurance Regulatory Commission) issued a document (Notice on Precautions Against the Risks of Bitcoins). Therein it classified digital currencies as a "virtual commodity" and as such prohibited financial companies from dealing in digital currencies and instructed third-party payment service processors to stop dealing with Chinese digital currency exchanges like Bit China.[26] In 2014, several Chinese banks, including some large state-owned banks and some local banks, stopped providing services to Bitcoin exchanges. The Notice additionally demanded the reinforcement of the oversight of Internet websites providing Bitcoin registration, trading, and other services. Moreover, it also warned about the risks of utilising the Bitcoin system for money laundering. Up to now, the European Union (EU) has passed no specific legislation regarding the status of digital currencies as money. However, in October 2012, the European Central Bank (ECB) issued a report on virtual currency schemes which also partially examines the proliferation of Bitcoin. According to this document, the ECB considers Bitcoin as a digital representation of value which can be used as alternative to money under certain circumstances [40]. Still in its last 2015 report, the ECB puts the emphasis on the fact that digital currencies are not a full form of money as defined in the economic literature and cannot be considered as money or currency from a legal perspective [41].

The situation remains uncertain in Europe because there is not a specific Directive and single EU member states have not passed specific laws on the matter so far. The general orientation is to adopt the current legislation already in place in order to deal with digital currencies in Europe. The Electronic Money Directive 2009/110/EC identifies electronic money according to three criteria [42]: (1) electronic storage, (2) issuance upon receipt of funds, and (3) accep-

[25] This is a recent innovation of modern states. For example in the USA, prior to the Coinage Act of 1857, foreign coins (generally Spanish, English, and Austrian gold and silver pieces) circulated freely in the market.

[26] Those third-party payment service providers included PayPal-like online payment companies such as PerfectMoney, OKPay, etc., which provided an alternative way for online deposits and payments.

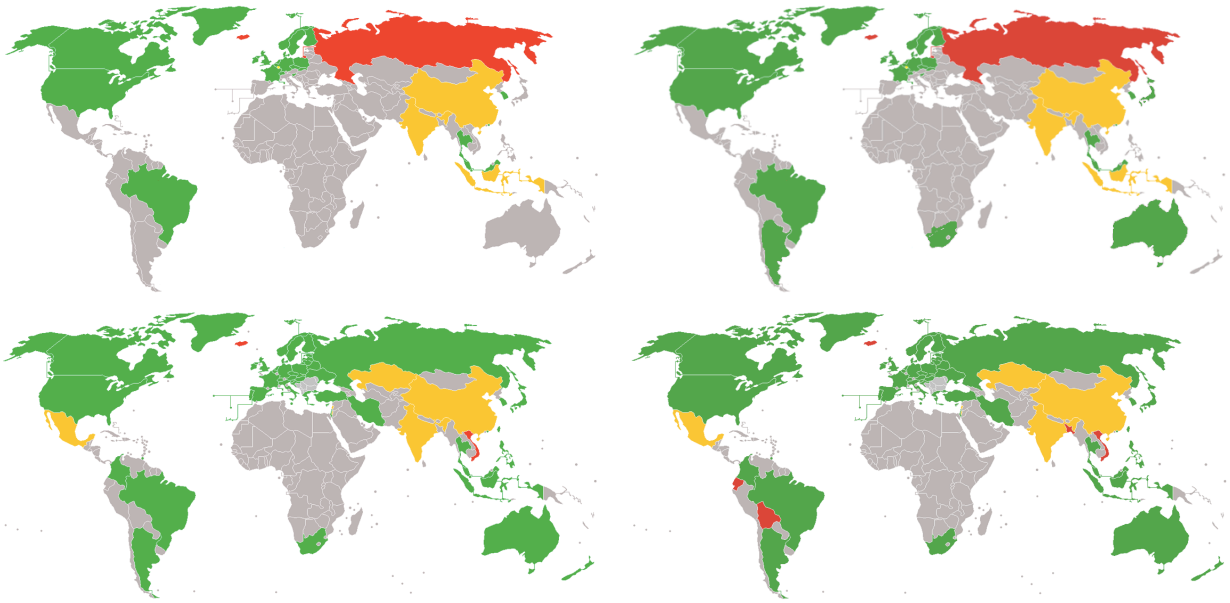

FIGURE 9: Legal status of digital currencies in different countries. From left to right and top to bottom: February 2014, March 2014, April 2014, and September 2014. Green: permissive countries, red: hostile countries, yellow: contentious countries, grey: unknown position. Data source: Markle Tree.

tance as a means of payment by a legal or natural person other than the issuer. With respect to the first characteristic, every digital currency is monetary value stored on the computer of the participants in the P2P network. With respect to the third characteristic, digital currencies can be used to buy goods and services from third parties outside of the P2P network. However, digital currencies cannot be considered e–money because the mining activity doesn't imply an issuing of digital currencies on receipt of funds, i.e., miners do not receive funds in return for their activity. However, according to this directive, service providers that issue digital currencies upon payment of fiat currency could be considered e-money issuers. The Payment Services Directive 2007/64/EC does not apply to digital currencies [43]; payment institutions defined by the Directive are not allowed to issue electronic money. In line with the risk analysis of virtual currency schemes by the ECB [40], the London-based European Banking Authority (EBA), which is part of the Eurosystem and has the objective of maintaining financial stability in Europe and safeguarding the integrity, efficiency and orderly functioning of the banking sector, issued a warning to consumers on digital currencies on the 12th of December 2013 [44]. The EBA's report was followed on the 4th of July 2014 by an opinion document on digital currencies [45]. The EBA points out that it is unlikely that a EU/EEA member state will declare a digital currency as legal tender. Were this to happen, a digital currency would become a fiat currency backed by a central authority. Indeed, the status of EU banknotes and coins as legal tender is defined by Article 128 (ex-Article 106 of the EC Treaty) of the Treaty on the Function-

ing of the European Union (TFEU). The exclusive right to authorise the issue of banknotes and approve coin volume issuance within the euro area is given to the ECB. Therefore, it would be necessary to amend the TFEU if a digital currency were declared legal tender.

The status of not being a legal tender has some practical real-life consequences. For example, users cannot compel merchants or vendors to accept their coins. Moreover, the number of alternative coins is so high (currently there are over 500 digital currencies in circulation [35]) that holding one digital currency over another one may be risky because merchants may change their allegiance to digital currencies over time, switching between various digital currency schemes. Moreover, there is no guarantee that merchants, who accept digital currencies are then, later on, able to spend them. For instance, simply paying an invoice depends on the voluntary consent of other market participants willing to accept digital currencies.

The no-legal-tender status is also associated with the absence of a public governing authority in charge of establishing and governing the rules for the use of a digital currency. This authority should in principle: (1) be responsible for the overall functioning of the digital currency infrastructure as a payment system; (2) be accountable for maintaining the integrity of the central transaction ledgers, the protocols, and any other core functional component of digital currency schemes; (3) be responsible for ensuring that all the actors involved comply with the scheme's rules and that the scheme complies with oversight standards; (4) provide exchange rate stability among digital currencies and between digital currencies and fiat currencies; (5) eventually act as redeemer of last resort.

Since digital currencies are not issued by public authorities, there is no reason for governments to assign legal tender status to digital currencies that are beyond their control or to establish a central authority that enforces exchange rate stability and acts as redeemer of last resort. Technically, these functions could indeed be directly embedded into the protocol of digital currencies by implementing the rules that governs the money supply and transaction mechanisms at the source code level. Already in place are experimental ledgers that come with a built-in Turing-complete programming language, which can be used to implement any monetary constraint or payment system feature, see Section 12.

7 GROUPS OF INTEREST

At the beginning the popularity of Bitcoin and other digital currencies was mostly limited to underground crypto-anarchist communities, following anarcho-capitalist ideologies. Namely, groups aiming at employing cryptography to enable individuals to make consensual economic arrangements transcending national boundaries and centralised authorities. Unfortunately,

those activities were often associated with the *counter economy*. This generally includes all the underground activities of civil and social disobedience outside of normative and statutory frameworks, at any place or time, chosen to prohibit, control, regulate, or tax [46]. In line with these theories, the New York Times traces the idea behind Bitcoin back to the "The Crypto Anarchist Manifesto" of 1988, by Timothy C. May [47] and [48].

Indeed, digital currencies and services like Silk Road, Black Market Reloaded and assassination markets have made it possible to trade illegal goods and services with little interference from the law, see Section 8. However, more recently, the popularity of digital currencies started to expand beyond the crypto-anarchist communities to capture the interest of practitioners (e.g., professional investors, financial experts, technologists, law firms, banks), academics and the general public at large, via increasing media attention and an active proselytising by Bitcoiners. In the remaining we provide some statistics on the interest on digital currencies, focusing on four categories: users, merchants, developers, and investors.

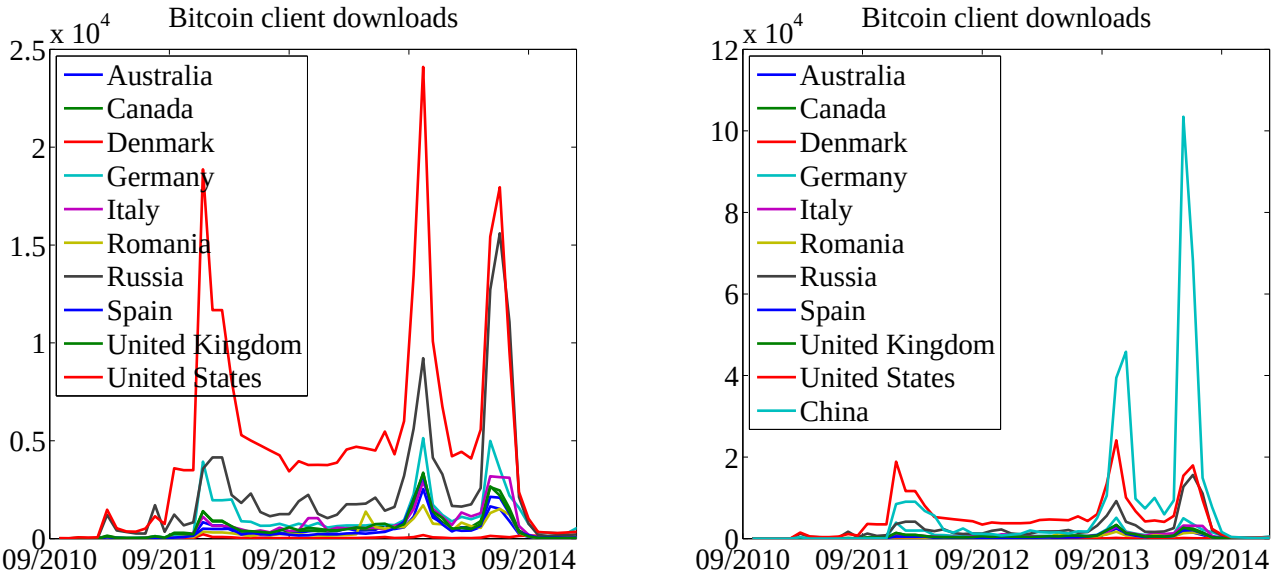

FIGURE 10: Bitcoin client downloads per country normalised by the complementary number of users that have direct access to the Internet. Data source: ITU (International Telecommunication Union) and Sourceforge. Internal calculation.

7.1 USERS

It is actually impossible to track the real use and rate of adoption of digital currencies worldwide. To estimate the number of users one could use three proxies: the number of wallets, the number of downloaded clients or the number of connected IPs to the networks.

However, all three proxies have some drawbacks. First, the number of wallets is impossible to count. Moreover, they can contain anything from zero to thousands of addresses each. Second, the number of client downloads does not give a good estimation either because of the existence of web wallets (and alternative ways of downloading the clients), the risk of counting multiple downloads by the same person and across different versions, and also because this method excludes users that may have downloaded the client from other mirrors. Finally, the account of connected clients is also a rough approximation because of the web wallets. Moreover, some users may not broadcast their IP address or simply may not launch the software unless they really need to. In the following we present a metric that can be used to rank a country according to the penetration of the Bitcoin technology among Internet users. However, the reader should be aware that, given the above-mentioned limitations, our results are only an approximate estimation of the real picture. In particular, we look at the number of Bitcoin clients downloaded by the users according to their IP address. This figure is normalised by the complementary percentage of citizens with access to the Internet network. For each country i the rank is computed as follows:

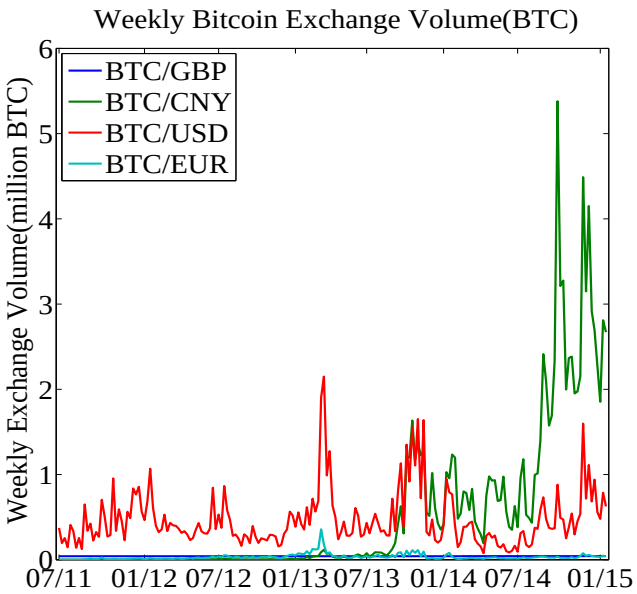

FIGURE 11: Weekly exchange volume of Bitcoins in the main trading platforms (Anxbtc, Bitcoin24, btc-e, Bitcoincentral, Bitcoinde, bitfinex, bitmarket, bitstamp, britcoin, btc china, campbx, coinfloor, hitbtc, huobi, kraken, lakebtc, MtGox, okcoin, rmbtb, tradehill) from July 2011 to January 2015. Data source: Bitcoinity. Internal calculation.

$$\text{Rank}_i := N_i \times (1 - \alpha_i) \tag{2}$$

where N_i is the number of downloads of the Bitcoin client in country i and α_i is the percentage of individuals using the Internet in the same country.

The computation is based on data from Sourceforge[27] and from ITU[28]. As the reference Bitcoin client we use Bitcoin Core (formerly Bitcoin-Qt) and Bitcoind (now bundled with Bitcoin

[27] Sourceforge is a web-based source code repository. It acts as a centralised location for software developers to control and manage free and open source software development. It publishes information on the number of Bitcoin wallet downloads per country per day [49], [50] and [51].

[28] ITU is the United Nations specialised agency for information and communication technologies [52].

Core) [53] and [54]. Bitcoin Core, developed by Wladimir J. van der Laan, is based on the original code by Satoshi Nakamoto. It is the oldest and most widely known Bitcoin client. According to our metric, Figure 10 shows that China, USA, Russia and Germany are the countries registering the larger interest in Bitcoin. It is surprising to observe that although the conversion of Bitcoin to Yuan is prohibited in China, the country well outperforms all the others included in the sample, see Section 8.

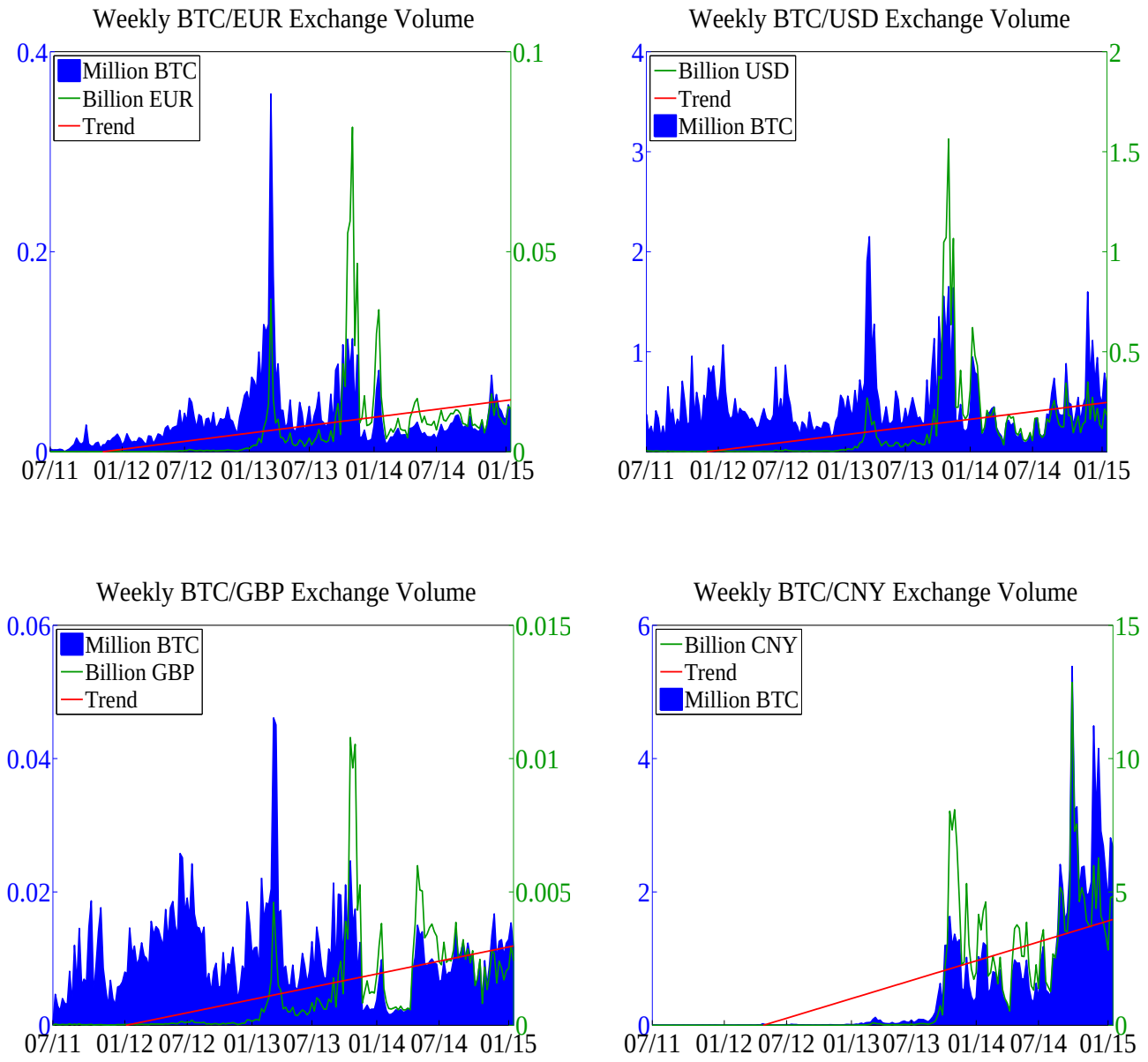

FIGURE 12: Weekly exchange volume of Bitcoins in the main trading platforms (Anxbtc, Bitcoin24, btc-e, Bitcoincentral, Bitcoinde, bitfinex, bitmarket, bitstamp, britcoin, btc china, campbx, coinfloor, hitbtc, huobi, kraken, lakebtc, MtGox, okcoin, rmbtb, tradehill) and against the major hard currencies (USD, GBP, EUR, CNY) from July 2011 to January 2015. Data source: Bitcoinity. Internal calculation.

Volume in BTC	Year	BTC/USD	BTC/EUR	BTC/GBP	BTC/CNY
Mean	2012	404833 (91.09%)	23320 (5.25%)	11794 (2.65%)	4506 (1.01%)
(weekly)	2013	650294 (65.91%)	63608 (6.45%)	13225 (1.34%)	259549 (26.31%)
	2014	343025 (22.33%)	23059 (1.50%)	7131 (0.46%)	1163197 (75.71%)
St. Deviation	2012	205498	11401	5230	3796
(weekly)	2013	460848	54599	8474	438822
	2014	205045	12179	3952	960218
Volume in USD	**Year**	**BTC/USD**	**BTC/EUR**	**BTC/GBP**	**BTC/CNY**
Mean	2012	3147387 (89.83%)	220411 (6.29%)	95505 (2.73%)	40219 (1.15%)
(weekly)	2013	173744312 (52.09%)	13308177 (3.99%)	2537553 (0.76%)	143965181 (43.16%)
	2014	171547907 (22.33%)	11750245 (1.64%)	3554263 (0.50%)	530584398 (73.96%)
St. Deviation	2012	1682033	163329	54862	35771
(weekly)	2013	322865053	22231294	3792220	332101759
	2014	113491426	7633762	2119485	335344667

TABLE 3: Annual mean and volatility of the Bitcoin market volume exchanged in major trading platforms and expressed in BTC and USD. Platforms: Anxbtc, Bitcoin24, btc-e, Bitcoincentral, Bitcoinde, bitfinex, bitmarket, bitstamp, britcoin, btc china, campbx, coinfloor, hitbtc, huobi, kraken, lakebtc, MtGox, okcoin, rmbtb, tradehill.

Note that our statistic measures the interest in Bitcoin expressed not only by users but also by miners and developers (which start to outweigh from 2013). In fact, the previous versions of Bitcoin Core were originally used both, by users and miners, because the client included a "miner" which generated Bitcoins (via the CPU). The version history can be found here [55]. Back to the period from 2009 to the beginning of 2012, the network was in its infancy and the amount of hashing power was low (around 10 GH/s). Mining via CPU was the standard practice. However, the network is now very large and requires the use of dedicated hardware and software. According to Figure 2 in early 2015 the hash rate was around 330 million GH/s. Since Bitcoin Core is resource intensive and requires sufficient bandwidth and storage to accommodate the full size of the blockchain to be downloaded, from around 2013 it is mostly used by developers and miners in combination with specific mining hardware. For more details on mining, see Section 3 and 11. Instead, end-users prefer online clients such as Armory, MultiBit, or Electrum. See [49] and [56] for a full list of Bitcoin clients. The predominant position of China with respect to other countries is also confirmed by looking at other statistics. The first is the comparison between the volumes of major currency pairs: BTC/USD, BTC/EUR, BTC/GBP and BTC/CNY, see Figure 11, 12 and Table 3. The second is the statistics on the market share distribution between miners. In this regards, in Section 11 we show an increasing volume of Bitcoins mined by Chinese mining pools. Finally, the end-users interest in digital currencies can be assessed also by observing the popularity in the mass communication media. Figure 13 (left) shows the trend over the past few years of new Wikipedia pages and tweets which contain the world "Bitcoin". Figure 13 (right) represents the number of members registered in Bitcoin Talk

[57]. Bitcoin Talk is by far the most popular forum where people interested in the technical details and the development of Bitcoin software can talk to each other. The forum is also a place for people who are interested in mining, in trading and in the economics of Bitcoin.

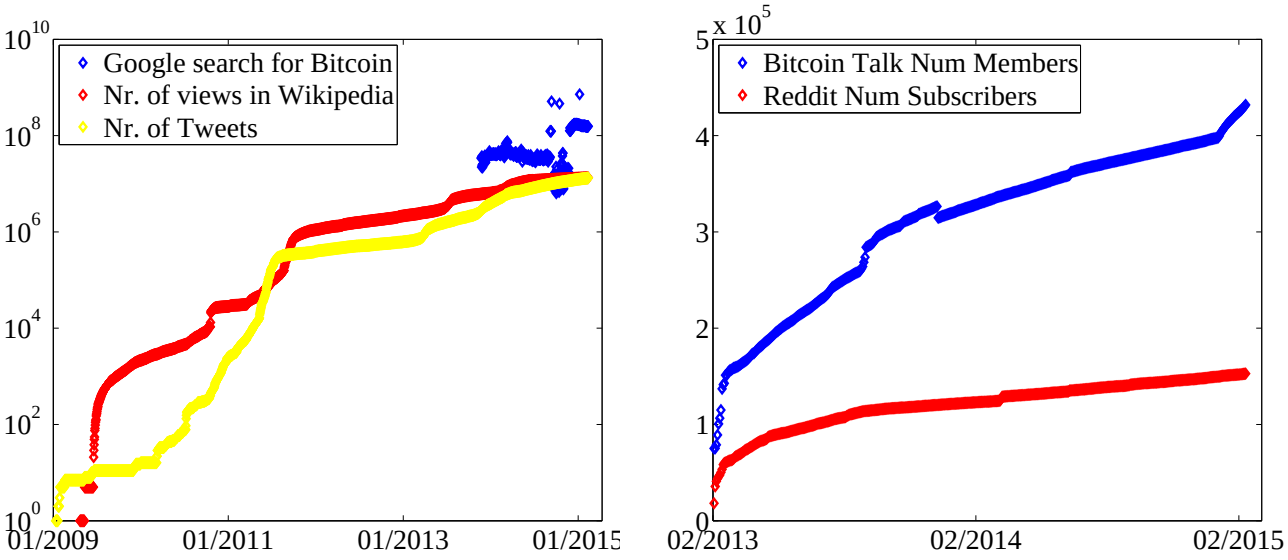

FIGURE 13: Left: Google search index size for Bitcoin, number of daily views of Bitcoin's Wikipedia page and number of daily tweets that contain the word "Bitcoin". Data source: Google, Wikipedia, Twitter. Right: Cumulative number of registered users in Bitcoin Talk and Reddit/Bitcoin number of subscribers. Data source: Bitcointalk and number of subscribers to $/r/Bitcoin$. Internal calculation.

7.2 MERCHANTS

Depending on their interaction with the "real" world, the ECB [40] defines three type of digital currencies: (1) *Closed virtual currency schemes.* These are basically generated and used only within online games. (2) *Virtual currency schemes with unidirectional flow.* These currencies usually only have an inflow. There is a conversion rate for purchasing the digital currency, which can be used to buy virtual goods and services, but in exceptional cases also to buy real goods and services. (3) *Virtual currency schemes with bidirectional flows.* In this respect, digital currencies are considered on the same level as any other convertible currency, with two exchange rates (buy and sell), and can subsequently be used to buy virtual or real goods and services. This is the scheme applied to Bitcoin and other digital currencies that are gradually becoming accepted by vendors and online shops worldwide. This is an increasing trend which is depicted in Figure 14. In particular, Figure 14 (left) shows the number of real venues listed in Cointerest that accept Bitcoin and other digital currencies [58], the number of merchants listed on Coinbase [59] and the number of eBay stores accepting Bitcoins and/or Litecoins as means of payment. Figure 14 (right) shows the downloads of the Bitcoin client from Sourceforge [60],

the number of hosts using Blockchain's My Wallet service [61] and the number of consumer wallets listed on Coinbase [59]. Digital currencies are commonly conceived as, exist and are stored only as bits in computers. However, recently some ATMs have been installed. Similar to traditional ATMs, people can withdraw paper money backed by digital currencies, especially Bitcoin. Table 4 shows the current rank of countries by number of ATMs already installed.

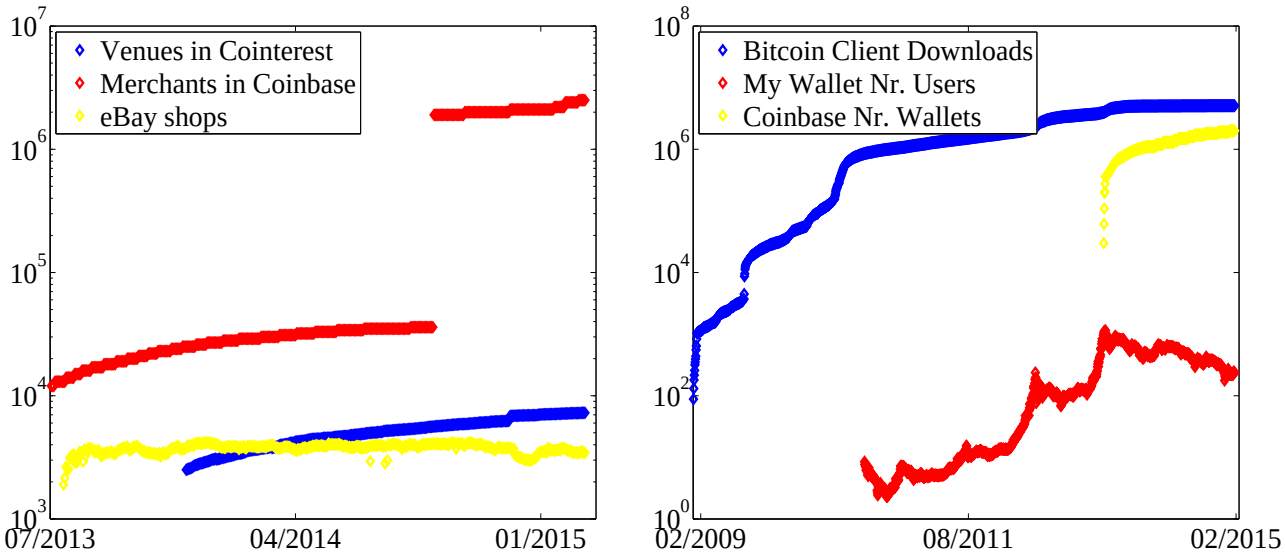

FIGURE 14: Left: Number of venues that accept Bitcoin and are listed in Cointerest, number of merchants listed on Coinbase, number of listing shops on eBay. Right: Downloads of the Bitcoin client from Sourceforge, number of hosts using Blockchain's My Wallet service, number of consumer wallets listed on Coinbase. Internal calculation.

7.3 DEVELOPERS

Often developers' activities are considered as a proxy to anticipate the future evolution of a given technology. Indeed, one of the most important indicators predicting the success of a new technology platform is what we call "developer mindshare". This concept refers to the amount of time and effort developers are devoting to using and improving given technologies and platforms.

