U.PORTO

FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

Blockchain governance: reducing trusted third parties with Decred Project

Marcelo de Almeida Martins

Dissertation

Master in Economics and Innovation Management

Supervised by

Maria Isabel Gonçalves da Mota Campos

Pedro José Ramos Moreira de Campos

2020

Acknowledgments

I would like to thank my mentors Isabel Mota e Pedro Campos for the guidance, support and for always aiming for the highest standards they knew I could reach, and to all professors at the Economics and Management School of University of Porto for the knowledge shared during the classes.

To my family, for the support given during the long hours of reading, script coding and debugging and the writing of this research.

To those who laid the foundations that brought us to a moment where freedom is not inconceivable anymore.

Abstract

Decred is a cryptocurrency with its own blockchain and has several similarities with Bitcoin but implements a governance model that resembles a company with thousands of shareholders. These stakeholders invest their coins, get the right to direct the project as they see fit and are rewarded for doing so. Everyone else not invested may use the coin as a means of exchange, trading it for goods or services or utilizing other services provided by the blockchain as the digital notary. This research investigates how Decred Project created its own version of money and implemented security measures to improve governance and remove trusted third parties from money issuance and e-voting. This topic is particularly relevant to those who want to investigate the use of blockchain technologies to improve governance and avoid the tyranny of the majority. In order to reach our goal, we use multi agent simulation and statistical modeling to verify in what extent price variance impacts investor's decision to keep Decred in their portfolio. We also tested the effect of the number of devices providing network security on price variance and verified that Decred is capable of providing a predictable, scarce, trustworthy digital asset.

JEL-codes: D20, D40, D72, E43, G12, G28, G38, O31

Keywords: governance, blockchain, decred, bitcoin, security, e-voting, proof-of-work, proof-of-stake, consensus, money, cryptoassets, cryptocurrencies

Resumo

Decred é uma criptomoeda que usa sua própria blockchain e possui várias semelhanças com o Bitcoin, mas implementa um modelo de governança que se assemelha a uma empresa com milhares de acionistas. Essas partes interessadas investem as suas moedas, obtêm o direito de conduzir o projeto como bem entenderem e são recompensadas por isso. Todos os demais que não são partes interessadas podem usar a moeda como meio de troca, trocando-a por bens ou serviços ou utilizando outros serviços fornecidos pela blockchain como o cartório digital. Esta pesquisa investiga como o Decred Project criou a sua própria versão de dinheiro e implementou medidas de segurança para melhorar a governança e remover terceiros de confiança da emissão de dinheiro e da votação eletrónica. Este tópico é particularmente relevante para aqueles que desejam investigar o uso de tecnologias de blockchain para melhorar a governança e evitar a tirania da maioria. Para atingir o nosso objetivo, usamos simulação multiagente e modelação estatística para verificar em que medida a variação de preços impacta a decisão do investidor de manter Decred no seu portfólio. Também testamos o efeito do número de dispositivos que fornecem segurança de rede sobre a variação de preço e verificamos que o Decred é capaz de fornecer um ativo digital previsível, escasso e confiável.

Códigos-JEL: D20, D40, D72, E43, G12, G28, G38, O31

Palavras-chave: governança, blockchain, decred, bitcoin, segurança, votação eletrónica, proof-of-work, proof-of-stake, consenso, dinheiro, criptoativos, criptomoedas

