Joint Discussion Paper Series in Economics

by the Universities of

Aachen · Gießen · Göttingen
Kassel · Marburg · Siegen

ISSN 1867-3678

No. 04-2018

Andreas Hanl

Some Insights into the Development of Cryptocurrencies

This paper can be downloaded from
http://www.uni-marburg.de/fb02/makro/forschung/magkspapers

Coordination: Bernd Hayo • Philipps-University Marburg
School of Business and Economics • Universitätsstraße 24, D-35032 Marburg
Tel: +49-6421-2823091, Fax: +49-6421-2823088, e-mail: hayo@wiwi.uni-marburg.de

Some Insights into the Development of Cryptocurrencies*

Andreas Hanl†

February 5, 2018

Abstract

Cryptocurrencies such as Bitcoin might revolutionize the economy through enabling peer-to-peer based transactions by abolishing the need for a trusted intermediary. As for now, Bitcoin remains to be the best recognized cryptocurrency, in particular in terms of market capitalization. However, as this paper shows, there are plenty of alternatives. This paper outlines the historical roots which have led to the creation of privately emitted, cryptography based digital currencies. Additionally, this paper discusses future possible hurdles of the development of cryptocurrencies and outlines features which might influence the success of a cryptocurrency. Insights into the beginning of cryptocurrency development are gained by analysis of the publicly available DOACC dataset. The paper does so by providing an overview of the techniques and mechanisms used by cryptocurrencies. It shows that newly created cryptocurrencies tend to be very similar in some properties in the early stages but new features and more diversity developed in more recent years. Additionally, newly created cryptocurrencies tend more and more to create a fixed number of coins before the initial announcement in order to sell these in Initial Coin Offerings. Even when the amount of premining increases over years, it remains at lower levels on the aggregate.

Keywords: Cryptocurrency; Bitcoin; Blockchain, Cryptography; Digital Money; E-Money

JEL Codes: E40, E42

*This paper has benefited from comments by and discussions with Walter Blocher, Alexander Günther, Philipp Kirchner and Jochen Michaelis. The work on this project was supported by a PhD-scholarship provided by the University of Kassel.

†Department of Economics, University of Kassel, Nora-Platiel-Str. 4, 34109 Kassel, Germany; E-mail: hanl@uni-kassel.de.

1 Introduction

For ages and ages, money has in most cases been a centralized system, mostly state-issued. Even though electronic payments got more important in the last decades (Bagnall et al. 2016), money remained under a centralized governmental control. However, the last financial crisis of 2007ff. has not only shown a loss of trust in these central institutions, it has also given rise to "cryptocurrencies" — the best known being typically Bitcoin. The idea of Nakamoto (2008) was to provide a system where agents could conduct payments without the need for trust in other parties. The (still) unknown founder(s) of Bitcoin enable this by the creation of the "blockchain" which is ultimately an implementation of the distributed ledger technology. By the combination of cryptographic methods and concepts which have been known in computer science for years (Narayanan and Clark 2017), Nakamoto (2008) has solved the problem of double spending without the need for a trusted third party. With this technology, it would no longer be a necessary condition to trust in an institution which would have the ultimate power to destroy the system. Indeed, this motive also becomes clear from Bitcoin's "Genesis Block" which includes the text *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*, possibly showing Nakamoto's aversion against traditional central intermediaries. Moreover, this aversion against central intermediaries might have motivated Bitcoin's reliance on a maximum number of coins — thereby offering a protection against inflationary tendencies which, historically, have set an end to so many currencies.

Hundreds of alternatives, so called "altcoins", have joined Bitcoin which still remains to be the most important one in terms of market value, market capitalization, daily transactions and business acceptance (Sapuric et al. 2017). Table 1 shows some estimates of the number of cryptocurrencies being present. Tarasiewicz and Newman (2015) find that by August 2014 more than 1,500 concepts based on Bitcoin have been discussed, and on GitHub more than 4,000 Bitcoin forks existed. Currently, there are more than 14,000 forks of the Bitcoin source code on this platform. Even if GitHub is not the only platform in charge for the launch of a new cryptocurrency, it has been an important player in the early stage development. In that sense, the GitHub figure might be understood as some upper limit as not every fork will result in a new proposal of a cryptocurrency. When it comes to exchange markets, `Coinmarketcap.com` now lists more than 900 cryptocurrencies whereas about 440 of them have a market capitalization of more than one million US-dollars. However, market volumes reveal that the cryptocurrencies — even in total — only have little impact on the economies so far. In comparison to narrow money measures, the ecosphere of cryptocurrencies accounts for only some per mill of the "traditional" money. Moreover, a large number of cryptocurrencies has market values which are pretty small, so that the number of cryptocurrencies to be taken seriously is reasonably smaller. These numbers clearly reveal that there must be a huge amount of cryptocurrencies which did not succeed on the market. This includes a number of scam-coins intended to only benefit their creators (Tarasiewicz and Newman 2015). The Description of a Cryptocurrency (DOACC) dataset was built around cryptocurrency announcement postings on the bitcointalk forum, the traditional way of announcing of a new cryptocurrency in the early stages of the

Table 1: Estimates about the size of the cryptocurrency ecosystem (as of January 11, 2018)

Source	Estimated size
Coinmarketcap.com	903
Tarasiewicz and Newman (2015) (Bitcointalk, 8/2014)	>1,500
DOACC	2,896
Tarasiewicz and Newman (2015) (GitHub, 8/2014)	4,096
Cryptocoincharts.info	4,552
GitHub	14,528

ecosphere (Tarasiewicz and Newman 2015). With its coverage being between the exchange platform figure and the number of GitHub forks, it plausibly reflects the number of cryptocurrency proposals of the early stage development. However, it should be noted that the DOACC number might overestimate the true number of cryptocurrencies being in circulation by the end of 2016 as some concepts have not reached the market or already dropped out of it.

In this paper, I present some descriptives on how the cryptocurrencies developed, what was common in the past, and what is common more recently. To do this, I use the DOACC dataset which covers 2,896 different cryptocurrency announcements up to September 2016. I track the development of consensus-schemes and hash-algorithms, of confirmation times and premining shares. On top of that, the paper provides brief explanations of the underlying technical concepts. Further, it shows the hurdles which occurred in the past and how new cryptocurrencies proposals take existing weaknesses into account.

The paper proceeds as follows. Section 2 gives an overview on the historical background of the cryptocurrencies, develops a definition of what can be understood as a cryptocurrency and further, it outlines hurdles for the future development. Section 3 analyzes the cryptocurrency ecosphere using the DOACC dataset. It provides descriptives on the development regarding the number of announcements, consensus schemes, cryptographic algorithms, block and confirmation times and premining. Additionally, section 3 investigates to what extent newer cryptocurrency proposal take weaknesses of their predecessors into account and what cryptocurrencies might need to take into account be successful in the future. Section 4 concludes the paper.

2 The Development of Cryptocurrencies

2.1 The Road to Bitcoin

Double-spending might be seen as the digital counterpart of counterfeit notes and coins, e.g. enabling attackers to spend monetary values more than once. Preventing double-spending requires either trust into the trading partner being honest or an intermediary party ensuring that digital tokens are only spent once. However, relying

on such an intermediary will require trust into this party as it is concerned with the processing of the payment. In small societies, determining whether someone is trustworthy is relatively easy. With the development of the internet, though, even knowing about the real identity of a counterpart becomes particularly difficult. Online shopping requires the conduction of payments, but handing over confidential payment details to an unknown party – in the early era of the internet typically via unsecured connections – is dangereous (Narayanan et al. 2016). The risk of fraudulent use of the transmitted data led to the upcoming of intermediaries such as PayPal. Such companies act as trusted party when it comes to payments as they store the necessary information for the complement of the payment. By relying on such an intermediary, the buyer did not need to share credit card information with the seller, and the seller could ask for a payment without having to frighten the customer. Moreover, such parties ensured that double-spending of electronic monetary values became impossible. However, this is done on the cost of reliance on a central intermediary. Hence, the problem which Nakamoto (2008) solved is at least as old as the internet for private users.

The Bitcoin proposal combined different approaches which reach back at least to the end of the 1980s. One might see the work of Nakamoto (2008) not as presenting new technologies, but rather as a way of combination of already existing technologies, e.g. by using the concepts of linked timestamping, Merkle trees, public keys as identities and proof-of-work which all have been created years before the Bitcoin proposal (for a detailed overview see, e.g., Narayanan and Clark 2017). One of the first predecessors was DigiCash which was founded in 1989 (Narayanan et al. 2016). The idea goes back to Chaum (1992). The aim of DigiCash is simply privacy: from linking data, anyone with access to the respective data can learn a lot about any specific person. Which might be good on the one hand, e.g. regarding the determination of credit default risks, might be highly problematic when information gets into the wrong hands (Chaum 1992). DigiCash provides a solution to that, namely by generating electronic notes which cannot be linked together. However, accepting such notes requires a central intermediary to prevent double spending. Even if the idea of DigiCash is now nearly three decades old, it is still an ongoing problem. A customer might be more willing to hand-over credit card details to a trusted party than to an online shop for privacy or fraud concerns, thus making the customer effectively using a third-party service such as PayPal.

Hashcash which was proposed by Back (1997) was originally thought as a protection against spam. The idea is straightforward, as it requires computational effort to be allowed to execute a specific task. Sending e-mails is a cheap task, and sending thousands of it is cheap as well. However, with the proposal of Back (1997), sending e-mails would require to solve a computationally hard puzzle, effectively putting some cost on each sent e-mail. As long as these costs are small, the typical e-mail user would not be affected much, but sending spam would become unreasonably expensive. Bitcoin borrowed this idea of a proof-of-work for its concept.

Two monetary predecessors of Bitcoin are "b-money", proposed by Dai (1998), and "Bit Gold", proposed by Szabo (2005). For the latter, there seems to be evidence that Szabo had the idea already in 1998 – or about 10 years before the invention of Bitcoin (Narayanan et al. 2016). B-money directly proposes a system where every

participant keeps a copy of the record (the distributed ledger in Bitcoin). However, Dai (1998) argues that this proposal is impractical and then offers a solution where only some participants keep the ledger. Bit Gold argues that traditional money crucially depends on a trusted third party which might not be optimal as there is the potential to destroy the currency by inflationary pressures (Szabo 2005). Therefore, Szabo (2005) proposes a system which relies on a proof-of-work mechanism to reduce trust to a minimal level by setting up decentralized chains.

However, Bitcoin is different for some reasons from b-money and Bit Gold. First, newly created Bitcoin tokens are a way of compensation for the provision of additional security of the blockchain. This is also clear form the decreasing amount of newly created Bitcoins, effectively replacing the incentive provided by the mining reward by voluntarily added transaction fees. Moreover, it is not the puzzle solutions constituting the tokens, but rather the mining puzzle is a way to secure the ledger (Narayanan and Clark 2017). Second, both b-money and Bit Gold rely on a time stamping service which requires at least some trust. Szabo (2005) argues that this is one of the crucial points in his design. However, Bitcoin relies on an agreed order of transactions, and this order is created by a decentralized consensus process. It would require large computational power to change the timely order of transactions. Additionally, as not only blocks on the blockchain are interlinked, but also transactions, changing the timely order of the ledger is comparatively hard. Third, under the two cited predecessors, the mechanism of determining the valid ledger is less clear than for Bitcoin. With Bitcoin, the longest chain prevails, and miners typically choose the longest chain as the starting point for mining. Even if two solutions of the puzzle are found separately, effectively generating a fork of the blockchain and dividing the miners into two groups, in the next round it is likely that one group of miners will find a solution faster than the other group. This will lead to a then longer blockchain to which all miners from the other group will change to (Nakamoto 2008).

The historical outline reveals that Bitcoin has borrowed from a number of different resources, and has technically improved some of the above named proposals. Bitcoin combines the distributed ledger of b-money with computationally hard puzzles from Hashcash with electronically issued notes from DigiCash, in a decentralized way as proposed by Bit Gold. This combination created an electronic payment system which functions on a peer-to-peer basis. Of course, other technical developments had an impact on the development of Bitcoin as well, e.g. the development of the Merkle root concept around 1991 which is used by the Bitcoin protocol (Narayanan et al. 2016). However, none of the above cited proposals has brought it to such a large recognition as Bitcoin did.

The basic structure of a blockchain-based cryptocurrency like Bitcoin is as follows (Nakamoto 2008): network participants keep a version of the distributed ledger which is organized in blocks. Each block consists of different transactions referring to past transactions. These blocks are interlinked by a hash signature, thereby generating a timely order of transactions and blocks which is the so-called blockchain. Consensus needs to be found to add a block on to the existing blockchain. There are different designs of that consensus algorithm, e.g. proof-of-work or proof-of-stake to name the most important ones. The main idea behind that consensus algorithm is

to make it reasonably costly to add blocks to the blockchain. Any transaction needs to be included into a block to be considered as recorded on the blockchain.