In this perspective, Bitcoin and, more generally, digital currencies are a hit with developers, according to data collected on GitHub. This is illustrated by the increase in GitHub repositories that mention Bitcoin. GitHub is a web-based hosting service mostly for code development projects, but also for non-code types of files. GitHub offers both paid plans for private repositories, and free accounts for open source projects. GitHub currently has over 11.7 million repositories, making it the largest code host in the world. Therefore, most developers (or at least the ones working on Bitcoin projects) generally have a GitHub account. Finally, GitHub is also

Country	#ATM	Country	#ATM	Country	#ATM
USA	88	Germany	4	UAE	1
Canada	67	Mexico	3	South Africa	1
Australia	16	Japan	3	Ireland	1
UK	13	Denmark	3	Kyrgyzstan	1
Netherlands	12	United States	3	Philippines	1
Finland	11	Slovakia	2	Bulgaria	1
Singapore	10	South Korea	2	Isle of Man	1
Czech Republic	8	Malaysia	2	Hungary	1
Hong Kong	7	Brazil	2	Serbia	1
China	7	Romania	2	Portugal	1
Spain	6	France	2	Ukraine	1
Italy	6	Austria	2	Thailand	1
Switzerland	5	Argentina	2	Croatia	1
Israel	4	Belgium	2	Sweden	1
Slovenia	4	Indonesia	2	Saudi Arabia	1
Poland	4	Taiwan	1	Paraguay	1

TABLE 4: Number of Bitcoin ATM per Country. Data source: Coindesk. Data taken on: 11th Dec 2014

the place where many startups usually host their own private source code [62]. GitHub is thus a good starting point to look at what is the Bitcoin technology trend. Developer mindshare is measured by running a query that tells us how many projects reference Bitcoin or Litecoin on GitHub. In order to quantify the general level of interest surrounding digital currencies, we compare Bitcoin and Litecoin with alternative e-money and electronic payment systems like Authorized.net, Stripe, Paypal and Ripple. Authorized.net is the Internet's most widely used payment gateway with a user base of over 300,000 merchants [63]. Stripe provides payment solutions for web developers who want to integrate a payment system into their projects via Stripe's API [64]. Moreover, Stripe backs the Stellar project, see Section 12.4. Ripple is an Internet protocol called RTXP, see Section 12.4. It is an open source software for facilitating financial transactions (payments, exchanges and remittances) [65]. This comparison is a bit forced but it can yield some insight into what is conspiring in terms of mindshare. Figure 15 shows that Bitcoin related projects multiplied about 500 times over the last three years, from 25 projects in January 2011 to 17,360 in May 2014. Paypal, the most widely used payment acquirer, processing over USD 4 billion in payments in 2011, had only 4,829 forked repositories in Github in May 2014. It is worth noting that we only have access to the open source projects on GitHub and cannot filter the projects according to their relevance. As such, the values in Figure 15 (left) should be used as an indication of the real unknown trend. Finally, to better

illustrate the attention given to digital currencies by investors and traders, it is also relevant to show the daily trading volume registered on the Bitcoin blockchain, see Figure 15 (right).

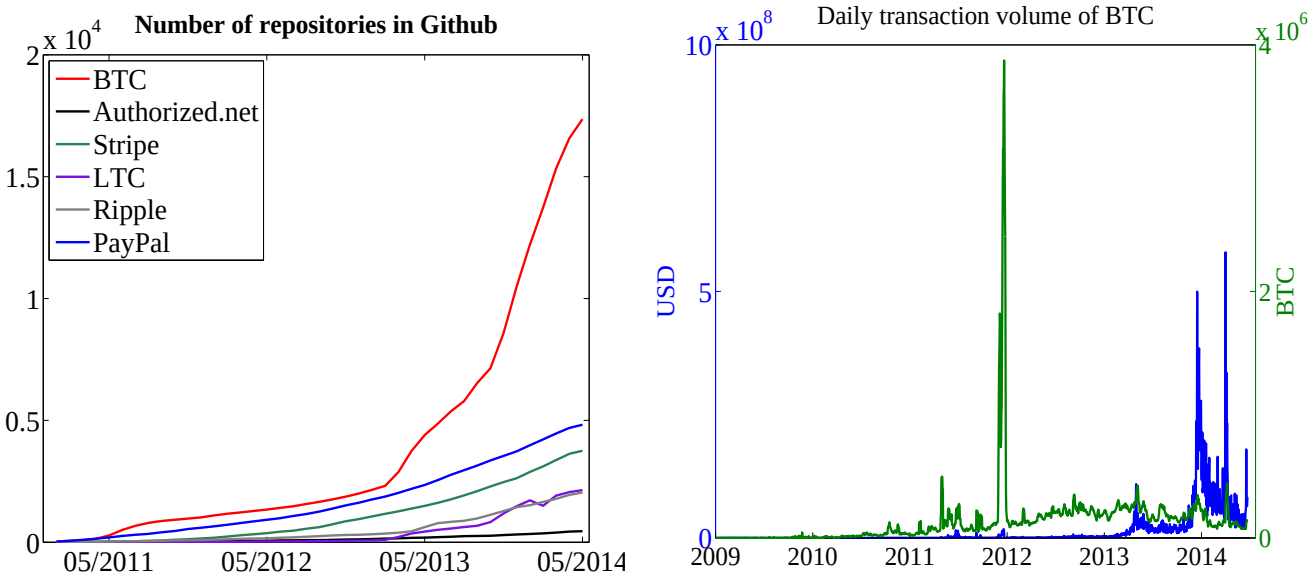

FIGURE 15: Left: Cumulative number of forked repositories included in GitHub for different projects. Right: Daily transaction volume of Bitcoin registered in the blockchain. Data source: Blockchain.info. Internal calculation.

7.4 INVESTORS

To grasp the dimension of the investment into the Bitcoin space we start by plotting the relative capital investment (and its growth rate) into Bitcoin-related startups from the period mid-2012 to mid-2015 and we compare it to other business sectors. As shown by Figure 16, the relative share of capital investment in Bitcoin-related startups pale if compared to other sectors like transportation or hospitality. However, Bitcoin is the fastest growing area of startup investments (followed by photo sharing and physical storage) with an annual growth rate near to 150%, see Figure 17. To better understand the capital allocation into the Bitcoin ecosystem we use information and databases for startups provided by Bitangel, Coinfilter, Coindesk, Crunchbase and Cbinsight to analyse the investment in startups during the window 2012-2015 [66], [67], [68], [69] and [70].

As shown in Table 5, for the purpose of our analysis we split the Bitcoin businesses into six different industry categories: Capital Markets, Payment and Remittance, Financial Services, Blockchain Applications, Mining Industry and Miscellaneous. According to this classification, Figure 18 – which takes data from Table 6, shows the quarterly funding amount and number of deals for startups in different Bitcoin industries.

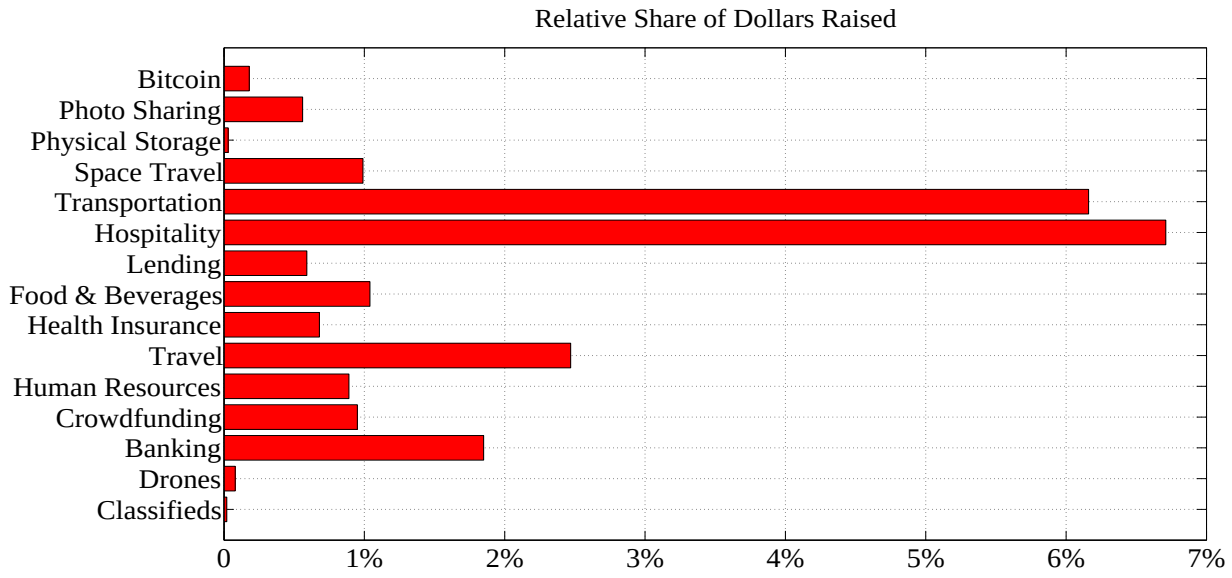

FIGURE 16: Relative Capital investment into different startup businesses during the period mid-2012 till mid-2015. Data source: Mattermark. Internal calculation.

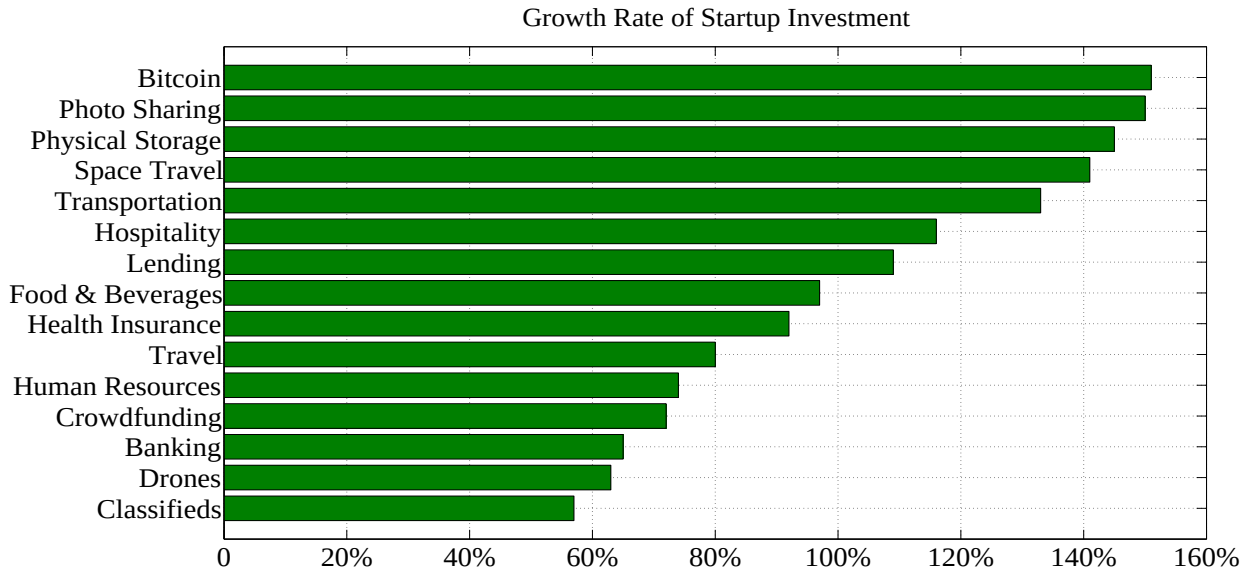

FIGURE 17: Relative rate of growth of capital investment into different startup businesses during the period mid-2012 till mid-2015. Data source: Mattermark. Internal calculation.

The investments mainly concentrate in three categories: Payment & Remittances, Mining Industry, and Capital Market. Figure 19 shows that in an increasing number of deals the Bitcoin industry has raised more than USD 10 million in a single round. For each industry category, Figure 20 depicts the startups that raised most of the capital. For example, in the first quarter of 2015, Coinbase and 21 Inc raised the record-high funding amounts of USD 75 million and USD 111 million, respectively. According to this criterion, for each category, the top startups

Capital Market	Payment and Remittance	Financial Services	Blockchain Application	Mining Industry	Miscellaneous
Exchange	Payment	Accounting	Smart Contracts	Mining Solutions	Bitcoin Faucet
Derivatives	Remittance	Security	Blockchain API	Mining Pool	Tipping
Commodity	Wallet	ATM			Messaging
Institutional Trading		Market and			
Crowdfunding and		Data Analysis			
Crypto Equity					

TABLE 5: Classification of business categories in the Bitcoin industry.

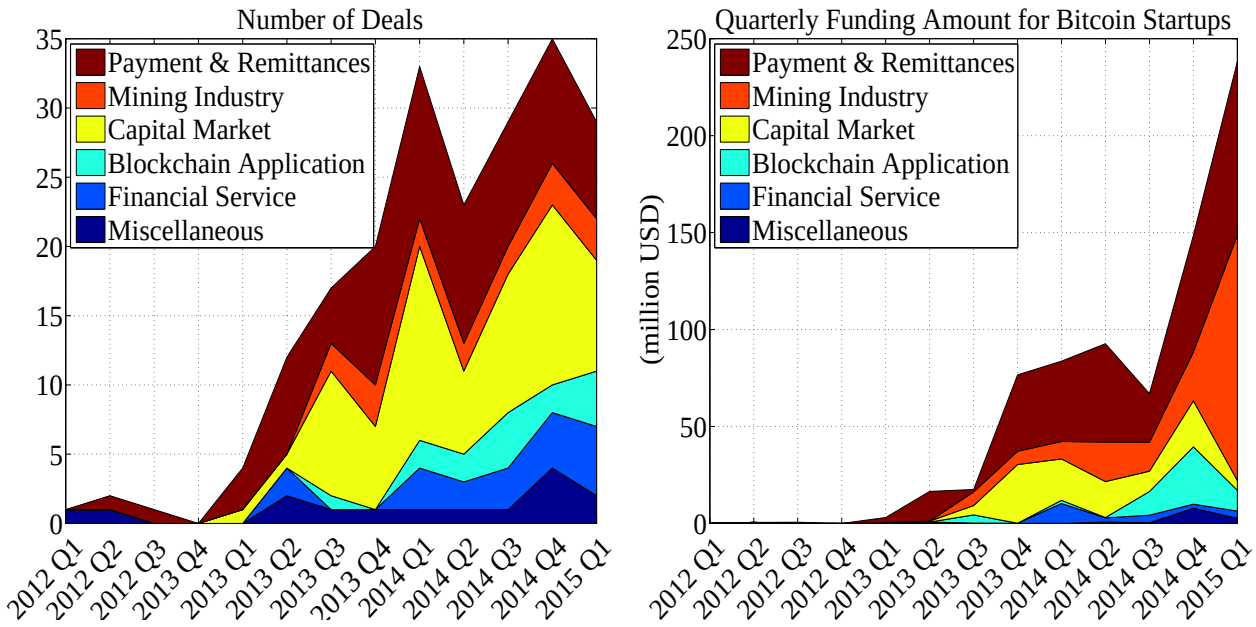

FIGURE 18: Left: Quarterly number of deals for startups in different Bitcoin industries. Right: Quarterly funding amount for startups in different Bitcoin industries. Data source: Bitangel, Cbinsight, Coinfilter, Coindesk, Crunchbase. Internal calculation.

are Coinbase (Payment & Remittance), 21 Inc (Mining Industry), Bitstamp (Capital Market) and Blockstream (Blockchain Application). Figure 21 shows the total investment deals (broken down by funding size) in each category during the period 2012–2015. Figure 22 shows the total of investment deals (broken down by industry category) for different funding sizes during the period 2012–2015. We use five different funding sizes expressed in US Dollars: < 0.1 million; 0.1–0.5 million; 0.5–1 million; 1–10 million; > 10 million. It is interesting to note that: (1) Payment & and Remittances and Capital Market are the more active categories attracting the largest number of investment deals; (2) Mining Industry and Blockchain Application are the two categories with the largest average amount of funding raised per individual deal; (3) Mining Industry and Payment & Remittances dominate the top rounds of funding per size (i.e.,

Year	Payment & Remittance		Mining		Capital Market		Blockchain apps.		Fin. Services		Miscellaneous	
	(Nr. deals)	(Funding)	(Nr. deals)	(Funding)	(Nr. deals)	(Funding)	(Nr. deals)	(Funding)	(Nr. deals)	(Funding)	(Nr. Deals)	(Funding)
1Q12											1	0.03
2Q12	1	0.02									1	0.50
3Q12	1	0.60										
4Q12												
1Q13	3	2.64			1	0.40						
2Q13	7	15.31			1	0.50			2	0.12	2	0.59
3Q13	4	1.26	2	7.00	9	4.82	1	4.20			1	0.20
4Q13	10	39.40	3	6.85	6	30.25					1	0.13
1Q14	11	41.41	2	9.00	14	21.37	2	1.60	3	10.26	1	0.03
2Q14	10	50.70	2	20.40	6	18.54	2	0.20	2	2.10	1	0.75
3Q14	9	25.01	2	14.96	10	10.52	4	12.19	3	3.92	1	0.34
4Q14	9	60.17	3	25.20	13	23.70	2	29.60	4	2.08	4	7.85
1Q15	7	89.47	3	126.50	8	5.10	4	10.70	5	3.72	2	2.65
Total	73	327.59	17	209.91	68	115.19	15	58.49	19	22.19	15	13.07

TABLE 6: Number of deals and funding amount (million USD) in different Bitcoin startup business areas. Bitangel, Cbinsight, Coinfilter, Coindesk, and Crunchbase.

individual deals with size larger than USD 10 million).

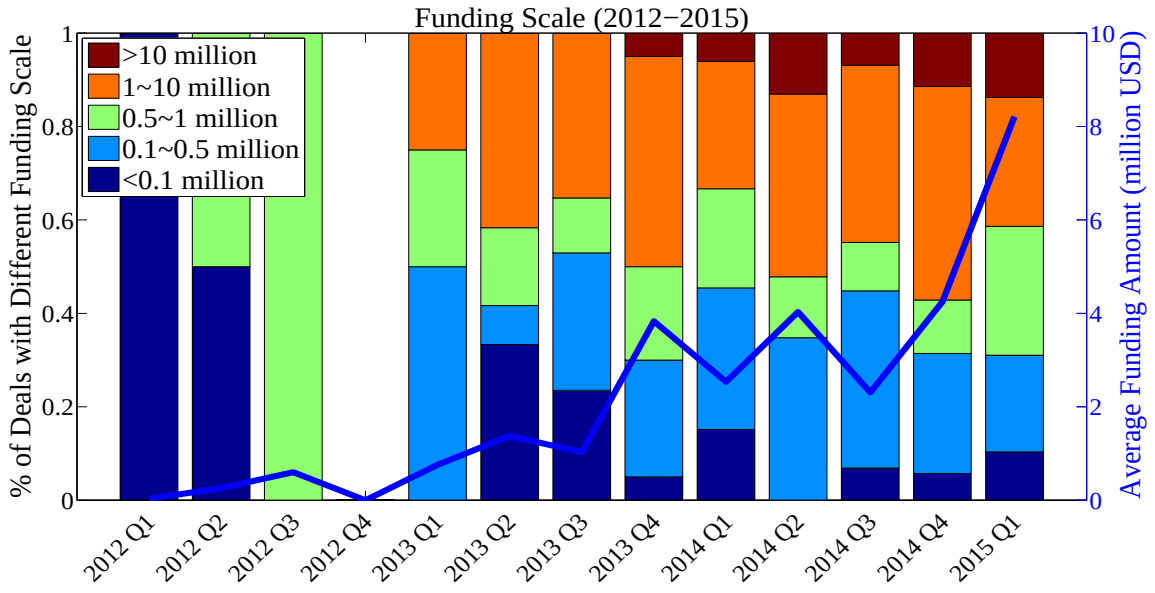

FIGURE 19: Bar chart: Percentage of deals in different funding scales, from Q1/2012 to Q1/2015. Line chart: Average funding amount per deal in each quarter. Data source: Bitangel, Cbinsight, Coinfilter, Coindesk, Crunchbase. Internal calculation.

We conclude by observing that from 2013 there is an investment trend with the potential to become even larger than the dot-com boom (a historic information technology bubble covering roughly 1997−−2000). From 2012 to 2015, the average funding amount for a single deal doubles every year. During the dot-com boom we saw a lot of capital flowing into companies that later failed. Thus, as happened in this case, venture capital funds risk flowing into low quality deals. The first red flag is the presence of scams. Indeed, a recent study identified 192 Bitcoin-related scams (categorised into four groups: Ponzi schemes, mining scams, scam wal-

lets and fraudulent exchanges) which brought to the loss of USD 11 million for about 13,000 victims during the period 2011-2014 [71].

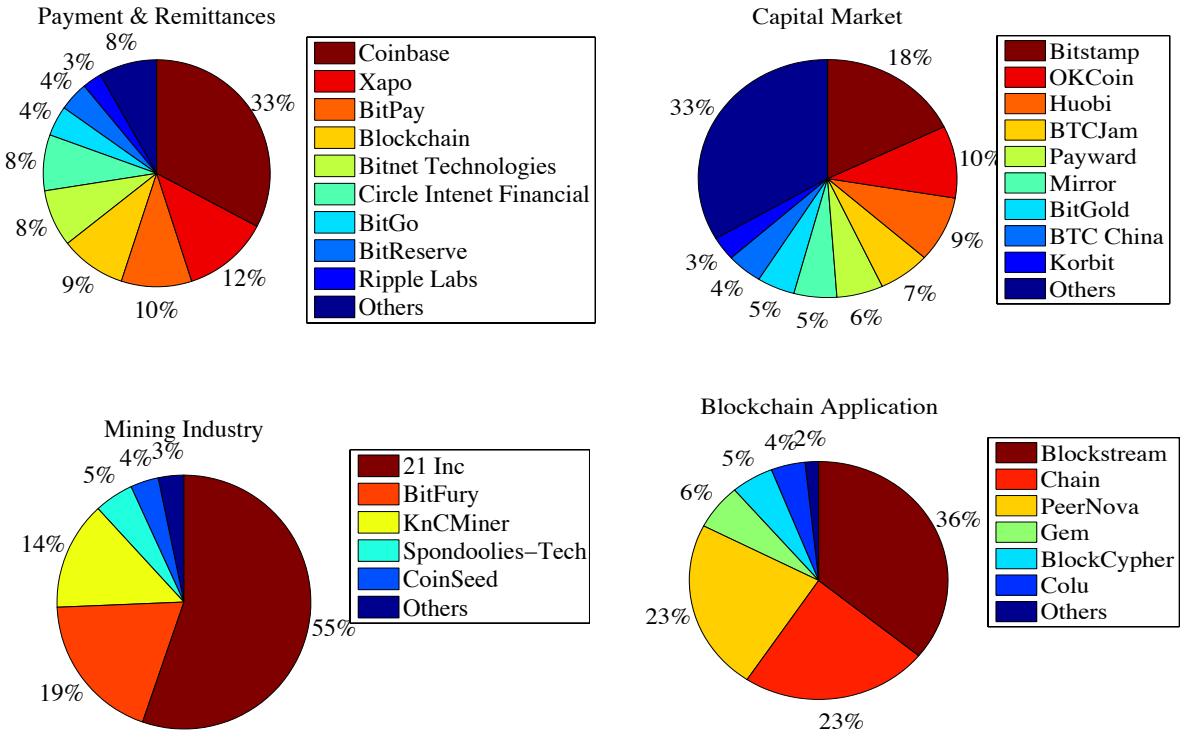

FIGURE 20: Funding distribution among startups within some main categories, from Q1/2012 to Q1/2015. Data source: Bitangel, Cbinsight, Coinfilter, Coindesk, Crunchbase. Internal calculation.

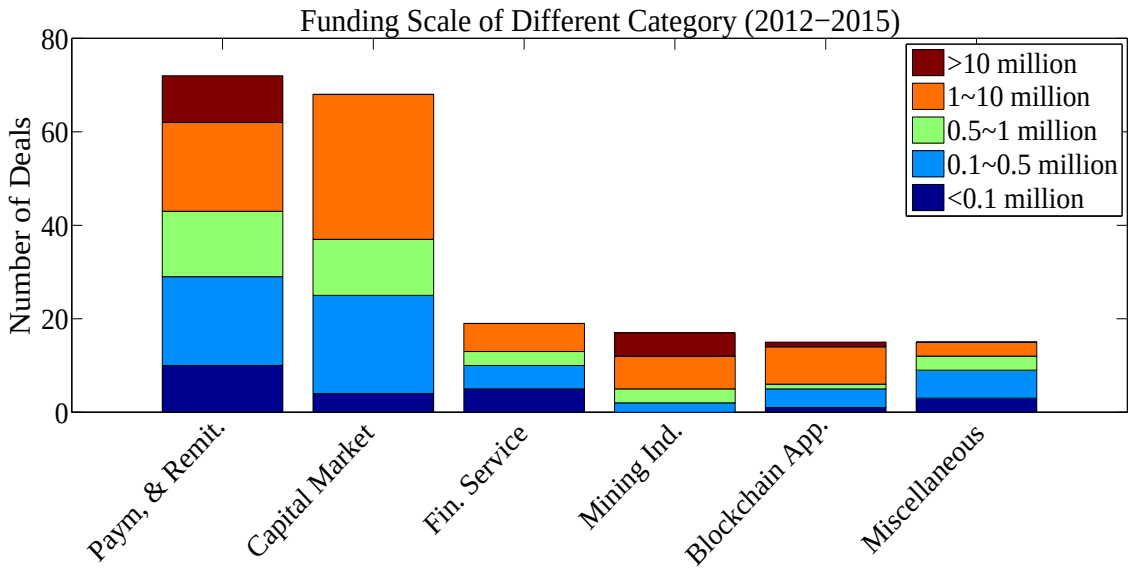

FIGURE 21: Total investment deals in different category, divided by funding scales, from Q1/2012 to Q1/2015. Data source: Bitangel, Cbinsight, Coinfilter, Coindesk, Crunchbase. Internal calculation.

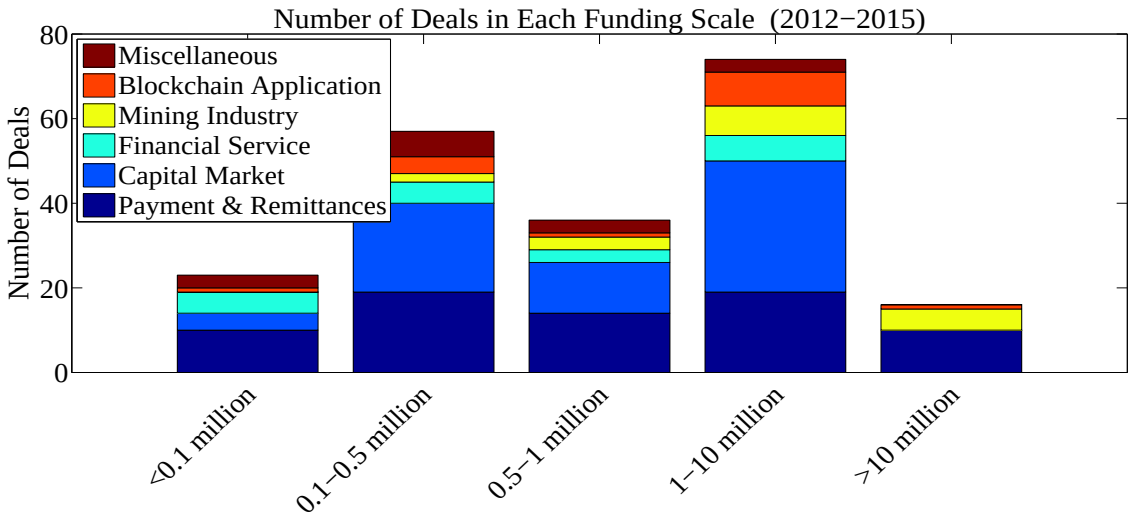

FIGURE 22: Number of deals in each funding scale, from Q1/2012 to Q1/2015. Deals in each funding scale are further divided into business categories. Data source: Bitangel, Cbinsight, Coinfilter, Coindesk, Crunchbase. Internal calculation.

7.5 GOVERNMENTAL AND PRIVATE FINANCIAL INSTITUTIONS

The potential impact of digital currencies is acknowledged by both governments and financial institutions. A number of governmental and private bodies have already started investing in blockchain-related projects. Here we briefly describe some of these initiatives; the list is by no means exhaustive, and intends to provide an overview of the penetration level of blockchain technologies in banks worldwide.

United Kingdom In 2014, the Bank of England established a specific Digital Currency Unit in the Monetary Policy Department. This unit is doing fundamental research on the economic implications and technological potential of distributed-consensus protocols. The British government also recently invested over GBP 10 million in blockchain-related projects [72].

Canada Bank of Canada is working intensively on digitalising fiat currencies. In November 2015, Bank of Canada will host a conference on electronic money and payments [73].

United States

- The Federal Reserve Bank of St. Louis may be collaborating with IBM to develop a new decentralised payment and monetary infrastructure [74].
- The Federal Reserve Bank of Cleveland conducted preliminary investigations into credit disintermediation and peer-to-peer lending, and will continue to monitor developments.

- The Federal Reserve Bank of New York is working on the sustainability and profitability of digital currencies, especially Bitcoin. In two Liberty Street Economics blogs, they (1) suggest that the low profitability of Bitcoin mining could concentrate mining in the areas in which electricity is cheapest, and (2) discuss the possibility of digital currency networks being able to block unsavoury transactions because of the consensus process.

- The US Treasury Department is considering digital identification systems for AML, anti-terrorist financing and financial inclusion purposes. It is examining the transferability of non-state issued digital identities. In the US, financial institutions cannot legally rely on identity verification conducted by another private company, but the EU are currently passing legislation to allow it for certain internet payments (not blockchain-based).

Netherlands De Nederlandsche Bank started a new project in early 2015 to consider the impact of technological innovation in finance. It has a broad scope: examining implications on payments, credit intermediation, investment and insurance, mapping out the main innovations and how they have been perceived within the finance industry. DNB will now use scenario analysis to map how different sectors could develop, which they will use to optimise the regulatory environment.

Private banks A number of private financial institutions are also currently investigating applications of blockchain technologies.

- CBW Bank, a small community bank based in Kansas and over a hundred years old, has partnered with Ripple Labs to launch a new payment tool called "ONE Card". What sets it apart from its competition is its ability to facilitate real-time settlement, allowing customers to receive funds instantly [75].