Contents

Acknowledgments ii

Abstract iii

Resumo iv

List of tables vi

List of figures vii

Glossary viii

1. Introduction 1

2. The technology behind the digital money 4

2.1. The chain of blocks 5

2.2. Blockchain and proof-of-work security 5

2.3. Incentives and inflation 6

2.4. Types of distributed ledgers 8

2.5. Bitcoin governance and consensus rules 10

2.6. Privacy and fungibility 12

2.7. Blockchain beyond the digital money 12

2.8. E-voting and new models of governance 13

3. Decred Project 16

3.1. Decred fundamentals and issuance 16

3.2. Blockchain security 17

3.3. On-chain and off-chain governance and decentralisation 23

4. Assessing blockchain governance 25

4.1. Methodology 25

4.2. Simulation: the InvalidationGame 25

4.3. Security increases opportunity cost 29

4.4. Testing governance hypotheses 38

4.5. OLS model and regression tree 53

4.6. Discussion of results 56

5. Conclusions and further research 60

Appendix 64

References 65

List of tables

Table 1 – Result of 100 000 90%/10% PoW simulated attacks 28
Table 2 – Result of 100 000 45%/55% PoW simulated attacks 29
Table 3 – Result of 100 000 45%/55% PoW + 70/30 PoS simulated attacks 29
Table 4 – Decred Proof-of-Work equipment and network hashpower 32
Table 5 – Decred Proof-of-Stake cost of (internal) attack 32
Table 6 – Total cost (PoW + PoS) of an attack against Decred on 10 Feb 2020 32
Table 7 – Bitcoin Proof-of-Work equipment and network hashpower on 10 Feb 2020 33
Table 8 – Total cost (PoW) of an attack against Bitcoin on 10 Feb 2020 33
Table 9 – Decred and Bitcoin supply and exchange rates on 10 Feb 2020 34
Table 10 – Decred and Bitcoin network size (hashpower) in Th/s on 10 Feb 2020 34
Table 11 – Most expensive blockchain to attack (external/internal) on 10 Feb 2020 34
Table 12 – Total cost of internal/internal attacks on 10 Feb 2020 35
Table 13 – Most expensive to attack (internal/internal) on 10 Feb 2020 36
Table 14 – Result of 100 000 49.99%/50.01% PoW simulated attacks 38
Table 15 – Result of 100 000 49.99%/50.01% PoW+PoS simulated attacks 38
Table 16 – Decred blockchain expected and observed results 39
Table 17 – Correlation between issued Decred coins and staked percentage 40
Table 18 – Correlation between Decred price and staked percentage 41
Table 19 – Correlation between Return in USD per ticket and staked percentage 43
Table 20 – Correlation between Decred price and network difficulty 44
Table 21 – Correlation between Bitcoin price and block mining difficulty 44
Table 22 – Correlation between Decred price (close) and privacy mix rate 45
Table 23 – Correlation between expected and observed Decred coin issuance 46
Table 24 – Decred ticket voters per block 47
Table 25 – Expected and observed cumulative Decred ticket vote chance 48
Table 26 – Correlation between expected and observed Decred ticket vote chance 48
Table 27 – Decred founders' and airdroppers' pre-mine issuance and expenditure 49
Table 28 – Correlation between Decred and Bitcoin prices (close) in USD 51
Table 29 – Observed average of turnout and approval percentage 53
Table 30 – OLS model: Decred Price (USD) as dependent variable 54
Table 31 – Regression Tree Rule Coverage 55
Table 32 – Regression Tree, Variable Importance Score 56

List of figures

Figure 1 – Proof-of-Work-based blockchain 6
Figure 2 – Bitcoin network right after the Bitcoin Cash "fork" 11
Figure 3 – Bitcoin and Decred estimated supply growth curves until June 2039 17
Figure 4 – Security curve created by PoW+PoS combined authentication 31
Figure 5 – Issued Decred coins and staked percentage 40
Figure 6 – Decred price and staked percentage (PoS security) 41
Figure 7 – Return in USD per ticket and staked percentage (PoS security) 42
Figure 8 – Decred price and network difficulty (PoW security) 43
Figure 9 – Bitcoin price and network difficulty (PoW security) 44
Figure 10 – Decred price variance and coins in private transactions 45
Figure 11 – Expected and observed Decred coin issuance 46
Figure 12 – Observed cumulative frequency of Decred ticket vote chance 48
Figure 13 – Decred founders' pre-mine expenditure of original transactions 50
Figure 14 – Decred and Bitcoin prices (close) in USD 51
Figure 15 – Votes by proposal in Decred Politeia voting platform (off-chain) 52
Figure 16 – Votes by proposal to change consensus rules (on-chain) 52
Figure 17 – Regression Tree with Hashrate and Staked Percentage 55