By relying on cryptography, payers and payees can conduct payments even in low-trust environments. Indeed, Wüst and Gervais (2017) show that blockchain-based technologies are especially useful when users are unknown or not trustworthy. However, this does not mean that trust is completely phased out of the system, rather it is a change in the institution the trust needs to be put in. Before Bitcoin, trust has either been in the other party, or in the central intermediary. With Bitcoin, this trust is not longer necessary, but it is replaced by trust in the Bitcoin protocol itself, i.e. in its cryptographic properties (Blocher et al. 2017). As Bitcoin can replace trust into the other party or the financial intermediary by trust into a cryptographic protocol, it becomes a candidate for payments in low trust environments, e.g. with online black markets[1]. One example for such a black market was Silk Road trading drugs, weapons, pornography and narcotics – everything paid for with Bitcoins (Christin 2013). In such markets, neither sellers nor buyers are typically willing to handle over information making them identifiable, and consequently, trust is low. Hence, the situation is comparable to the beginning of the internet with nobody wanting to handle over credit card information, and Bitcoin fitted into that niche. As a blockchain-based technology is useful when agents are unknown or when trust is low (Wüst and Gervais 2017), one would expect Bitcoin (and other cryptocurrencies as well) to be comparatively present in such black markets. The literature suggests that this indeed played a role: Christin (2013) shows that up to 9% of the trading volume at Bitcoin exchanges was caused by a single platform only, namely Silk Road. The estimates of Janze (2017) point into a similar direction, suggesting that darknet markets evolved alongside the development of cryptocurrencies, especially Bitcoin.

2.2 Definition

With Bitcoin, the development of electronic means of payment has shown a new perspective: it is now possible to think about financial processes without the need for a traditional, trusted intermediary, e.g. a bank or an online payment service. Several thousand cryptocurrencies have joined the ecosphere around Bitcoin. However, giving a clear definition of what constitutes a cryptocurrency is difficult. The literature has brought out some definitions of a cryptocurrency. An overview of possible definitions is given by Baur et al. (2015), identifying four key features of a cryptocurrency:

- Absence of external regulatory barriers
- Establishment of peer-to-peer functions
- Usage of public internet infrastructures and

[1]Of course, the technology of "blockchain" is not only usable for illegal activities, there are plenty of legal uses, also outside of the emission of digital currencies, e.g. the provision of public registers. One example is the United Nations' World Food Programme which set up a blockchain based program in Jordan to fight hunger. Such programs are typically in place where infrastructure is missing, and hence, trust among participants is to be expected low.

- Implementation of private-public-key cryptography for secure transactions

First – and most obvious – cryptocurrencies are computer programs which, as a currency, issue own monetary units. However, these units do not have a direct physical counterpart (e.g. coins or banknotes), nor do they have an underlying asset (Kristoufek 2013). This does not mean that cryptocurrencies cannot appear physically[2], but it means that they are designed electronically and coins or banknotes are just derivatives for convenience of them. Moreover, these tokens derive their value from the community being willing to accept and to exchange it for goods or other forms of value. In that sense, they are comparable to fiat money.

Second, cryptocurrencies are typically independent of governmental activities. Thereby, they belong to the group of alternative currencies in the sense of Hileman (2014) as mining is not ruled by a government but by the protocol, and cryptocurrencies do not necessarily serve as official or de facto tender. However, one could think of a governmental-issued digital currency like the e-krona for Sweden (Sveriges Riksbank 2017), but traditional monetary institutions like central banks or the IMF do not regard this as being part of the cryptocurrency movement (European Central Bank 2012; He et al. 2016)

Third, cryptocurrencies aim at improving the economic activities between at least two individuals by imitating money functions even if cryptocurrencies cannot be fully recognized as money (Yermack 2015), at least not for larger groups. However, for smaller groups or communities, cryptocurrencies might fulfill these functions, and might be considered to act as money for these communities (Ali et al. 2014).

Fourth, transferability of tokens typically uses internet infrastructures, but not a trusted third party (Ametrano 2016). This allows a large group of individuals to access that technology. Basically, this feature is one of the reasons why cryptocurrencies are attributed to potentially give the un- and underbanked people access to financial services (Mas and Lee 2015).

Fifth, cryptography is a central concept in the construction of a cryptocurrency, in order to create and manage the ledger (Ahamad et al. 2013; Gandal and Hałaburda 2014). One might interfere that cryptography is also present when it comes to traditional banking services, e.g. online-banking. However, it plays a different role in both systems. In traditional banking systems, cryptographic functions are implemented to ensure the privacy of the system, i.e. to keep outsiders out of it. Therefore, cryptography works at the entry points in traditional banking services. This is different for cryptocurrencies where cryptographic functions are at the heart of the system. Cryptocurrencies are built around a specific (set of) cryptographic function(s), also protecting the system from insiders. Even though Bitcoin as the leading cryptocurrency is based on blockchain technology, organizing a ledger in this respect is not a necessary condition. For example, "iota" uses an algorithm called "tangle", and thereby constitutes a cryptocurrency without a blockchain (Popov 2017).

Taking all the stated factors into account condenses in the following definition:

[2]One example for a physical representation of Bitcoin are Casascius coins. On these coins, a QR-code sticker can be affixed. This sticker contains the public key or the Bitcoin address on its visible side, and the private key for the use of the Bitcoin on its invisible side.

Cryptocurrency: A cryptocurrency is a computer readable program protocol built around a single (or a set of specific) cryptographic function(s). It issues electronic tokens denominated in their own unit of account according to the rules set out in the protocol. Cryptocurrency tokens are intrinsically worthless, but intended to represent values within a specific community. They are issued as electronic economic instruments with monetary features enabling users to transfer these tokens fast and securely without the need for any further intermediary than the protocol itself.

Besides this technical definition, cryptocurrencies attract specific communities and can thereby show specific social and economic processes. In particular, around a specific cryptocurrency, an ecosystem can evolve, e.g. of specialized hardware suppliers and merchants accepting units of that specific cryptocurrency. Hence, cryptocurrencies are typically surrounded by a community.

Digital currencies can be either open or closed, i.e. usable or unusable outside a virtual world (Hileman 2014). This outlines the importance of a community being willing to accept a cryptocurrency for real-world activities.

Digital currencies can be either centralized or decentralized (Hileman 2014). Bitcoin is a decentralized cryptocurrency However, it is possible to think of a cryptocurrency which has a central instance. This might be useful for at least two things: First, the central instance might be able to promote the adoption process of the cryptocurrency, e.g., it could use not distributed tokens from the premining amount to pay for the necessary infrastructure. Second, the central instance might have an advantage in performing innovation processes. That is, as the adoption of a new proposal is not subject to a long-lasting voting process, but rather to nearly immediate changes, it might enable a centralized cryptocurrency to perform policy tasks and hence, to adapt to economic conditions. However, cryptocurrencies are typically decentralized (Ametrano 2016; Ahamad et al. 2013). In contrast, central bank digital currencies will typically be centralized systems, and hence, as perceived by European Central Bank (2012) and He et al. (2016), should be considered as some different subgroup of digital currencies.

While altcoins use the same building blocks as Bitcoin to implement a currency, altchains use some principles of the cryptocurrencies to create non-currency use-cases (Antonopoulos 2014). One prominent example for this might be the creation of smart contracts, e.g. with Ethereum as being one example[3]. A cryptocurrency does not always need its own blockchain, instead, it could function upon existing infrastructures. These "Meta-Coins" (also called meta-chains or blockchain-apps) run on top of an existing blockchain (Antonopoulos 2014). Still, this falls under the definition of a cryptocurrency, as it does not require setting up any own infrastructure. Using the existing infrastructure might also increase compatibility, thereby possibly accelerating the adoption. As these meta-coins can add features to a current blockchain, they might also be seen as a way of innovating an existing

[3]In technical terms, Ethereum both provides a platform for the creation and execution of smart contracts, but it also issues tokens named "Ether" which it also uses to pay for the execution of smart contracts created for the Ethereum protocol. In this sense, the creation of a currency is not the primary purpose of Ethereum. Other example of altchains are Namecoin and NXT (Antonopoulos 2014).

cryptocurrency without the need for a hard fork.

Monetary authorities might find it useful to issue their own digital currency (Michaelis 2017). In fact, some central banks have started to investigate the potential of a digital currency (Sveriges Riksbank 2017; Fung and Hałaburda 2016; Barrdear and Kumhof 2016). Historically, there are examples of privately emitted monies (typically with a central issuer), but the rule is a state-issued form of money. This is purely different for cryptocurrencies as they are by now only privately issued. A central bank emitted and managed digital currency is in contrast to cryptocurrencies not independent of governmental actions. The supply of money will be steered by a central instance, i.e. the central bank, enabling the conduct of monetary policy. Furthermore, a central bank digital currency is a claim, namely against the central bank. Therefore, it is nothing different from a banknote which is also a claim on the central bank's balance sheet – with the only difference that a digital currency would not need to exist in physical terms. Besides, central bank governed digital currencies have a physical counterpart in the narrow sense, namely the traditional banknotes and coins and central bank digital currencies might be seen as a derivative of these. Even if the exchange rate is not at parity, the digital money will be a supplementary or a successor of the physical money. Thus, a digital currency emitted by any central bank is fundamentally different from the privately created cryptocurrencies such as Bitcoin — both historically and technically. However, one might discuss whether such a digital US-dollar or Euro is really a cryptocurrency, even if it is built around a specific cryptographic algorithm or on blockchain technology. This is also in line with the definition of the European Central Bank (2012) who claim virtual currencies to be *"unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community"*. Even though virtual currencies cover more digital currencies than just cryptocurrencies, it shows that the ECB's notion of a central bank issued digital currency would possibly not fall under the cryptocurrency definition. A similar perception for the IMF can be found in He et al. (2016). Hence, as implied by the arguments above and the findings of Baur et al. (2015), one might use the term "cryptocurrency" for the non-governmental digital currencies only, and use "central bank digital currency" for the governmental counterpart, even though a central bank-controlled digital currency based on cryptography and directly enabling peer-to-peer transactions would fall under the above stated definition of a cryptocurrency.

2.3 Some Hurdles for the Future Development of Cryptocurrencies

Given the high number of cryptocurrencies, the question of whether cryptocurrencies will succeed naturally arises. It is clear that not all of the cryptocurrencies currently circulating around will have a bright future. Many of them will not be able to gain large adoption and will then drop out of the market. In some sense, this might be viewed as the adoption of the idea of Hayek (1978) as competition will select the winning currency.

However, some might be able to succeed, not necessarily at large, but at least

in their specific niches. There are – at least – economic, technical and regulatory hurdles which might prevent a cryptocurrency from gaining success of which some might be easier to overcome than others. One single cryptocurrency might not be able to overcome these barriers alone, rather they show up as working candidates or proof-of-concepts on which further development can be built upon. Some development ideas might condense into a new cryptocurrency or a meta-coin. Having this in mind, one might be able to explain the large number of cryptocurrencies.

Economic hurdles

First, there are economic barriers. As with Bitcoin, cryptocurrencies might face high exchange rate volatilities. This is problematic as price denominations need to be adjusted frequently (Yermack 2015). Even more, including some proportion of Bitcoin might improve the risk-return-tradeoff in a portfolio (Brière et al. 2015), thereby driving down the incentive to use it aside from investment purposes (Blocher et al. 2017). Consequently, the real world usage is relatively low as everyone tends to hold the tokens rather than using it for the exchange of goods and services. The high volatility of the exchange rate may be a problem of the early stages. Indeed, the study of Cermak (2017) suggests that the volatility of Bitcoin could decrease to traditional fiat currencies values by 2020.

Another economic problem is the construction with upper caps on total token issuance. With more widespread adoption, a limited supply implies increasing valuations, thereby causing agents to hold cryptocurrency tokens instead of trading them on markets. Put differently, there might only be few tokens offered on a given exchange for any given price, thereby causing a "thin market" for which small changes in supply or demand of cryptocurrency tokens can lead to considerable price impacts (Hanl and Michaelis 2017). However, as Dimpfl (2017) shows, there are more and less liquid exchanges trading Bitcoin, so that the concern of a less liquid market might not hold for every exchange. Anyway, this empirical finding might change in the future. The DOACC dataset has total coin values for 2,504 observed cryptocurrency announcements. The majority (97.3%) of cryptocurrency proposals relies on a specific limit on token issuance. Peercoin provides an example for a cryptocurrency which does not rely on an overall cap. Instead, it relies on an algorithm giving rise to low rate of inflation (King and Nadal 2012). Thus, there are ways to overcome the fixed limit of cryptocurrency token issuance, but specifying growth rates or adapting the upper limit can be problematic, in particular because of the decentralized nature of cryptocurrencies.

Especially around Bitcoin, a discussion on the future of transaction fees has developed (see, e.g., Houy 2014). In particular under investigation is whether the low transaction fees of the early days of Bitcoin can persist in the future. This question will gain further importance as the mining reward diminishes eventually to zero, replacing the miner's incentive to secure the network by transaction fees. Hence, there will be a connection between security and the amount of fees provided (Houy 2014), and both factors can drive down the success of Bitcoin or any other cryptocurrency. The cryptocurrency "iota" aims to fix the transaction fee issue being present in the Bitcoin implementation. The main idea of "iota" is that each transaction confirms two previous transactions (Popov 2017). Thereby, the network is not split into

transactions issuers and transactions approvers (i.e. miners), but rather users hold up the network and the ledger as they use it. As there is, consequently, no need to pay miners for the approval of transactions, transaction fees become obsolete.

Currencies, and thereby cryptocurrencies as well, are typical examples of network goods. Thus, it is not sufficient for any cryptocurrency to implement an improvement over current financial intermediation systems to gain large adoption as a means of payment, but rather that there needs to be a large enough mass of users being willing to switch. Governmental support, the provision of infrastructure, the adoption by a large user, e.g. a merchant, or monetary instability would help cryptocurrencies succeed (Luther 2015; Blocher et al. 2017), but it will be hard to overcome the existing network effects for cryptocurrencies without some promoting help from outside, in particular as payment behaviors seem to be relatively stable over time. Even though cryptocurrencies might not succeed as a broadly used medium of exchange, they might be useful for specific niches.