- The Estonian bank LHV Bank is experimenting with coloured coins called "Cuber", as a "cryptographically protected" certificate of deposit [76].

- The biggest Australian banks (ANZ, Westpac and Commonwealth Banks of Australia) are trialling with blockchain technology. The main purposes are payment tracking and payment settlements between subsidiaries [77].

- Barclays Accelerator invested in three blockchain startups (Safello, Atlas Card, and Blocktrace) to favour the integration of the blockchain with traditional banking infrastructure [78].

- The Swiss bank UBS opened a Blockchain Research Lab hosted by the Canary Wharf-based fintech accelerator space Level39 [79].
- Goldman Sachs is the leading investor in the USD 50 million fundraising campaign of Circle [80].
- Citibank is piloting three blockchains and experimenting with Citicoin [81].
- The Bank of New York Mellon is working on a proprietary consensus protocol with a built-in coin called VK Coin [82].
- The United Services Automobile Association opened a Bitcoin Research Unit [83].
- BNP Paribas and Euroclear are considering using distributed ledgers to settle securities [84].
- Santander is experimenting with blockchain to see how it may be used in traditional banking. The bank found 20 to 25 use cases where the blockchain may be used (from payments to smart contracts) [85].
- The Banco Bilbao Vizcaya Argentaria (BBVA) is among a group of backers who have invested USD 75 million in Coinbase under its private equity subsidiary, BBVA Ventures [86].
- In the Netherlands, ABN Amro, ING, and Rabobank are investigating the possibility of implementing a blockchain in their payment systems [87].
- Western Union is exploring a pilot program with distributed payment protocol provider Ripple Labs [88].

Other stakeholders In parallel, growing attention is given to the blockchain technology by leading technology market players, such as Samsung [89], IBM [90], Nasdaq [91], the New York Stock Exchange [92], and INTEL [93].

8 REGULATION

Current financial laws, ordinances, directives and regulations that impact also Bitcoin-related businesses are so complex and unsteady that an exhaustive and comprehensive picture of the legal status in different jurisdictions is impossible. However, in this section we will try to provide a short, concise map that can help to understand the different general approaches adopted

so far. Indeed, digital currencies present challenges for any definite classification and definition of these instruments within the framework of existing nation-state legal systems. Government, law enforcement agencies, market authorities and lawmakers are trying to fit digital currencies into existing legal frameworks. However, the result obtained so far is poorly fragmented and coordinated. Based on data from Merkle Tree [94], Figure 9 tracks the evolving regulatory landscape in different countries.

MtGox Fraudulent Activity Shows Up in the Blockchain

Figure 23 shows an abnormal volume of Bitcoin exchanged between addresses at the end of 2011. The peak is almost three times larger than the Bitcoin monetary base. We find that this abnormal volume was caused by MtGox's controversial reallocation of customers' coins between different MtGox addresses. There are about BTC 500,000 bouncing around from the 16th of November 2011 to the 8th of December 2011. To have the whole picture, we need to go back to the 19th of June 2011, when MtGox claimed to have been hacked. According to MtGox's press release [95] "an unknown person logged into the compromised admin account, and with the permissions of that account was able to arbitrarily assign himself a large number of Bitcoins, which he subsequently sold on the exchange, driving the price from 17.50 to 0.01 within the span of thirty minutes. With the price low, the thief was able to make a larger withdrawal (approximately BTC 2,000) before our security measures stopped further action." After that episode, customers began to worry about MtGox's capability to control the coins and launched many protests by calling for a "proof of solvency". To convince the community, Mark Karpeles (CEO of MtGox) announced publicly that he would have transferred BTC 424,242.424242 to a predefined address. Considering the anonymous property of Bitcoin, it's generally hard (if not impossible) to identify the owner of the address. However, it was found that on the 23rd of June 2011 the following chat was recorded in IRC [96]:

> "<MagicalTux> go1dfish: I'll send 424,242.42424242 BTC from a bunch of 50kBTC addresses (and maybe on 42kBTC) to one."
>
> "<MagicalTux> anyway, going to send to 1eHhgW6vquBY... the 424,242.42424242 BTC."

Notice that MagicalTux was Mark Karpeles' online alias. At the same time, a transaction (time-stamp 2011-06-23 06:50:15) with the exact same amount was shown in block 132,749 [97]. We find that in the following months, a series of complex transactions were made and the amount was gradually broken up into 10 addresses with 50,000 BTC. On the 16th of November 2011, all coins from the 10 addresses were bundled together again in block 153,509 [98]. From then on, the huge sum of coins (ca. BTC 500,000 in total) began to bounce around. That amount was transferred between different disposable addresses with irregular frequency. Figure 23 (right) compares the total transaction volume in the Bitcoin blockchain and the transaction volume linked to the BTC 500,000 only transferred by Karpeles. Obviously, the two quantities move synchronously. Notice that on the 6th of June 2011 the volume reached the highest peak when MtGox transferred (randomly) the total sum by 15 times. The bouncing continued until the 8th of December 2011. After that day, the sum began to be reduced, being divided equally into different blocks up to the point that it completely vanished as shown in Figure 24. Similar studies have been conducted by Nilsson [99].

So far we observe only preliminary and sometimes faint steps in this direction consisting mostly in public alerts and position documents to inform consumers and investors about the risks surrounding the use of digital currencies. The biggest regulatory concerns are related to two interrelated aspects: anonymity and decentralisation. The FBI in a recent report writes that Bitcoin provides a venue for individuals to generate, transfer, launder, and steal illicit funds with some anonymity [100]. Indeed, Bitcoin firstly emerged as means of payment in the deep web and unique accepted currency on Silk Road, an online black market best known as a plat-

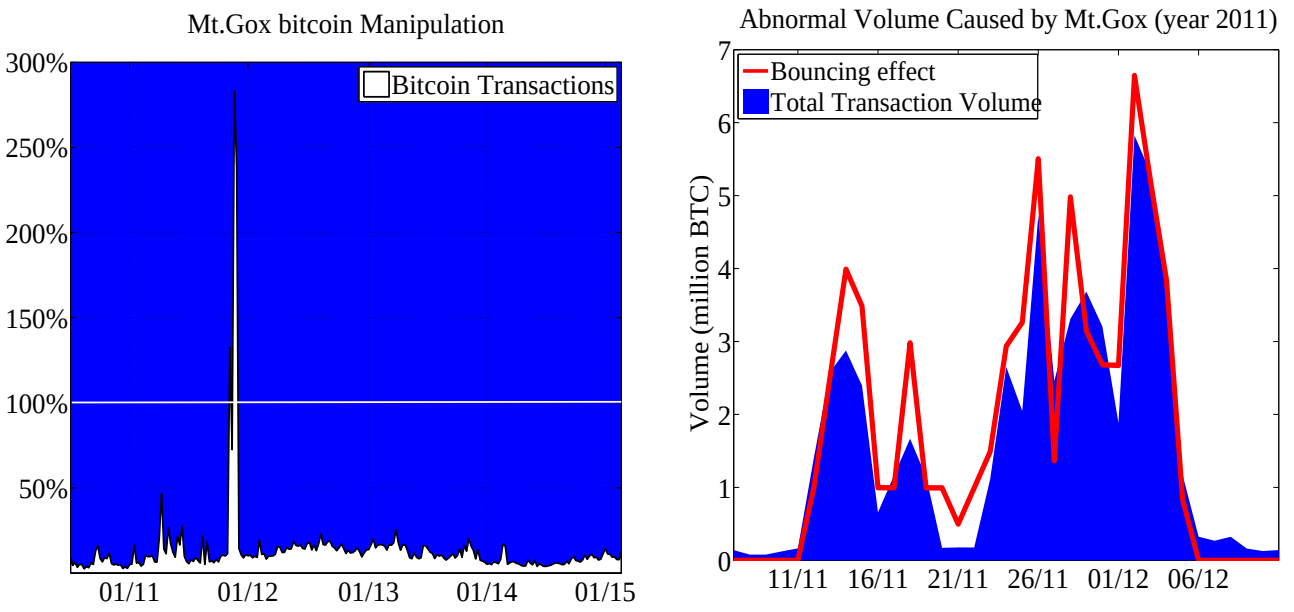

FIGURE 23: Left: Volume of Bitcoin transactions as percentage of the Bitcoin monetary base. MtGox's Bitcoin manipulation shows up in the blockchain with a spike of transactions at the end of 2011. Right: Comparison between the bouncing effect caused by MtGox and the total Bitcoin transactions for the period from November to December 2011. Data source: Bitcoin blockchain. Internal calculation.

form for selling illegal drugs. Silk Road was operated as a Tor hidden service, enabling online users to browse it anonymously and securely without being monitored. The website was launched in February 2011. The investigations coordinated by the FBI brought to its shutdown in September 2013. Silk Road generated sales revenue totalling over BTC 9.5 million and collected commissions from these sales totalling over BTC 600,000. Although the BTC/USD exchange rate varied significantly during that period, these figures are roughly equivalent today to USD 2.85 billion in sales and approximately USD 180 million in commissions. In November 2013 Silk Road 2.0 went online and still run by the former administrators of Silk Road, Ross Ulbricht. It too was shut down and the alleged operator arrested in November 2014. The operation called "Onymous" involved the police forces of 17 countries [101]. On the 29th of May 2015, Ulbricht was sentenced to life in prison [102]. Nevertheless, we do not expect that Mr Ulbricht's harsh sentence – intended to serve as a warning to others –, will have much effect.

In fact, the closing down of the Silk Road and Silk Road 2.0 marketplaces has simply cleared the way for competitors like Evolution, Agora, Alphabay and many others [103]. On the top of this, inclined scepticism towards digital currencies have been fuelled by cyber attacks, failures and bankruptcies of many (first-wave) electronic trading platforms during the last years. The most infamous example is MtGox, a Bitcoin exchange based in Tokyo handling 70-80% of all Bitcoin transactions in 2012-2013, which on 28 February 2014 filed for bankruptcy protection reporting that it had lost about 754,000 of its customers' Bitcoins, and around 100,000 of its

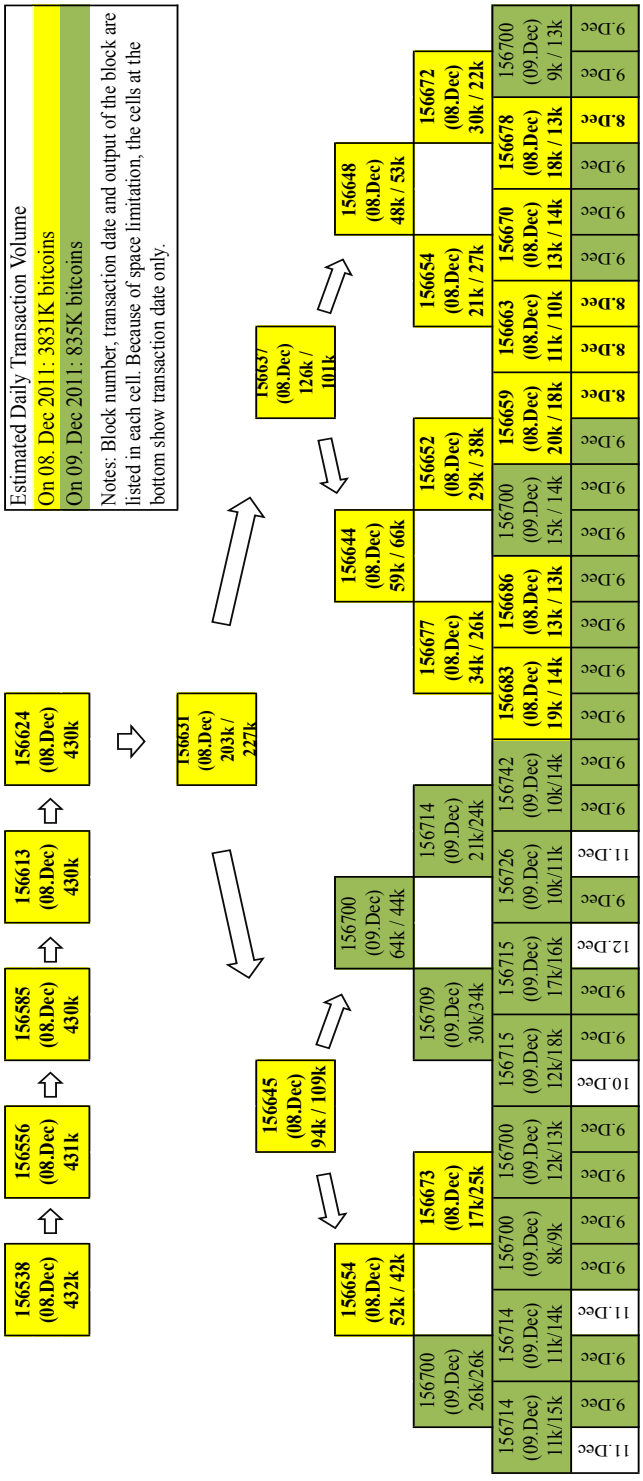

FIGURE 24: MtGox Bitcoin manipulation. Transaction tracing of post-bouncing period. Data source: Bitcoin blockchain. Internal calculation.

own Bitcoins, totalling around 7% of all Bitcoins in circulation at that time, and worth around USD 473 million near the time of the filing [104] [105]. Well before MtGox's bankruptcy in 2014, Moore and Christin [106] showed that nearly half of all exchanges had disappeared in the previous three years, wiping out the accumulated savings of many new users. One may consider these problems as temporary market fallacies reflecting the novelty and complexity of the technology and the naivety of many of the young entrepreneurs who started exchanges. However, these many failures and bankruptcies raised broader consumer protection concerns among regulators. Another aspect that is critical for regulators is the irreversibility of digital currency transactions. In contrast, electronic payment systems such as credit cards provide mechanisms to protect consumers against unauthorised and accidental transfers, see Section 4.2. The absence of such protection, which often are codified into laws, produces some concerns among regulators. All the above-mentioned concerns result in assigning digital currencies a permissive, contentious or hostile status by jurisdictions.

Hostile jurisdictions. Hostile countries include Bangladesh, Bolivia, Kyrgyzstan, Ecuador, and Iceland in which the banning applied only to the purchases of digital currencies because of the capital controls instituted in 2008 to stop money flight on the Króna. Under these rules, buying Bitcoins in Iceland is illegal. However, selling Bitcoin is still permitted, as it entails a movement of capital into Iceland, not out [107], [108], [109].

Contentious jurisdictions. Among those countries in a contentious status, there is China which does consider digital currencies as "virtual goods" and embraces restrictive policies. It prohibits the use of digital currencies by consumers to purchase real goods and services but allows their trading by individuals. Moreover, on the 5th of December 2013, the People's Bank of China passed a law prohibiting financial institutions in China from trading, underwriting or offering insurance in Bitcoin. In addition, websites in China that provide trading services are required to report investors' identities to regulators and take steps to prohibit money laundering [110]. These first moves by the People's Bank of China seem clearly aimed at removing digital currencies from mainstream use and limit them only to determined enthusiasts. In May 2014, the CEOs of five major China-based digital currency exchanges (OKCoin, Bitcoin China, BtcTrade, CHbitcoin and Huobi) jointly did not attend the Global Bitcoin Summit in Beijing and jointly pledged to comply with state policies and regulations. The move was reportedly made by the businesses due to recent adverse actions from the People's Bank of China, which has moved to more strictly enforce rulings meant to more firmly separate its traditional financial services sector from the emerging domestic Bitcoin economy. Thailand is another country with

a contentious status. Firstly, in July 2013 the central bank of Thailand declared that Bitcoin's non-legal tender status might have rendered its use illegal [111]. However, in March 2014 the situation improved after the statement by the bank of Thailand which better clarifies that Bitcoin is not illegal but warns consumers that it is not a currency and that its use comes with inherent risks. Apart from China and Thailand other countries like Indonesia, India, Jordan, Lebanon, Russia, Taiwan and Vietnam imposed some restrictions on the use and exchange of digital currencies [112], [94]. Starting from December 2014 (in coincidence with the Ruble crisis) the position of various Russian authorities and organisations turned against Bitcoin. The Russian politicians and lawmakers started to debate over whether Bitcoin and digital currencies should have been banned as part of a broader effort to stop capital flight. In early 2015, Russia's media regulator (Roskomnadzor) acted on a Court order and blocked several Bitcoin-related websites [113]. In 2015 a Russian state-owned media outlet reported that Russian authorities have issued warnings against using Bitcoin, saying the digital currency is a "money surrogate" which people may "play" with but not "use" it as tender and therefore treating it as a parallel currency is illegal [114]. By the end of 2015 Russian legislation is planned to implement fines for users who are found to create, mine, or issue Bitcoin or other digital currencies [115].

Permissive jurisdictions. Finally, the group of permissive countries includes the USA, most of the south America and European countries, Canada, Japan and Australia. For those countries the awkward problem is to understand whether digital currencies are commodities or currencies under their legal-regulatory framework. In the next pages we will focus on the comparison between the Bitcoin regulation in USA and in Europe.

8.1 REGULATION IN THE US

In the USA the federal reference is the regulatory guideline issued in by the Financial Crimes Enforcement Network (FinCEN), which is an agency within the US Treasury Department. FinCEN distinguishes between "users"[29], "administrators"[30], and "exchangers"[31]. A user of con-

[29] A user is an individual or legal entity that obtains digital currency to purchase goods or services on the user's own behalf.

[30] An administrator is an individual or legal entity that issues digital currencies, and who has the authority to redeem them from circulation.

[31] An exchanger is an individual or legal entity that exchanges digital currencies for real currencies, funds, or other digital currency.

vertible[32] digital currency is not a money service business (MSB) under FinCEN's regulations and therefore is not subject to registration, reporting, and record-keeping regulations. However, an administrator or exchanger which accept and transmit or buy and sell convertible digital currency is an MSB and specifically a money transmitter, unless in some exceptional cases.[33] MSBs must enforce Anti-Money Laundering (AML) and Know Your Client (KYC) measures [117]. AML and KYC are generally applied to all financial intermediaries in the business of currency exchange and they have been extended to people or business dealing with digital currencies.

New York. Recently, the New York State Department of Financial Services (NYDFS) stepped into Bitcoin space by proposing new regulation. This is the first attempt to issue ad-hoc regulations for Bitcoin-related businesses in order to safeguard customer assets, protect consumers from fraud and abuse, prevent money laundering and other illicit activity, and enforce measures against cyber crime [118]. This regulation, called BitLicense, is intended to apply only to financial intermediaries. This definition includes: (1) transmission; (2) storage, holding, custody maintenance or control of digital currencies on behalf of others; (3) buying and selling (crypto-to-crypto and crypto-to-fiat exchange service); (4) control, administration, issuance of a digital currency. It is worth observing that most of the above described activities already required an MSB licence by FinCEN. Thus, very few new businesses will be captured by this regulation. Exemptions from the license include: (1) users who issue loyalty and customer reward schemes, redeemable only within a predefined distribution channel or online market place; (2) business models where digital currencies are embedded in gift card mechanisms; (3) security systems for customers' digital currencies; (4) development and dissemination of software; 5) developers and businesses who engage in transmitting digital currency for non-financial purposes.[34]; (6) merchants and consumers that use digital currencies solely for the purchase or sale of goods or services or for investment purposes; (7) banks that are chartered under the New York Banking Law may be exempt from licensing with approval by the NYDFS superintendent.

Those businesses that will be impacted by BitLicense will be required to comply with the following rules: (1) capital requirements and protection of assets[35]; (2) record-keeping;[36] (3)

[32] According to FinCEN, this term refers to those digital currencies which either have an equivalent value in real currency, or acts as a substitute for real currency.

[33] For example, the miner that uses digital currency solely for the miner's own purposes and not for the benefit of another, is not an MSB under FinCEN's regulations. For a broader explanation [116].

[34] This is likely referring to the development of digital currency "stacks" that are built on top of the blockchains and offer the promise of a vast array of non-financial uses of the blockchain technology.

[35] Prohibition from selling, lending, or otherwise encumbering any custodial assets on their own accord.

[36] Registry with records of customer identification and account connections, statements made to customers

AML, KYC and reporting requirements;[37] (4) cyber security and consumer protection. Each licensee is obliged to establish and maintain an effective cyber security program;[38] and disclose specific information and threats associated with digital currencies to customers.[39] However, some concerns have been raised against certain aspects of the proposed Bitlicense. For example the Digital Asset Transfer Authority advances the following critiques: (1) the scope of regulated activities is too broad; (2) new AML requirements may pose serious privacy issues and require untenable data collection requirements; 3) risks of stifling innovation and imposing excessive burdens for technology companies; (4) need for a broader, transparent, tailored-made, and proportionate framework; (5) leveraging blockchain technology to increase privacy-enabling identity verification and effective oversight [119]. After some months of adjustments, the new rules, the first by a US state, have been issued on the 3rd of June 2015. One good aspect of this regulation is that companies that want both a BitLicense and an MSB license (under FinCEN) can work with the state regulator to have a "one-stop" application submission to cover the requirements for both. Although the industry thinks that New York's new rules are an improvement over the original proposals laid out in July (and revised in December) of 2014, they are still considered problematic especially in terms of costs and invasion of customers' privacy. As a result, many companies like Kraken, BitFinex, BTC Guild, LocalBitcoins, Genesis Mining, and many others are no longer offering their services to users in the New York area [120].

California. Similarly to New York, also the Assembly of California recently issued a specific Bitcoin legislative proposal (AB-1326 Virtual currency) [121]. The bill is still preliminary and certainly subject to change. However, the basic rule is that it will prohibit a person from engaging in any digital currency business unless the person is licensed by the Commissioner of Business Oversight or is exempt from the licensure requirement. Certain minimum conditions would also be required. According to the current state, the licence (or exemption from license) is required by all those persons who conduct either one of the following types of activities in-

and counterparts, general accounting ledgers, and detailed information on each transaction.

[37] As a general rule, the candidate will firstly undergo an initial risk assessment on legal, compliance, financial, and reputational risks associated with the licensee's activities, services, customers, counterparts, and geographic location. The licensee must then establish, maintain, and enforce an AML program based on the initial risk assessment. Some special activities will be required. For example, a customer who exceeds USD 10,000 in aggregate transactions over a 24 hour period must be reported, as well as any other suspicious transaction that may signal money laundering, tax evasion, or other illegal activities.

[38] Licensee must generate a written cyber security policy addressing areas such as network and physical security, access controls, business continuity, capacity and performance planning, and incident response.

[39] Potential material risks, such as digital currency's lack of governmental backing, shifting regulatory risk, the irreversible nature of digital currency transactions, and the general instability and volatility of the trading market.

volving a California resident: (1) maintaining full custody or control of digital currency on behalf of others; (2) providing conversion or exchange services of fiat currency into digital currency or the conversion or exchange of digital currency into fiat currency or other value, or the conversion or exchange of one form of digital currency into another form of digital currency. California's bill follows similar principles seen in the BitLicense. However, at the moment it brings some differences. For example, California's bill would require all licenses to hold and maintain a bond or trust account in USD for the benefit of its customers in the form and amount as specified by the commissioner. In determining the minimum amount of capital that must be maintained by a licensee, the commissioner considers a variety of factors (e.g., the size and composition of the licensee's total assets, including the position, liquidity, risk exposure, and price volatility of each type of asset, the composition of the licensee's total liabilities, including the size and repayment timing of each type of liability). The commissioner can impose a civil penalty for a violation of California's bill provisions. Moreover, a licensee that intentionally makes a false statement, misrepresentation, or false certification in a record filed or required to be maintained under this division or that intentionally makes a false entry or omits a material entry in such a record is guilty of a felony. However, as in the case of BitLicense, also for the AB-1326 there are many opposers who think that the bill is too premature and technically inaccurate [122].

8.2 REGULATION IN EUROPE

The situation in Europe is very different compared to the USA. There is hardly any specific law, directives or regulations on digital currencies at the EU level. Moreover, single member states have continuously provided new regulatory guidances by often adopting different approaches on the topic. In this regards, the EBA highlights the need to define, in the long term, a harmonised regulatory framework which secures the operation of digital currencies to authorised subjects and defines, among other things, the requirements for capital and governance of market participants and the separation of customer accounts from business accounts. In the short term, the EBA identified the urgent need to mitigate the risks arising from the interaction between the digital currency schemes and regulated traditional financial services [44]. Thus, the EBA invited the national supervisory authorities to discourage financial intermediaries from buying, selling or holding in deposit digital currencies [45]. EBA sustains its position by providing a long list of more than 70 risks associated to digital currencies across several categories: (1) risks to users; (2) risks to non-user market participants; (3) risks to financial integrity; (4) risks to payment systems and payment service providers in conventional fiat currencies; (5)

risks to regulatory authorities. Starting from Figure 1 in [44], we collapse together similar risks, we discard non-specific digital currency-related risks (i.e, risks that may apply also to any other activity carried out in the traditional financial sector) and then we summarise the most relevant and important ones in Table 7.

Macro Category	Subcategory	Description of the Risks
Risks to users	Risks that arise irrespective of intended usage	Risk of an exchange acting negligently/fraudulently or being hacked
		Risk of significant or unexpected exchange rate fluctuation (significant volatility)
		Fraudulent manipulation of: (1) personal computing power by hackers; (2) fees by mining pools; (3) protocol by the majority of the miners.
		Counterparty risk, especially in presence of anonymity.
		Risk of wallets/exchange thefts, hacking or soft/hardware malfunction.
		User is in violation of applicable laws and regulation or unable to legally enforce the contracts.
	Risks that arise when	No guarantee that digital currencies are accepted by merchants.
		Risk of suffering loss due to payment errors because of the irreversibility of transactions.
		User cannot access their digital currencies after losing password/keys to their wallet.
	Investment Risks	User suffers loss as a result of prices/exchange rates being manipulated.
		Risk of investing in a fraudulent or Ponzi digital currency investment scheme.
Risks to non-user market participants	Risks specific to exchanges	Exchange is unable to fulfil payment obligations denominated in digital or fiat currencies.
		Exchange lacks adequate governance arrangements to oversee transactions and lacks safeguards against hacking.
	Risks specific to merchants	Risk of double-spending if the verification process is compromised or corrupted.
		For spot sales: risk that the merchant is not able to spend or convert the digital currencies received. For future sales: absence of hedging instruments.
Risks to financial integrity	Money laundering and terrorist financing risks	Criminals are able to launder proceeds of crime because they can deposit and transfer digital currencies anonymously, rapidly and irrevocably.
		Criminals or terrorists use the digital currency remittance systems and accounts for financing purposes or to disguise the origin of criminal proceeds.
	Risks of financial crime	Risk to escape from regulated financial sector and trade in illegal traffic/activities.
		Criminals may avoid seizure of assets and confiscation, as well as international embargoes and financial sanctions.
		Tax evaders are able obtain income denominated in digital currencies, outside monitored traditional payment systems.
Risks to payment systems and PsP in FCs	Payment service providers in fiat currencies offering also digital currency payment services suffer loss and reputational risk when providing unregulated digital currency services that subsequently fail to legally or economically perform.	
Risks to regulatory authorities	Reputational risks	Regulators decide to regulate digital currencies but the chosen regulatory approach fails.
		If regulators do not regulate digital currencies there is the risk that the viability of regulated financial institutions is compromised as a result of their interaction with digital currencies.
		Regulation and supervision of conventional financial activities is circumvented by unregulated "shadow" activities that incur the same risks.
	Legal	Regulator is subject to litigation as a result of introducing regulation that renders pre-existing contracts illegal/unenforceable.
	Risks to competition objectives	Trade-off between a regulation that guarantees market stability and a regulation that boosts innovation.

TABLE 7: Risks associated to the use of digital currencies. Data source: EBA.

Germany. Germany has been one of the first European countries to step in and, already back to August 2011, the German Federal Financial Supervisory Authority (BaFin) declared Bitcoins to be a "Rechnungseinheiten" (unit of account under German law) [123]. Rechnungseinheiten are like currency units in that they are units of account, but unlike currency units they do not have a legal tender status and therefore qualify neither as foreign currency nor as foreign banknotes and coins. Moreover, within the meaning of the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz) digital currencies are not considered e-money because there is no issuer establishing claims against himself by issuing digital currencies. The designation treats Bitcoins as a kind of "private money" or complementary currency used as a means of payment in settlement accounts by virtue of private-law agreements. This classification has legal and tax implications. While US regulators have chosen to focus on the obligations of the exchangers and administrators, German regulators have concentrated their efforts on regulating the users by classifying digital currencies as units of account. This classification implies that users are subject to 25% capital gains tax if they hold the currencies for less than one year. According to BaFin, mining does not require any authorisation. However, an authorisation requirement may arise from additional circumstances. This applies when an existing market is maintained with the contribution paid by the users. This is for instance the case if persons advertise on the market that they regularly purchase and sell digital currencies. Another example is that of mining pools commercially sharing the profits from mined and sold digital currencies in return for computing power provided by the user. As general rule, if digital currencies are traded, they are deemed to be "financial instruments" requiring authorisation. In accordance with the Kreditwesengesetz, the trading must be conducted commercially or on a scale which requires a commercially organised business undertaking. Key examples of this are: principal broking services, multilateral trading systems, investment and contract broking, as well as proprietary trading. In those cases, a banking licence or specific authorisation should be required. However, wherever the question of an authorisation requirement will be submitted, a differentiation has to be made in terms of technical implementation and the respective terms of the contracts and transactions [124].

France. The Banque de France declared that digital currencies are considered units of account but cannot be regarded as a means of payment, or even as e-money in the sense defined by the French Monetary and Financial Code, as they are not issued on the receipt of funds. This interpretation and classification is equivalent with the German one. Moreover, unlike e-money, there is no legal obligation to reimburse digital currencies owners at face value and at any time. At the same time, l'Autorité de contrôle prudentiel et de résolution (ACPR) acknowl-

edges exchange and payment transactions in digital currencies but requires actors to obtain a licence as payment service providers [125].