Glossary

ASIC device	Mining device used to perform repetitive hash calculations spending electricity to provide Proof-of-Work security to the blockchain
Confirmation	Each additional block added to the blockchain increases the difficulty for the attacker to erase that transaction
Cryptoasset	Digital representation of value and contract rights generated, stored and exchanged using blockchains, including coins (digital money) and tokens
Double-spending	Strategy that consists in spending a transaction previously spent in another block. "Double" is a misnomer because the attacker can re-spend the same transaction many times. It requires access to computation power to recreate a number of blocks until the block where that transaction was originally spent
Fork (blockchain)	An accidental or intentional change in protocol (or consensus mechanism) that creates another path forward
Proof-of-Work	Consensus mechanism that demands work from a party, generally processing time from a computer, to prevent spam and other forms of system or network abuse, which heavily depends on costly equipment and electricity use
Proof-of-Stake	Alternative consensus mechanism to provide security to a blockchain that uses other forms of validation

1. Introduction

"The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up 'toxic assets', The Times has learnt." (Elliott & Duncan, 2009). This is the second paragraph of the newspaper article whose title is written in the first mined block of Bitcoin blockchain, called 'Genesis block'. The actual message reads: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" and the article explains a new phase of a rescue plan as a development of the 2008 financial crisis (Bitcoin Community, 2017).

Banks' bail out started after the beginning of the crisis and that was not the first or the last time. In 1983, Margaret Thatcher explained that "there is no such thing as public money; there is only the taxpayers' money" (Thatcher, 1983). Actually, there is also the creation of new money when central banks perform a process called 'Quantitative Easing' (QE) (Bank of England, 2019), but this one was huge, unprecedented and highly impacted the value of money, exchange rates, taxation and fiscal policies, and consequently, the taxpayers' money. A decade after the crisis, bankers and CEOs from those private institutions moved on, leaving their 'troubled assets' and debt behind for someone else to pay. (Wall Street Journal, 2018). "That 'someone else' is you.", Ms Thatcher would certainly add. That was not the first time, or the last[1], that Central Banks bought 'junk' bonds[2].

Investment and commercial banks, mortgage lenders, insurance companies, and savings and loan associations exposed customer's assets by taking more risk than they could afford to and covered their losses with new money, although not all QEs are fully financed by money creation. The world became very inventive in this decade of entrepreneurship, innovation, unicorns and taxpayers' money. Innovation programmes are the new "free lunch". Now the 'investors' sign up for no-reimbursable money, taking advantage of innovation policies that reserved to the state the role of entrepreneurship. There is one difference in *modus operandi*: the banks were placing bets first and having the government covering their losses (or not) after the fact; now they get the free money first, and if the initiative sinks, they are already covered. Entrepreneurship and innovation without risk. It is

[1] "ECB: Our response to the coronavirus pandemic", available at https://www.ecb.europa.eu/home/search/coronavirus/html/index.en.html, last accessed 14 July 2020.
[2] "ECB predicted to beef up asset purchases with shift into 'junk' bonds", available at https://www.ft.com/content/41b3d01d-029b-469a-be4b-8b1967455472, last accessed 14 July 2020.

necessary to quote Ms Thatcher one more time to remind the taxpayers that it would be very pleasant to say "(…) 'spend more on this, expand more on that.' We all have our favourite causes—I know I do. But someone has to add up the figures. Every business has to do it, every housewife has to do it, every Government should do it" (Thatcher, 1983).

In 2019, the European Parliament decided to add up the figures in a report with the warnings that the different supervisory authorities have issued, including the market developments and key financial stability risks that show that "leveraged finance, comprised of high-yield bond and leveraged loans, has since the global financial crisis approximately doubled in size both in the US and in the EU, though in absolute terms the US exposure is much higher." (European Parliament, 2019).

It is unlikely that someone with the knowledge of economics and cryptography as demonstrated by Satoshi Nakamoto in his paper[3] and creating a cryptocurrency (or digital money) would make such an allusion by chance. One may interpret that Bitcoin is also an attempt to create a sound notion of money, but the paper starts with a simpler statement, that "commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments." (Nakamoto, 2008, p. 1).