Decentralization among the users of a specific cryptocurrency might cause additional problems. It is easily questionable whether a cryptocurrency can adjust fast enough to economic and technical conditions, e.g. security vulnerabilities. This is a two-sided discussion for at least two aspects. First, slow adoption might prevent bad ideas from being implemented. One might argue that this was indeed the intention to provide the public with an instrument to protect against central instances abusing their instruments and power. However, when there is the objective need to adjust the details of the cryptocurrency, then slow adjustments might be problematic. Hence, the features governing the implementation of new features might protect the cryptocurrency against errors and therefore provides resistance, while it prevents, on the other hand, the cryptocurrency from being as innovative as it could be. Second, the improvement proposal needs to be hardcoded by developers and installed by the miners. This gives miners the possibility to "vote" on their desired improvements. Miners' preferences are not necessarily overlapping with the preferences of the users, and it might become even more problematic with the formation of large mining pools. This might incentivize users to switch to another cryptocurrency, thereby harming the cryptocurrency they came from.[4]

Technical hurdles

Technical barriers form the second category of reasons which might prevent a large success of cryptocurrencies. There is an ongoing debate on the energy consumption of cryptocurrencies (Böhme et al. 2015; Bhaskar and Lee 2015). Especially for Bitcoin, mining inefficiency seems to be prominent, with energy consumption estimates equal to the power consumption of Ireland (O'Dwyer and Malone 2014). In this respect, the development of cryptocurrencies such as Primecoin or GridCoin might be considered as improvements as they aim at generating intrinsically useful proofs (Halford 2014; King 2017). Moreover, some have questioned the pseudonymity provided by Bitcoin (Meiklejohn et al. 2013; Biryukov et al. 2014), arguably giving rise to concerns that users are not that anonymous as one would expect it. If anonymity

[4]Besides, also miners might not have the same preferences. One example is the ongoing discussion about "Lightning" and "SegWit" for Bitcoin.

is one of the reasons for using cryptocurrencies, then weaknesses in the provision might harm the adoption on a larger scale. Cryptocurrencies such as "ZCash" might be seen as improvements for the stake of anonymity (Hopwood et al. 2017). Further, there are considerations about the security of cryptocurrencies, both from a conceptual point of view (Giechaskiel et al. 2016), and from a practical point of view (Karame et al. 2012; Courtois et al. 2014; Courtois et al. 2016; Apostolaki et al. 2017). Besides all that, critics have questioned whether the Bitcoin blockchain can upscale enough to handle the requested amount of transactions. This is also mirrored in the discussion of "Lightning" and "SegWit". The question underlying the discussion is at least twofold, namely, first, the increase of the blocksize for each of the Bitcoin blocks and, second, whether the structure of the block should be altered in that sense that signatures are separated. Different views on how this should be handled have then led to the forking of the Bitcoin blockchain, thereby splitting Bitcoin into Bitcoin and Bitcoin Cash in August 2017. Moreover, only a few months later, Bitcoin Gold became a spin-off of Bitcoin by changing the proof-of-work algorithm to Equihash which is not efficiently computable on "Application Specific Integrated Circuits" (ASICs). Surprisingly, these forks have led to an increase of Bitcoin's valuation, and both Bitcoin Gold and Bitcoin Cash carry positive valuations on cryptocurrency exchanges. Hence, one might conclude that open issues like the Bitcoin related scalability debate have a monetary equivalent, and solving these issues consequently drives up market valuations, or in other words, users' willingness to invest.

Regulatory hurdles

The last group of barriers are regulations being enforced by governmental authorities. As Rogoff (2017) argues, regulating instances could easily use their toolkit to bring some cryptocurrencies in advantage or in disadvantage. However, due to its typically decentralized structure, it might be practically difficult to impose a ban on the usage of any specific cryptocurrency (Hałaburda and Sarvary 2015), although any regulatory authority can increase the hurdles to reach the entry points, e.g. by banning exchanges, cryptocurrency ATMs or by a ban on merchant's cryptocurrency acceptance. Thereby, the regulator can drive down the utility of a cryptocurrency regarding it features as a means of exchange. One example for this is Germany's Federal Financial Supervisory Authority which prohibits cryptocurrency ATMs as operating such a device would constitute financial commissions business subject to regulatory approval. This notion makes it unreasonably costly to run an official cryptocurrency ATM, effectively ruling out such devices and consequently, increases the hurdle to acquire cryptocurrency tokens. Typically, such kind of actions will favour some state-run (digital) currency, and it might rule out its private counterpart. Put differently, there is no reason why a central bank should – without any struggle – let a private counterpart money gain large success. In comparison to the economic and technical barriers, this might be one of the hardest constraints to overcome as regulatory authorities can use their tools to prevent any cryptocurrency from being successful (Rogoff 2017). Consequently, a cryptocurrency cannot gain success with at least passive support of the regulatory instances, that is, without the regulatory authority letting the digital counterpart money pass the respective

threshold. However, for the adoption of a cryptocurrency active support would be helpful, but one might suspect that governmental agencies would only support some state-run digital currency.

3 Analysis of the Cryptocurrency Ecosphere

3.1 Data and Evaluation Strategy

The analysis in this paper is based on the DOACC dataset, which uses Open Web Ontology Techniques to offer meta data about cryptocurrencies. The data were sampled by Graham Higgins who manually recorded it from March 2014 to September 2016 by following the announcements on bitcointalk forums. As Higgins himself claims to have missed only few cryptocurrencies during the collection period, the DOACC dataset can give valuable insights in the first years of cryptocurrency formation. However, as some cryptocurrencies are only transient phenomena, the DOACC covers some dead ends. Anyway, these announcements, though, have also formed the cryptocurrency ecosystem as well and are part of the history of cryptocurrency development. Data from before March 2014 was added by Higgins by methodically cross-referencing information from the web. The DOACC dataset creator stopped recording data for cryptocurrency announcements in 2016 as the launch of a cryptocurrency changed from verifiable GitHub repositories to more broadly specified and described Initial Coin Offerings with less detailed technical information.

The dataset covers a time frame from the foundation of Bitcoin until September 2016[5]. In general, the dataset covers up to 19 variables for each cryptocurrency, but only five of them are covered for each observed announcement[6]:

To validate the plausibility of the DOACC dataset, I compared the data with Farell (2015) and Tarasiewicz and Newman (2015). The results are shown in Table 5. It reveals, that in most cases the data provided by the DOACC seems to be correct. However, some differences occur. This includes minor differences in the announcement date, but also major differences like the consensus scheme or the hashing algorithm. This is not only applicable to the comparison with the DOACC dataset, but also differences between Farell (2015) and Tarasiewicz and Newman (2015) exist. This points to the problem of different data origins. Particularly, Farell (2015) uses the cryptocurrency's website when a whitepaper is unavailable, naturally implying differences as a cryptocurrency's website is likely to include recent changes, while an announcement on GitHub, on bitcointalk or a whitepaper might not. Besides that, the validity check reveals that name duplicates might be a problem, especially as they can have different technical specifications. This is the case for "Cryptonotecoin", "Mastercoin" and "Paycoin". This points out a problem of decentralization, namely that no central instance can ensure that duplicates are created, including creation on bad purposes such as fraud. To sum up, the DOACC dataset seems to be plausible. Anyway, one has to pay attention that technical details recorded in a whitepaper or on a cryptocurrency's website might have changed

[5]The dataset is made available at `https://github.com/DOACC/individuals` under the Open Database License (ODbL).

[6]Further explanation can be found at `https://minkiz.co/data`.

since its announcement. Nonetheless, the DOACC dataset provides a unique possibility to gain insights into the early stages of cryptocurrency development, especially for the time announcements were typically placed in bitcointalk forum (Tarasiewicz and Newman 2015).

The time covered by the DOACC dataset can be seen as a shortcoming as it does not cover the most recent past. However, as the launch process changed from forking a GitHub repository to a more Initial Coin Offering based approach, the most recent past differs from the early stage of cryptocurrency development. Moreover, it is the largest freely available compilation of meta data of cryptocurrencies which I am aware of. Further, the dataset covers most of the relevant cryptocurrencies traded on exchanges at the time being. The DOACC dataset covers 2,896 entries with observations reflecting cryptocurrency announcements on `bitcointalk.org`. Even though it does not cover the most recent past, it should be sufficient to gain reasonable insights into the early stages of cryptocurrency evolution.

However, there are some additional shortcomings which should be kept in mind during the analysis of the DOACC dataset. First, only five variables are recorded for the whole dataset. This necessarily means that any observation can miss a maximum number of 14 variables. This might be less problematic for the location of the source code or the coin's website but it might introduce some bias in the analysis, e.g. for the amount of premining. Second, there is no uniform classification of values. In particular, this is true for the amount of premining, which for some cases is given as an absolute number of cryptocurrency tokens, and sometimes is given as a percentage share. However, as well as for the missing values, this shortcoming is due to the data sampling strategy. As it is based on the announcement made on the bitcointalk forum, it is subject to the cryptocurrency creator's choice of presentation. Equalizing the form of presentation is manual datawork, and, hence, might be subject to errors. Third, the dataset is only a snapshot of the time a specific cryptocurrency was announced. Additionally, the dataset does not cover any indicator whether a cryptocurrency has changed since its announcement. The longer the observation has been in the DOACC dataset, the more likely it gets that changes have occurred to this cryptocurrency. Thus, the DOACC dataset can only serve as a first approximation on the technical details of a specific cryptocurrency, and whenever the technical details are of interest, the cryptocurrency's technical information needs to be assessed directly. Fourth, the DOACC dataset does not incorporate the economic importance of a single cryptocurrency. Instead, the following analysis gives the same weight to all observations, thereby neglecting the differences in influence the different cryptocurrencies might have. Arguably, this might overestimate the impact of economically not relevant cryptocurrencies and underestimate the impact of the economically most relevant ones. Thus, the larger cryptocurrencies, such as Bitcoin, might have a much stronger impact on the cryptocurrency ecosystem than small proof-of-concept cryptocurrencies. However, it is nonetheless important to have a widespread view on the ecosphere as it allows to explore the whole bandwidth of cryptocurrencies.

Table 2: Number of newly announced cryptocurrencies by year

Cryptocurrency announcements	
2009	1
2010	0
2011	12
2012	10
2013	269
2014	1739
2015	694
2016	171

3.2 Overview of Development

Since the introduction of Bitcoin by Nakamoto (2008), the number of cryptocurrencies available has largely increased, according to the DOACC dataset to nearly 2,900 different cryptocurrencies. The first cryptocurrency covered by the dataset is Bitcoin, and the last one is ZCash which was founded in September 2016. Table 2 provides an announcements by years[7]. First, it can be seen that in the beginning years, e.g. the first years after the introduction of Bitcoin, the overall number of newly founded cryptocurrencies is low. Thus, until 2013, cryptocurrencies are virtually negligible. However, in 2013 the number increased to 269 and reached its peak in 2014 with more than 1,700 newly announced cryptocurrencies. Then, the number of newly founded cryptocurrencies started to decrease, which might be a result of research and development focusing more on existing concepts rather than creating new ones, and it might also reflect the early stages of shifting to a more ICO-based announcement procedure. As the dataset does not fully cover 2016, one should be cautious in interpreting the number for this year.

The development of cryptocurrencies might be related to the price development of Bitcoin. The first price on `Coindesk.com`'s price index is dated to July 26, 2010. The study of Kristoufek (2013) suggests that there is a relationship between the price and the interest into a cryptocurrency, thereby generating both positive and negative feedback effects. The interest generated by the price dynamics of Bitcoin might not only be limited to Bitcoin but it might also transfer to the whole cryptocurrency ecosphere. Hence, this would lead to the conclusion that higher prices and media attention on Bitcoin should also lead to higher numbers of newly created cryptocurrencies, at least for the first years. That this might be true can be seen from the number provided in Table 2. Kristoufek (2015) argues that Bitcoin gained even more attention when it reached the 1,000 dollar mark in late November and December 2013. One might presume that the current price increase to levels up to 19,000 US-dollars might be caused by feedback effects, eventually causing a bubble on the cryptocurrency market, and that media attention might have played a significant role for private investors. Moreover, real world developments like the

[7]However, one should notice that there were no announcements in 2010. Hence, this year will not show up in the subsequent analysis.

legalisation of Bitcoin in Japan (Sapuric et al. 2017) and the formation of the Bitcoin derivatives might have lowered the hurdle to invest into cryptocurrencies.

However, founding a cryptocurrency does not necessarily require being a tech-expert. There have been online tools around which adapt the code to the creator's preferences. Moreover, copying the source code of an existing project is pretty simple, and naming the new cryptocurrency can then result in the creation of a new one. The DOACC dataset provides the opportunity to search for duplicates. To identify possible duplicates of Bitcoin, I used four variables to describe the protocol:

- The total number of tokens is 21,000,000.
- The blocktime is 600 seconds.
- The cryptocurrency is secured by a proof-of-work consensus scheme.
- The underlying cryptographic algorithm is SHA-2-256.

Generating a subset of the DOACC dataset with the description generates between 10 and 65 cases, depending of whether missing values are excluded or not. These cryptocurrencies are likely to be similar or nearly similar to Bitcoin. However, there might be differences as the description only focussed on four of the 19 variables, thereby neglecting some features which might distinguish these cryptocurrencies from Bitcoin.