Switzerland. Also in Switzerland, at the time of writing, a specific Bitcoin legislation is not in place. However, the Swiss Financial Market Supervisory Authority (FINMA) is endowed with supreme authority over the financial markets (and Bitcoin in particular) and reports directly to the Swiss parliament. FINMA received the mandate from the parliament to apply the current banking and financial laws, ordinances, directives and regulations also to Bitcoin-related businesses. In performing its mandate, FINMA adopts a very strict interpretation of the current financial market laws and regulations [126]. FINMA explicitly considers Bitcoin as a means of payment which means that under Swiss law, Bitcoin is comparable to "foreign currency" even though it is not a legal tender. Therefore, any financial intermediary which does business with Bitcoins, must in principle comply with the Swiss AML and Banking Acts. With regards to money laundering, in the revised AML Ordinance (AMLO-FINMA SR. 955.033.0) that will come into force on the 1st of January 2016, the Swiss regulator takes into account the increasing digitalisation of payment transactions [127]. In this respect cashless payments of goods and services amounting to CHF 5,000 a month and/or CHF 25,000 a year to traders in Switzerland can be made without formal client identification. As regards digital currencies however, FINMA does not make any concessions owing to heightened money laundering risks. With regards to the Banking Act, each business model is assessed individually to establish which licensing requirements must be complied with. A banking licence may be required in some cases. This is generally the case when an individual or legal entity accepts money on a commercial basis from clients and keeps it in their own accounts. The same applies to providers who accept Bitcoins from clients and administer Bitcoin holdings for clients. For more information see the FINMA Factsheet "Bitcoins" dated 25 June 2014 [126] and the Federal Council report [128] on digital currencies in response to the Schwaab (133687) and Weibel (134070) postulates dated 25 June 2014.

Italy. In Italy, as in the other EU jurisdictions, digital currencies are not *ex-ante* subject to any regulation at this time. However, so far Banca d'Italia published three opinion documents and supervisory bulletins: (1) warnings on the use of digital currencies issued on the 30th of January 2015 ; (2) notice on digital currencies on the 30th January; (3) notice of the Financial Intelligence Unit for Reporting on digital currencies issued on the 2nd of February 2015 [129], [130] and [131]. According to the notice released on the 30th of January 2015, the purchase, use and acceptance of digital currencies must be considered lawful activity, i.e., the parties are

free to transact in amounts not expressed in legal tender. Moreover, in the same bulletin Banca d'Italia instructs financial institutions to follow the EBA's recommendation of avoiding buying or investing in digital currencies until a formal legal framework has been established [45]. Finally, Banca d'Italia alerted consumers on the presence of specific Bitcoin-related risks: (1) the issuance and management of digital currencies, including currency conversion in traditional activities are not subject to supervision by Banca d'Italia or of any other Italian authority; (2) in case of fraudulent conduct, bankruptcy or cessation of trading platforms, there are no specific regulatory safeguards designed to cover losses and traditional instruments of protection such as deposit guarantee systems are not in place. The notice by the Financial Intelligence Unit of Banca d'Italia on the 2nd of February 2015 states that businesses dealing in digital currencies, including holding them and exchanging them for fiat currencies, are not required to comply with any AML/KYC regulations. However, the recipients of the Legislative Decree no. 231/2007 (the Italian AML Act), when offering Bitcoin-related services, in order to prevent the use of the economic and financial system for money laundering and terrorist financing, must identify the operations involved with digital currencies, detecting any suspicious elements.

United Kingdom. Differently from other European jurisdictions, the regulatory position on digital currencies is not yet clear in the United Kingdom. In September 2013, the UK regulators communicated that Bitcoin-based businesses would not be required to register with regulators, at least for the time being, while their regulatory position is considered. The first orientation among UK regulators was to treat Bitcoin not as money, but instead as "single-purpose vouchers", which could imply a VAT tax liability on any Bitcoins that are sold. However, the UK tax agency (HM Revenue and Customs) brief treats digital currencies like any other form of payment for tax purposes [132] and [133]. The HMRC set out the rules on the tax treatment of income received from, and charges made in connection with mining, trading, payment processing or services involving digital currencies, specifically for VAT, Corporation Tax, Income Tax and Capital Gains Tax. Next to the tax guidance of HMRC, not much has happened relating to a comprehensive regulatory initiative. In the UK, the Financial Conduct Authority (FCA) is a regulatory body that operates independently of the UK government, and regulates financial firms providing services to consumers and with the goal to maintain the integrity of the financial markets. It focuses on the regulation of conduct by both retail and wholesale financial services firms. In the last years, several Bitcoin-related businesses have approached the FCA seeking clarification on the legalities of operating their business. However, the FCA so far has not issued any guidance or comments on the regulation of digital currencies. In practice, the outcome has been that Bitcoin businesses in the UK are not obliged to register with or

be authorised by the FCA. However, the UK has a well-established tradition of self-regulation. Therefore, a number of Bitcoin businesses act in accordance with the FCA rules, even though they are not required to do so. This approach seems to favour an organic development of the UK Bitcoin ecosystem by allowing business to adopt their own interpretations of the rules. However, this approach may also generate some opacity and uncontrolled risks, especially in terms of money laundering, that may even stifle the Bitcoin expansion in the UK. The UK AML regulations of 2007 are enforced by a number of entities, principally the HMRC, the FCA, but also some others. However, there exists still no formal obligation to prevent money laundering through dealings made in Bitcoin. This is quite remarkable if compared to the US and the other EU member states previously analysed. However, this appears to be a temporary situation. In March 2015 the UK Treasury officially clarified that the government intends to apply AML regulation to digital currency exchanges in the UK, to support innovation and prevent criminal use. The HM Treasury warns that: "Compliance with money laundering requirements will introduce significant resource and compliance burdens which may well reduce the number of issuers down to those who have the financial backing to satisfy these requirements". At the same time, the HM Treasury expressed its intention to directly collaborate with the British Standards Institution and the digital currency industry in order to develop new voluntary standards for consumer protection in the area of digital currencies [134] and [135].

We conclude this section by pointing out two open issues. The first regards the duality of digital currencies as a commodity (or property) and a currency, which is likely to create a gap between the US and the EU approaches regarding the legal nature of digital currencies. So far, the US authorities seem to classify digital currencies as commodities. This could bring digital currencies under the regulatory umbrella of the US Commodity Futures Trading Commission. Instead, the first general interpretations by the EU member states seems to consider digital currencies as units of account and therefore as "virtual currencies" on payment platforms. The second issue relates to the different degrees of legal and regulatory intervention adopted by the jurisdictions. This depends on the divergent positions taken by regulatory *unexceptionalists* (those who are in favour of full regulation of this new emerging technology related to digital currencies) on the one hand and by regulatory *exceptionalists* (those who prefer specific circumscribed measures instead of over-regulating the whole emerging technology) on the other. In the last years, with respect to Internet-based activities, we have observed an exceptionalist approach by lawmakers and regulators [136]. Regulatory responses to social networking sites like Facebook are a prime example of Internet exceptionalism. Rather than regulating these sites like other websites, regulators have sanctioned laws specific to social networking

sites, e.g., verify users' age and data protection. In effect, regulation of social networking sites can differ considerably from offline enterprises and also from other websites as well. We observe a similar ad-hoc specific intervention also in Bitcoin-related business models. In some cases, the Internet-based Bitcoin-related activities are truly unique or special and should be regulated accordingly. Regrettably, exceptionalism can simply reflect potentially harmful regulatory alarmism, especially towards Internet entrepreneurs and their investors. It can also distort the marketplace between Bitcoin enterprises and their offline competition. In extreme cases, unjustified regulatory intervention may also stunt the growth of the Bitcoin ecosystem.

9 DEFLATIONARY PROPERTY

Under the framework of various theories of money, in this section we try to understand the inflationary properties of digital currencies in general and Bitcoin in particular within the Bitcoin economy.

The supply mechanism of digital currencies is usually considered as an alternative solution by those monetarists and Austrian economists who think that inflation is intimately related to the money supply: (1) from a monetarist perspective, price inflation is always a monetary problem and depends on how fast the money supply grows [137]; and (2) for the Austrian school, inflation refers to the increase in the quantity of money not being offset by a corresponding increase in the demand for money [138]. In particular, for the Austrian business cycle theory the volatility in the rate of change of the money supply (i.e., credit expansion and credit contraction) is considered to be the major source of boom-bust cycles [139]. The quantity theory of money, simply stated, says that any change in the amount of money in a system will change the price level. Figure 25 (left) portrays the growth rates of money and the nominal gross domestic product during the last 50 years in the US with varying degrees of turbulence and price swings. Monetarists maintain that money should be "neutral" and this should be achieved by setting money growth at a particular percentage and sticking to this percentage indefinitely. The essence of this way of thinking is that there is no relation between a constant rate of monetary growth and the rate of growth in real output. Digital currencies embrace this characteristic because the total supply is by design finite, its rate of change is not volatile and both the current and future growth rate are known a priori. Figure 25 (right) shows the money growth rate up to the year 2140 for the case of Bitcoin. As we explained in Section 3, Bitcoins are created each time a user discovers a new block. By considering the time taken to generate the last 2016 new blocks, the protocol adjusts the mining difficulty such to keep a constant time rate of 10 minutes per block creation. The number of coins generated per block is set to decrease

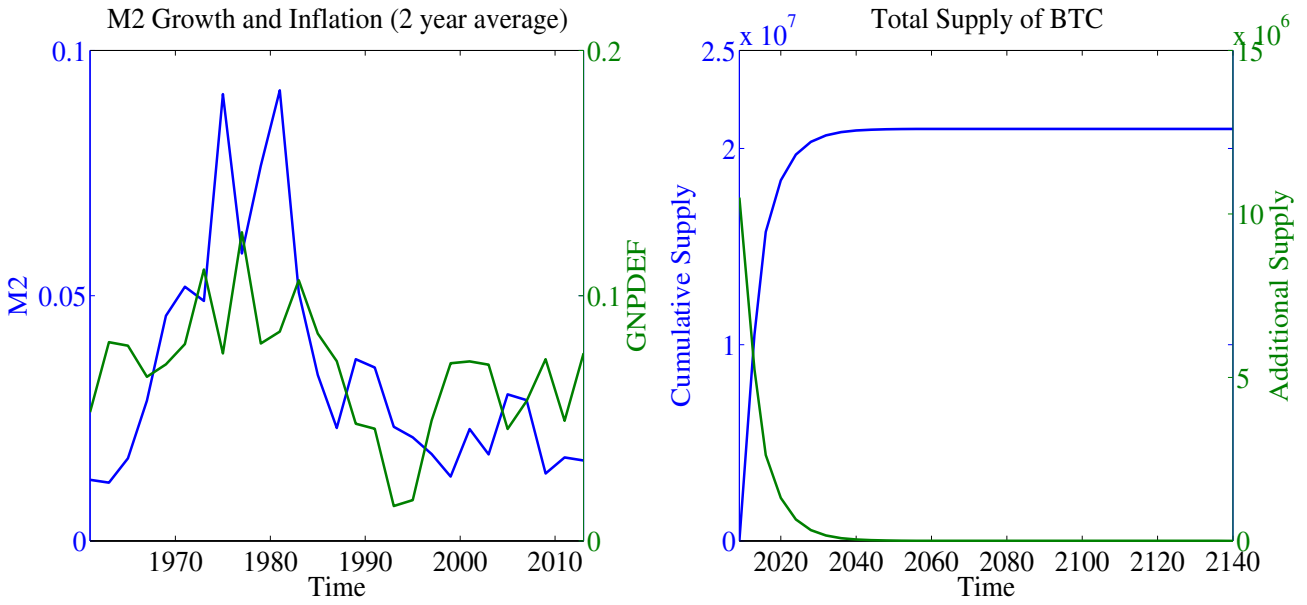

FIGURE 25: Left: M2 money supply growth rate and inflation as measured by the GNP price deflator. Data from 1961 to 2013 are taken from the Fred database. Series IDs are GNPDEF and MSNS. Right: The total Bitcoin supply is by design finite and its rate of change is not volatile and both the current and future growth rate are by design known a priori.

geometrically, with a 50% reduction every 210,000 block (i.e., about four years). The result is that the number of Bitcoins in existence will never exceed 21 million. A similar supply control mechanism is in place also for other digital currencies such as Litecoin which has a similar growth rate than Bitcoin even though with a four time larger money supply.[40]

However, relatively simple monetary rules or policies can promote economic stability because people can easily learn the rules, hence making it easier for them to coordinate their beliefs [140], [141]. In contrast, deflationary currencies like Bitcoin, which has a decreasing monetary-growth-rate, can be detrimental for the economy. We learn from modern economic theory that deflationary currencies: (1) bring unemployment because wages do not adjust downward and would require a continuous adjustment of prices for all goods and services; (2) carry an intrinsic value because they promise to buy more goods "tomorrow" than "today" and consequently incentivise people to build savings instead of borrowing money; (3) become increasingly illiquid, expensive and volatile, rendering them less useful, with less merchants incentivised to accept them.

One could indirectly assess Bitcoin's deflationary property by comparing the quantity of coins held for hoarding with respect to the quantity used in transactions and trading. Indeed,

[40]The initial reward for each Litecoin block is 50 Litecoins. The rate of Litecoin generation is halved every 840,000 blocks (i.e., 4 times the blocks compared to Bitcoin). However, the generation of Litecoin blocks is 4 times faster than that of Bitcoin, thus the money supply of Litecoin will follow the same pattern as that of Bitcoin with about 3/4 of all Litecoins being generated by 2020.

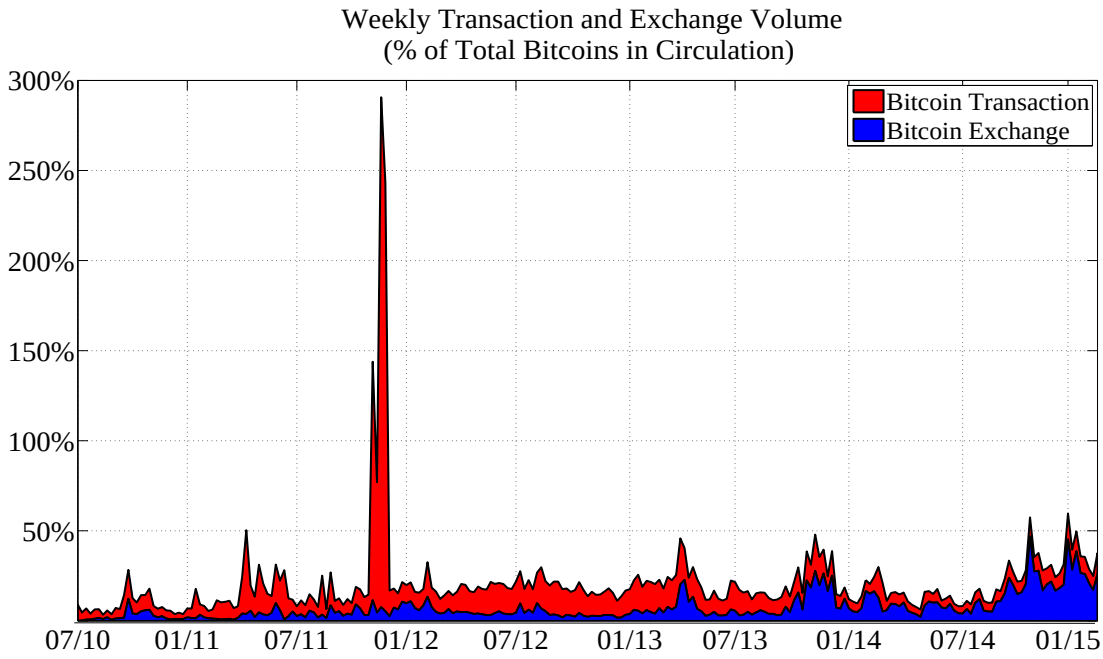

FIGURE 26: Relative percentage of the weekly Bitcoin transactions registered in the blockchain and the Bitcoin volume exchanged in the major trading platforms with respect to the Bitcoin monetary base. Data source: Bitcoinity and Blockchain. Internal calculation.

Figure 26 shows that the majority of Bitcoins issued so far are stored and do not circulate into the consumer markets for goods and services or into the financial markets for trading or remittance. For the period 2011–2015, the quantity of coins in circulation oscillated around 25% of the monetary base, with peaks of about 50%. Moreover, the figure shows that during the last months of 2014, the weekly volume of Bitcoins, exchanged in the major trading platforms, overcame the volume of transactions registered in the blockchain and touched the historical high of 50% of the monetary base. [41]

The statistics in Figure 26 combined with Figure 27 (left), highlighting Bitcoin volatility, confirms that Bitcoin suffers from all the drawbacks of a deflationary currency. Figure 27 (left) shows the 30-day volatility of the BTC/USD exchange rate expressed in standard deviations (StdDev) as follows:

$$StdDev = \frac{1}{30}\sqrt{\sum (x_t - \mu)^2}\,, \quad x_t = \mathsf{Log}(BTC/USD_t - BTC/USD_{t-1}).$$

Over the last few months of 2014, the volatility of BTC/USD started to decrease. However, it remains at levels of magnitude that are significantly higher than any other fiat currency in circulation. Although in the literature there is no general consensus on the factors affecting exchange rates and their volatility, the lack of liquidity could be one possible explanation for

[41] This trend is mostly driven by the BTC/CNY market, see Figure 12.

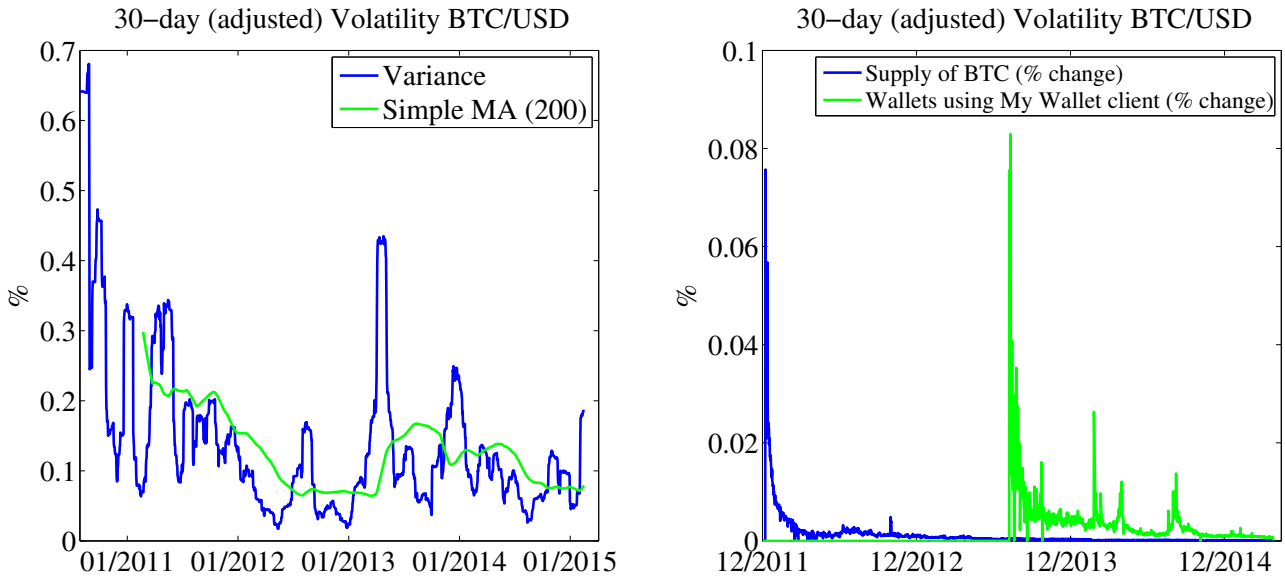

FIGURE 27: Left: 30-day volatility of BTC/USD measured as the following standard deviation. Right: Rate of change of the number of downloads of My Wallet clients compared to the rate of change of the Bitcoin money supply. Data source: Blockchain.info. Internal calculation.

the volatility. This makes Bitcoin a terrible store of value. To ensure liquidity, an increasing number of traders should constantly be willing and ready to buy and sell Bitcoins at the prevalent market price. Unfortunately, the paradox of deflationary currencies like Bitcoin is that the more people start using the currency, the higher the value of the currency will be which, in turn, leads to an increment of hoarding, to a deflation rate and volatility.

However, not all digital currencies have a finite supply or are deflationary as Bitcoin. Some popular digital currencies indeed follow an inflationary supply mechanism. Dogecoin, for example, after all the block halvings are over, will be produced at a constant rate of 10,000 Dogecoin per block, forever. Since in this case the generation of each block takes one minute, this implies about 5,256 billion Dogecoins every year. Also Peercoin is supposed to grow about 1% per year due to its PoS system [142], [143]. Moreover, with the introduction of the fractional reserve system, also the money supply of fixed supply currencies like Bitcoin can be expanded well beyond the limits imposed by the protocol. Already at present, Bitcoins can be created not only from mining but also from lending. This is exactly the process called “money creation”. Then, while the monetary base is fixed and known a priori, the total supply would end up exceeding the number of mined coins because of peer-to-peer lending, where borrowers and lenders meet directly. As example of such services see, for instance [144], [145]. Since digital currency lending currently is not explicitly regulated, there is no fractional reserve requirement. The money multiplier is therefore theoretically infinite. In any case, there exists a natural cap because those who are willing to lend will not find infinitely many borrowers with

sufficient creditworthiness. The business of Bitcoin lending deserves more attention as it is only at the beginning and could evolve to become more significant in the near future. [42]

We conclude with two considerations on peer-to-peer lending and money supply. First, lending and the related adoption of digital currencies in business-to-business and business-to-consumer transactions will likely start to increase when the volatility starts to decline. Second, as long as the user base keeps growing faster than the Bitcoin money base, Bitcoin will likely remain in deflation. Figure 27 (right) compares the rate of change of the number of downloads of My Wallet clients with the rate of change of the Bitcoin money base. The number of wallet hosts using the My Wallet service is, however, only a rough approximation of the real number of users in the Bitcoin network because users may adopt alternative desktop, mobile, web, and hardware wallets or they may possess more than one individual wallet.

10 MARKET EFFICIENCY

According to economic theory, the *law of one price* should hold for a single good that is traded in competitive markets with no transaction costs and no barriers to trade. However, in practice, details about market microstructure are important in determining whether violations of the law can occur.

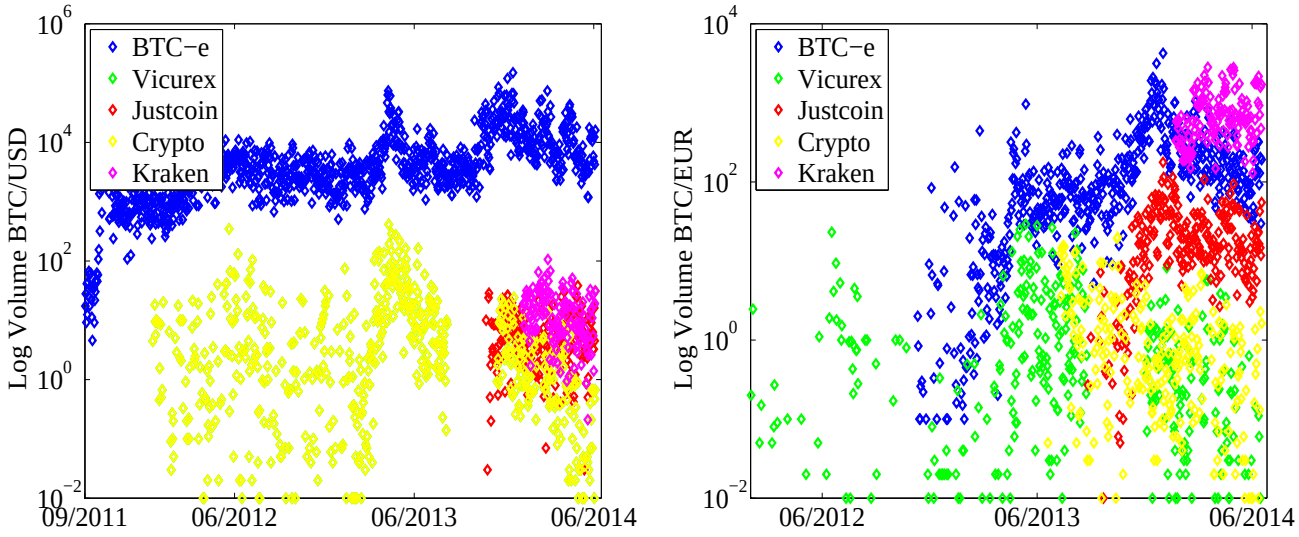

FIGURE 28: BTC daily trading volume on major trading platforms. Data source: Bitinfocharts. Internal calculation.

In this section, we shed light on several liquidity aspects of the digital currency exchange

[42] In May 2005, a New York-based Bitcoin company called Terra Group Inc., launched Tera Global: a Bitcoin lending and borrowing facility program for financial market participants [146].

market and on the premium required by investors for using less liquid trading platforms. In our analysis, we compare the volumes and the currency pairs of BTC/USD and BTC/EUR quoted by major trading platforms from January 2012 to June 2014. The digital currency exchange market is relatively young (about 5 years old) and for this reason investors and traders face problems related to liquidity premiums and higher inter-dealer broker costs coupled with difficulties in finding executable prices. In the long run, stronger competition together with adequate and clearer regulation will turn the digital currency exchange into a mature market characterised by low commissions, more stable exchange rates and aligned quotations among trading platforms.

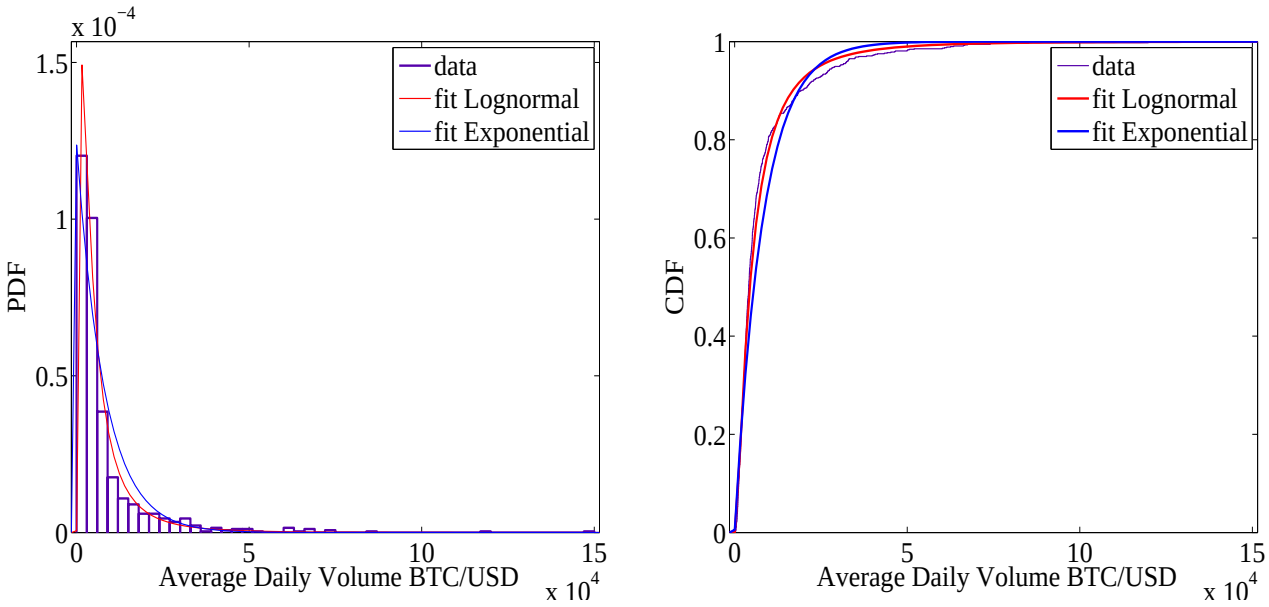

FIGURE 29: Average volume BTC/USD among trading platforms for the period January 2012–June 2014. Left. Probability density function. Right. Cumulative density function. Data source: Bitinfocharts. Internal calculation.

At present, BTC/USD and BTC/EUR are the most traded crypto-to-fiat pairs in the market. Hereafter we will use volume as a proxy for liquidity. Some descriptive statistics with data taken from [147] are presented in Tables 8 and 9 and plotted in Figures 28, 29, 30, and 31. Figure 31 (left) indicates high correlation between the trading volume of BTC/EUR and BTC/USD. The correlation on the positive-lag side is significantly higher than on the negative-lag side, which implies that, in the long term, the BTC/EUR exchange market is following the BTC/USD market.

Test 1: Exchange rate dispersion "without" platforms. For the period under analysis (January 2012–June 2014), BTC-e is the broker-dealer with the highest volume per trade, see Figure 28. Therefore, BTC-e is the platform where liquidity providers can be found more easily

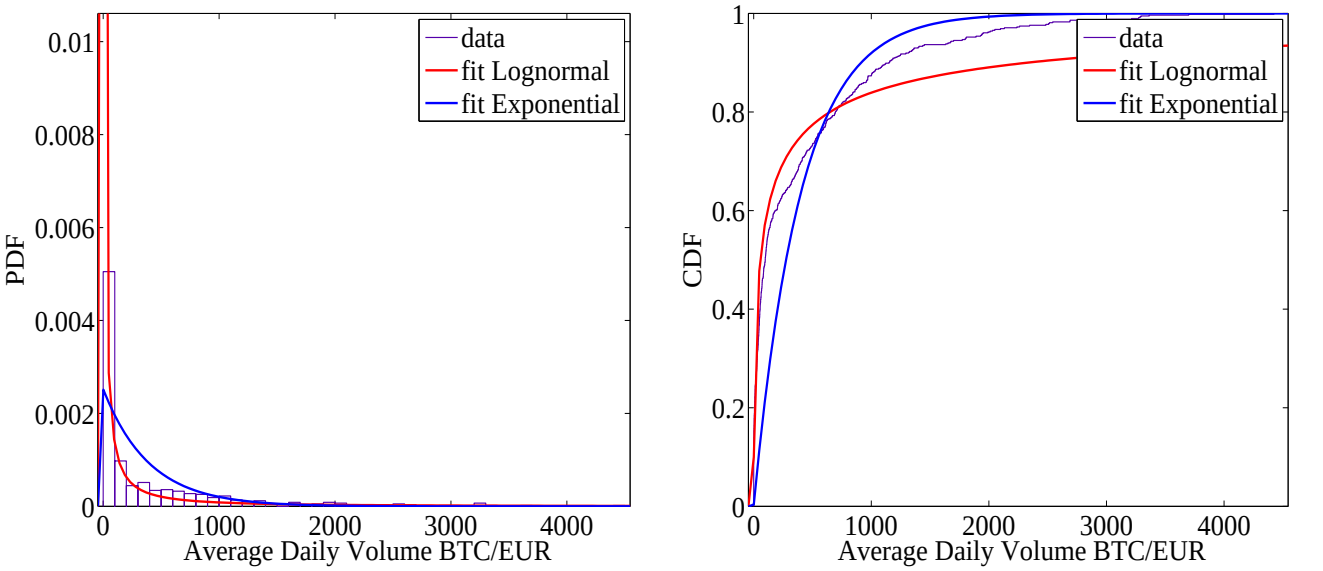

FIGURE 30: Average volume BTC/USD among trading platforms for the period January 2012–June 2014. Left. Probability density function. Right. Cumulative density function. Data source: Bitinfocharts. Internal calculation.