Besides cryptocurrencies, the technologies behind the blockchain allow for a secure transfer of digital assets, or analogue assets anchored in the blockchain, between "two willing parties (…) without the need for a trusted third party" (Nakamoto, 2008, p. 1). Blockchains can also be used as timestamping machines for system logs and digital notaries, distributed databases for voting platforms and to authenticate users, messages and digital assets.

This research investigates how Decred Project, a cryptocurrency project, created its own version of money and implemented security measures to improve governance and remove trusted third parties from money issuance and e-voting. This topic is particularly relevant to those who want to investigate the use of blockchain technologies to improve governance and avoid the tyranny of the majority.

In order to reach our goal, we use multi agent simulation and parametric tests to answer the following questions: could price variance impact investor's decision to keep Decred in their portfolio? Could the number of devices providing network security impact price variance? Is Decred capable of providing a predictable, scarce, trustworthy digital asset?

[3] Available at https://nakamotoinstitute.org/bitcoin/, last accessed 06 June 2020.

Following this introduction, the second chapter starts with a brief explanation of the technologies behind the blockchain, the governance of money and the use of blockchains for public governance. The third chapter introduces Decred Project, incentives to launch attacks against blockchain to obtain profit, how Decred improves the governance of consensus rules, funding and the minimisation of attacks. Chapter 4 presents the findings of this research using simulations and statistical hypothesis test. Finally, the fifth chapter addresses remaining unsolved questions by the governance model implemented with the use of blockchains.

2. The technology behind the digital money

In the last decades researchers have been trying to digitally replicate the use and exchange values[4] of money, as well as its currency properties: fungibility, scarcity, divisibility, transferability and durability (Menger, 2009).

But money itself must be understood before the introduction of the digital money and blockchains. Menger (2009) defines money as the commodity of commodities because "certain commodities came to be money quite naturally, as the result of economic relationships that were independent of the power of the state. (…) Money is not the product of an agreement on the part of economizing men nor the product of legislative acts. No one invented it. As economizing individuals in social situations became increasingly aware of their economic interest, they everywhere attained the simple knowledge that surrendering less saleable commodities for others of greater saleability brings them substantially closer to the attainment of their specific economic purposes" (Menger, 2007, p. 262). Without money, "specialization of function and division of labor could not go very far if we had to continue to rely on the barter of product for product. In consequence, money has been introduced as a means of facilitating exchange, and of enabling the acts of purchase and of sale to be separated into two parts" (Friedman, 2002, p. 14).

When it comes to currency, the medium of exchange, Hayek points that "the genuineness of metallic money could be ascertained only by a difficult process of assaying, for which the ordinary person had neither the skill nor the equipment, a strong case could be made for guaranteeing the fineness of the coins by the stamp of some generally recognised authority which, outside the great commercial centres, could be only the government". Then Hayek reaches the problem of power imbalance when he argues that "it is evident that, as coinage spread, governments everywhere soon discovered that the exclusive right of coinage was a most important instrument of power as well as an attractive source of gain [...] at least so long as people had no alternative but to use the money they provided. During the Middle Ages, however, the superstition arose that it was the act of government that conferred the value upon the money" (Hayek, 1990, pp. 29, 30).

---

[4] Menger explains that "Use value, therefore, is the importance that goods acquire for us because they *directly* assure us the satisfaction of needs that would not be provided for if we did not have the goods at our command. Exchange value is the importance that goods acquire for us because their possession assures the same result *indirectly*." (Menger, 2007)

In 1976, Hayek foresaw the creation of private money: "the question at once arises whether it would not be equally desirable to do away altogether with the monopoly of government supplying money and to allow private enterprise to supply the public with other media of exchange it may prefer." (Hayek, 1990, p. 26).

2.1. The chain of blocks

The blockchain is a distributed ledger used to securely store transactions in a network of participating nodes, transparent to every node. Consensus rules validate the transactions before they are added to the blocks, which are secured by a distributed timestamp server proving their existence and reinforcing the ones before them (Nakamoto, 2008).

A transaction is a chain of digital signatures[5]. Digital signatures depend on a pair of keys for each owner. The owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner. New transactions are broadcast to all nodes, then collected into blocks. To avoid double-spend attempts, the earliest transaction is the one that counts, otherwise a trusted central authority would be necessary (Nakamoto, 2008).