From the twelve cryptocurrencies founded in 2011, ten use a proof-of-work scheme while only two use a proof-of-stake mechanism. Additionally, eight use the same hashing algorithm as Bitcoin whereas the other four use Scrypt, with Litecoin being one of the first Scrypt-adopters. These numbers reveal that there is only low variety given the possible extent the technology would be able to use. Regarding the retarget time — which is to be understood as time until the mining difficulty adjusts to network conditions — this is identical to Bitcoin for all observations the DOACC dataset has non-missing values in 2011. Evaluating the total number of cryptocurrency tokens for the six cryptocurrencies covered by the DOACC dataset reveals that four out of these six are similar to Bitcoin, Litecoin offers a four-time-multiple of Bitcoin total coin amount while only Freicoin offers much more coin tokens in total. Again for this, the similarity is obvious.

3.3 Consensus Schemes

Distributing a blockchain-based ledger among network participants requires coordination to determine what the valid ledger is, especially with respect to different possible proposals. In that sense, a cryptocurrency community has to find a way to prevent double spending, i.e. spending a specific token twice. However, as cryptocurrencies are typically decentralized and hence do not have any central authority, there is the need for a scheme which determines the right ledger and protects the system against changes from the outside, and the main concept is to make additions to any blockchain reasonably costly.

There are different consensus schemes in place. For example, Bitcoin uses a "proof-of-work"-scheme, while other cryptocurrencies rely on "proof-of-stake" or

other schemes. I will briefly outline how these schemes work before analyzing the development of consensus schemes in the cryptocurrency ecosphere.

Proof of Work (PoW) was first introduced to the field of cryptocurrencies with Bitcoin in 2009. As shown in Table 3 it is the protection scheme with the highest usage among cryptocurrencies. The idea behind a proof-of-work scheme is straightforward: In order to be allowed to add a block to the blockchain, the creator of the block has to put some effort, i.e. computational work, into it. This proof needs to be hard to generate, but easy to proof (Bhaskar and Lee 2015). In Bitcoin, this is done via the implementation of a SHA-2-256 algorithm which is required to generate a hash value below a specified target (Nakamoto 2008). As the calculation of a hash is not reversible, miners need to try different combinations to reach the target value. As this is a brute-force process, it requires a lot of work to find a valid solution. However, verifying the solution should be easy, i.e. enabling other networkers to check quickly whether the miner has done right. This is covered by the hash function as it is comparably easy to calculate the signature of any specified block. The probability to find a block under a PoW scheme effectively depends on the miner's ability to calculate hash values, i.e. on the available computational power (Bhaskar and Lee 2015).

Proof of Stake (PoS) came up in February 2011 and is, according to Table 3, the second most common consensus scheme among cryptocurrencies. One example for which proof-of-stake has been implemented is Peercoin. In contrast to a PoW-scheme, under proof-of-stake, the probability does not depend on hashing power but on coinage, i.e. on the time and the amount a user keeps specific cryptocurrency tokens (King and Nadal 2012). Effectively, with an higher amount held, the stake held in the respective cryptocurrency is higher, and hence, the probability to generate a block. As the probability to find a block ultimately does not depend on computational power, a PoS scheme is less energy consuming compared to a PoW-scheme (King and Nadal 2012). Hence, PoS might be seen as addressing problems which have occurred in PoW as PoS is less prone to be reliant on specialized hardware.

Proof of Burn (PoB) was introduced to the field of cryptocurrencies in March 2014. One example for a cryptocurrency working on a proof-of-burn basis is ChanceCoin. The idea of proof-of-burn is to send cryptocurrency tokens to a verifiable non-spendable address, i.e. to one address which has not been generated from a private key (Bhaskar and Lee 2015). This makes generating a block costly, which is the same idea underlying PoW-schemes.

Proof of Resource (PoR) which is used, e.g., by SafeCoin was first introduced in April 2014. Under that kind of consensus schemes, users have to proof that they own specific resources, i.e. in terms of CPU power, bandwidth, uptime or storage. Having these resources (or a set thereof) is in principle costly.[8] This

[8] Further information on that kind of algorithm can be found at `https://github.com/maidsafe/resource_proof`.

kind of consensus scheme might be understood as an enhancement by giving cryptocurrencies other resources instead of hashing power to use.

Proof of Capacity (PoC) is also known as Proof-of-Space. This consensus scheme was first introduced in November 2014 and is, e.g., used by GadgetCoin. The idea of this kind of consensus scheme is to prevent users to register large amount of fake addresses/accounts (Dziembowski et al. 2015). In many cases, computer users have free disk space anyway, and the idea of Proof-of-Capacity is to ask users to store non-trivial amounts of data so that registering an address is costly. Hence, users will not have the incentive to register an unlimited number of addresses. The proof then works by the network asking for some bits of the data at random positions so that miners have at least to store large parts of the data, with the clear disadvantage of requiring the transmission of large amount of data in the first place to the party requested to proof (Dziembowski et al. 2015). Proof-of-capacity might be understood as a special case of a proof-of-resource system as disk capacity is ultimately a resource owned by the miners.

Delegated Proof of Stake (DPoS) which the DOACC dataset first records in February 2014. As outlined in Schuh and Larimer (2017) for BitShares, under DPoS users vote within their transactions on the blocks signed by witnesses (formerly called delegates). These witnesses are elected from the cryptocurrency users and are by definition each equally powerful. Thereby, voting allows user to decide whom they trust.

Proof of Research was created by GridCoin in 2014 and it tries to address one central problem of proof-of-work-consensus schemes, namely, that the data created within the mining process are only usable for the creation of blockchain blocks (Halford 2014). GridCoin uses the BOINC-network — a distributed computer network using computational capacities to solve scientifically relevant problems. This might be seen as an improvement over typically intrinsically worthless hashes which only serve for the protection of the cryptocurrency. To address for different endowments of "researchers" not only those with the most powerful hardware get paid: GridCoin also uses the concept of proof-of-stake (regarding "research age") to ensure payments to "researchers" with less powerful hardware[9]. Another proposal of such research based consensus scheme is Primecoin, effectively searching for prime number chains (King 2017)

As mentioned by Bhaskar and Lee (2015), there might be further schemes which can be used for some proof, e.g. an exchange might it find worthy to proof its solvency or its reserves to attract more users. Besides from that, a cryptocurrency is not only limited to a single consensus scheme. Instead, cryptocurrencies can use multiple schemes, e.g. a proof-of-work-scheme for some initial period and a proof-of-stake scheme when the cryptocurrency becomes more established (Hałaburda and

[9]For further information see GridCoin's wiki at `http://wiki.gridcoin.us/Proof-of-Research`.

Table 3: Consensus Schemes

DPoS	2	PoC	1	PoS	1185	PoW-PoS	44
PoB	3	PoR	4	PoW	1652	unknown	5

Sarvary 2015). The reason is straightforward, as in the beginning only few users have a stake in the system, and in later periods there might be the need to stop waste of resources induced by PoW. Again, this might be seen as an improvements over early stage cryptocurrencies as it allows to use different algorithms for different stages, thereby being able to collect the respective benefits. One example for such a planned change is Ethereum which will partially shift to PoS with its Casper update.

As the DOACC dataset covers announcement dates for each observed cryptocurrency, the structure and development of the consensus algorithms can be analyzed. There is no need to exclude specific observations from the dataset for the analysis. First, Table 3 reveals that PoW and PoS are the most common options, accounting for nearly 98% of the cryptocurrencies. Regarding the cryptocurrencies which do neither use PoW nor PoS directly, a majority uses a combination of these two schemes. These findings are in line with the results of Farell (2015) who also finds a majority using PoW and PoS or a combination thereof in the analysis of the 21 economically most important cryptocurrencies. However, the figures reported by the DOACC dataset for PoW and PoS are larger than the figures reported by Farell (2015), indicating some deviation of the economically important cryptocurrencies from the average announced cryptocurrency. Moreover, Farell (2015) shows that PoW is the most considerable consensus scheme when market capitalizations are taken into account.

Second, as shown in Figure 1up until 2014, PoW was the main consensus algorithm. However, from 2015 onwards, the majority of newly founded cryptocurrencies uses PoS. Thus, there is clear change from working-based to stake-based consensus algorithms.

3.4 Cryptographic Algorithms

Table 4 depicts the hashing functions used by the cryptocurrencies covered by the DOACC dataset. Again, as this variable contains a value for each observed cryptocurrency, it was not necessary to exclude any cryptocurrency observation from the dataset. However, it should be noted that some of the stated algorithms are a combination of others, implying that the numbers shown in Table 4 might underestimate the true usage of a specific algorithm. From that, the variety of cryptography used becomes apparently clear. Some important cryptographic functions will be outlined briefly before the analysis of their development among the cryptocurrencies.

Secure Hashing Algorithm (SHA) has three major subgroups: SHA-1, SHA-2 and SHA-3. For each type, there is a specified algorithm which generates the hash values. The latest algorithm, officially named SHA-3, is also known as Keccak. Keccak won the competition of being the algorithm in charge for SHA-3 in 2012. For each subgroup, there can be different lengths of the

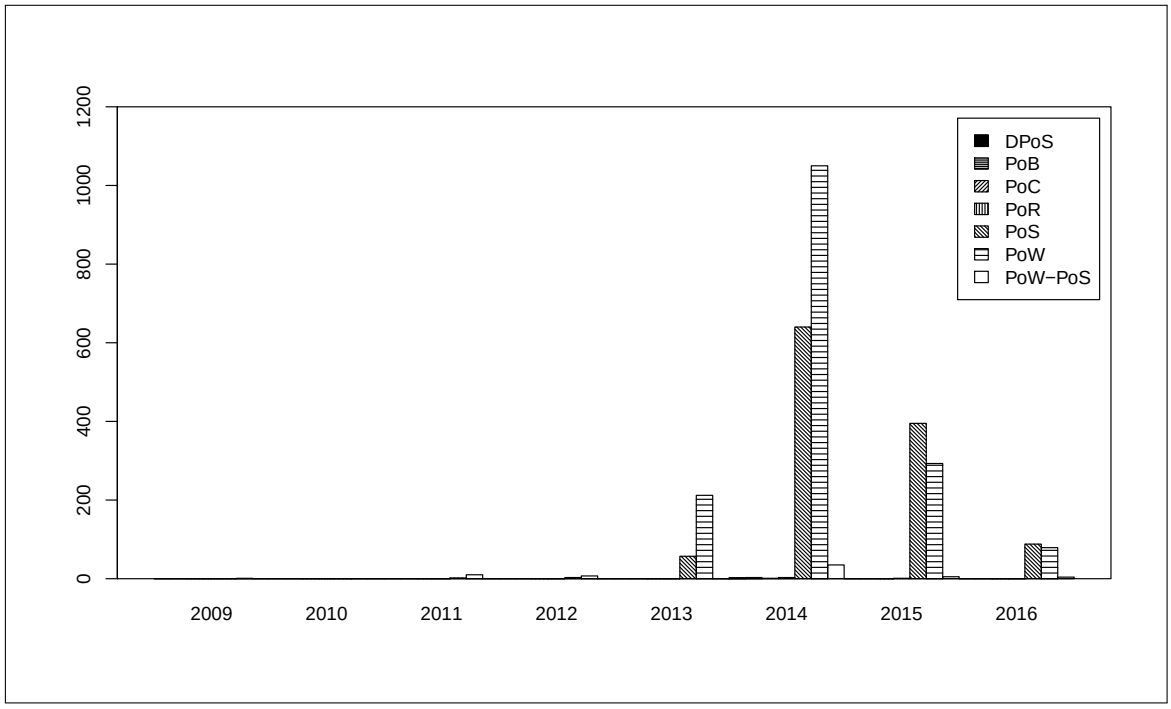


Figure 1: Number of consensus schemes

Table 4: Number of cryptocurrencies using a specific hashing algorithm

3s	3	intercoin	1	primegap	1	shanghai	1
bcrypt	1	jackpot	1	quark	62	Skein	5
BLAKE	14	JH	1	qubit	17	stackhash	1
BLAKE2b	2	Luffa	1	radix	1	t-inside	1
BMW	1	lyra2re	6	realpay	1	thiamine	1
boinc	1	m7	2	ripple	4	trisha	4
c11	2	MD5	1	roulette	1	twe	1
c29	1	mhash	1	salsarg	4	Twister	1
captcha	1	momentum	5	scrypt	1207	unknown	16
cryptonight	32	momsha	1	scrypt-j	40	velvet	1
Dagger	6	myriad	25	scrypt-j-n	2	Whirlpool	3
dcrypt	2	NeoScrypt	1	scrypt-n	47	x11	481
droplp	1	nist5	22	scrypt-n-f	1	x11gost	1
ellipticcurve	3	nist6	2	scrypt-n-m	1	x12	1
folding	1	novel	8	scrypt-n-r	3	x13	203
fresh	9	Obelisk	1	SHA-1-256	2	x14	9
friction	1	ocean	1	SHA-2-256	431	x15	71
Fugue	2	pluck-128	3	SHA-2-512	1	x17	2
Grøstl	4	prime6	1	SHA-3-256	25	xg	1
hefty1	7	primechain	5	SHA-3-512	1	yescrypt	1
hive	1	primeconstellation	1	Shabal	1	zr5	1

outcome, e.g., SHA-2-256 produces a hash of 256bit length, while SHA-2-512 produces a 512 bit long one. Bitcoin as one of the major cryptocurrencies uses SHA-2-256 and is therefore an example for this group of algorithms. The SHA-algorithm group accounts for about 460 different cryptocurrencies.