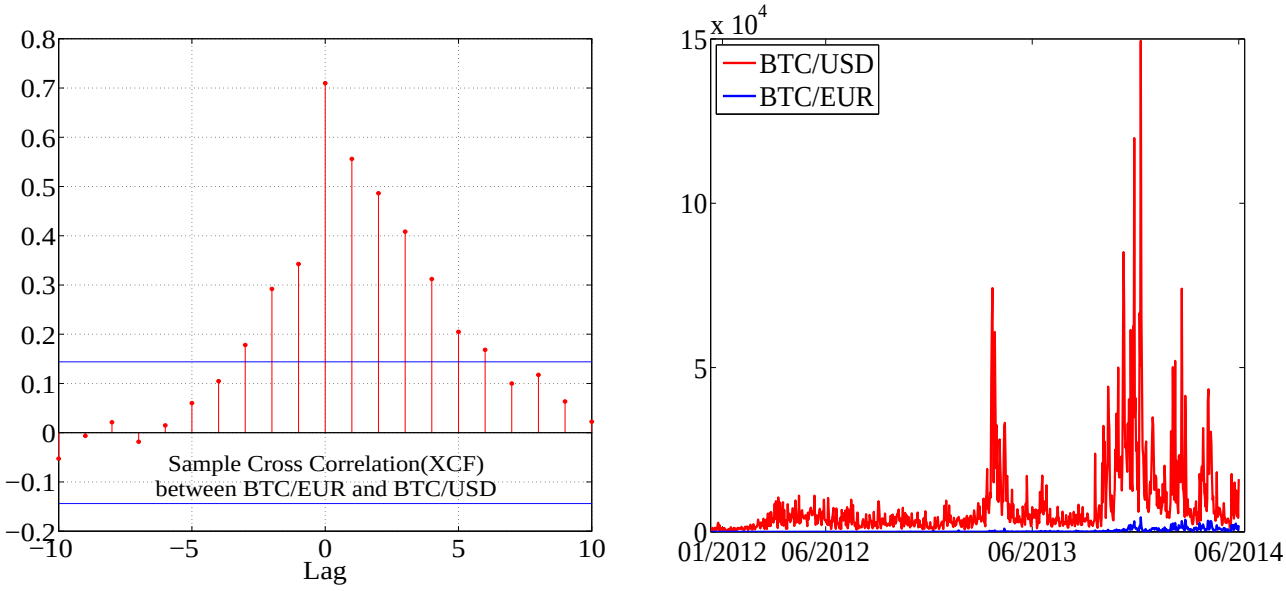

FIGURE 31: Left: Cross-correlation between trading volume BTC/USD and BTC/EUR. Right: Average BTC/USD and BTC/EUR volume among trading platforms. Data source: Bitinfocharts. Internal calculation.

than in other trading platforms. The price dispersion among the major trading platforms for the BTC/USD and BTC/EUR pairs is an indicator that captures the distance of a currency pair quoted in a given platform to the same currency pair quoted in the reference platform (in our case, BTC-e). The average exchange rate dispersion (Δ^1) across different trading platforms i

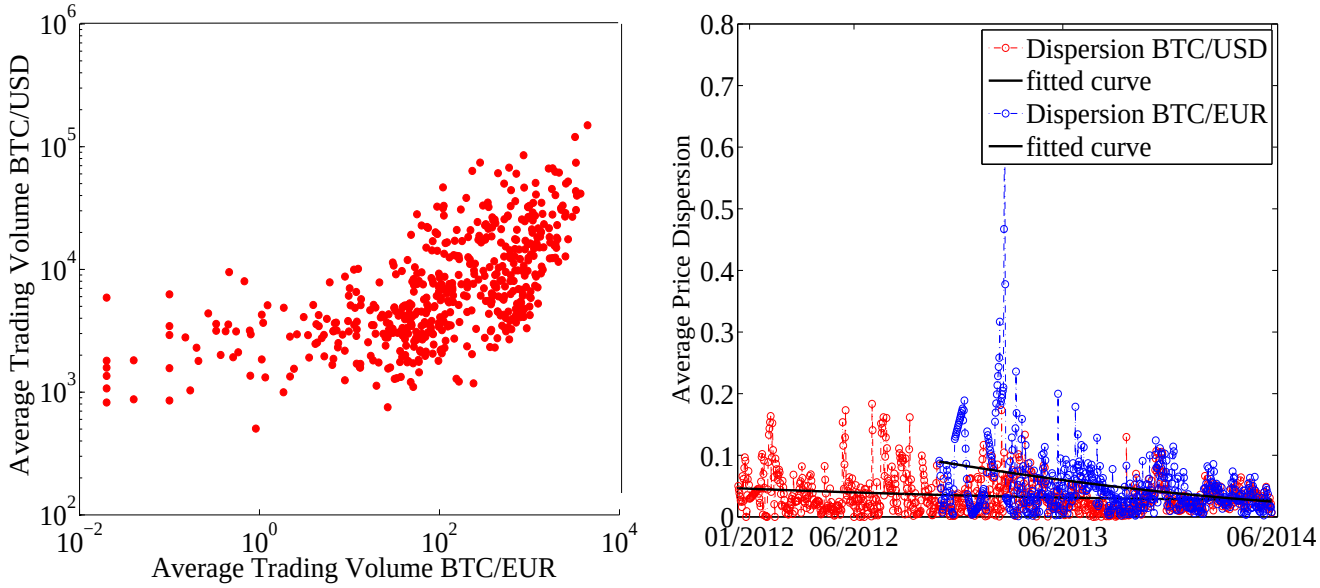

FIGURE 32: Left: Correlation between trading volume BTC/EUR and BTC/USD (log-log plot). Right: Average exchange rate dispersion Δ across trading platforms with reference BTC-e.

(with i=Kraken, Vicurex, Justcoin, Crypto) with respect to BTC-e, is computed as follows:

$$\Delta^1 := \frac{1}{n}\sum_{i=1}^{N}\left|\frac{(BTC/X)^i}{(BTC/X)^B} - 1\right| \in [0,1]. \tag{3}$$

B stands for BTC-e and X is either USD or EUR. The results are shown in Figure 32 (right) in a scale that starts from zero indicating the lower price dispersion.

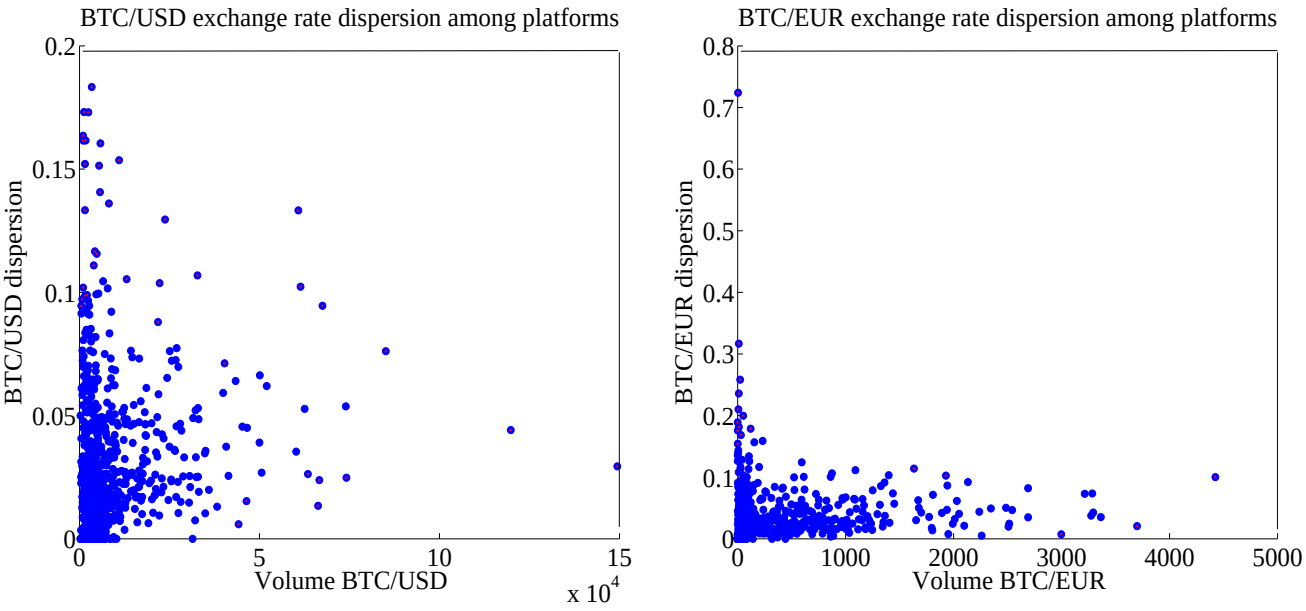

FIGURE 33: Correlation between volume and exchange rate dispersion across trading platforms.

	Distribution Lognormal	
Log likelihood	-8769.36	
Domain	$-\infty < y < \infty$	
Mean	7607.03	
Variance	$1.14565\text{e}+08$	
Parameter	Estimate	Std. Err
mu	8.3909	0.0350258
sigma	1.04492	0.0247878
	Estimated covariance of parameter estimates	
	mu	sigma
mu	0.0012268	$4.36461\text{e}-18$
sigma	$4.36461\text{e}-18$	0.000614437

	Distribution Exponential	
Log likelihood	-8893.37	
Domain	$0 \leq y < \infty$	
Mean	8042.92	
Variance	$6.46885\text{e}+07$	
Parameter	Estimate	Std. Err
mu	8042.92	269.599
	Estimated covariance of parameter estimates	
	mu	
mu	72683.7	

TABLE 8: Statistics of average volume across trading platforms for the currency pair BTC/USD. Period: January 2012-June 2014.

From our analysis, Δ^1 decreases over time both for BTC/USD and BTC/EUR. Lower exchange rate dispersion across trading platforms could be favoured by many factors, e.g., higher frequency trading or higher levels of market liquidity (here proxied by volume). However, volume and Δ^1 are weakly correlated as shown in Figure 33. In particular, for the period under analysis: $Corr(\text{Volume}_{BTC/USD}, \Delta^1_{USD})$ =0.1774 and $Corr(\text{Volume}_{BTC/EUR}, \Delta^1_{EUR})$ =0.0549.

Test 2: Exchange rate dispersion "within" platforms. An arbitrage opportunity arises when investors can earn riskless profits without making net investment. In the digital currency exchange market, arbitrage may occur whenever an investor can indirectly exchange, via an intermediate digital currency, one fiat currency A for another fiat currency B at a cheaper exchange rate rather than applying the direct exchange rate fiat-to-fiat (F2F) between A and B. If we take

	Distribution Lognormal	
Log likelihood	-3804.58	
Domain	$-\infty < y < \infty$	
Mean	3814.45	
Variance	$6.67886\text{e}+10$	
Parameter	Estimate	Std. Err
mu	4.0306	0.120159
sigma	2.90378	0.0850746
	Estimated covariance of parameter estimates	
	mu	sigma
mu	0.0144382	$-7.89786\text{e}-18$
sigma	$-7.89786\text{e}-18$	0.00723769

	Distribution Exponential	
Log likelihood	-4078.47	
Domain	$0 \leq y < \infty$	
Mean	396.898	
Variance	157528	
Parameter	Estimate	Std. Err
mu	396.898	16.4238
	Estimated covariance of parameter estimates	
	mu	
mu	269.74	

TABLE 9: Statistics of average volume across trading platforms for the currency pair BTC/EUR. Period: January 2012-June 2014.

the example of Bitcoin, when the following equation does not hold

$$BTC/USD = BTC/EUR \times EUR/USD \tag{4}$$

then, a so-called "triangular" arbitrage opportunity emerges. We capture evidence of triangular arbitrage in the Bitcoin market by using two similar metrics:

$$\begin{cases} \Delta^2 := \frac{1}{n}\sum_{i=1}^{N}\left|\frac{(BTC/EUR)^i}{(BTC/USD)^i} \times (EUR/USD) - 1\right|, \\ \Delta^3 := \left|\Lambda \times (EUR/USD) - 1\right|, \end{cases}$$

where:

$$\Lambda = \sum_{i=1}^{N}\left[\omega_i^{EUR}(BTC/EUR_i)\right] / \sum_{i=1}^{N}\left[\omega_i^{USD}(BTC/USD_i)\right] \tag{5}$$

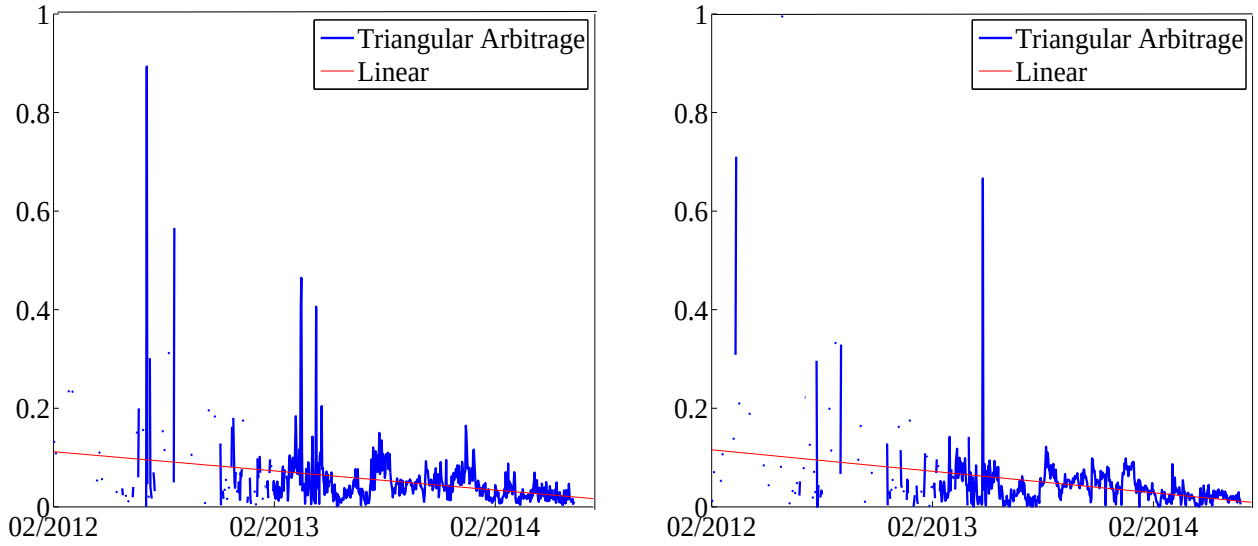

FIGURE 34: Average intensity of triangular arbitrage within trading platforms. Left: Δ^2. Right: Δ^3.

$$\omega_i^{EUR} = \frac{\text{Volume}_i^{EUR}}{\text{Total Volume}^{EUR}}, \quad \omega_i^{USD} = \frac{\text{Volume}_i^{USD}}{\text{Total Volume}^{USD}} \tag{6}$$

and i= BTC-e, Kraken, Vicurex, Justcoin, Crypto. When either Δ^2 or Δ^3 is bigger than zero, then the market is inefficient. Figure 34 shows an improvement in Bitcoin market efficiency over time. Fewer incidences and lower intensity of triangular arbitrage opportunities are signals that the electronic currency exchange market is becoming more efficient.

11 DISTRIBUTION OF INCOME AND WEALTH

This section describes the market structure and the income distribution in the digital currency economy. We will try to analyse both the supply (i.e., miners) and the demand (i.e., users) side by considering market-share and wealth distribution. The analysis will focus only on Bitcoin, which is the most important and frequently used digital currency (see Section 5).

11.1 USERS

By definition, it is impossible to have a clear picture of the individual users and their wealth in the Bitcoin economy. Specifically, the only information provided by the blockchain is the number of addresses and their respective balance over time. Although, various solutions have been proposed to aggregate different Bitcoin addresses presumably belonging to the same entity,

e.g., [148], [149], [150], the most straightforward and incontrovertible method is to consider each address as an individual Bitcoin user.[43] However, we are aware that this is not an exact representation of the Bitcoin economy (for example, because the same user may hold multiple addresses).

To consider the distribution of the wealth we take two interrelated indicators: the Gini coefficient and the Lorenz curve. The Gini coefficient [153] can be calculated from unordered size data as half of the Relative Mean Difference (RMD), which is the average absolute difference between every possible pair of values, divided by the mean size μ:

$$G = \frac{RMD}{2} \in [0, 1],$$

with

$$RMD := \frac{MD}{\mu} \quad \text{and} \quad MD := \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} |x_i - x_j|,$$

where

x_i : wealth (balance) of address i, with $x_i > 0$;

n : population size (total number of addresses with positive balance).

The other measure we use is the Lorenz curve [154] which can be represented by a function $L(F)$ where

F : is the cumulative portion of the addresses in the Bitcoin economy represented on the horizontal axis;

L : is the cumulative portion of the total wealth or positive balance represented on the vertical axis.

For a discrete probability function $f(y_i)$, let y_i, $i = 1, .., n$, be the points with non-zero probabilities indexed in increasing order $(y_i < y_{i+1})$. The Lorenz curve is then the continuous piecewise linear function connecting the points (F_i, L_i), $i = 0, ..., n$, where $F_0 = 0$, $L_0 = 0$, and for $i = 1, ..., n$:

$$F_i = \sum_{j=1}^{i} f(y_j),$$

$$L_i = \frac{S_i}{S_n} \quad \text{with } S_i = \sum_{j=1}^{i} f(y_j) y_j.$$

[43] Some methods for "clustering" Bitcoin addresses have been proposed by [151], [148] and [152], among others.

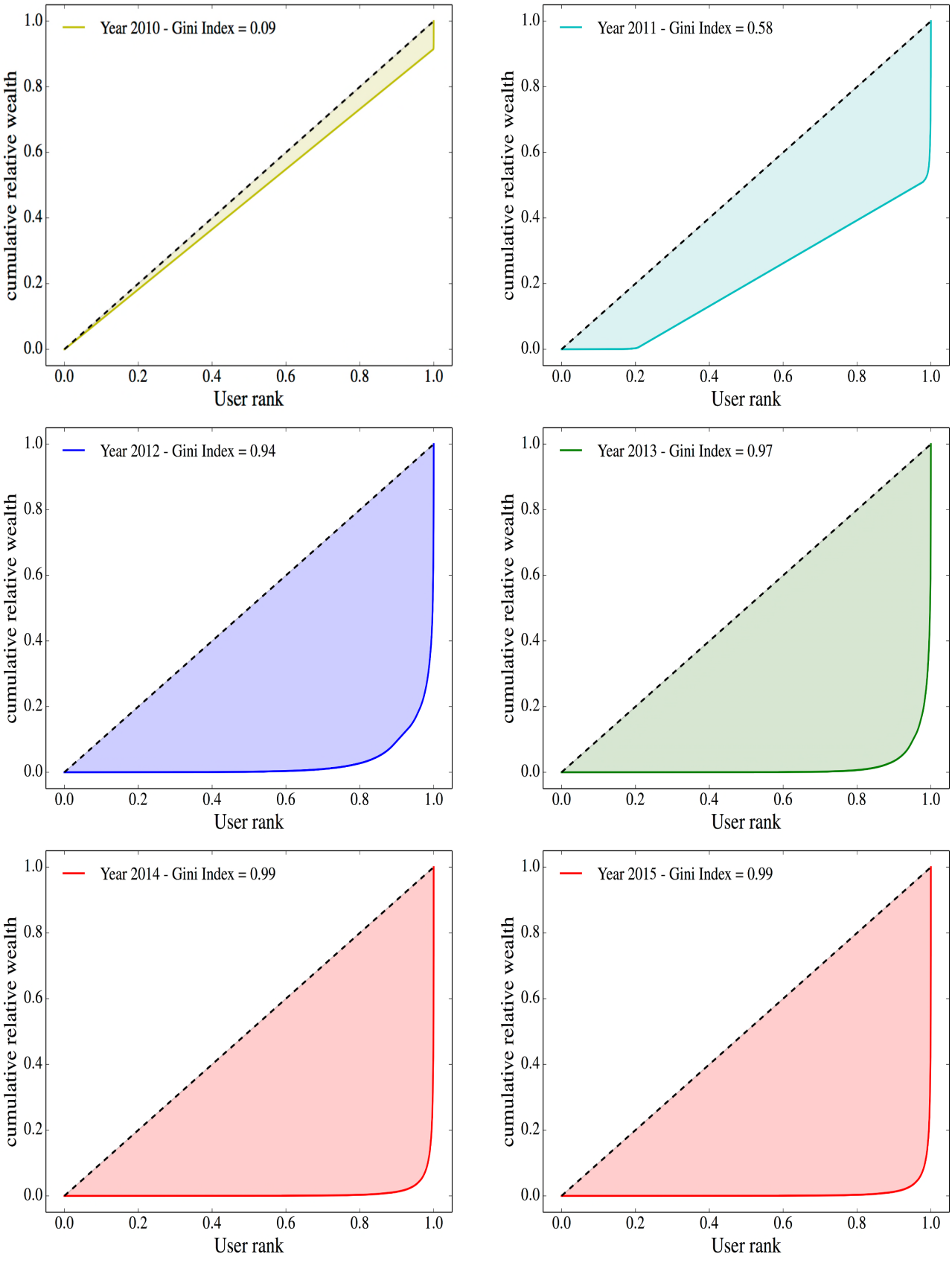

FIGURE 35: Lorenz Curve and Gini Coefficient for the Bitcoin Economy. Data source: Bitcoin blockchain. Internal calculation.

The relation between the Gini coefficient and the Lorenz curve is as follow. The Gini coefficient is the ratio of the area bounded between the line of perfect equality (45 degree line) and the observed Lorenz curve and the total area below the line of perfect equality. The higher the coefficient, the more unequal the distribution is. In the Figure 35 this is given by the ratio between the coloured area and the area below the 45 degree line. The figure shows the percentile of addresses sorted by the amount of Bitcoins held (x-axis) with respect to the percentile of the Bitcoin monetary base (y-axis). In 2009, $G \sim 0$ and the Lorenz curve approximates the 45 degree line. For that year, every address held almost the same amount of Bitcoins and the wealth was equally distributed among addresses. In the subsequent years, as seen in Figure 35, G increased almost to one and the Lorenz curve departed from the 45 degree line. In 2015, the wealth distribution among addresses is dramatically unequal where few addresses hold almost the whole amount of Bitcoins ever supplied.

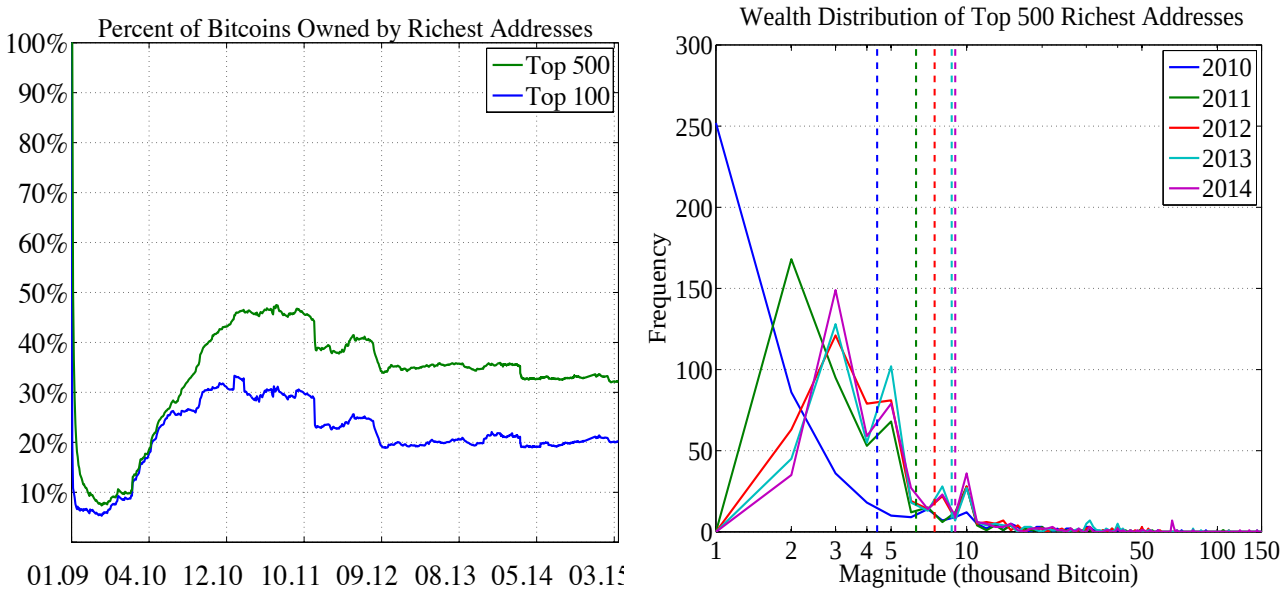

FIGURE 36: Left: Relative wealth of the top 100 and 500 richest Bitcoin addresses. Right: Wealth distribution among the top 500 richest Bitcoin addresses (with x-axis log-transformed). Data source: Bitcoin blockchain. Internal calculation.

Paradoxically, this undesirable economic outcome is exactly the opposite of what the first Bitcoiners from the crypto-anarcho-libertarian community would have expected. The wealth inequality may partly be explained by the proliferation of new addresses registered during recent years. This is a result of the growing adoption of Bitcoin, either by new users or early adopters. In fact, the number of addresses is correlated with the number of users and also with the number of transactions. It is even an advisable "best practice" to use different addresses for each new transaction. Moreover,the change back in each transaction is loaded into a new address. Figure 1 shows that the number of transactions per day skyrocketed during the last

years: from 2011 to 2015 they grew from ∼1,000 to ∼130,000 transactions per day. Thus, the increasing inequality is not due to the "rich get richer and the poor get poorer" phenomenon but, at least partly, due to the increased number of Bitcoin transactions. Indeed, by monitoring the relative wealth of the top 100 and 500 richest addresses in the last years we observe that it remains almost constant, see Figure 36 (left). However, Figure 36 (right) shows that the distribution of the wealth among the 500 richest addresses became more unequal over the last five years.

11.2 MINERS

As described in Section 3, the supply of a digital currency is generally determined by its generation algorithm which defines, in advance, under which rules the currency will be generated and supplied. Miners use special software to solve the mathematical cryptography problems and verify the network transactions. Generally, two incentive mechanisms are put in place which reward this computationally and energy intensive activity: (1) block rewarding, i.e., the assignment of newly issued coins; and (2) transaction fees. As the amount of transaction fees is negligible at the moment, as seen in Figure 3 (right), the majority of miners' income originate from block rewards. For example, for each solved Bitcoin block, a miner can earn 25 Bitcoins in reward. This reward is periodically cut in half every four years. After 21 million mined Bitcoins, the reward will fall to zero and no further Bitcoins will be created [155]. According to the supply scheme, from 2012 to early 2015, the total supply will be BTC 1,312,500, approximately BTC 3,595 per day. Since this supply of Bitcoin is predetermined, the actual earnings for mining depend on the appreciation/depreciation of Bitcoin with respect to other hard currencies, see Figure 25 (right). This can be observed by taking as an example the exchange rate BTC/USD. Figure 37 (right) shows that the mining revenue is highly correlated with the BTC/USD exchange rate. As mentioned, miners have a second potential source of revenue (which will become the only source of revenue once all coins have been created) which is the transaction fee. When listing a transaction, the sender can also agree to pay a fee to speed-up the verification. The fees are optional, but 97 % of the transactions in 2014 included a fee, most often set at the default rate of the standard client software, i.e., BTC 0.0001, see Section 4.1.

During the last years, the hardware industry developed new solutions to tackle the increasing mining difficulty:[44]

[44] The term "difficult" refers to an estimate about how hard it is to mine (find) a new block. The difficulty also ensures a limited supply. Therefore, mining gets more difficult counterbalancing the increasing computing power in the network, which is measured in hashes per second.