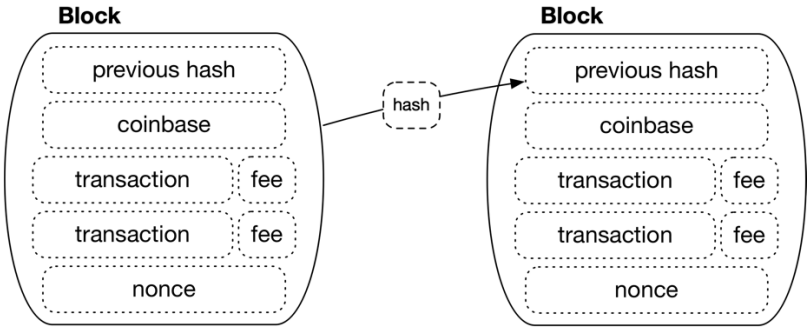
2.2. Blockchain and proof-of-work security

With Bitcoin[6] everyone can be in control of their own money, not the trusted third party (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016). To stay in control, the user must keep the coins in their 'wallet'. The 'wallet' is a reference to the pair of keys previously introduced, specifically the private key, the one that signs the transactions and must be kept secret. The private key is usually referred as the 'seed'[7], a set of mnemonic words where each one represents part of the key. If the user leaves their coins in an exchange platform, a broker, they might go bankrupt or just vanish with the user's Money (ibidem).

Proof-of-Work maintains blockchain security by creating a hash of the previous block and inserting it into the next. For a hash to be valid it must have a number of leading binary zeroes predetermined by the algorithm. If the hash is invalid, the miner increases the 'nonce', 'number used only once', and tries again. The more leading zeroes the algorithm requires, the harder it is. Figure 1 shows how the blocks are connected creating a blockchain.

[5] A brief notion of cryptography: https://stakey.club/en/a-brief-notion-of-cryptography/, last accessed 06 June 2020.
[6] Learn more about Bitcoin at https://en.bitcoin.it/wiki/Main_Page, last accessed 06 June 2020.
[7] PGP word list: https://en.wikipedia.org/wiki/PGP_word_list, last accessed 06 June 2020.

Figure 1 – Proof-of-Work-based blockchain



Source: own elaboration

Proof-of-work is essentially one-CPU-one-vote. The longest chain has the greatest proof-of-work effort invested in it, representing the decision of the majority. As long as the majority of CPU power is controlled by honest nodes, the honest chain will be the longest one, surpassing other chains. The longer the chain the more secure the previous blocks become, because exponential work would be necessary to recreate the chain from the point where an adversary wants to make an arbitrary change, catch up and surpass the honest chain.

Miners may pull resources together and coopete, cooperating in a pool of miners and competing with other pools to find the hash that validates the block. The incentives are shared in the pool according to the processing capacity of each miner (Eyal, 2015).

Open source software also contributes a great measure to security, transparency, auditability, replication of code and interoperability.

2.3. Incentives and inflation

Mineable cryptocurrencies create money by issuing new coins. The first entry in the block is called 'coinbase' and it creates and sends the coins to an address chosen by the miner. This reward is the incentive for the work on the block, spending electricity on the processing and wearing out the machines. To compensate increases in hardware power and new miners joining the competition, difficulty is adjusted by a moving average targeting an average number of blocks per hour. Machines lose their usefulness more quickly when difficulty increases leading to a competition in terms of fixed costs (space rent and cost of machines and cooling equipment) and efficiency of the machines (cost of electricity per billions of hashes per second and cooling equipment).

The incentives can also be funded with transaction fees because the user signing the transaction decides if the miner will get a fee for the processing work. On the other hand, the miner includes in his block the transactions with higher fees because he wants to maximise his profit. The fees are important to select which transactions will be mined and to reduce transaction spam (Nakamoto, 2008).