Scrypt was initially described by Percival (2009). It came up with Tenebrix in September 2011 (Tarasiewicz and Newman 2015) and now accounts for about 1,300 different cryptocurrencies with the majority using the original Scrypt-proposal directly. In contrast to the SHA-group, Scrypt is more memory intensive than SHA, making it more resistant against mining on specialized hardware, especially ASICs. Besides the stated original Scrypt algorithm, there exist several subgroups. Scrypt-N, as used by YACoin (May 2013), adds a factor to make the used storage capacity adjustable, while Scrypt-Jane is ultimately a Scrypt-N implementation with some differences in the hashing algorithm (Tarasiewicz and Newman 2015). Scrypt has innovated the cryptocurrency ecosphere by the provision of a more ASIC-resistant algorithm for PoW consensus schemes.

Cryptonight came up in the mid of 2012 and now accounts for 32 cryptocurrencies. The standard of cryptonight was described by Seigen et al. (2013) and is, as Scrypt, a memory-hard hashing function. The specific design feature of Cryptonight is that it should not be efficiently computable on hardware above CPUs, i.e. ruling out GPU, Field Programmable Gate Arrays (FGPAs) and ASIC architectures. Effectively, these were the hardware components which have led to the sharp increase of the Bitcoin network hashrate over time and hence, Cryptonight might be seen as the reaction of the cryptocurrency ecosphere to this Bitcoin-related problem. Within its design, Cryptonight uses Keccak which is the underlying hashfunction of SHA-3 The 2014-introduced CryptoNoteCoin uses Cryptonight (Tarasiewicz and Newman 2015).

X-... is a group of algorithms from X-11 to X-17 where the integers display the number of different hashing algorithms used. In particular, the crucial point in these X-... algorithms is to combine up to 17 different hashing functions, thereby providing a stronger resistance against the creation of specific mining hardware.[10] Taken as a group, X-... covers nearly 770 cryptocurrencies. The main subgroup according to the DOACC dataset is X-11 followed by X-13. The group of combined algorithms came up in January 2014 with Darkcoin. According to the webpage of the cryptocurrency "Dash"[11], mining a cryptocurrency using X11 on a GPU is less energy consuming and possible at lower hardware temperatures compared to Scrypt. Hence, using X11 should be more efficient in comparison to Scrypt, but a dedicated analysis of the efficiency of different hashing algorithm is not within the scope of this paper. Anyway, the X-... class might be understood as improvement, e.g. by the provision of a higher resistance against the failure of a single hashing algorithm.

[10] Further, this should provide an additional layer of resistance if a single cryptographic function would be broken.

[11] See `http://www.dash.org/x11/`.

The numbers provided in Table 4, and even more prominent Figure 2, reveal that Scrypt, X-... and SHA account for approximately 90 percent among newly announced cryptocurrencies. A more detailed view on that specific aspect is given by Figure 3. With Bitcoin being the only cryptocurrency founded in 2009, SHA-2-256 was the main hashing algorithm from the beginning and SHA remained to be the major group across 2011 and 2012. However, it can be seen that Scrypt gains larger shares in each of the years, effectively leading to 2013 where Scrypt was the major hashing algorithm among the newly founded hashing algorithms[12]. For 2014 and 2015, the X-... algorithms became more and more important. From the overall pattern it is observable that SHA is getting less important, while other algorithms become more important. The shift in the hashing algorithm might also reflect the development of more specialized hardware for the Bitcoin mining process which might lead to a concentration of hashing power. In particular, the development of ASICs has to be named. ASICs are specially designed hardware components which can generate hashes much faster than a normal CPU or GPU can, thereby making mining on standard computer hardware uneconomically (Narayanan et al. 2016). To protect against this, memory-intensive functions like Scrypt or combinations of hashing algorithms are used.

Besides that, the cryptocurrency ecosphere shows at least some path dependence: Bitcoin might have set some standards which were, at least in the beginning, copied by other cryptocurrencies. A similar pattern is observable for the consensus schemes. However, as the cryptocurrency ecosystem is getting more mature, it is becoming more diverse and the initial impact of Bitcoin forming the cryptocurrency ecosphere is reduced.

3.5 Block Times

Cryptocurrencies achieve decentralization by the usage of the distributed ledger technology, typically via blockchain implementations. Thus, they create an ordered sequence of transactions between the network participants' accounts. This sequence is divided into blocks. The DOACC dataset has block time values for 2,112 cryptocurrencies, or for about 73% of the whole dataset. However, some background check reveals at least partial problems. First, there seems to be an overlap in names for InsanityCoin, one with a blocktime of 12 hours, the other one of only 3 minutes. Second, for some cryptocurrencies blocktime and retarget time seem to be interchanged according to current specifications. Hence, one should be cautious in interpreting the numbers provided here.

For the covered cryptocurrencies the mean blocktime is 139.3 seconds, or nearly 2 minutes and 20 seconds. However, there is considerable variation in the blocktimes. The longest blocktime is found with InsanityCoin with a blocktime of 12 hours. The majority (2,020) of cryptocurrencies covered by the DOACC dataset has blocktimes shorter than Bitcoin while only a minority has equal (78 cases) or longer (15 cases)

[12]However, this analysis lacks the incorporation of exchanges rates and market volumes. This would enable to determine the economically important patterns. However, such an analysis is beyond the scope of this paper. Anyway, a look on the leading cryptocurrencies reveals some heterogeneity, covering SHA-2-256, Scrypt and other algorithms.

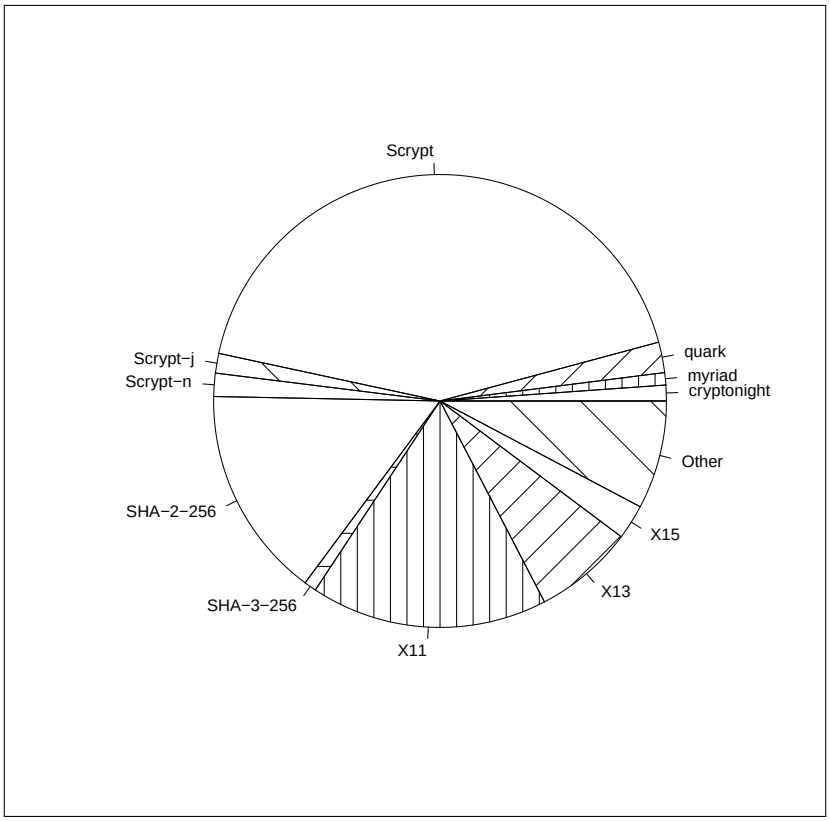


Figure 2: Overview of the most important hashing algorithms.

blocktimes.

Figure 4a shows a decrease of the mean blocktime as the cryptocurrency ecosphere gets more mature. However, taking only blocktime into account is not enough, calculating the average time for a transaction to settle also requires to know about the recommended number of confirmations.

3.6 Confirmation

There are two explanations why a user should wait at least for some blocks when determining whether a transaction has settled or not. First, blockchains sometimes generate forks. This happens when two miners independently find a solution to the cryptographic puzzle underlying the cryptocurrency. In later rounds, though, one miner (or one group of miners) will eventually find a block faster than the others (other groups), generating the longer blockchain to which everyone will switch. As the network switches to one specific blockchain, this will generate the need for a new inclusion of some transactions after the fork has resolved (Nakamoto 2008). However, this only gives rise to a waiting time of only a few blocks as a fork is publicly observable. Second, the more striking reason for a waiting time is the possibility of an attacker trying to modify the ledger after a specific transaction has occurred. One might think of this as the attacker trying to recover the funds which he sent to a specified account. However, changing the blockchain will require some work, and hence, the attacker needs to redo the work required to generate a block for

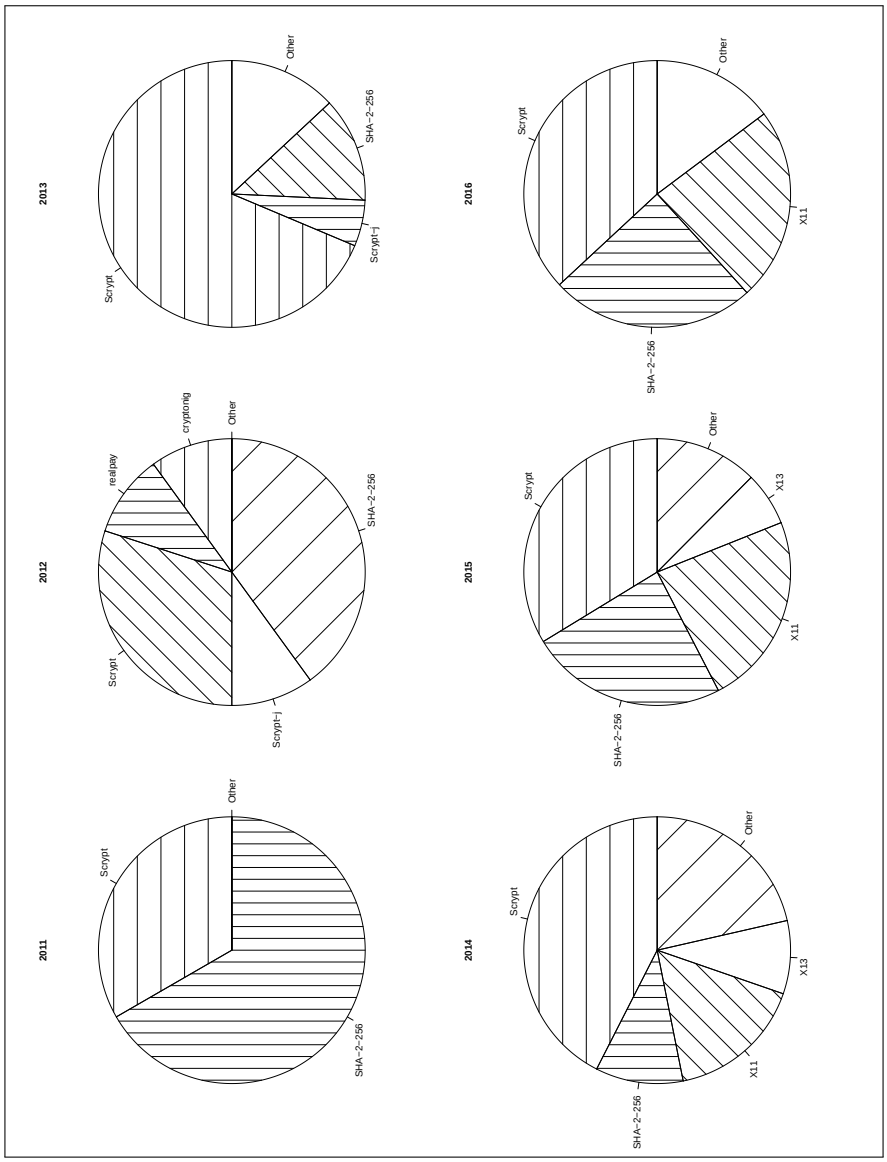
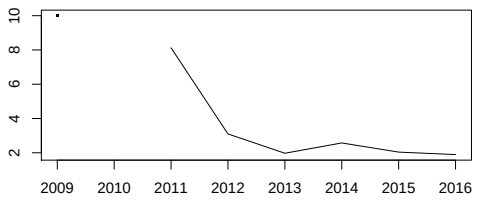
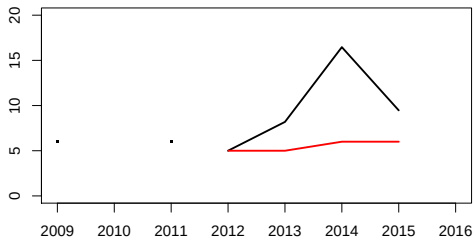


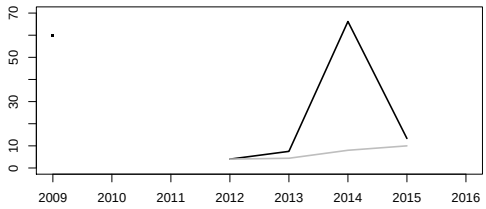
Figure 3: Development of the hashing algorithms by years.



(a) Mean blocktime in minutes



(b) Median and mean number of recommended confirmations, median in red, mean in black



(c) Mean time in minutes to reach the recommended number of confirmations, mean in black, median in gray

Figure 4: Block- and confirmation times

each of the blocks he is behind. Consequently, the more blocks a possible attacker is behind, the harder it gets to alter the blockchain and thereby, with more and more following blocks, a transaction is more secure. Nakamoto (2008) shows that the probability of an attacker being successful depends on its probability to form a block, i.e. the hashing rate under a PoW consensus scheme. Thus, the higher the concentration of power within a specific cryptocurrency, the higher should be the number of confirmations required.