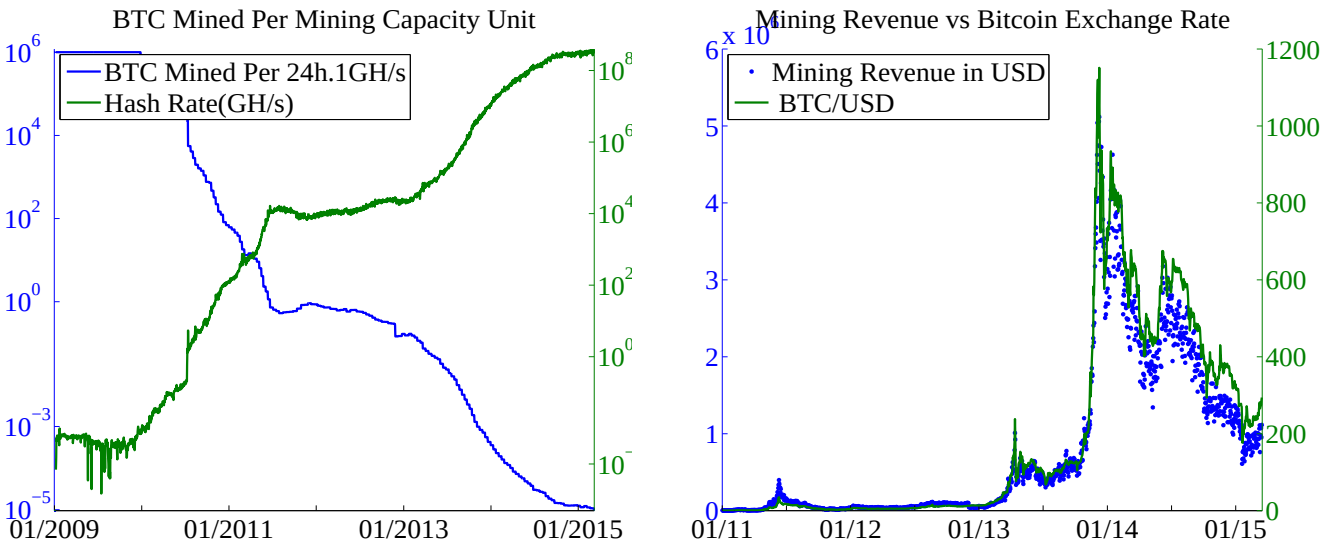

FIGURE 37: Left: Amount of Bitcoins that could be mined by the mining capacity of 1 GH/s per day, compared to the hash rate in GH/s. Right: Mining revenue and exchange rate from 01/2011 to 03/2015. Data source: Blockchain.info and Blocktrail. Internal calculation.

(a) CPUs. At the beginning of the Bitcoin network, miners used CPU-powered algorithms to mine Bitcoins. This method is no longer viable now that the network difficulty level is too high for this approach.

(b) GPUs. Later, the GPU (Graphical Processing Unit) substituted the CPU. The massively parallel nature of some GPUs allowed for a 50x to 100x increase in mining power while using far less power per unit of work.

(c) FPGAs. Then, the Field Programmable Gate Array (FPGA) technology substituted the GPU-based one. With the launch of Butterfly Labs FPGA "Single", the mining hardware landscape gave way to specially manufactured hardware dedicated to mining Bitcoins and other digital currencies. The strength of the FPGAs was their increased power efficiency. A typical 600 MH/s GPU consumes upwards of 400w of power, whereas a typical FPGA mining device provided a hash-rate of 826 MH/s at 80w of power.

(d) ASICs. The ultimate technology is now represented by the Application Specific Integrated Circuits (ASICs). Unlike FPGA's, an ASIC cannot be repurposed to perform other tasks than mining. The inflexibility of an ASIC is offset by the fact that it offers a 100x increase in hashing power while reducing power consumption compared to all the previous technologies.

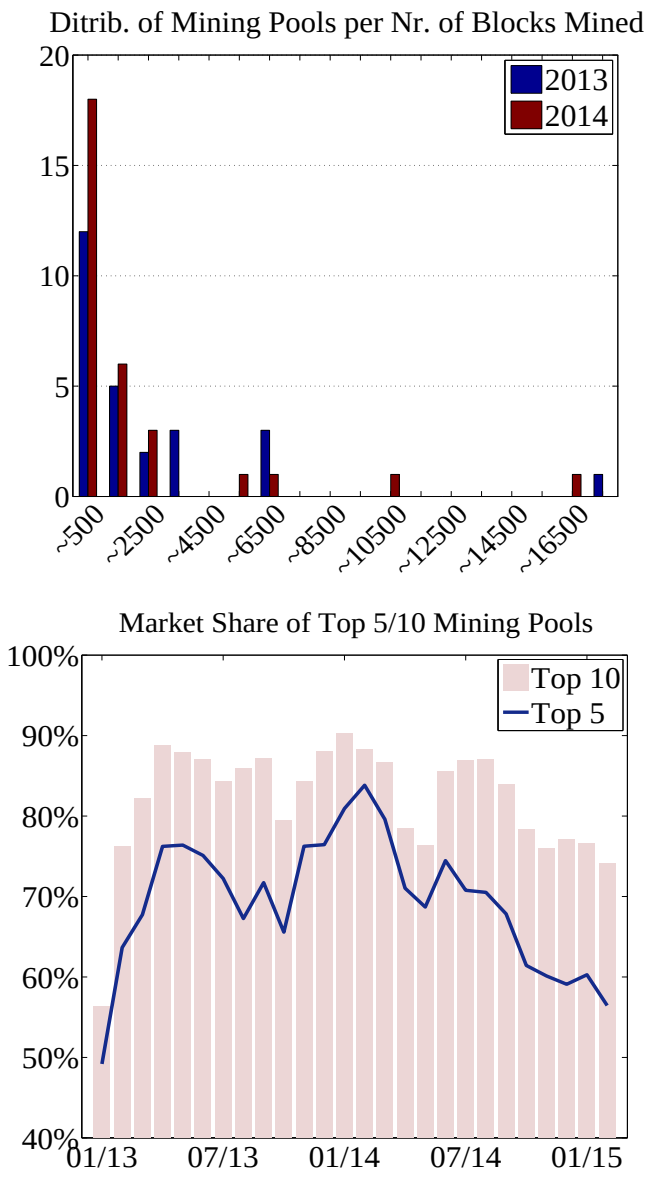

FIGURE 38: Top: Distribution of mining pools per number of blocks. Bottom: Market share of top 5 and 10 mining pools. Data source: Blocktrail. Internal calculation.

For each new block, only the miner who solves the hashing problem the fastest gets rewarded. This rule makes the mining market extraordinarily dynamic and competitive. According to the Bitcoin mining hardware producer Butterfly Labs, the speed of their most advanced dedicated product can be as fast as 725 GH/s [156]. The green line in Figure 37 (left) shows the hash rate needed to solve a block during the time from 2009 to 2015. As consequences of the intense competition, the hash rate increased exponentially in the past six years. In March 2015, the hash rate achieved 391 million GH/s, which means that to solve a block, even with the most advanced technology, one still needs 539,310 hashing units working simultaneously. At the same time, the blue line indicates how many Bitcoins could be mined per day with one unit of mining capacity (1 GH/s). As a result the unit capacity dropped dramatically. According to the data of March 2015, 1 GH/s could only mine BTC 0.0000095 per day, approximately USD 0.0027 at the current exchange rate. The development of dedicated hashing hardware gave origin to the first mining industry. Currently, there exist two forms of production processes:

(1) Solo mining.

(a) In house.

(b) Remote (i.e., cloud mining).

- Hosted mining. In this case, miners pay a monthly rental fee for a range of Bit-

coin ASIC mining systems and rent a dedicated physical machine for their sole use hosted by the service provider.

- Virtual hosted mining. The most common solution is Amazon's Elastic Cloud Computing (EC2) platform. This is a virtual private server where one can install the mining software. Other solutions exist in the form of agreements with advance payments for a year's service or a "pay-as-you-go" model.
- Leased hashing power. With this service, miners can specify the amount of hashing power they want, on a one-year contract without the need of a dedicated physical or virtual computer.

(2) Mining pools. Miners organise by distributing smaller and simpler algorithms. The combination of all the work done in a pool allows it to solve harder hashing problems and earn digital currencies which then are distributed throughout the pool based on the individual contributions. Indeed, the mining difficulty level is becoming so high that it is practically impossible for soloists to make a profit mining. Therefore, most of the miners prefer to join mining pools which vary according to the different mining methods utilised (merged[45] or single) and the fee/reward system [157].

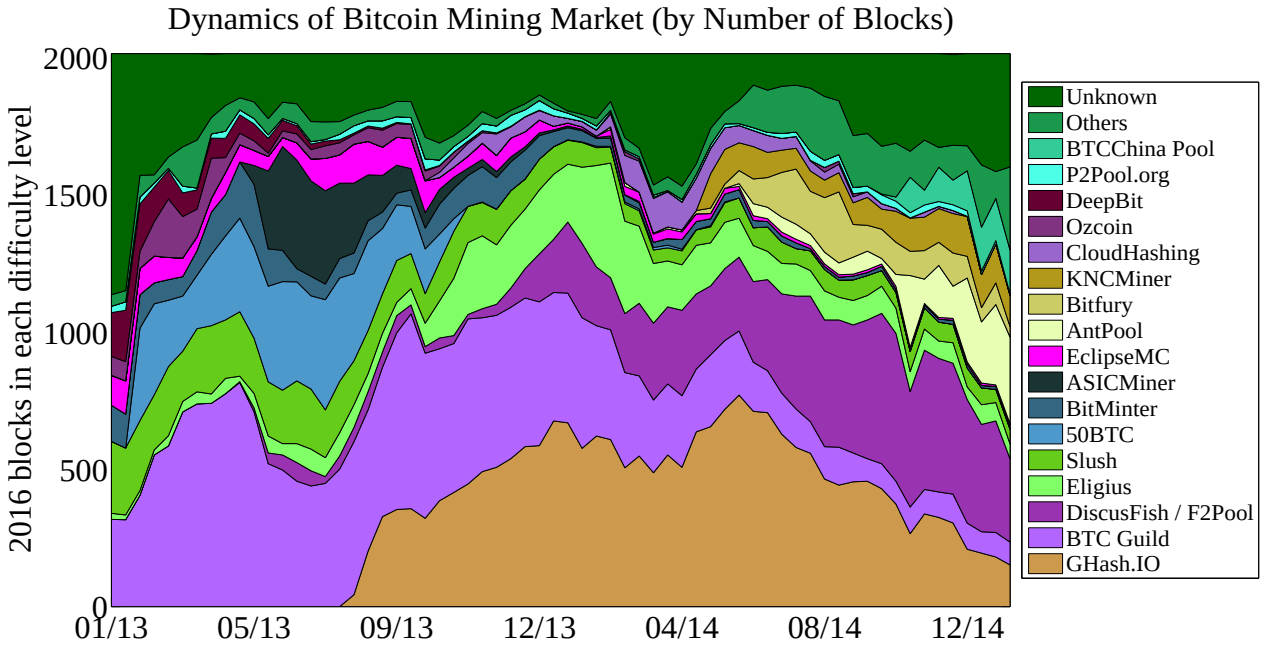

FIGURE 39: Top 17 mining pools (out of 40) per number of blocks mined. The figure shows the number of blocks mined by different mining pools in each difficulty level, which changes every 2016 blocks. Period: from January 2013 to February 2015. Data source: Blocktrail. Internal calculation.

[45] Merged mining allows miners to mine on multiple blockchains at the same time with the same hashing. Namecoin was the first protocol to support merged mining, see Section 12.2.

Country	Miner	Tot. Blocks (January 2013 - February 2015)	Av. # Blocks (January 2013 - February 2015)	Tot. Blocks per Country (%)
China	DiscusFish/F2P	12,936	235.2	19,839 (15%)
	ASICMiner	3,127	107.8	
	AntPool	2,365	94.6	
	BTCChina Pool	1,036	103.6	
	BW Pool	353	176.5	
	Avalon + Huobi	13	6.5	
Europe	GHash.IO	21,888	465.7	34,454 (27%)
	Slush	7,825	122.3	
	KNCMiner	2,326	105.7	
	DeepBit	1,384	51.3	
	Polmine	895	28.0	
	TripleMining	128	2.0	
	BTCMP	8		
USA	Eligius	7,906	135.5	8,042 (6%)
	MaxBTC	78	7.1	
	CoinLab	58	4.1	
Global	BTC Guild	24,246	378.8	44,474 (34%)
	50BTC	6,406	164.3	
	BitMinter	3,882	60.7	
	EclipseMC	2,903	45.4	
	Bitfury	2,353	98.0	
	CloudHashing	1,824	45.6	
	Ozcoin	1,686	37.5	
	P2Pool.org	11,74	18.3	
Unknown	Others	22,217	347.1	22,217 (17%)

TABLE 10: Numbers of blocks mined by major mining pools over time. Data source: Blocktrail, Bitcoin Wiki. Internal calculation.

As mining hash rates soar, mining technology develops at a faster pace. This creates great uncertainty for the future distribution of the mining market. In terms of the market concentration ratio, the market share of the top 5 and top 10 largest mining pools diminished steadily during the end of 2014 and also kept diminishing during the first months of 2015. However, the market share remains highly unequally distributed. During the period 2013-2015, the cumulative market share of the largest 10 pools relative to the total market hovered in the 70%–80% range, see Figure 38. One possible explanation for this high market concentration is the introduction in mid 2012 of the Stratum mining protocol which, differently from the obsolete getwork protocol, shifted the mining power to pool managers [158]. In early 2014 Ghash.IO came close to 51% hashing power. In effect, a malevolent mining pool controlling 51% of the hash-

ing power could exploit the Bitcoin network for financial gain. In order to eliminate this threat, GHash.IO temporarily stopped accepting new independent mining facilities to the Ghash.IO pool. In June 2014, GHash.IO again came very close to 51% of the global hash-rate percentage, showing the previous actions to artificially lower the hash-rate to be ineffective.[46] In order to provide a more granular statistics on the distribution of the total revenue we take data from Blocktrail [160] and, for the period January 2013 to February 2015, we rank the largest mining pools with respect to both the number of blocks mined and the fees earned, see Figures 39 and 40. In Figure 41 we also show the evolution of the market share per geographical area by combining data from Blocktrail [160] with the background on mining pools provided by Bitcoin Wiki [157]. As one can observe from Table 10, during the period January 2013–February 2015 European and Global[47] miners dominated the market with a leading role played by Ghash.IO and BTC Guild. However, from the second part of 2014 some Chinese mining pools such as Antpool, DiscusFish/F2Pool, and BTC China gradually increased their market share.[48] This is confirmed by the mining dynamics in Figure 41 which tracks the time evolution of the market share per country.

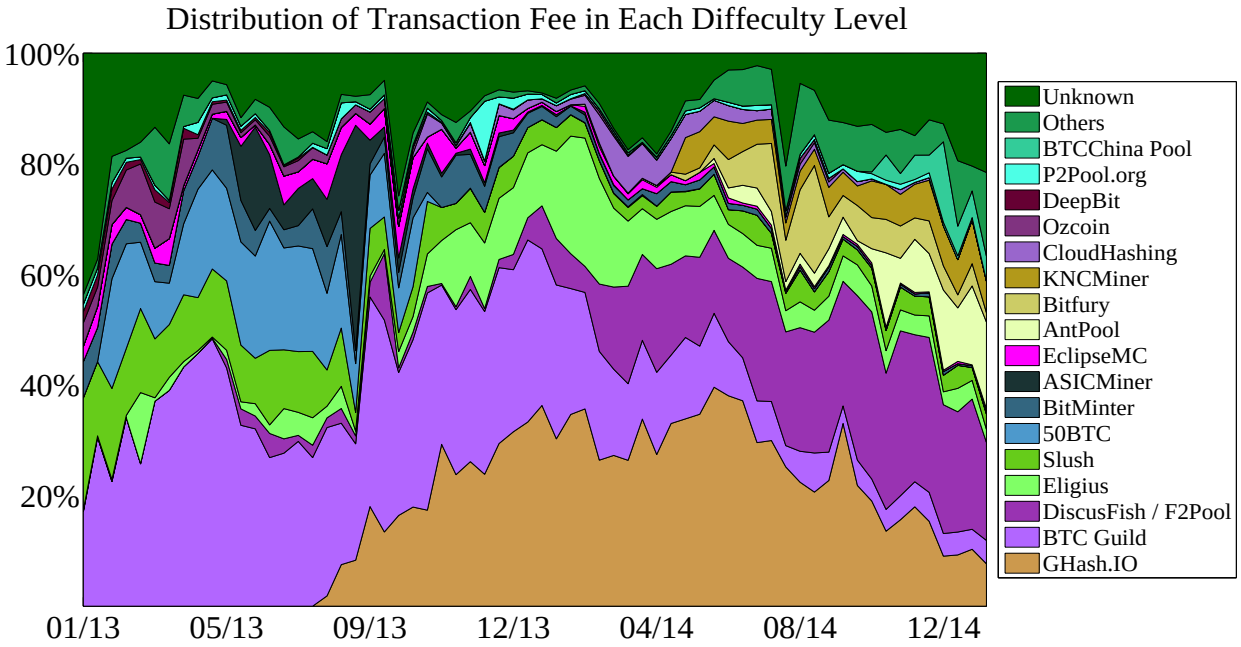

FIGURE 40: Top 17 mining pools (out of 40) per relative amount of fees earned. In each difficulty level, transaction fees collected by each mining pool are summed up and compared to the total fees earned and collected by the market. Period: From January 2013 to February 2015. Data source: Blocktrail. Internal calculation.

[46] Recently, GHash.IO gathered a round table of the key players in the Bitcoin economy to resolve this situation once and for all [159].

[47] Those pools that set their servers in different countries or even continents are labelled as "Global".

[48] Among the other large mining pools there are KnCMiner, Eligius and Bitfury.

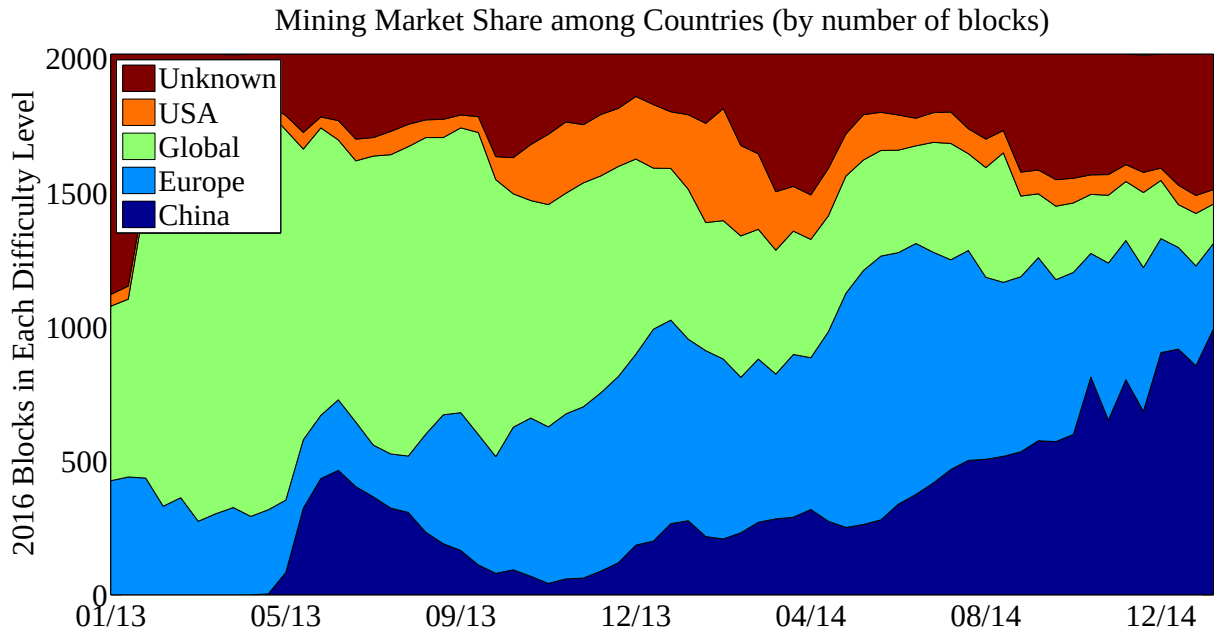

FIGURE 41: Top mining activity per country. Mining pools are classified per country of operation. Many mining pools operate in different countries (e.g, BTC Guild and BitMinter run their mining operation in both USA and Europe), so they are classified as "Global". Period: from January 2013 to February 2015. Data source: Blocktrail, Bitcoin Wiki (comparison of mining pools). Internal calculation.

12 ALTERNATIVE APPLICATIONS OF BLOCKCHAIN TECHNOLOGIES

Any socio-economic area that requires: (1) underwriting and execution of unilateral or bilateral contracts; (2) transmission of information or opinions; (3) exercising of voting rights among (anonymous) individuals and/or legal entities to be executed trustworthy, verified and recorded on public registries, may be potentially affected by network-based, distributed-consensus ledgers or simply: "blockchain technologies". These ledgers make it possible to jointly create, evolve and keep track of a unique single repository of transactions or other pre-coded events (sequentially ordered) over a shared network. For instance, the documentation of the ownership passages from one user to another of specific information or rights. The bookkeeping process is maintained, validated, and administered without the need of a single point of control (and hence, point of failure). Every transaction that occurs between participants in the network is inextricably embedded in a truly tamper-proof record system(s). Every one can download the blockchain(s) at any time and view every transaction in near real-time. While still preserving anonymity and privacy, the balance of each "account" (i.e., the address) and the details of historical transactions can be checked at any point in time by anyone, see Section 3.

Until now, the most salient manifestation of the blockchain technologies has been Bitcoin as the first digital currency application. However, after the first wave of enthusiasts and overly ideological Bitcoiners "blinded" by their belief in a rapid displacement of the US Dollar and other hard currencies by Bitcoin, the community started focusing on alternative applications of the blockchain technology.[49] Alternative blockchain-based applications include other "digital currencies", "asset registries", "application stacks", and "asset-centric technologies" [162]. In the following, we can only provide a partial picture of the current situation because most of these applications are still at their dawn and are rapidly evolving.

12.1 DIGITAL CURRENCIES

We have already extensively covered the topic of digital currencies in this report. At the time of writing there are over 500 young digital currencies following different money supply mechanisms, transaction and verification network protocols [35]. Although Bitcoin still remains the dominant currency in terms of use and capitalisation, other digital currencies, in the near future, may start to be largely used as an alternative to Bitcoin, see Section 5.

To give the reader an insight into the future development of digital currencies, we start by considering that a currency should simultaneously satisfy the following needs: be a *medium of exchange*, a *unit of account*, and a *store of value*. In the upcoming digital era characterised by a cashless and a massively connected society utilising high frequency transnational transactions, we think a currency should satisfy a fourth need which is the maximisation of the *utility of reward*. By utility of reward we mean the capacity of a currency to reduce market frictions and, in doing so, allowing their users to make efficient expenditure decisions. We have seen in Section 3 that a digital currency is generally associated with a digital wallet containing the currency. The extension of the concept of a "single" wallet to that of a "universal" wallet (or multi-currency wallet) has the potential to reduce boundaries and constraints when using digital currencies. A universal multi-currency wallet, e.g., [163], with instant conversion between the supported currencies, allows users to spend (even in a single transaction) different digital currencies. Moreover, with universal wallets one can send digital currencies through Facebook, LinkedIn, Twitter, e-mail, etc. If the recipients do not have a wallet, they will receive a notification with a link to redeem the funds. The recent introduction of Google Wallet [164] and Apple Pay [165] results in a more general adoption of digital wallets and equivalent technologies, which in turn will lead to higher adoption of digital currencies.

[49] On this matter, an interesting comment was made by Reddit's CEO Yishan Wong [161], who praised the technology but called out the Bitcoin community for being overly ideological.

Next to decentralised digital currencies, partially or fully centralised digital currencies could emerge. Some big private corporations, e.g., [166], [90], and [167] are taking the first steps towards the creation of currency-based environments with the purpose of (1) reducing their legacy costs of back-end infrastructures and (2) increasing the marketability of their already in-place branded currencies, e.g., loyalty programs, vouchers, credits. In the near future, we foresee the diffusion of community-based digital currencies or "brand" currencies that will serve specific community needs. Already now, anyone without particular technical skills can use off-the-shelf tools like [168] that allow the creation of a personal digital currency with its own blockchain, based on different possible proof of work algorithms, like X11, Scrypt or SHA256. Moreover, there are already payment networks such as Ripple [65] enabling different digital currencies to be transferred easily between members. In the end, the combination of universal wallets with a multi-currency system will increase the utility of reward of all the digital (centralised or decentralised) and hard currencies used for daily, real-time, and cross-border transactions.

12.2 ASSET REGISTRY

By asset registry we refer to all those applications that link digital currencies (or more in general, digital tokens) to tangible assets like databases, stocks, bonds, certificates, etc. Although for the time being, the technology still needs refinement, asset registry applications like "colored" coins, Counterparty, Mastercoin, and Namecoin have already been brought to the market.

- Colored Coins are applications for digital representation and management of real world assets (e.g., stocks, bonds, securities, precious metals, commodities) on top of the Bitcoin blockchain [169]. While originally designed to support the exchange of digital currencies, blockchain scripting languages have the potential to store small amounts of metadata on the blockchains. Metadata summarises information about the most diverse types of data (from images to source code in JavaScript, Python, and Basic) that users can store in the blockchain. The procedure is as follows: first the users convert theirs messages into hexadecimal values and then they convert the resulting hexadecimal strings into addresses. Those addresses are considered to be "fake" because they are used only to transmit the hidden information contained in the addresses. When someone transfers a digital currency to one of those "fake" addresses, as soon as the transaction will be mined, the information will be released and stored forever in the blockchain [170]. Although the storage of useless large amounts of data pollutes the blockchain and has the poten-

tial to generate the "blockchain bloat" problem [171] [172], certain types of data may contain useful information. This is the case for Colored Coins. These are applications with the purpose of "coloring" Bitcoins and turning them into general tokens which represent real assets or services and whose value: (1) is independent from the face value of the Bitcoin, (2) depends on the value of the underlying real asset/service, and (3) on the credit worthiness of the issuer. In this context creditworthiness represents the willingness and capability of the issuer to redeem the Colored Coins in exchange for the corresponding real asset/service. In principle one can represent digital assets on different blockchains, however, Colored Coins are usually implementations at the Bitcoin blockchain level and do *not* use auxiliary digital currencies. The adoption of the Bitcoin blockchain as a low-cost means of recording transactions of digital assets allows the users to benefit from the technical features of the Bitcoin network: transactions are easy, immutable, non-counterfeitable, robust, transparent and traceable, and come with a low transaction fee, no extra currency layers (XCP, MSC). Moreover, the technology is supported by core Bitcoin developers. Potential applications of Colored Coins may include [173]: smart property,[50] company bonds/stocks,[51] deterministic contracts, demand deposits[52], coupons, access and subscription to offline services (e.g., museums and subways) and online services (e.g., applications). In detail, to issue a Colored Coin one needs to generate a "colored" address which must be held in "colored" wallets managed by a color-aware clients like Coinprism [174], Coloredcoins [175] via Colu [176] or CoinSpark [177]. The addresses should contain an asset description and some general instructions (the so-called "color" definition). The information may, for example, include the type of asset to be transferred, who is issuing it, the name of the asset, how much of the asset is being issued, and a description of the asset. In effect, one can encode into a Bitcoin address a certain amount of a digital asset linked to a real asset.[53] The instructions will then be used by color-aware nodes in order to validate colored transactions. In order to be able to transfer Colored Coins to other users, the issuer should add a tiny amount of Bitcoins to the newly generated colored address. Colored transactions are normal

[50]The ownership of physical assets like cell phones, vehicles or real estates could be transferred via Colored Coins which entitle the owner access and control over the asset.

[51]A company could issue Colored Coins representing bonds and/or equities. Possible coupons, dividends and voting rights will be automatically transferred to the owners of the coins.

[52]They are similar to bonds but in this case the issuer guarantees to redeem the token for its face value at any time.

[53]Note that, in practice, the "coloring" process is just an abstract concept by which a ticker symbol and a unique hash is attached to the addresses.

Bitcoin transactions recognised by the standard Bitcoin network, but must satisfy additional constraints to be recognised by color-aware nodes. As such, a Colored Coin wallet can create a Bitcoin transaction that encodes sending certain units of a specific real asset/service from the initial issuing address to a new address. This is the so-called Colored Coin genesis transaction and it must specify the rules that the inputs/outputs should follow. Although there are several Colored Coin algorithms, the standard of choice for the structure of color-aware transactions is usually order-based coloring and in its simplest form, it requires that: (1) inputs and outputs are sorted by color, with uncoloured coins at the end; (2) inputs and outputs must use the same order of colours; (3) for each color, the total value of all inputs must be equal to the total value of outputs. These order-based coloring transaction rules are necessary to determine if Bitcoins held at some future time are colored or not and if so, which color they have. The idea is that by following a chain of transactions that can be traced back to the color's genesis one should be able to recognise the color [173] [178]. This is especially helpful if after the Colored Coin genesis transaction the coins have been involved in several transactions with multiple inputs and multiple outputs.