Inflation in a blockchain is limited to the creation of new coins and is a predictable process managed by the consensus rules of the network. Coin price reflects the expectation the participants have about the utility of the network and the creation of new money. For Hayek, the imperfect gold standard "had three very important advantages: it created in effect an international currency without submitting national monetary policy to the decisions of an international authority; it made monetary policy in a great measure automatic and thereby predictable; and the changes in the supply of basic money which its mechanism secured were on the whole in the right direction" (Hayek, 2009, p. 41). So, gold had no governance issues, was predictable and its production was stimulated or discouraged according to its value. It is also true for mineable cryptocurrencies.

The source of money has been a problem for a very long time. In 1983, Margaret Thatcher made a warning that hit a great part of the problem. She said: "Let us never forget this fundamental truth: the State has no source of money other than money which people earn themselves. If the State wishes to spend more it can do so only by borrowing your savings or by taxing you more" (Thatcher, 1983). But Ms Thatcher did not mention that the government may also create new money out of thin air, the 'Quantitative Easing', because it controls the supply of money (Bank of England, 2019). Friedman explained the difference in his key propositions of monetarism. He wrote that "Government spending may or may not be inflationary. It clearly will be inflationary if it is financed by creating money, that is, by printing currency or creating bank deposits", not the case of borrowing or taxation (Friedman & Goodhart, 2003, p. 86). It means that the creation of new money devalues the currency, and this is the reason for being one of the most important consensus rules and the basis of the risk-reward Proof-of-Work (PoW) mining.

Hayek also flagged the control of money supply when he wrote that "a money deliberately controlled in supply by an agency whose self-interest forced it to satisfy the wishes of the users might be the best. A money regulated to satisfy the demands of group interests is bound to be the worst possible. (…) The government monopoly of the issue of money was bad enough so long as metallic money predominated. But it became an unrelieved

calamity since paper money (or other token money), which can provide the best and the worst money, came under political control" (Hayek, 1990, p. 31).

When it comes to paper money, the fiat currency becomes a technical monopoly. Competition will not provide an effective limit because the private issuer wants to issue more currency until the market value of the additional currency equals the cost of the paper where it is printed. The government tasks then are to set an external limit to the amount of money and to prevent counterfeiting (Friedman, 1960).

But there is the agency problem, that appears on Hayek's argument: "There is no reason to doubt that private enterprise would, if permitted, have been capable of providing as good and at least as trustworthy coins." But, "since the function of government in issuing money is no longer one of merely certifying the weight and fineness of a certain piece of metal, but involves a deliberate determination of the quantity of money to be issued, governments have become wholly inadequate for the task and, it can be said without qualifications, have incessantly and everywhere abused their trust to defraud the people" (Hayek, 1990, pp. 25, 30).

Put this way, to provide 'good and trustworthy coins' that satisfy the wishes of its users, issued in a predictable manner and according to its value, the private enterprise needs good governance, that comes with good consensus rules for money issuance and payment processing, topic that will be connected in the following sections.

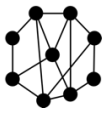
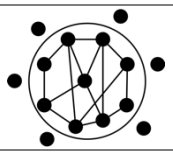
2.4. Types of distributed ledgers

Blockchain architectures can be categorised regarding the openness of transaction validation (validate/commit) and the openness of participation (read/write) in the transactions (European Commission, 2019). The right governance architecture is paramount to deliver the freedom and power the users demand:

- Permissionless: anyone with the right hardware can validate or commit transactions.
- Permissioned: only a number of selected nodes can validate or commit transactions.
- Public: anyone can participate in transacting using the protocol.
- Private: only selected participants can participate in transacting using the protocol.

Table 1 shows these types of blockchain architectures, their common use cases (or prospects) found in the market and what a network with such architecture looks like.