As shown in Figure 4b, the number of recommended confirmations increased, both in terms of the median and the mean. One might think that this reflects changes within the cryptocurrency ecosphere, e.g. some concentration of the mining process. This might be due to mining pools which – in particular for Bitcoin – now account for a large share of the hash rate and thus, have a larger potential to abuse this power, leading to a higher number of recommended confirmations from the beginning on. However, there is large variance around the mean, ranging from only few recommended confirmations up to about 30 .

However, focusing on the number of confirmations only is missing the important point of the time associated with waiting. As for the same number of recommended

confirmations, cryptocurrencies with a shorter blocktime will settle transactions faster. One example for this is the comparison of Bitcoin with Litecoin. As long as both need six confirmations to consider a transaction as safe, Litecoin generates a faster confirmation with faster blocktimes of only 2.5 minutes. Hence, one should additionally focus on the confirmation time which is the product of the recommended number of confirmations and blocktime. This kind of calculation has been done in Figure 4c. With the exception of 2012 and 2013, both with an only limited number of observations, confirmation time is increasing over time due to higher number of recommended confirmations. Both the median and the mean are below typical times of bank transfers[13] , giving cryptocurrencies an advantage over those traditional financial services.[14]

The confirmation times shown in Figure 4c imply waiting until a transaction can be viewed as guaranteed. At least for Point-of-Sale transactions, this time might be too long as it forces customers as well as merchants to wait or to take some risks, i.e. with a transaction not being included into a block. This might prevent both customers as well as merchants from using cryptocurrencies. This risk consideration might be one important hurdle which cryptocurrencies need to overcome to gain large market acceptance rates. There are at least some intermediaries which enable merchants to get an instantaneous confirmation of the transaction, thus, making payments with Bitcoins (or any other cryptocurrency) comparable to electronic card payments (Blocher et al. 2017).

3.7 Premining

One possibly important source of income for the creators of a cryptocurrency are the revenues from the sale of premined cryptocurrency tokens: Creators generate a predetermined amount of tokens and then distribute this to some audience, maybe in exchange for some monetary equivalent[15]. The audience might be some interested public, or some inhabitants of a geographic area (e.g. Iceland for the case of AuroraCoin). There are different reasons why creators want to use this: The creators can pay themselves, e.g. for the effort they had put into the creation. In particular, this becomes important when the cryptocurrency is not only a copy of an existing one but when there is real innovation in it, e.g. the development of infrastructure or new algorithms like the provision of a smart contract platform like Ethereum. Furthermore, such payments would in general be usable to build infrastructure at the side of merchants, thereby mitigating the hurdle created by network effects. As argued by Blocher et al. (2017), this payment for infrastructure is unlikely to be paid by a single actor. However, it might pay off for a central shareholder to pay for the infrastructure as more acceptance might turn into higher market valuations, generating a

[13] According to Blocher et al. (2017), intra-European bank transfers must settle within one bank working day, but bank-transfers to outside the EU typically take longer, up to 20 days when it comes to transfers into developing countries.

[14] However, there are developments to make bank transfers faster, e.g. with SEPA Instant Payments within Europe it should be possible to transfer funds instantaneously (Blocher et al. 2017), thereby attacking the advantage of fast private alternatives such as cryptocurrencies.

[15] This monetary equivalent can either in traditional state-issued money, or in other cryptocurrency tokens, i.e. altcoins.

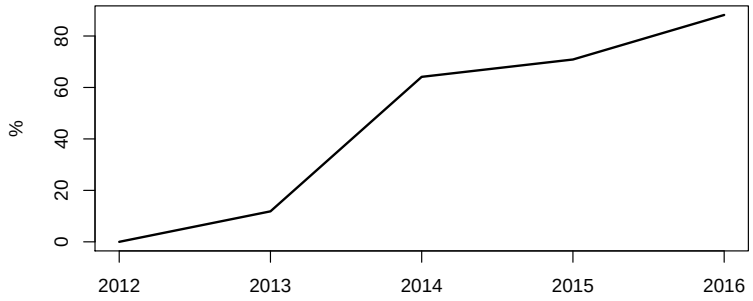


Figure 5: Share of cryptocurrencies which apply a premining strategy compared to those cryptocurrencies which do not apply such a mechanism.

higher value for the kept share of tokens. Thus, it might be in the self-interest of a central shareholder to make investments into any specific cryptocurrency[16].

One example for a cryptocurrency with premining is AuroraCoin. Introduced in 2014, AuroraCoin is a Litecoin fork and thereby a Bitcoin successor, and employs a premine of 50% of the total tokens. These tokens are not formally thought for the creators but are intended to be distributed among Iceland's population (AuroraCoin 2014). The idea behind this is to generate a critical mass of possible users. Besides from infrastructure provision, generating a critical mass of possible users reduces the two-sided network effects being at work during the introduction of a (crypto)currency.

According to Figure 5, the total share of cryptocurrencies using at least some premining is increasing over time. This also displays the development of the initial coin offerings (ICOs). However, not all ICOs are really useful in economic terms or offer benefits to investors. Hence, one should be cautious when investing into a newly founded cryptocurrency.

The DOACC dataset covers observations for the amount of premining involved. However, not every observation is useful as the amount of premined tokens needs to be compared to some value. One natural candidate for this would be the total amount of issued tokens. Hence, I had to exclude observations without an upper limit on token issuance which is the case for 68 observations. As the values inserted into the variable for the premining is not following a standardized pattern, I manually calculated the share of premining for the whole dataset. Doing all these kind of corrections leaves 1,461 observations left which is half of the DOACC dataset.

The analysis of the relative amount in Figure 6 of premining reveals that creators are not necessarily greedy, at least not for the observations covered by the DOACC dataset. Regardless of whether cryptocurrencies not using premining are

[16]However, this argument is intuitive but lacks an economic background calculation. As investments into infrastructure can be very high, the costs can outweigh the gain in market value of the kept tokens. Then, for the central shareholder, it would be rational not to invest into the cryptocurrency but to only divert the money generated by the ICO.

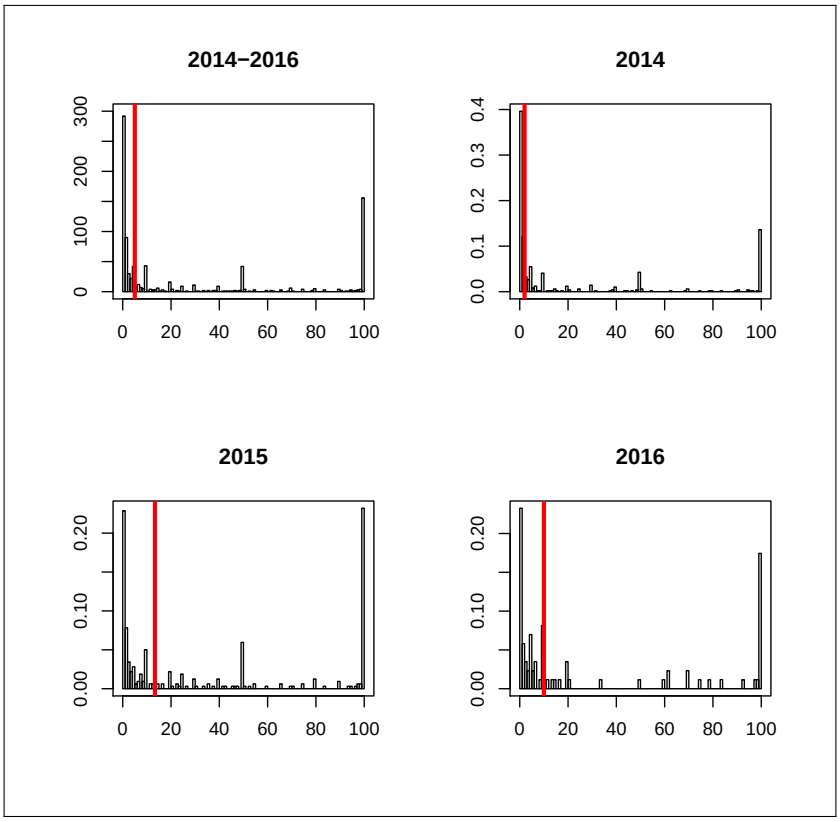


Figure 6: Share of premined coins (excluding those coins which do not apply premining). Red line markes the median.

included or not, the overall pattern shows that premining in total is low compared to the total number of coins. The typical pattern in the figures is a larger mass of cryptocurrencies around zero, a small peak at about 50% of the total tokens and a second larger peak at 100% with the second peak being greater than the first one. Besides, the figures show that the median of the premining amount is increasing over time which again highlights the importance of ICOs[17]. Not all of these tokens are necessarily distributed. As Conley (2017) reports, the typical figure is to hold 20% of the coins generated back on the creators' side.

3.8 Determinants of success

From the analysis of Table 1 and especially from the more in-depth analysis of the DOACC dataset provided in this paper, it should be clear that the number of cryptocurrencies created and possibly circulating around is rather large. However, there seems to be a significant amount of cryptocurrencies which are dead ends, not only in terms of market capitalization but also in the degree of innovation they provide for the cryptocurrency ecosystem. In fact, some of the cryptocurrencies now present in the ecosphere are thought to be scam, and others are just clones

[17]However, one should be cautious in this interpretation. Not every premined coin is thought for an ICO, nor is there any indication which cryptocurrency is more important than another one, e.g. in terms of economic impact or in the degree of innovation it offers.

of already existing cryptocurrencies (Tarasiewicz and Newman 2015). The history of any specific cryptocurrency cannot be neglected, though, as their creators had specific ideas in mind (Hałaburda and Sarvary 2015). For example, some coins have been founded for increased anonymity, e.g. ZCash (Hopwood et al. 2017), some for the sake of tipping, and some try to target specific niche communities (Tarasiewicz and Newman 2015). Furthermore, some cryptocurrencies might be necessarily seen as experiments, e.g. of a new algorithm or a new business model. Hence, one might conclude that the high number of cryptocurrencies is also due to proof of concepts (Tarasiewicz and Newman 2015). Furthermore, the development of any specific cryptocurrency might be at least partially explained by weaknesses of existing cryptocurrencies.

Whether a cryptocurrency will gain large success crucially depends on its features. By choosing specific design features, creators can determine the success of their cryptocurrency. As competition among cryptocurrencies is still in progress and a clear winner can only hardly be determined, naming success factors is necessarily difficult. However, some potential factors shall be outlined.

Generally, cryptocurrencies are thought to provide benefits, e.g. in the fields of transaction irreversibility, protection against identity theft, reduction of transaction costs or faster innovation (Mas and Lee 2015). Even though there were downsides on these factors, it seems to be intuitive that successful cryptocurrencies will fulfill these factors to an reasonable extent. Failing to address those features can lead to a shy-away behavior of users and thus, to the failure of a cryptocurrency proposal.

Network effects play a crucial role in the formation of currency schemes. The analysis of the DOACC dataset has shown that this is also applicable to the cryptocurrency ecosphere. For instance, Bitcoin as the first cryptocurrency has shaped the cryptocurrency ecosystem quite strongly. Hence, one might conclude that path-dependent processes might have been at work and Bitcoin might have benefited from its first-mover advantage, gaining a relatively large user base and thereby securing it today's success. However, these network effects are not only in place in the competition among cryptocurrencies, but also in the competition in cryptocurrencies with traditional payment systems. For most countries, such systems work reasonably well, and consequently, cryptocurrencies need to provide a relatively large advantage to overcome the existing network effects (Hałaburda and Sarvary 2015). Compatibility to existing electronic payment systems might foster the adoption of a cryptocurrency as a means of payment, but it is doubtful whether the providers of the existing infrastructures would be willing to provide cryptocurrency interfaces in particular in the light that cryptocurrencies would be able to operate without such intermediaries. Overcoming these network barriers might thus require a relatively strong player, effectively putting state-run digital currencies in advance.

Regarding the regulatory efforts which become more and more prominent in recent times, a cryptocurrency being able to fit into the regulations imposed by any government might have a clear advantage. This does not only cover technical features, but also the creator's or community ability to convince any regulatory authority to accept a cryptocurrency, e.g. like with Bitcoin's "legalization" in Japan due to a revision of Japan's Payment Services Act.

In particular, community and user-based specifics can largely determine whether

a cryptocurrency can be successful. In fact, a cryptocurrency which is unable to attract any community being willing to accept it is likely to be unsuccessful. First, users can support any specific cryptocurrency. This is a two-sided effect, as users can be both consumers and merchants, thereby providing the necessary mass to overcome network effects. Second, users can try to lobby for a cryptocurrency, thereby opening paths for successful development. However, it is not only user- or community-driven behavior which can determine the success of a cryptocurrency. In technical terms, any cryptocurrency candidate offering both consumers and merchants a higher degree of convenience might be advantageous to a less convenient alternative (Mas and Lee 2015). Convenience might include the creation of additional usages, e.g. the creation of smart contracts. Further, it is provided by fast transaction settlement, i.e. keeping waiting times for both consumers and merchants short enough. Moreover, the cryptocurrency proposal needs to target the community, i.e. to satisfy their needs. In that sense, it is not only technical finesse what counts, but rather it requires support of a community. As cryptocurrencies are examples of fiat monies, they largely rely on the trust set into them. Hence, a cryptocurrency being better able to develop universal trust might be more likely to succeed on the market than a less trusted cryptocurrency (Hałaburda and Sarvary 2015). Developing this trust can be done by, e.g., the provision of high security, scalability, low error rates or low volatilities on the exchanges. Additionally, this might include the convenience provided the ability to restore private keys if a user has lost it (Mas and Lee 2015). Moreover, being able to adjust features in sound and user-benefiting way might generate an additional increase in the likelihood of success.