- Counterparty [179] is a peer-to-peer financial platform and a distributed, open-source Internet protocol built on top of the Bitcoin blockchain and a network as a service for the reliable publication and time-stamping of its messages. Similar to Colored Coin applications, Counterparty works by storing extra data in regular Bitcoin transactions, which makes every Counterparty transaction a Bitcoin transaction, albeit a very small one. When Counterparty transactions are broadcast to the Bitcoin network they are verified by Bitcoin miners and saved in the Bitcoin blockchain to make a secure, verifiable record. Counterwallet (the free web-based wallet for Counterparty) makes it possible for anyone to create tokens which represent assets, coins, derivatives and, more generally, smart contracts that are then owned by the address they were issued from. Ownership enables the users to issue more units of the original token, lock the supply, change the description, and customise other settings. Once the issuance is confirmed by the Bitcoin network, the tokens can be freely traded on the Counterwallet decentralised exchange against XCP (the native token used in the Counterparty marketplace) and other tokens. Indeed, the role of XCP is central since Counterparty cannot function without it. XCP ultimately represents the value of the network because users need to spend a small amount of it in order to create new assets, make bets, and perform callbacks on callable assets. XCP is the first digital currency using proof-of-burn principle. Although this mechanism could be inter-

esting in multi-currency systems in order to get rid of old or less used currencies, it has attracted some criticisms because, in order to generate XCP, one should send Bitcoins to a particular address that renders the Bitcoins provably and permanently unspendable [180]. This means that the Bitcoins used to generate XCPs are lost outside the money supply forever. Although Colored Coin and Counterparty applications have similar end-user utilities, technically, they are quite different. The main differences between these protocols are the following:

- Bitcoin-based versus native currency. In contrast to Colored Coin applications, Counterparty relies on the XCP currency. This matters in terms of price exposure and volatility risk.
- Association of asset ownership. Colored Coin applications allow users to put the data in the transaction output (after the OP_RETURN operator) which must be retained in the subsequent transaction outputs via order-based coloring transaction rules. The risk is that if a Colored Coin is handled by a wallet which is not colored-coin aware, the output containing data will not be reproduced and the Colored Coins will lose their color, i.e., they will lose their contents forever. Instead, Counterparty imposes a clearer separation between Bitcoins and data. All the ownership, issuance, order, betting and other data is directly stored in the blockchain. There is no relationship between stored data and transaction outputs. Instead, each Counterparty transaction adds data to the global Counterparty history. Thus, if an address has 100 AAA coins, it will continue to have those coins until a Counterparty transaction is signed by the owner of that address who sends them somewhere else.
- Another fundamental difference is that coloring schemes are optimised for robust functionality by inserting the most data within the current size constraints of the OP_RETURN operator (40 Bytes) and only sometimes in one additional multisignature address. Instead, Counterparty can store more data because by default the data is encoded in the form of multisignature addresses. In the context of digital currencies, a multisignature address requires a combination of n multiple private keys and allows for m persons (with $m \geq 2$) to send funds if a sufficient number $1 < n \leq m$ of signatories have signed and approved the transaction [181], [182].
- Customisation of assets. Differently from Counterparty, Colored Coins are practically just a thin layer on the Bitcoin network and therefore they can adopt the very same features offered by Bitcoin (e.g., they can handle unconfirmed transactions). However, customisation brings also some risks.

- Risk of losing the underlying assets/services. The metadata used to customise the assets by Colored Coin applications is hosted on the issuer's own server. If the server goes down the information is lost or users have to rely on a mirror server. Moreover, the coins can accidentally be uncoloured if the order-based coloring rules are not correctly implemented in the coins-aware clients. These risks do not exist in the Counterparty system.
- Authenticity of the underlying assets/services. This problem emerges because the issuer of the Colored Coins may not have any rights on the underlying assets or services. In order to prevent fraud, Colored Coins have developed a method called proof of authenticity (based on the SSL certificated of the issuer) that allows end-users to verify if the entity is the legitimated issuer of the underlying assets/services [183]. The proof of authenticity is not possible with Counterparty.

- Mastercoin [184] is a meta protocol layer that enables new digital currencies, digital assets and communication protocols to exist on top of the Bitcoin blockchain.[54] In practice, the Mastercoin layer will allow: (1) user-defined currencies; (2) decentralised exchange between any two currencies in the Mastercoin network; (3) on-blockchain price feeds; (4) on-blockchain bets; (5) savings addresses where a transaction from a savings address can be reversed within N days (with N set for each address) by a "guardian address". The original motivation of using a new protocol layer on top of Bitcoin instead of issuing a new alternative digital currency, like everyone else was doing at that time, is explained by J.R. Willet in the Mastercoin white paper [185]: "New protocol layers on top of the Bitcoin protocol will increase Bitcoin values, consolidate our message to the world, and concentrate our efforts, while still allowing individuals and groups to issue new currencies with experimental new rules [...]" Similar to Counterparty which functions with XCP, Mastercoin has its own built-in token (MSC) which uses a similar proof-of-burn principle as XCP. Practically, the Mastercoin protocol pays for its own software development, by "bootstrapping" itself into existence, assigning a trusted entity (the Mastercoin Foundation) to hold funds and hire developers. Through this process, called crypto-IPO, in 2013 Mastercoin software developers sold their newly created digital currencies in exchange for Bitcoins and in so doing raising USD 5 million worth of Bitcoins [186]. Ultimately, the Mastercoin Foundation wants to keep the development of the Mastercoin layer as decentralised as possible. This is an open-source approach that is pretty much followed by other similar projects in the Bitcoin 2.0 space. Mastercoin's executive director Ross

[54] "Master" is an acronym for Metadata Archival by Standard Transaction Embedding Records.

Gross says: "Ultimately we want to move into a decentralised structure where we as team do not actually own anything or manually hire and fire but rather a Decentralised Autonomous Application (DAA) does" [187]. As of March 2015, Mastercoin converged into a bigger project called Omni Layer. Omni Layer is a communications protocol that uses the Bitcoin blockchain to enable features such as smart contracts, non-state currencies and decentralised peer-to-peer exchanges [188]. A common analogy that is used to describe the relationship of the Omni Layer and Bitcoin is that of HTTP and TCP/IP. Omni Layer, like HTTP is the application layer on top of the more fundamental transport and internet layer of TCP/IP which is Bitcoin. Still in beta version, the Omni Layer project includes thought leaders from Ethereum, among many others. Indeed, Mastercoin inspired the idea of Ethereum [189] because it was first extended by Vitalik Butolik (the inventor of Ethereum) who proposed the so-called "ultimate scripting" [190], a general-purpose stack-based programming language that Mastercoin could include to allow two parties to make a contract on an arbitrary mathematical formula. This mechanism was still quite limited, allowing only three stages (open, fill, and resolve) with no internal memory and being limited to two parties per contract. However, it was the first true seed of the Ethereum idea. Now, within the new project Omni Layer, Mastercoin technology will be used to support a decentralised record-keeping network Factom [191], a decentralised Internet provider MaidSafe [192], and a currency-backed token project Tether [193]. The difference between the protocol features of Colored Coin applications (especially Coinprism), Counterparty, and Mastercoin are summarised in Table 11.

- Namecoin [194] is a decentralised open source information registration and transfer system based on Bitcoin.[55] Namecoin was the first fork of Bitcoin and still is one of the most innovative digital currencies. It was the first to implement merged mining[56] and a decentralised DNS. Namecoin records consists of a key and a corresponding value which can be up to 520 bytes in size. Each key is a path within the DNS namespace preceding the name of the record. The key "d/example" signifies a record stored in the DNS namespace "d" with the name "example" and corresponds to "example.bit" website. The registered domain names are not subject to control by ICANN and are resistant to hijacks and external attacks by central authorities or criminal. According to the Namecoin project members, the proposed potential uses for Namecoin, besides domain name registration, include: identity systems messaging systems, personal namespaces, notary/time-stamp systems,

[55] The Namecoin codebase consists of the Bitcoin codebase with relatively minor changes. The mining procedure is identical but the blockchain is separated, thus creating Namecoin branch.

[56] Namecoins are mined as a free by-product of Bitcoin mining.

Protocol Features	Colored Coins	Counterparty	Mastercoin
Open Source	✓	✗	✓
Atomic Bitcoin/Asset and Asset/Asset swap	✓	✗	✗
Send multiple assets in single transaction	✓	✗	✗
Send assets to multiple recipients	✓	✗	✗
Asset divisibility	Any from 0 to 18 places	Either 0 or 8 places	Either 0 or 8 places
Tolerant to Blockchain reorganisations	✓	✗	✗
Prevents asset name squatting	✓	✓	✗
Proof of authenticity	✓	✗	✗
Asset creation cost	Bitcoin fees	Bitcoin fees	Bitcoin fees
Asset transfer cost	Bitcoin fees	Bitcoin fees	Bitcoin fees
Associate contract with asset	✓	✗	✗
Asset icon	✓	✗	✗
Dividends	✓	✓	✓
Voting	✓	✓	✗
Locked assets	✗	✓	✗
Callable assets	✓	✓	✗
Compatible with decentralised exchange	✓	✓	✓
Operational decentralised exchange	✗	✓	✓
Decentralised exchange can be used with BTC only	✓	✓	✓
Compatible with micropayment channels	✓	✗	✗
SPV	✓	✗	✗
Support for unconfirmed transactions	✓	✗	✗
Other non asset related features	✗	✓	✓

TABLE 11: Comparison between Colored Coin applications, Counterparty and Mastercoin.

alias systems, issuance of shares/stocks, protection of online free-speech rights by making the web more resistant to censorship, and storing identity information (e.g., GPG key, BTC address, TLS fingerprints).

12.3 APPLICATION STACKS

Application Stacks are "non-currency" blockchain-based platforms used for the development and execution of complete applications on top of decentralised networks like Bitcoin. By complete applications we mean Distributed Autonomous Organisations (DAOs). DAOs are the most complex form of decentralised automation to date. The simplest and first form of DAO was Bitcoin. Other more complex forms of this concept consist of autonomous agents, smart contracts, decentralised applications (Dapps) [195], and decentralised organisations [196]. A DAO can be thought of as an organisation that, under a predefined set of rules, runs completely autonomously (without any human control outside of some degree of effort necessary to build the software/hardware infrastructure the AI autonomous agents runs on) in a decentralised,

transparent, and secure publicly auditable, open-source software, distributed across the computers of the stakeholders. Current application stacks that allow the implementation of decentralised automatons, and DAOs more in general, are NXT, Ethereum and Eris, which distinguish themselves based on their core focus.

- NXT [197] is a safe, transparent and decentralised system for sharing data and allowing payments with people all over the world. All the functionalities can be accessed via a web browser. It uses a protocol similar to Litecoin based on a proof-of-stake principle such that the user does not need high-performance computing capacities to support the NXT network. In contrast to Litecoin, and in addition to basic transactions, NXT supports: (1) an alias system that allows people to store and transfer data among each other; (2) a decentralised voting system; and (3) a fully functioning decentralised asset exchange system. All together, these features allows for the creation of Dapps, and DAOs more in general, on top of NXT. Of particular interest is the NXT voting system [198] that allows NXT network users to design different polls on topics of their choice and set the rules for voting (either binary or sliding scale). Other members of the NXT network (or even a subgroup) are entitled to cast their votes via a small fee either in NXT coins or other "personal" assets which can be issued within the NXT network. The poll organisers can also determine how the votes are weighted. For an example, votes can be weighted by how much of an asset a wallet holds. A rule that can be helpful for voting mechanisms, where the approval depends on the percentage of the capital held by those casting their vote.[57]

- Ethereum [189] is an open-source platform to build distributed, next-generation, and decentralised applications in social systems, financial systems, and gaming interfaces, all in a peer-to-peer fashion. Ethereum can be regarded as a universal programmable blockchain on top of which many different types of decentralised tokens (with their own specific embedded rule-enforced codes) can be built. Ethereum implements a decentralised database, a system of digital token and an encryption scheme and, in addition to this, it also creates a Turing-complete scripting language which allows anyone to deploy their own application on top of the Ethereum blockchain. Ethereum makes it easy to implement new and alternative digital currencies but more importantly, it allows for the creation of much more sophisticated applications, such as communication systems like Skype, social networks like Twitter or cloud storages like Dropbox. However, the pecu-

[57] The capital may represent the equity of a legal entity and those with voting rights can then be the shareholders in a general assembly.

liarity of this new protocol is that all these applications are completely decentralised in the sense that they do not actually depend on any single point of control. With Ethereum it is also possible to build decentralised applications interacting directly with other decentralised applications by eliminating the need for a centralised overseers.

- Eris [199] is a distributed application open-source software stack that allows users to build their own secure, low-cost, run-anywhere data infrastructure using blockchain and smart contract technology. Eris offers development tools that help developers to build, test, deploy, and operate interactive applications where the application logic is reliably and securely executed by a distributed network. These applications can be tailored to the specific needs of communities, businesses, governments, and anybody else, who, by using smart contracts to manage their data-driven relationships themselves, can go beyond off-the-shelf platform architectures and standard marketplaces. Eris consists of two open source packages. The first is eris:db which is a fully-programmable, fully controllable, open-source blockchain database and smart contracts machine. The eris:db client allows developers to: (1) design, create, deploy, and manage their own blockchain; (2) benefit from having a parameterised smart contract in the genesis block which is capable of managing the consensus and security mechanism of the blockchain through the use of smart contracts [200]. The second component is eris:server: a distributed application server which displays distributed applications in an ordinary web browser. eris:server [201] harmonises actions across various modules which act as distributed file stores, distributed data stores (blockchains), or other utility modules. Dapps that operate on the eris:server are able to have authenticated, user-authorised, and harmonised interactivity with distributed file stores via IPFS hypermedia distribution protocols [202], as well as the following distributed data stores: eris:db, Tendermint [203], Bitcoin [204], and Ethereum [189]. When combined, eris:db and eris:server allow: (1) developers to harmonise the building of their distributed applications with a blockchain specifically designed for their applications' needs; (2) interaction among different blockchains with the possibility of API data acquisition, data processing, and atomic swaps.

12.4 ASSET-CENTRIC TECHNOLOGY

Asset-centric platforms exploit the properties of distributed-consensus ledgers but differ from them because they don't use public ledgers. Examples are Stellar and Ripple which use "private" ledgers and Hyperledger which allows for a decentralised control even without the need to use a native digital token.

- Stellar [205] is an open-source project and non-profit organisation backed by the online payment company Stripe [64]. Stellar is a decentralised multi-currency exchange and a payment network which supports the original idea of Bitcoin and extends it by allowing transactions into any currency of choice, whether that currency is fiat or digital, via a distributed-consensus network. Very similar to the Bitcoin network, Stellar is a network of servers (which any Stellar user can run) located in different geographical areas containing data and applications of Stellar's users. The information contained in all those servers constitutes a public ledger and each server contains a copy of it which is used to verify new transactions. Of course, the larger the number of servers, the more robust the network becomes. Differently from the Bitcoin network, the Stellar network requires the presence of intermediaries, called "gateways", which act as market makers and bridge the gap between the physical and the virtual world. Gateways are Stellar users who: (1) are specialised in taking and holding certain types of assets (e.g., hard currencies, certificates, bonds, and other assets) deployed on the Stellar network by other users; (2) issue corresponding redeemable and exchangeable digital credits for each deposited asset; (3) honour the withdrawal of the real assets upon request. The ledger records the real assets as digital credits (issued by the gateways) which are transferable within the network. All money transactions in the Stellar network (except the native digital currency of Stellar) occur in the form of credit issued by gateways. The innovation of Stellar is the creation of a global marketplace for the exchange and transmission of real assets in the form of digital credits. In practice, there exists a real-time, automated distributed exchange which allows the users to place in the Stellar ledger offers to buy/sell digital credits. Offers, which are public commitments to exchange one type of credit for another at a predetermined price, constitute a unique orderbook distributed in the Stellar network. The Stellar distributed exchange allows: (1) users to buy and sell digital credits; (2) gateways to convert digital credits in multi-currency transactions. The native coin of Stellar is used as an intermediary currency between any digital credit pair whenever the pair is illiquid. For example, if the pair New Zealand Dollar (NZD) and EUR is not liquid enough, Stellar looks for offers on the network asking for NZD in exchange for Stellar coins. It simultaneously looks for an offer asking for Stellar coins in exchange for EUR. The network then exchanges the corresponding quantities and sends the resulting EUR credit to the user. This interoperability of the Stellar distributed exchange increases the utility reward of money because one can use any credit balance in one's wallet to transfer a specific denominated credit to another person. For example, user A, who holds only USD credits, can transfer EUR credits to user B who then can withdraw by using a gateway supporting

EUR.

- Ripple [65] is a decentralised real-time gross settlement system, currency exchange, and remittance network based on a new algorithm for Byzantine consensus in the synchronous case. Released in 2012, Ripple supports the transmission of different types of assets: fiat currencies, digital currencies, commodities or certificates like loyalty rewards. In a similar fashion to Stellar, to join the Ripple system, a user is required to activate his/her account by converting the assets into IOUs via "gateways" [206]. Gateways are special users (mostly online financial services) that link the Ripple network to the rest of the world. They take custody and honour withdrawal of real assets. Only the IOUs will be exchanged and transferred within the Ripple network. The IOUs get their value from gateway's agreement to honour the obligation that the issuances represent. So it may happen that the market value of the IOU BTC issued by gateway A has a different price to the IOU BTC issued by the gateway B. In contrast, the native currency of Ripple (XRP) is not represented by an IOU and is not connected to gateways. Moreover, it is not mined and it is instead created and distributed directly by Ripple. This helps make XRP a convenient bridge currency to facilitate currency exchanges between pairs of assets that are not liquid. XRP is also needed as deposit in each account because a small transaction fee is required in order to prevent spamming and maintaining network costs. After being paid, the fee is then destroyed and not paid to any one. At its backbone, Ripple is a distributed database with a ledger which records in real-time all the transactions and keeps automatically updating the users' balance in any assets. Like for the Bitcoin protocol, also for Ripple anyone can download the ledger and examine the accounts, balances, and transactions for each anonymous user. When changes are made to the ledger, the servers connected to the Ripple protocol will mutually agree to change their copy of the ledger via a process called Ripple Protocol Consensus Algorithm (RPCA). With respect to the other standard synchronous consensus protocols, alternative to the asynchronous ones like Bitcoin, the RPCA introduces a new component called the Unique Node List (UNL). Each server (i.e., node) s in the Ripple network maintains a list of other "trusted" servers called UNL that s will query when determining consensus. Thus, only the votes approved by the other members of the UNL of s are considered when determining consensus (as opposed to every node in the network as in the example of the Bitcoin network). Since s creates its own UNL, this should in principle represents a subset of the network which, taken collectively, is trusted by s not to collude in order to generate Byzantine errors.[58]

[58] The RPCA concept of trust is similar to the Hawala payment systems [207] which is primarily located in the

The Ripple protocol brings the advantage of preventing "forks" in the network. This is possible by combining the fact that each node votes only proposals coming from trusted nodes in its same UNL and at the same time nodes may have different UNLs. This result is achieved with 5f +1 resilience [208]. This means that, in the presence of f Byzantine failures, the protocol will maintain correctness if at least the 80% of UNL servers agree on the transaction, and $f \leq$ (n-1)/5.[59] To give a benchmark, the Byzantine Generals problem with synchronous and reliable communication reaches consensus as long as $f \leq$ (n-1)/3, [11], [209]. As a secondary effect, the Ripple network agreement[60] is achieved as long as the cardinality of the intersection between any two UNLs is bigger than 1/5 of the larger UNL in the pair. And this must hold for all the pairs. To conclude, the RPCA is secure and guarantees that consensus is achieved in finite time with only two binding conditions: (1) the Byzantine failures are equal or lower than (n − 1)/5; and (2) the cardinality of the intersection between any two UNLs is bigger than 1/5 of the larger UNL in the pair. Initially, under the lead of Jed McCaleb (a former developer at MtGox), Ripple wanted to build the "internet of value" . Now Ripple's mission is to enhance and connect the current legacy systems and to enable the creation of new systems by providing financial institutions with a common ledger to clear and settle transactions in real-time and at the lowest possible cost. So Ripple started out as the most basic layer in the financial chain (especially for domestic and cross-currency payments), offering the opportunity to scale-up and potentially replace the whole SWIFT and SEPA layers. The fact that the RPCA: (1) allows anyone to define the set of trusted "authorities" to build centralised consensus in a distributed network; (2) is not based on miners, PoW or PoS principles; (3) embraces digital and hard currencies or any other certificate (via IOUs); (4) does not depend on a highly-volatile underlying token, makes Ripple attractive to banks and other financial institutions. Currently, a number of banks (e.g., Commonwealth Bank in Australia and Fidor Bank in Germany) and payment networks (e.g., Western Union) are starting to use Ripple as settlement infrastructure technology to clear transactions (via distributed ledgers) and settle obligations with the final goal to lower costs, offer better products, and faster times to market, [210], [211]. However, Ripple provides only the settlement or ledgering component for payment systems and facilitate their connectivity. Other critical aspects related to jurisdiction or network specific rules, governance, and standards are provided

Middle East, Africa, and India operating outside of, or parallel to, traditional banking, financial channels, and remittance systems.

[59] Correctness means that Ripple is able to discern the difference between a correct and fraudulent transaction.

[60] Agreement is the property of a decentralised-consensus protocol to maintain a single global truth in the face of a decentralised accounting system.

by existing systems and operators.

- Hyperledger[212] goes beyond the idea of a single and unique standardised database shared in a distributed public network by anonymous parties. Hyperledger envisions a world characterised by innumerable interoperable, what they call, consensus pools (i.e., ledgers) operated by different parties for different purposes. For instance, local markets for particular types of assets participated by a specific set of users under ad hoc rules that serve specific needs. Under this context, Hyperledger offers the infrastructure for the creation and management of those various ledgers. Differently from solutions based on public ledgers, Hyperledger especially addresses the requirements of those financial institutions and companies in the need of a shared data layer that must be kept private instead of public. In this way, any secondary party can participate in a particular distributed-consensus process and can have access to the same universal records of truth (i.e., records of the transactions) to which the other participants have access to, without that information necessary being available to the general public. With respect to the other ledgers, Hyperledger brings two novelties:

  (1) it is not based on a native currency (in principle, this means less regulatory risk and less technical overhead) and anyone can use the blockchain without the need of handling a built-in token;

  (2) it is not based on a single public ledger but allow users to deploy multiple private ledgers for specific asset classes (for example, a ledger for tradable liabilities of bank A in jurisdiction a and a ledger for tradable liabilities of bank B in jurisdiction b or even a ledger for the loyalty scheme of company C). This gives privacy control to the users over the ledgers and control over who participates in the network. Thus, rather than trust-less networks like Bitcoin, activities in Hyperledger work in a similar fashion like common projects shared in the cloud among collaborators: a certain degree of trust must exist (e.g., in the form of shared identity) in the real world among those users that want to partner with each other by joining the same consensus pool.

  As a consequence of these two characteristics, Hyperledger: (1) does not require any transfer fee between users within the same pool (i.e., using the same ledger); (2) is immune to spamming attacks that can be an issue for decentralised public ledgers like Bitcoin or Ripple [171]; (3) is not based on any mining process and the running of a node becomes a light-weight activity which can be extended to more than one independent

consensus pool (i.e., different ledgers for specific assets) at the same time; (4) it requires some synchronisation mechanism to exchange assets between different pools; (5) security can be set to different levels according to the type and size of the pool; (6) reduces the incentive for single nodes to conduct illegal activities or attack the network because they are not anonymous and they will be recognised by the other nodes and eventually by external parties. To conclude, with respect to Bitcoin there are some similarities and some substantial differences. In terms of similarities with respect to Bitcoin, Hyperledger follows a similar private-public key management infrastructure for signing and submitting transactions and the similarity is also extended to multi-signature transactions. In terms of differences, the Hyperledger consensus process is very different from Bitcoin-like protocols, because, similarly to Ripple, it is a derivation of the core protocol "practical Byzantine fault tolerance" [213]. The later is the root for a whole family tree of subsequent protocols that have been developed later with some slight changes with respect to increasing efficiency in high latency networks in order to render them more robust in some failure scenarios. Unlike asynchronous systems (e.g., Bitcoin) for these type of synchronous systems there is an upper bound to the number of failed malicious nodes that can be tolerated, which is 33.3% [11], [209]. So although, double-spending attack do not exist, the transaction is not executed if the system is unavailable or the number of failed malicious nodes is larger than one third. Moreover, individual single attacks may occur if a node independently decides to reject certain transactions.

There are also other asset-centric applications at an earlier stage, such as Clearmatics and Open Transactions. Clearmatics [214] is developing a decentralised marketplace for all those contracts that at the moment are negotiated over-the-counter without a clearing house. Clearmatic's aim is to create a Decentralised Clearing Network (DCN) that allows the reduction of counterparty risk, speed-up of settlements, lowering of costs and margin requirements, increase of traceability and transparency. The principle behind this is to offer users predefined smart contracts that mimic derivatives or the possibility to design custom smart contract via a Turing-complete programming language hosted on the DCN. Open Transactions [215] is an open-source project that has the goal of allowing users to issue and manipulate any type of digital assets (e.g., digital currencies, Ricardian contracts, and smart contracts). To conclude, by comparing asset-centric technologies with Bitcoin-like technologies, one may observe that the first ones allow for immediate transactions but rely on trusting networks of gateways and servers. While, the second ones need a confirmation time that may take several minutes and running full nodes (i.e, mining) is expensive, but they grant full decentralisation and do not require trust in third external parties.

References

[1] Jeremy Rifkin. *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*. Macmillan, 2014.

[2] Alvin Toffler, Wally Longul, and Harry Forbes. *The Third Wave*. Bantam books New York, 1981.

[3] Franklin Allen, James McAndrews, and Philip Strahan. E-finance: an Introduction. *Journal of Financial Services Research*, 22(1-2):5–27, 2002.

[4] Manuchehr Shahrokhi. E-finance: Status, Innovations, Resources and Future Challenges. *Managerial Finance*, 34(6):365–398, 2008.

[5] Matthew Hollow. Pre-1900 Utopian Visions of the 'Cashless Society'. *MPRA Paper No. 40780, posted 20. August 2012 23:29 UTC*, 2012.

[6] Michael Woodford. Doing Without Money: Controlling Inflation in a Post-Monetary World. *Review of Economic Dynamics*, 1(1):173–219, 1998.

[7] Claudia Costa and Paul De Grauwe. *Monetary Policy in a Cashless Society*, volume 2696. Centre for Economic Policy Research, 2001.

[8] Charles AE Goodhart. Can Central Banking Survive the "IT" Revolution ? *International Finance*, 3(2):189–209, 2000.

[9] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 1:2012, 2008.

[10] Andreas M Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies."* O'Reilly Media, Inc.", 2014.

[11] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[12] Cryptocoin Talk. `https://cryptocointalk.com/forum/178-scrypt-cryptocoins/`, 2014. (Date last accessed: 22-September-2014).

[13] Bitcoin Wiki. Tragedy of the Commons. `https://en.bitcoin.it/wiki/Tragedy_of_the_Commons`, 2014. (Date last accessed: 01-September-2014).

[14] Blockchain. http://blockchain.info, 2015. (Date last accessed: 01-June-2015).

[15] Bitcoin Wiki. Bitcoin Symbol. https://en.bitcoin.it/wiki/Bitcoin_symbol, 2015. (Date last accessed: 10-Aug-2015).

[16] Nacha. https://www.nacha.org, 2015. (Date last accessed: 01-June-2015).

[17] Wikipedia. Direct Debit. https://en.wikipedia.org/wiki/Direct_debit, 2015. (Date last accessed: 01-June-2015).

[18] European Commission. Single Euro Payments Area (SEPA). http://ec.europa.eu/finance/payments/sepa/index_en.htm, 2015. (Date last accessed: 01-June-2015).

[19] Edwin N Mwangi. *Adoption Of Bitcoin In Kenya, A Case Study Of Bitpesa.* PhD thesis, University Of Nairobi, 2014.

[20] Chiraag Patel. USD 307 Bn to be Spent on Cross Border Shopping by 2018, says PayPal. http://letstalkpayments.com/307-bn-spent-cross-border-shopping-2018-says-paypal, 2015. (Date last accessed: 01-June-2015).

[21] Aalok Jariwala. Ripple About to Change How You Send Money Crossborder. http://letstalkpayments.com/ripple-about-to-change-how-you-send-money-crossborder, 2015. (Date last accessed: 01-June-2015).

[22] Bitcoin Wiki. Transaction Fees. https://en.bitcoin.it/wiki/Transaction_fees, 2015. (Date last accessed: 01-June-2015).

[23] Pelle Braendgaard. The May Scale of Money Hardness and BitCoin. http://blog.stakeventures.com/articles/2012/03/07/the-may-scale-of-money-hardness-and-bitcoin, 2015. (Date last accessed: 01-June-2015).

[24] Kristov Atlas. Weak Privacy Guarantees for SharedCoin Mixing Service. http://www.coinjoinsudoku.com/advisory, 2015. (Date last accessed: 01-June-2015).

[25] Bitcoin Wiki. Mixing Service. https://en.bitcoin.it/wiki/Mixing_service, 2015. (Date last accessed: 01-June-2015).

[26] Bitcoin Wiki. Bitcoin Laundry. https://en:bitcoin:it/wiki/BitcoinLaundry, 2014. (Date last accessed: 01-June-2014).

[27] Share Coin. https://sharedcoin.com, 2015. (Date last accessed: 01-June-2015).

[28] Bitcoin wiki. CoinJoin. https://en.bitcoin.it/wiki/CoinJoin, 2015. (Date last accessed: 01-June-2015).

[29] Visa. Earnings Results 2015. http://investor.visa.com/financial-information/quarterly-earnings/default.aspx, 2015. (Date last accessed: 01-June-2015).

[30] Discover. SEC Filings. http://investorrelations.discoverfinancial.com/phoenix.zhtml?c=204177&p=irol-sec, 2015. (Date last accessed: 01-June-2015).

[31] Western Union. Quarterly Results. http://ir.westernunion.com/investor-relations/financials/quarterly-results/default.aspx, 2015. (Date last accessed: 01-June-2015).

[32] Mastercard. MasterCard Incorporated. Reports: Second-Quarter 2015. http://investor.mastercard.com/investor-relations/financials-and-sec-filings/quarterly-results/default.aspx, 2015. (Date last accessed: 01-June-2015).

[33] David Yermack. Is Bitcoin a Real Currency? An Economic Appraisal. Technical report, National Bureau of Economic Research, 2013.

[34] Wikipedia. Private Currency. http://en.wikipedia.org/wiki/Private_currency, 2015. (Date last accessed: 01-June-2015).

[35] CoinMarketCap. https://coinmarketcap.com/all.html, 2015. (Date last accessed: 01-June-2015).

[36] Ferdinando M Ametrano. Hayek money: the cryptocurrency price stability solution. *Available at SSRN 2425270*, 2014.

[37] Angela Rogojanu, Liana Badea, et al. The issue of competing currencies. case study–bitcoin. *Theoretical and Applied Economics*, 21(1):103–114, 2014.

[38] David Garcia, Claudio J Tessone, Pavlin Mavrodiev, and Nicolas Perony. The Digital Traces of Bubbles: Feedback Cycles Between Socio-Economic Signals in the Bitcoin Economy. *Journal of The Royal Society Interface*, 11(99):20140623, 2014.

[39] Adam Hayes. A Cost of Production Model for Bitcoin. *Available at SSRN*, 2015.