From a technical perspective, some features generating success have already been mentioned, e.g. the provision of security or anonymity. Moreover, the DOACC dataset analysis reveals that newer cryptocurrencies tend to have shorter blocktimes, although this did not (yet) lead to the replacement of Bitcoin as the leading cryptocurrency. Furthermore, the ability to adjust can be a crucial feature, and Bitcoin's fork into now three types of Bitcoin exemplifies this. From an economic point of view, the upper cap on the total token issuance can be viewed as problematic as the now implemented rules do neither account for macroeconomic variables, e.g. inflation or the state of the business cycle nor for some speculative behavior like the formation of bubbles (Mas and Lee 2015). However, conducting policy was not one of the aims when cryptocurrencies emerged, but as they gain now more and more attention, such topics step onto the agenda.

The relatively vague outlined features might influence the likelihood of a success of cryptocurrency. However, it needs to be mentioned that the probability of a success will not only depend on a cryptocurrency's technical features, but also on the community, the time and the place. Put differently, technical features of a specific implementation might be practically irrelevant for the day-to-day users as they are concerned with the possible uses, e.g. a cryptocurrency's usefulness as money or investment vehicle. Hence, it might be users and not technical details determining the success or failure of a cryptocurrency. Economic literature has shown that technical superiority does not necessarily ensure survival on the market (David 1985; Liebowitz and Margolis 1995). Winning features might change over

time. Moreover, some countries might be more prone to adopt a cryptocurrency than others (Hileman 2015), thereby displaying the different cultures around the world. Furthermore, there might be trade-offs in the achievements of different targets, but it is far beyond the scope of this paper to judge whether such trade-offs exist and how they can be addressed.

4 Conclusion

By analyzing the DOACC dataset, this paper has shown that cryptocurrencies are more than just Bitcoin. There exist plenty of alternative cryptocurrencies and each has some specific target. From its inception in 2009, it took nearly five years until the number of newly founded cryptocurrencies began to rise sharply. Especially at the beginning, cryptocurrencies used to be very similar to the original Bitcoin implementation. Thus, Bitcoin has shaped the ecosphere and formed the path of the development. However, as the cryptocurrency ecosystem gets more mature, the arising side effects such as a concentration of hashing power have led to that cryptocurrencies are now more and more distinct from Bitcoin. The analysis of the DOACC dataset revealed that consensus is mainly driven by a proof-of-work or a proof-of-stake mechanism, even though there were alternatives. Moreover, cryptography has developed a large variety of algorithms which also show up in the cryptocurrency ecosystem. However, only a small set of these algorithms are used by the majority of cryptocurrencies. Nowadays, cryptocurrencies typically use shorter blocktimes than Bitcoin's ten minute target while the recommended number of confirmations is increasing. The latter may be thought to be an indicator for the concentration of power within the cryptocurrency ecosphere, e.g. by the formation of large mining pools. The analysis shows an increase of the confirmation time. Furthermore, premining is getting more important over time. The analysis has shown typical peaks for premining shares. First, there are many coins which do not use premining at all or which have low premining shares. Second, there is a share of cryptocurrencies which have half of their total token generated at their inception and third, there is a larger peak of cryptocurrencies which generated (nearly) all of their total supply at their creation.

The future of cryptocurrencies is quite unclear. Especially regulatory efforts might prevent cryptocurrencies from escaping their being of a niche phenomenon. Furthermore, there is no clear candidate which will ultimately succeed. Bitcoin might be a natural candidate to think of because of network effects and path dependence. However, there is no clear measure which features of a cryptocurrency are necessary or sufficient for future success. Even worse, it remains unknown whether only one cryptocurrency can succeed, or if the equilibrium allows for a set of different cryptocurrencies, with the competition between the different cryptocurrencies as realization of the currency competition in the sense of Hayek (1978). For success on the market, one important property will be the ability to adjust to economic and regulatory conditions. In particular, any cryptocurrency needs to balance the need for a fast enough velocity to stay innovative while maintaining resistance against bad proposals. Nonetheless, it is not only technical features, but also users perception of usefulness which will determine the potential of any cryptocurrency. Anyway, it

the future might show that the winner is a state-run digital currency, as the arising network effects and regulatory barriers are easier to overcome for some governmental money. After all, money will then persistent to be state-issued.

Whether cryptocurrencies will succeed or not remains an open question. However, they impose serious pressure on traditional financial structures, the research efforts taken by so many central and commercial banks are evidence of that. Even when cryptocurrencies remain to be a niche phenomenon, their gain for the economy might be visible in the innovation they force at the level of traditional financial intermediaries.

Future research may investigate determinants of a successful adoption of cryptocurrencies in more detail. From such an analysis it might be possible to conclude some features which a cryptocurrency needs to cover for a successful adoption and to prevent market failure. Further research needs to outline the economic consequences of cryptocurrencies leaving their niches, both for the economy and for business.

References

[1] Ahamad, ShaikShakell, Madhusoodhnan Nair, and Biju Varghese (2013). "A Survey on Crypto Currencies". In: Proceedings of the International on Advances in Computer Science, pp. 42–48. DOI: 02.AETACS.2013.4.131.

[2] Ali, Robleh, John Barrdear, Roger Clews, and James Southgate (2014). "The Economics of Digital Cryptocurrencies". In: *Bank of England Quarterly Bulletin Q3*, pp. 276–286.

[3] Ametrano, Ferdinando M. (2016). *Hayek Money: The Cryptocurrency Price Stability Solution*. DOI: 10.2139/ssrn.2425270.

[4] Antonopoulos, Andreas M. (2014). *Mastering Bitcoin*. O'Reilly Media.

[5] Apostolaki, Maria, Aviv Zohar, and Laurent Vanbever (2017). "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies". In: *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE. DOI: 10.1109/sp.2017.29.

[6] AuroraCoin (2014). *AuroraCoin AUR*. https://github.com/baldurodinsson/auroracoin-project/.

[7] Back, Adam (1997). *[ANNOUNCE] hash cash postage implementation*. http://www.hashcash.org/papers/announce.txt.

[8] Bagnall, John, David Bounie, Kim P. Huynh, Anneke Kosse, Tobias Schmidt, Scott Schuh, and Helmut Stix (2016). "Consumer Cash Usage: A Cross-Country Comparison with Payment Diary Survey Data". In: *International Journal of Central Banking* 12.4, pp. 1–61.

[9] Barrdear, John and Michael Kumhof (2016). *The macroeconomics of central bank issued digital Cryptocurrencies*. Bank of England Staff Working Paper No. 605.

[10] Baur, Aaron W., Julian Bühler, Markus Bick, and Charlotte S. Bonorden (2015). "Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co". In: *Open and Big Data Management and Innovation*. Springer International Publishing, pp. 63–80. DOI: 10.1007/978-3-319-25013-7_6.

[11] Bhaskar, Nirupama Devi and David Kuo Chuen Lee (2015). "Bitcoin Mining Technology". In: *Handbook of Digital Currency*. Ed. by David Lee Kuo Chuen. San Diego: Academic Press, pp. 45 –65. DOI: B978-0-12-802117-0.00003-5.

[12] Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore (2015). "Bitcoin: Economics, Technology, and Governance". In: *Journal of Economic Perspectives* 29.2, pp. 213–238. DOI: 10.1257/jep.29.2.213.

[13] Biryukov, Alex, Dmitry Khovratovich, and Ivan Pustogarov (2014). "Deanonymisation of Clients in Bitcoin P2P Network". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS 14*. ACM Press. DOI: 10.1145/2660267.2660379.

[14] Blocher, Walter, Andreas Hanl, and Jochen Michaelis (2017). "Revolutionieren Kryptowährungen die Zahlungssysteme?" In: *Wirtschaftspolitische Blätter* 64.4, pp. 541 –552.

[15] Brière, Marie, Kim Oosterlinck, and Ariane Szafarz (2015). "Virtual currency, tangible return: Portfolio diversification with bitcoin". In: *Journal of Asset Management* 16.6, pp. 365–373. DOI: 10.1057/jam.2015.5.

[16] Cermak, Vavrinec (2017). "Can Bitcoin Become a Viable Alternative to Fiat Currencies? An Empirical Analysis of Bitcoins Volatility Based on a GARCH Model". In: *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2961405.

[17] Chaum, David (1992). "Achieving Electronic Privacy". In: *Scientific American*, pp. 96–101.

[18] Christin, Nicolas (2013). "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace". In: *Proceedings of the 22Nd International Conference on World Wide Web*. WWW '13. Rio de Janeiro, Brazil: ACM, pp. 213–224. DOI: 10.1145/2488388.2488408.

[19] Conley, John P. (2017). *Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings*.

[20] Courtois, Nicolas, Guangyan Song, and Ryan Castellucci (2016). "Speed Optimizations in Bitcoin Key Recovery Attacks". In: *Tatra Mountains Mathematical Publications* 67.1, p. 103. DOI: 10.1515/tmmp-2016-0030.

[21] Courtois, Nicolas T., Pinar Emirdag, and Filippo Valsorda (2014). *Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events*. Cryptology ePrint Archive, Report 2014/848. https://eprint.iacr.org/2014/848.

[22] Dai, Wei (1998). *B-Money*. http://www.weidai.com/bmoney.txt.

[23] David, Paul A. (1985). "Clio and the Economics of QWERTY". In: *American Economic Review* 75.2, pp. 332–337.

[24] Dimpfl, Thomas (2017). *Bitcoin Market Microstructure*. https://ssrn.com/abstract=2949807. DOI: 10.2139/ssrn.2949807.

[25] Dziembowski, Stefan, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak (2015). "Proofs of Space". In: *Advances in Cryptology – CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*. Ed. by Rosario Gennaro and Matthew Robshaw. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 585–605. DOI: 10.1007/978-3-662-48000-7_29.

[26] European Central Bank (2012). *Virtual Currency Schemes*. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[27] Farell, Ryan (2015). *An Analysis of the Cryptocurrency Industry*. Wharton Research Scholars, 130. University of Pennsylvania.

[28] Fung, Ben S. C. and Hanna Hałaburda (2016). *Central Bank Digital Currencies: A Framework for Assessing Why and How*. Bank of Canada Staff Discussion Paper No. 2016-22.

[29] Gandal, Neil and Hanna Hałaburda (2014). *Competition in the Cryptocurrency Market*. Bank of Canada Working Paper 2014-33.

[30] Giechaskiel, Ilias, Cas Cremers, and Kasper B. Rasmussen (2016). "On Bitcoin Security in the Presence of Broken Cryptographic Primitives". In: *Computer Security – ESORICS 2016*. Springer International Publishing, pp. 201–222. DOI: 10.1007/978-3-319-45741-3_11.

[31] Hałaburda, Hanna and Miklos Sarvary (2015). *Beyond Bitcoin*. Palgrave Macmillan. DOI: 10.1057/9781137506429.

[32] Halford, Rob (2014). *Gridcoin - Crypto-Currency using Berkeley Open Infrastructure Network Computing Grid as Proof of Work*. URL: https://bravenewcoin.com/assets/Whitepapers/gridcoin-white-paper.pdf.

[33] Hanl, Andreas and Jochen Michaelis (2017). "Kryptowährungen - ein Problem für die Geldpolitik?" In: *Wirtschaftsdienst* 97.5, pp. 363–370. DOI: 10.1007/s10273-017-2145-y.

[34] Hayek, Friedrich August von (1978). *Denationalisation of Money - The Argument Refined*. Institute of Economic Affairs.

[35] He, Dong, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes (2016). *Virtual Currencies and Beyond: Initial Considerations*. URL: http://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.

[36] Hileman, Garrick (2014). *A History of Alternative Currencies*. https://www.hillsdale.edu/wp-content/uploads/2016/02/FMF-2014-A-History-of-Alternative-Currencies.pdf.

[37] Hileman, Garrick (2015). "The Bitcoin Market Potential Index". In: *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, pp. 92–93. DOI: 10.1007/978-3-662-48051-9_7.

[38] Hopwood, Daria, Sean Bowe, Taylor Hornby, and Nathan Wilcox (2017). *Zcash Protocol Specification*. URL: https://github.com/zcash/zips/blob/master/protocol/protocol.pdf.

[39] Houy, Nicolas (2014). *The Economics of Bitcoin Transaction Fees*. Gate Working Paper No. 1407. DOI: 10.2139/ssrn.2400519.

[40] Janze, Christian (2017). "Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets". In: *Twenty-third Americas Conference on Information Systems, Boston, 2017*.

[41] Karame, Ghassan O., Elli Adroulaki, and Srdjan Capkun (2012). *Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin*. URL: http://eprint.iacr.org/2012/248.pdf.

[42] King, Sunny (2017). *Primecoin: Cryptocurrency with Prime Number Proof-of-Work*. URL: http://primecoin.io/bin/primecoin-paper.pdf.

[43] King, Sunny and Scott Nadal (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. https://peercoin.net/assets/paper/peercoin-paper.pdf.

[44] Kristoufek, Ladislav (2013). "BitCoin meets Google Trends and Wikipedia: Quantifiying the relationship between pehnomena of the Internet era". In: *Scientific Reports* 3,3415. DOI: 10.1038/srep03415.

[45] Kristoufek, Ladislav (2015). "What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis". In: *PLoS ONE* 10.4. Ed. by Enrico Scalas, e0123923. DOI: 10.1371/journal.pone.0123923.

[46] Liebowitz, Stan J and Stephen E Margolis (1995). "Path dependence, lock-in, and history". In: *Journal of Law, Economics, and Organization* 11, pp. 205–22.

[47] Luther, William J. (2015). "Cryptocurrenciens, Network Effects and Switching Costs". In: *Contemporary Economic Policy* 34.3, pp. 553–571. DOI: 10.1111/coep.12151.

[48] Mas, Ignacio and David Kuo Chuen Lee (2015). "Bitcoin-Like Protocols and Innovations". In: *Handbook of Digital Currency*. Ed. by David Lee Kuo Chuen. San Diego: Elsevier, pp. 417–451. DOI: 10.1016/b978-0-12-802117-0.00021-7.

[49] Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage (2013). "A fistful of bitcoins". In: *Proceedings of the 2013 conference on Internet measurement conference - IMC 13*. ACM Press. DOI: 10.1145/2504730.2504747.

[50] Michaelis, Jochen (2017). "Die Konkurrenz umarmen: Digitales Zentralbankgeld". In: *ifo Schnelldienst* 70.22, pp. 17–20.

[51] Nakamoto, Satoshi (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf.

[52] Narayanan, Arvind and Jeremy Clark (2017). "Bitcoins academic pedigree". In: *Communications of the ACM* 60.12, pp. 36–45. DOI: 10.1145/3132259.

[53] Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton Univers. Press.

[54] O'Dwyer, K.J. and D. Malone (2014). "Bitcoin Mining and its Energy Footprint". In: *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014)*. Institution of Engineering and Technology. DOI: 10.1049/cp.2014.0699.

[55] Percival, Colin (2009). "Stronger Key Derivation via Sequential Memory-Hard Functions". In:

[56] Popov, Serguei (2017). *The Tangle*. URL: https://iota.org/IOTA_Whitepaper.pdf.

[57] Rogoff, Kenneth (2017). *Crypto Fool's Gold?* https://www.project-syndicate.org/commentary/bitcoin-long-term-price-collapse-by-kenneth-rogoff-2017-10.

[58] Sapuric, Svetlana, Angelika Kokkinaki, and Ifigenia Georgiou (2017). "In Which Distributed Ledger Do We Trust? A Comparative Analysis Of Cryptocurrencies". In: *MCIS 2017 Proceedings*.

[59] Schuh, Fabian and Daniel Larimer (2017). *BitShares 2.0: General Overview*. URL: http://docs.bitshares.org/_downloads/bitshares-general.pdf.

[60] Seigen, Max Jameson, Tuomo Nieminen, Neocortex, Antonio M. Juarez, and CryptoNote (2013). *CryptoNight Hash Function*. URL: https://cryptonote.org/cns/cns008.txt.

[61] Sveriges Riksbank (2017). *The Riksbank's e-krona project. Report 1.* http://www.riksbank.se/Documents/Rapporter/E-krona/2017/rapport$_e krona_1 70920_e ng.pdf$.

[62] Szabo, Nick (2005). *Bit Gold*. URL: http://nakamotoinstitute.org/bit-gold/.

[63] Tarasiewicz, Matthias and Andrew Newman (2015). "Cryptocurrencies as Distributed Community Experiments". In: *Handbook of Digital Currency*. Ed. by David Lee Kuo Chuen. San Diego: Elsevier, pp. 201–222. DOI: 10.1016/B978-0-12-802117-0.00010-2.

[64] Wüst, Karl and Arthur Gervais (2017). *Do you need a Blockchain?* Cryptology ePrint Archive, Report 2017/375. https://eprint.iacr.org/2017/375.

[65] Yermack, David (2015). "Is Bitcoin a Real Currency? An Economic Appraisal". In: *Handbook of Digital Currency*. Ed. by David Lee Kuo Chuen. San Diego: Elsevier, pp. 31–43. DOI: 10.1016/B978-0-12-802117-0.00002-3.

Table 5: Plausibility check of the DOACC dataset

Name	**Symbol**	**Inception**	**Blocktime (s)**	**Max. token issuance**	**Cryptographic Algorithm**	**Consensus Scheme**	**Source**
Bitcoin	BTC	1.2009	600	21m	SHA-256d	PoW	(1)
		1.2009		21m	SHA-256	PoW	(2)
	BTC	1.2009	600	21m	SHA-2-256	PoW	(3)
Namecoin	NMC	4.2011	600	21m	SHA-256d	PoW	(1)
		4.2011		21m	SHA-256	PoW	(2)
	NMC	4.2011	600	21m	SHA-2-256	PoW	(3)
SolidCoin	SC	8.2011	180	18.9m	SHA-256d	PoW	(1)
	SC	8.2011			SHA-2-256	PoW	(3)
GeistGeld	GG	9.2011	15	no limit	SHA-256d	PoW	(1)
	GG	9.2011			SHA-2-256	PoW	(3)
Tenebrix	TBX	9.2011	300	no limit	Scrypt	PoW	(1)
	TBX	9.2011			Scrypt	PoW	(3)
Fairbrix	FBX	10.2011	300	no limit	Scrypt	PoW	(1)
	FBX	10.2011			Scrypt	PoW	(3)
Litecoin	LTC	10.2011	150	**84m**	Scrypt	PoW	(1)
		10.2011		**84m**	Scrypt	PoW	(2)
	LTC	10.2011	150	**82m**	Scrypt	PoW	(3)
BlackCoin	BC	**2.2014**	60	no limit	**Scrypt**	PoS	(1)
		2.2014		no limit	**SHA-256**	PoS	(2)
	BC	**3.2014**			**Scrypt**	PoS	(3)
Darkcoin	DRK	1.2014	150	**≈22m**	X11	**PoW/PoS**	(1)
	DRK	1.2014		**84m**	X11	**PoW**	(3)
Peercoin	PPC	8.2012	600	**no limit**	**Scrypt**	**PoW/PoS**	(1)
		8.2012		**no limit**	**SHA-256**	**PoW/PoS**	(2)
	PPC	8.2012	600	**20.5m**	**SHA-2-256**	**PoS**	(3)
Dogecoin	DOGE	12.2013	60	**100bn**	Scrypt	PoW	(1)
		12.2013		**no limit**	Scrypt	PoW	(2)
	DOGE	12.2013	60	**100bn**	Scrypt	PoW	(3)
CloakCoin	CLOAK	**6.2014**	60	**4.5m**	X13	**PoW/PoSA**	(1)
		5.2014	60	**7m**	X13	**PoS**	(3)

Table 5: Plausibility check of the DOACC dataset

Name	**Symbol**	**Inception**	**Blocktime (s)**	**Max. token issuance**	**Cryptographic Algorithm**	**Consensus Scheme**	**Source**
Monero	XMR	**4.2014**	60	≈18.4m	Cryptonight	*Egalitarian PoW*	(1)
		5.2014		18.4m	Cryptonight	*PoW*	(2)
	XMR	**4.2014**	60	18.4m	Cryptonight	*PoW*	(3)
Primecoin	XPM	7.2013	60	**2bn**	Primechain	*rPoW*	(1)
	XPM	7.2013	60	**≈3.3m**	Primechain	*PoW*	(3)
Zetacoin	ZET	**8.2014**	30	160m	SHA-256d	PoW	(1)
	ZET	**8.2013**	30	160m	SHA-256d	PoW	(3)
Vertcoin	VTC	**1.2014**	150	84m	Scrypt-N	PoW	(1)
	VTC	**1.2013**	150	84m	Scrypt-N	PoW	(3)
Coiledcoin	CLC	**10.2011**	120	no limit	SHA-256d	PoW	(1)
	CLC	**1.2012**			SHA-2-256	PoW	(3)
Liquidcoin	LQC	**1.2012**	300	no limit	Scrypt	PoW	(1)
	LQC	**6.2013**			Scrypt	PoW	(3)
Freicoin	FRC	**6.2012**	600	100m	SHA-256d	**PoW**	(1)
	FRC	**2.2011**	600	100m	SHA-2-256	**PoS**	(3)
Talkcoin	TAC	5.2014	20	no limit	NIST5	PoW	(1)
Anoncoin	ANC	**10.2013**	180	4.2m	Scrypt	PoW	(1)
	ANC	**6.2013**		4.2m	Scrypt	PoW	(3)
Reddcoin	RDD	*1.2014*	60	109,000m	Scrypt	PoW/PoSV	(1)
	RDD	*2.2014*	60	109,000m	Scrypt	PoS	(3)
Quarkcoin	QRK	7.2013	30	247m	Quark	PoW	(1)
	QRK	7.2013	30	247m	Quark	PoW	(3)
FlorinCoin	FLO	6.2013	40	16m	Scrypt	PoW	(1)
	FLO	6.2013	40	16m	Scrypt	PoW	(3)
CryptoNotecoin	n/a	7.2014	-	-	Cryptonight	Egalitarian PoW	(1)
	CNN	7.2014	90	**1.8446bn**	Cryptonight	PoW	(3)
	CNC	7.2014	30	**18.4m**	Cryptonight	PoW	(3)
duckNote	XDN	*6.2014*	240	≈ 8590m	Cryptonight	Egalitarian PoW	(1)

Table 5: Plausibility check of the DOACC dataset

Name	**Symbol**	**Inception**	**Blocktime (s)**	**Max. token issuance**	**Cryptographic Algorithm**	**Consensus Scheme**	**Source**
	XDN	*5.2014*	240	≈ 8.59bn	Cryptonight	PoW	(3)
Boolberry	BBR	4.2014	120	≈18.45m	Wild Keccak	Wild Keccak PoW	(1)
	BBR	4.2014	120	18.4m	SHA-3-256	PoW	(3)
Bytecoin	BCN	3.2014	120	*184.46bn*	Cryptonight	PoW	(1)
		7.2012		*184.47bn*	Cryptonight	PoW	(2)
	BCN	7.2012	120	*184.5bn*	Cryptonight	PoW	(3)
Feathercoin	FTC	4.2013	150	336m	Scrypt	PoW	(1)
	FTC	4.2013	150	336m	Scrypt	PoW	(3)
iXcoin	IXC	**8.2011**	600	21m	SHA-256d	PoW	(1)
	IXC	**5.2011**	600	21m	SHA-2-256	PoW	(3)
iocoin	IOC	8.2011	600	21m	SHA-256d	PoW	(1)
Novacoin	NVC	2.2013	600	**no limit**	Scrypt	**PoW/PoS**	(1)
	NVC	2.2013		**2bn**	Scrypt	**PoS**	(3)
Mastercoin	MST	6.2013	35	**≈18.2m**	Scrypt	**PoS**	(1)
	MST	6.2013		**619,478.50**	Scrypt	**PoW**	(3)
	MSC	7.2013	35	**180.2m**	SHA-2-256	**PoW**	(3)
Ripple		**9.2013**		100bn	**ECDSA**	*Byzantine Consensus*	(2)
	XRP	**5.2013**		100bn	**ripple**	*ripple*	(3)
Dashcoin		1.2014		**22m**	**X11**	**PoW/PoS**	(2)
	DSH	7.2014	120	**184.5bn**	**Cryptonight**	**PoW**	(3)
Stellar		8.2014		**no limit**	**undefined**	**Byzantine Consensus**	(2)
	STR	8.2014	5	**100bn**	**SHA-2-256**	**PoS**	(3)
Bitshares					undefined	undefined	(2)
NXT		11.2013		**1bn**	Curve25519, SHA-256	**PoS**	(2)
	NXT	11.2013		**no limit**		**PoW**	(3)
Ybcoin		6.2013		**3m**	Scrypt	**PoW/PoS**	(2)
	YBC	6.2013		**200m**	Scrypt-J	**PoS**	(3)

Table 5: Plausibility check of the DOACC dataset

Name	**Symbol**	**Inception**	**Blocktime (s)**	**Max. token issuance**	**Cryptographic Algorithm**	**Consensus Scheme**	**Source**
Counterparty		*1.2014*		2.65m	SHA-256	**PoB**	(2)
	XCP	*2.2014*			SHA-2-256	**PoW**	(3)
NuShares/NuBits		**8.2014**		1bn	**undefined**	PoS	(2)
Nushares	NUSH	**6.2014**		1bn	**SHA-2-256**	PoS	(3)
NuBits	NBT	**9.2014**			**SHA-256**	PoS	(3)
Paycoin		**12.2014**		**12.5m**	SHA-256	PoW/PoS	(2)
	PYC	**8.2013**	60	**30m**	**Scrypt**	**PoW**	(3)
	XPY	12.2014	60	12.5m	SHA-2-256	Pow/PoS	(3)
ARCHcoin		*9.2014*		*16.2m*	Scrypt	PoS	(2)
	ARCH	*8.2014*	60	*≈16.2m*	Scrypt	*PoS*	(3)
Monacoin		3.2014		**105.12m**	Scrypt	PoW	(2)
	MONA	1.2014	90	**168m**	Scrypt	PoW	(3)
Faircoin		**11.2014**		**no limit**	**undefined**	PoS	(2)
	FAIR	**3.2014**		**50m**	**Scrypt**	PoS	(3)
BitcoinDark		7.2014		22m	SHA-256	**PoW/PoS**	(2)
	BTCD	7.2014	60	22m	SHA-2-256	**PoS**	(3)

Sources: (1) Tarasiewicz and Newman (2015), (2) Farell (2015), (3) DOACC.
Minor differences highlighted by *italic*, major differences by **bold** font.