[40] ECB. Virtual Currency Schemes. Technical report, European Central Bank - ISBN: 978-92-899-0862-7 (online October 2012), 2012.

[41] ECB. Virtual Currency Schemes. A Further Analysis. Technical report, European Central Bank - ISBN: 978-92-899-1560-1 (online February 2015), 2015.

[42] Parliament EU. Directive 2009/110/ec. taking up, pursuit and prudential supervision of the business of electronic money institutions, amending directives 2005/60/ec and 2006/48/ec and repealing directive 2000/46/ec, 2009 o.j. (l 267) 7. *Official Journal of the European Union*, 2009.

[43] Parliament EU. Directive 2007/64/ec. on payment services in the internal market amending directives 97/7/ec, 2002/65/ec, 2005/60/ec and 2006/48/ec and repealing directive 97/5/ec. *Official Journal of the European Union*, 2007.

[44] EBA. Warning to Consumers on Virtual Currencies. *European Banking Authority, EBA/WRG/2013/01*, 2013. https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf.

[45] EBA. Opinion on Virtual Currencies. *European Banking Authority, EBA/Op/2014/08*, 2014. https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf.

[46] Agorisminfo. http://www.agorism.info/, 2015. (Date last accessed: 01-June-2015).

[47] Tomothy C. May. The Crypto Anarchist Manifesto. http://www.groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html, 2014. (Date last accessed: 01-June-2014).

[48] Adrian Chen. Much Ado About Bitcoin. http://www.nytimes.com/2013/11/27/opinion/much-ado-about-bitcoin.html, 2015. (Date last accessed: 01-June-2015).

[49] Bitcoin Wiki. Clients. http://en.bitcoin.it/wiki/Clients, 2015. (Date last accessed: 01-June-2015).

[50] Bitcoinorg. Bitcoin Development. https://bitcoin.org/en/development, 2015. (Date last accessed: 01-June-2015).

[51] Sourceforge. http://sourceforge.net/home.html, 2015. (Date last accessed: 01-June-2015).

[52] ITU. http://www.itu.int, 2015. (Date last accessed: 01-June-2015).

[53] Bitcoin Wiki. Bitcoin Core, 2015. https://en.bitcoin.it/wiki/Bitcoin_Core, 2015. (Date last accessed: 01-June-2015).

[54] Bitcoin Wiki. Bitcoind. https://en.bitcoin.it/wiki/Bitcoind, 2015. (Date last accessed: 01-June-2015).

[55] Bitcoinorg. Bitcoin Core Version History. https://bitcoin.org/en/version-history, 2015. (Date last accessed: 01-June-2015).

[56] Bitcoin.org. Choose your Bitcoin Wallet. https://bitcoin.org/en/choose-your-wallet, 2015. (Date last accessed: 01-June-2015).

[57] Bitcointalk. http://www.bitcointalk.org, 2015. (Date last accessed: 01-June-2015).

[58] Cointerest. http://cointerest.org/map, 2015. (Date last accessed: 01-Feb-2015).

[59] Coinbase. https://coinbase.com/, 2015. (Date last accessed: 01-Feb-2015).

[60] Sourceforge. http://sourceforge.net/projects/bitcoin/, 2015. (Date last accessed: 01-June-2015).

[61] Blockchain. My Wallet Number of Users. https://blockchain.info/charts/my-wallet-n-users, 2015. (Date last accessed: 01-June-2015).

[62] Github. http://www.github.com, 2015. (Date last accessed: 01-June-2015).

[63] Authorized. http://www.authorize.net, 2015. (Date last accessed: 01-June-2015).

[64] Stripe. http://stripe.come, 2015. (Date last accessed: 01-June-2015).

[65] Ripple. http://www.ripple.com, 2015. (Date last accessed: 01-June-2015).

[66] Bitangel. http://www.bitangel.com, 2015. (Date last accessed: 01-June-2015).

[67] Coinfilter. http://www.coinfilter.com, 2015. (Date last accessed: 01-June-2015).

[68] Coindesk. http://www.coindesk.com, 2015. (Date last accessed: 01-June-2015).

[69] Crunchbase. http://www.crunchbase.com,, 2015. (Date last accessed: 01-June-2015).

[70] Cbinsight. http://www.cbinsight.com, 2015. (Date last accessed: 01-June-2015).

[71] Marie Vasek and Tyler Moore. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In *FC'15: Proceedings of the 19th International Conference on Financial Cryptography and Data Security*, 2015.

[72] UK Government. Digital Currencies: Call for Information. https://www.gov.uk/government/consultations/digital-currencies-call-for-information, 2015. (Date last accessed: 03-Aug-2015).

[73] Bank of Canada. The Annual Bank of Canada Conference on Electronic Money and Payments Funds Management and Banking Department, Currency Department, Bank of Canada. http://www.ssrn.com/update/ern/ernann/ann15079.html, 2015. (Date last accessed: 03-Aug-2015).

[74] Gertrude Chavez-Dreyfuss. Exclusive: IBM Looking at Adopting Bitcoin Technology for Major Currencies. http://www.reuters.com/article/2015/03/12/us-bitcoin-ibm-idUSKBN0M82KB20150312, 2015. (Date last accessed: 03-Aug-2015).

[75] Penny Crosman. CBW Bank Readies Launch of Real-Time Payments. http://www.americanbanker.com/news/bank-technology/cbw-bank-readies-launch-of-real-time-payments-1072921-1.html, 2015. (Date last accessed: 03-Aug-2015).

[76] Allen Scot. Estonia's LHV Bank: 'The Bitcoin Blockchain is the Most Tested and Secure for Our Applications'. http://cointelegraph.com/news/114599/estonias-lhv-bank-the-bitcoin-blockchain-is-the-most-tested-and-secure-for-our-applications, 2015. (Date last accessed: 03-Aug-2015).

[77] Duncan Riley. Westpac, ANZ trial Ripple's Blockchain Ledger System, but Say No to Bitcoin, for Now. http://siliconangle.com/blog/2015/06/09/westpac-anz-trial-ripples-blockchain-ledger-system-but-say-no-to-bitcoin-for-now/, 2015. (Date last accessed: 03-Aug-2015).

[78] Emily Spaven. Barclays Data Officer Praises Blockchain Tech at SWIFT Forum. http://www.coindesk.com/barclays-data-officer-praises-blockchain-tech-at-swift-forum/, 2015. (Date last accessed: 03-Aug-2015).

[79] Anna Irrera. UBS to Open Blockchain Research Lab in London. http://blogs.wsj.com/digits/2015/04/02/ubs-to-open-blockchain-research-lab-in-london/, 2015. (Date last accessed: 03-Aug-2015).

[80] Michael J. Casey. Goldman a Lead Investor in Funding Round for Bitcoin Startup Circle. http://www.wsj.com/articles/goldman-a-lead-investor-in-funding-round-for-bitcoin-startup-circle-1430363042, 2015. (Date last accessed: 03-Aug-2015).

[81] John Biggs. Citibank Is Working On Its Own Digital Currency, Citicoin. http://techcrunch.com/2015/07/07/citibank-is-working-on-its-own-digital-currency-citicoin/, 2015. (Date last accessed: 03-Aug-2015).

[82] Clint Boulton. BNY Mellon Explores Bitcoin's Potential. http://blogs.wsj.com/cio/2015/04/05/bny-mellon-explores-bitcoins-potential/, 2015. (Date last accessed: 03-Aug-2015).

[83] Gertrude Chavez-Dreyfuss. USAA Creates Research Team to Study Use of Bitcoin Technology. http://www.reuters.com/article/2015/05/10/us-usa-usaa-bitcoin-idUSKBN0NT2C620150510, 2015. (Date last accessed: 03-Aug-2015).

[84] Giulio Prisco. BNP Paribas Testing Plans to Add Bitcoin to its Currency Funds. https://bitcoinmagazine.com/21347/bnp-paribas-planning-add-bitcoin-currency-funds-successful-beta-test/, 2015. (Date last accessed: 03-Aug-2015).

[85] Oscar Williams-Grut. Santander is Experimenting With Bitcoin and Close to Investing in a Blockchain Startup. http://uk.businessinsider.com/santander-has-20-25-use-cases-for-bitcoins-blockchain-technology-everyday-banking-2015-6, 2015. (Date last accessed: 03-Aug-2015).

[86] John Adams. BBVA Wants Bitcoin's Tech, Not the Currency. http://www.paymentssource.com/news/technology/bbva-wants-bitcoins-tech-not-the-currency-3020380-1.html, 2015. (Date last accessed: 03-Aug-2015).

[87] Diana Ngo. ING, Other Major Dutch Banks Take Interest in Blockchain Tech. http://cointelegraph.com/news/113033/ing-other-major-dutch-banks-take-interest-in-blockchain-tech, 2015. (Date last accessed: 03-Aug-2015).

[88] Pete Rizzo. Western Union 'Exploring' Pilot Program With Ripple Labs. http://www.coindesk.com/western-union-pilot-program-ripple-labs/, 2015. (Date last accessed: 12-Aug-2015).

[89] Olga Kharif. Samsung Plans to Take Bitcoin Technology Beyond Virtual Currency. http://www.bloomberg.com/news/articles/2015-04-10/samsung-plans-

to-take-bitcoin-technology-beyond-virtual-currency, 2015. (Date last accessed: 03-Aug-2015).

[90] Giulio Prisco. Is IBM Building a Digital Cash for National Currencies? https://bitcoinmagazine.com/19586/ibm-building-digital-cash-national-currencies/, 2015. (Date last accessed: 15-July-2015).

[91] Pete Rizzo. Nasdaq Trading Technology to Power Bitcoin Marketplace Noble. http://www.coindesk.com/nasdaq-bitcoin-marketplace-noble/, 2015. (Date last accessed: 03-Aug-2015).

[92] Gerrard Hartley. New York Stock Exchange and Former Citigroup CEO Invest in Coinbase. https://www.cryptocoinsnews.com/new-york-stock-exchange-former-citigroup-ceo-invest-coinbase/, 2015. (Date last accessed: 03-Aug-2015).

[93] Giulio Prisco. Intel Joins the Blockchain Technology Race, Forms Special Research Group. https://bitcoinmagazine.com/19646/intel-joins-blockchain-technology-race-forms-special-research-group/, 2015. (Date last accessed: 03-Aug-2015).

[94] Merkle Tree. http://merkletree.io, 2015. (Date last accessed: 01-June-2015).

[95] Mt. Gox. Clarification of Mt.GOX Compromised Accounts and Major Bitcoin Sell-Off. https://web.archive.org/web/20110919162635/https://mtgox.com/press_release_20110630.html, 2011. (Date last accessed: 10-March-2015).

[96] Mt. Gox. http://pastebin.com/d7vp06hL, 2011. (Date last accessed: 10-March-2015).

[97] Bitcoin Block Explorer. http://blockexplorer.com/block/00000000000004bea72d0f390194b08162665a4fc99469c576338cd37164a15a, 2011. (Date last accessed: 10-March-2015).

[98] Bitcoin Block Explorer. http://blockexplorer.com/block/00000000000000fb62bbadc0a9dcda556925b2d0c1ad8634253ac2e83ab8382f, 2011. (Date last accessed: 10-March-2015).

[99] Kim Nilsson. The Missing MtGox Bitcoins. http://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html, 2015. (Date last accessed: 10-June-2015).

[100] FBI. Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity. *Federal Bureou of Investigation, USA*, 2012.

[101] Andy Greenberg. Not Just Silk Road 2: Feds Seize Two Other Drug Markets and Counting. http://www.wired.com/2014/11/dark-web-seizures, 2014. (Date last accessed: 01-June-2015).

[102] Andy Greenberg. Silk Road Creator Ross Ulbricht Sentenced to Life in Prison. http://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/, 2015. (Date last accessed: 01-June-2015).

[103] Digital Citizens Alliance. Busted, But Not Broken: The State of Silk Road and The Darknet Marketplaces. Technical report, Digital Citizens Alliance, 2014.

[104] Mtgox. https://www.mtgox.com, 2015. (Date last accessed: 01-June-2015).

[105] Jonathan Soble. Mark Karpeles, Chief of Bankrupt Bitcoin Exchange, Is Arrested in Tokyo. http://www.nytimes.com/2015/08/02/business/dealbook/mark-karpeles-mt-gox-bitcoin-arrested.html?_r=0, 2015. (Date last accessed: 20-Aug-2015).

[106] Tyler Moore and Nicolas Christin. Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In *Financial Cryptography and Data Security*, pages 25–33. Springer, 2013.

[107] PanAm Post. Resolución del Banco Central de Bolivia. http://www.scribd.com/doc/230438003/Resolucion-del-Banco-Central-de-Bolivia, 2015. (Date last accessed: 01-June-2015).

[108] NBKR. http://www.nbkr.kg/all_news.jsp?news_type=NBKRNews&lang=ENG, 2015. (Date last accessed: 01-June-2015).

[109] Stan Higgins. Ecuador Bans Bitcoin, Plans Own Digital Money. http://www.coindesk.com/ecuador-bans-bitcoin-legislative-vote, 2015. (Date last accessed: 01-June-2015).

[110] Charles Riley and Zhang Dayu. China Cracks Down on Bitcoin. money.cnn.com/2013/12/05/investing/china-bitcoin, 2014. (Date last accessed: 01-June-2014).

[111] Jake Maxwell Watts. Thailand's Bitcoin Ban is Not Quite What it Seems. http://qz.com/110164/thailands-infamous-bitcoin-crackdown-is-not-quite-what-it-seems, 2015. (Date last accessed: 01-June-2015).

[112] Wikipedia. Legality of Bitcoin by Country. http://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country, 2015. (Date last accessed: 01-June-2015).

[113] RT. Russian Media Watchdog Blocks Bitcoin Sites. http://rt.com/news/222215-russia-bans-bitcoin-sites, 2015. (Date last accessed: 01-June-2015).

[114] Jim Urquhart. Russian Authorities say Bitcoin Illegal. http://www.reuters.com/article/2014/02/09/us-russia-bitcoin-idUSBREA1806620140209, 2015. (Date last accessed: 01-June-2015).

[115] Caleb Chen. Russia Has Blocked Several Bitcoin Sites in Preperation for Russian Bitcoin Ban. https://www.cryptocoinsnews.com/russia-blocked-several-bitcoin-sites-preperation-russian-bitcoin-ban, 2015. (Date last accessed: 01-June-2015).

[116] FinCEN. Application of FinCEN's Regulations to Virtual Currency Mining Operations. *FIN-2014-R001 U.S. Dep. of Tresaury - Financial Crimes Enforcement Network, USA*, 2014.

[117] FinCEN. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. *FIN-2013-G001 U.S. Dep. of Tresaury - Financial Crimes Enforcement Network, USA*, 2013.

[118] NY Dep. of Fin. Serv. Regulation Of The Superintendent Of Financial Services – Virtual Currencies. http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf, 2014. (Date last accessed: 01-June-2015).

[119] Datauthority. http://info.datauthority.org/wordpress, 2015. (Date last accessed: 01-June-2015).

[120] Pete Rizzo. Bitcoin Exchanges Kraken and Bitfinex Cut Services in New York. http://www.coindesk.com/bitcoin-exchanges-kraken-and-bitstamp-cut-services-in-new-york/, 2015. (Date last accessed: 20-Aug-2015).

[121] Matt Dababneh. AB-1326 Virtual Currency. http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB1326, 2015. (Date last accessed: 01-June-2015).

[122] Nobitcoinlicense. https://nobitcoinlicense.org/, 2015. (Date last accessed: 25-Aug-2015).

[123] Jens Münzer. Bitcoins: Supervisory Assessment and Risks to Users. http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html, 2015. (Date last accessed: 01-June-2015).

[124] BaFin. Trading in Bitcoins. http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Jahresbericht/2013/jb_2013_II_9_2_trading_in_bitcoins.html, 2014. (Date last accessed: 01-June-2015).

[125] Banque de France. The Dangers Linked to the Emergence of Virtual Currencies: the example of Bitcoins. *Focus 10, Dec.2013, Banque de France*, 2013. https://www.banque-france.fr/uploads/tx_bdfgrandesdates/Focus10-the_dangers_linked_to_the_emergence_of_virtual_currencies_the_example_of_bitcoins-GB.pdf.

[126] FINMA. Bitcoins. *FACT SHEET 25.06.2014 - Swiss Financial Market Supervisory Authority*, 2014.

[127] FINMA. Verordnung der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor. https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/anhoerungen/abgeschlossene-anhoerungen/gwv-finma-revision/gwv_finma.pdf?la=de, 2015. (Date last accessed: 25-Aug-2015).

[128] Federal Council. Federal Council Report on Virtual Currencies in Response to the Schwaab (13.3687) and Weibel (13.4070) Postulates. http://www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf, 2014. (Date last accessed: 01-June-2015).

[129] Bank of Italy. Avvertenza sull'Utilizzo delle Cosiddette "Valute Virtuali". http://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf, 2015. (Date last accessed: 01-June-2015).

[130] Bank of Italy. Comunicazione del 30 Gennaio 2015 – Valute Virtuali. http://www.bancaditalia.it/pubblicazioni/bollettino-vigilanza/2015-01/20150130_II15.pdf, 2015. (Date last accessed: 01-June-2015).

[131] Bank of Italy. Utilizzo Anomalo Di Valute Virtuali. http://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione_UIF_su_VV.pdf, 2015. (Date last accessed: 01-June-2015).

[132] Tom Gullen. Bitcoin's UK Future Looks Bleak. https://www.scirra.com/blog/tom/4/bitcoins-uk-future-looks-bleak, 2015. (Date last accessed: 01-June-2015).

[133] HMRC. Bitcoin and Other Cryptocurrencies. *Policy Paper HM Revenue & Customs, Revenue and Customs Brief 9 (2014), UK*, 2014.

[134] HM Treasury. Digital Currencies: Response to the Call for Information. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf, 2015. (Date last accessed: 01-June-2015).

[135] Out Law. Anti-Money Laundering Rules to Apply to Digital Currency Exchanges in The UK. http://www.out-law.com/en/articles/2015/march/anti-money-laundering-rules-to-apply-to-digital-currency-exchanges-in-the-uk/, 2015. (Date last accessed: 01-June-2015).

[136] Eric Goldman. The Third Wave of Internet Exceptionalism. *The Next Digital Decade: Essays on the Future of the Internet*, pages 179–188, 2010.

[137] Milton Friedman. A Theoretical Framework for Monetary Analysis. *Journal of Political Economy*, 78(2):pp. 193–238, 1970.

[138] Ludwig Von Mises. *The Theory of Money and Credit*. Ludwig von Mises Institute, 1963.

[139] Walter Block and Kenneth M Garschina. Hayek, Business Cycles and Fractional Reserve Banking: Continuing the De-Homogenization Process. *The Review of Austrian Economics*, 9(1):77–94, 1996.

[140] Milton Friedman. A monetary and fiscal framework for economic stability. *The American Economic Review*, pages 245–264, 1948.

[141] Milton Friedman. A program for monetary stabilityfordham university press. *New York*, 1960.

[142] Dogecoin. http://dogecoin.com, 2015. (Date last accessed: 01-June-2015).

[143] Peercoin. http://peercoin.net, 2015. (Date last accessed: 01-June-2015).

[144] Bitbond. http://bitbond.net, 2015. (Date last accessed: 01-June-2015).

[145] Btcjam. https://www.btcjam.com/, 2015. (Date last accessed: 01-June-2015).

[146] Tera Exchange. http://www.teraexchange.com/lending.html, 2015. (Date last accessed: 01-July-2015).

[147] Bitinfocharts. http://www.bitinfocharts.com, 2015. (Date last accessed: 01-June-2015).

[148] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140. ACM, 2013.

[149] Sarah Meiklejohn and Claudio Orlandi. Privacy-Enhancing Overlays in Bitcoin. Technical report, University College London (Version 2015).

[150] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating User Privacy in Bitcoin. In *Financial Cryptography and Data Security*, pages 34–51. Springer, 2013.

[151] Fergal Reid and Martin Harrigan. *An analysis of Anonymity in the Bitcoin System*. Springer, 2013.

[152] Dániel Kondor, Márton Pósfai, István Csabai, and Gábor Vattay. Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network. *PloS one*, 9(2):e86197, 2014.

[153] Corrado Gini. Variabilità e mutabilità. *Reprinted in Memorie di metodologica statistica (Ed. Pizetti E, Salvemini, T). Rome: Libreria Eredi Virgilio Veschi*, 1, 1912.

[154] Max O Lorenz. Methods of Measuring the Concentration of Wealth. *Publications of the American statistical association*, 9(70):209–219, 1905.

[155] Bitcoin Wiki. Controlled Supply, 2015. https://en.bitcoin.it/wiki/Controlled_supply, 2015. (Date last accessed: 01-June-2015).

[156] Butterflylabs. http://www.butterflylabs.com, 2015. (Date last accessed: 01-June-2015).

[157] Bitcoin Wiki. Comparison of Mining Pools. https://en.bitcoin.it/wiki/Comparison_of_mining_pools, 2015. (Date last accessed: 12-Aug-2015).

[158] Nicolas Courtois. The day on which bitcoin has become centralized. http://blog.bettercrypto.com/?p=714, 2014. (Date last accessed: 25-Aug-2015).

[159] Bitcoin Wiki. GHash.IO. https://en.bitcoin.it/wiki/GHash.IO, 2015. (Date last accessed: 01-June-2015).

[160] Blocktrail. https://www.blocktrail.com/, 2015. (Date last accessed: 12-Jul-2015).

[161] Nermin Hajdarbegovic. Reddit CEO Thinks the World of Dogecoin, Slams 'Crazy' Bitcoiners. http://www.coindesk.com/reddit-ceo-thinks-world-dogecoin-slams-crazy-bitcoiners/, 2014. (Date last accessed: 15-May-2014).

[162] EBA. Cryptotechnologies, a Major IT Innovation and Catalyst for Change:4 categories, 4 Applications and 4 Scenarios An Exploration for Transaction Banking and Payments Professionals. Technical report, EBA Working Group on Electronic and Alternative Payments (Version 1.0, 11th May 2015), 2015.

[163] Holy Transaction. https://holytransaction.com/, 2015. (Date last accessed: 15-July-2015).

[164] Google. https://www.google.com/wallet/, 2015. (Date last accessed: 15-July-2015).

[165] Apple. https://www.apple.com/apple-pay/, 2015. (Date last accessed: 15-July-2015).

[166] Olga Kharif. Samsung Plans to Take Bitcoin Technology Beyond Virtual Currency. http://www.bloomberg.com/news/articles/2015-04-10/samsung-plans-to-take-bitcoin-technology-beyond-virtual-currency, 2015. (Date last accessed: 15-July-2015).

[167] John Biggs. Citibank Is Working On Its Own Digital Currency, Citicoin. http://techcrunch.com/2015/07/07/citibank-is-working-on-its-own-digital-currency-citicoin/#.rukgfh:q2gh, 2015. (Date last accessed: 15-July-2015).

[168] Coin Creator. http://coincreator.net/#home, 2015. (Date last accessed: 15-July-2015).

[169] Bitcoin Wiki. Colored Coins. https://en.bitcoin.it/wiki/Colored_Coins, 2015. (Date last accessed: 03-Aug-2015).

[170] Ken Shirriff. Hidden Surprises in the Bitcoin Blockchain and How They are Stored: Nelson Mandela, Wikileaks, Photos, and Python Software. http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html#ref9, 2015. (Date last accessed: 11-May-2015).

[171] Daniel Cawrey. Why New Forms of Spam Could Bloat Bitcoin's Block Chain. http://www.coindesk.com/new-forms-spam-bloat-bitcoins-block-chain/, 2014. (Date last accessed: 13-Jan-2015).

[172] Andrew Wagner. Ensuring Network Scalibility: How to Fight Blockchain Bloat. https://bitcoinmagazine.com/17824/how-to-ensure-network-scalibility-fighting-blockchain-bloat/, 2015. (Date last accessed: 15-July-2015).

[173] Meni Rosenfeld. Overview of Colored Coins. *White paper*, 2012.

[174] Coinprism. https://www.coinprism.com/, 2015. (Date last accessed: 15-July-2015).

[175] Colored Coins. http://coloredcoins.org/, 2015. (Date last accessed: 15-July-2015).

[176] Colu. http://colu.co/, 2015. (Date last accessed: 03-Aug-2015).

[177] CoinSpark. http://coinspark.org/, 2015. (Date last accessed: 03-Aug-2015).

[178] Yoni Assia, Vitalik Buterin, liorhakiLior Hakim, Meni Rosenfeld, Rotem Lev. Colored Coins Whitepaper. https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit#, 2013. (Date last accessed: 03-Aug-2015).

[179] Counterparty. http://counterparty.io/, 2015. (Date last accessed: 10-July-2015).

[180] Bitcoin Wiki. Proof of Burn. https://en.bitcoin.it/wiki/Proof_of_burn, 2015. (Date last accessed: 03-Aug-2015).

[181] Vitalik Buterin. Bitcoin Multisig Wallet: The Future of Bitcoin. https://bitcoinmagazine.com/11108/multisig-future-bitcoin/, 2014. (Date last accessed: 12-Jul-2015).

[182] Bitcoin Wiki. Multisignature. https://en.bitcoin.it/wiki/Multisignature, 2015. (Date last accessed: 12-Jul-2015).

[183] Coinprism. Proof of Authenticity of Crypto-assets with Coinprism. http://blog.coinprism.com/2014/09/10/proof-of-authenticity-of-cryptoassets/, 2014. (Date last accessed: 03-Aug-2015).

[184] Master Coin. http://www.mastercoinwallets.org/, 2015. (Date last accessed: 15-July-2015).

[185] Willet Jr. MasterCoin Complete Specification. *White paper*, 2013.

[186] Alex Brokaw. The People Who Burn Bitcoins. http://www.minyanville.com/business-news/editors-pick/articles/The-People-Who-Burn-Bitcoins-bitcoin/4/16/2014/id/54627#ixzz3i4GfzdVP, 2014. (Date last accessed: 03-Aug-2015).

[187] Tim Swanson. *Great Chain of Numbers. A Guide to Smart Contracts, Smart Property, and Trustless Asset Management, publisher = Creative Commons - Attribution 4.0 International.* 2014.

[188] Omni Layer. http://www.omnilayer.org/, 2015. (Date last accessed: 15-July-2015).

[189] Ethereum. https://ethereum.org/, 2015. (Date last accessed: 10-July-2015).

[190] Vitalik Buterin. Ultimate Scripting: A Platform for Generalized Financial Contracts on Mastercoin. http://vitalik.ca/ultimatescripting.html, 2015. (Date last accessed: 15-July-2015).

[191] Factom. http://factom.org/, 2015. (Date last accessed: 03-Aug-2015).

[192] MaidSafe. http://maidsafe.net/, 2015. (Date last accessed: 03-Aug-2015).

[193] Tether. https://tether.to/, 2015. (Date last accessed: 03-Aug-2015).

[194] Name Coin. https://namecoin.info/, 2015. (Date last accessed: 15-July-2015).

[195] D. Johnston, S.O. Yilmaz, J. Kandah, N. Bentenitis, F. Hashemi, R. Gross, S. Wilkinson and S. Mason. The General Theory of Decentralized Applications, Dapps. https://github.com/DavidJohnstonCEO/DecentralizedApplications#the-emerging-wave-of-decentralized-applications, 2015. (Date last accessed: 10-March-2015).

[196] Vitalik Buterin. DAOs, DACs, DAs and More: An Incomplete Terminology Guide. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/, 2015. (Date last accessed: 10-March-2015).

[197] NXT. http://nxt.org/, 2015. (Date last accessed: 10-March-2015).

[198] NXT. https://wiki.nxtcrypto.org/wiki/Voting_System, 2015. (Date last accessed: 10-March-2015).

[199] Eris Industries. https://erisindustries.com/, 2015. (Date last accessed: 10-July-2015).

[200] Eris Industries. https://erisindustries.com/products/erisdb/, 2015. (Date last accessed: 15-July-2015).

[201] Eris Industries. https://erisindustries.com/products/erisserver/, 2015. (Date last accessed: 15-July-2015).

[202] IPFS. http://ipfs.io/, 2015. (Date last accessed: 15-July-2015).

[203] Tendermint. http://tendermint.com/, 2015. (Date last accessed: 10-July-2015).

[204] Bitcoin. https://bitcoin.org/en/, 2015. (Date last accessed: 10-May-2015).

[205] Stellar. https://www.stellar.org/, 2015. (Date last accessed: 13-June-2015).

[206] Ripple. https://ripple.com/build/gateway-guide/, 2015. (Date last accessed: 01-Jul-2015).

[207] John F Wilson et al. Informal Funds Transfer Systems: An Analysis of the Hawala System. *International Monetary Fund*, 2003.

[208] David Schwartz, Noah Youngs, and Arthur Britto. The Ripple Protocol Consensus Algorithm. *Ripple Labs Inc White Paper*, 2014.

[209] Marshall Pease, Robert Shostak, and Leslie Lamport. Reaching Agreement in the Presence of Faults. *Journal of the ACM (JACM)*, 27(2):228–234, 1980.

[210] Sarah Todd. Banks Can Cherry-Pick the Best Bits from Bitcoin. http://www.americanbanker.com/news/bank-technology/banks-can-cherry-pick-the-best-bits-from-bitcoin-report-1073642-1.html, 2015. (Date last accessed: 03-May-2015).

[211] Evander Smart. Ripple Labs Cracks U.S. Banking with New Deal. https://www.cryptocoinsnews.com/ripple-labs-enters-us-banking/, 2014. (Date last accessed: 01-Mar-2015).

[212] Hyperledger. http://hyperledger.com/, 2015. (Date last accessed: 13-June-2015).

[213] Miguel Castro, Barbara Liskov, et al. Practical Byzantine Fault Tolerance. In *OSDI*, volume 99, pages 173–186, 1999.

[214] Clearmatics. http://www.clearmatics.com/, 2015. (Date last accessed: 01-Jul-2015).

[215] Open Transactions. http://opentransactions.org, 2015. (Date last accessed: 01-Jul-2015).