Table 1 – Blockchain archetypes

Blockchain type	Characteristics	Use cases	Visualisation
Public permissionless blockchains	Everyone can participate in the consensus mechanism. Everyone in the world is able to transact and see the full transaction log	Bitcoin, Decred, Litecoin	
Public permissioned blockchains	Everyone is able to transact and see the transaction log, but only restricted nodes can participate in the consensus mechanism	Ripple, Libra	
Private permissioned blockchains	Restricts both the ability to transact and view the transaction log to only the participating nodes in the system, and the owner of the blockchain is able to determine who can participate in the system and which nodes can participate in the consensus mechanism	Rubix, Hyperledger	
Private permissionless blockchains	Restrictions to transact and see the transaction log, but the consensus mechanism is open to anyone	(partially) Exonum	

Source: Modified from Table 2. Blockchain archetypes (European Commission, 2019)

The black dots are the validating nodes, meaning that they are able to validate the transactions in the network and participate in the consensus mechanism. The white dots represent participants in the network in the sense that they are able to transact, but they are not able to participate in the validation or in the consensus mechanisms. The ring indicates that only the nodes within the ring can see the transaction history. The visualisations without a ring mean that everyone with a connection to the Internet is able to see the transaction history of the blockchain (European Commission, 2019).

Among the permissioned blockchains in production, the one that caught everyone's attention is Facebook Libra. Libra claims to provide digital currency, but its whitepaper shows an intention to provide digital banking instead. The network is not open to any volunteer wishing to co-participate and help secure the blocks. To be an associate, the firm must buy voting rights, where USD 10 000 000 gives the rights of one vote (Facebook, 2019).

The Libra Reserve management will execute the Reserve Management Policy, which includes overseeing the "process of minting and burning Libra". As fiat money enters the economy, the reserve grows, the association mints Libra accordingly, and the reserve is

invested in low-risk and high-liquidity assets. Third-party liquidity providers will be allowed to exchange Libra for assets in the reserve (Facebook, 2019). It is very close to what Hayek envisioned in a time without the technology to remove the trusted third party, when he wrote that he would call institutions free to issue notes as simply 'banks', or 'issue banks' and "would announce the issue of non-interest bearing certificates or notes, and the readiness to open current cheque accounts, in terms of a unit" (Hayek, 1990, p. 46).

The Libra Network management will have the responsibility for the definition of the "process for managing the Libra protocol specification source control repository, including the process for reviewing and accepting changes to the protocol" and the rights to "explore permissionless blockchain technologies, and recommend to the board and council paths for transition to such technology" although such transition may never happen. The Libra council will publish recommendations suggesting the change of rules that will result in a 'hard fork', allowing the council to propose breaking changes to the Libra protocol (Facebook, 2019).

In a permissioned network, like Libra, the entity controlling the majority of nodes can freeze accounts, block payments and other messages. In permissionless networks, like Bitcoin and Decred, the majority of nodes decides the consensus rules and the acceptable transactions. As long as the honest nodes keep the longest chain, the network does not depend on a trusted third party, as shown in the next section.

2.5. Bitcoin governance and consensus rules

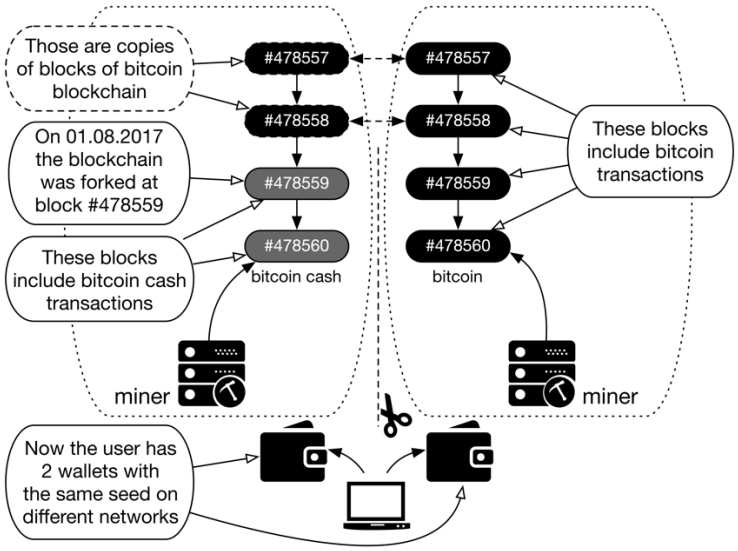
One of the definitions given by Rhodes (2007) to network governance is "game-like interactions, rooted in trust and regulated by rules of the game negotiated and agreed by network participants". Regarding public administration and public policy, he further explains that the "literature on governance explores how the informal authority of networks supplements and supplants the formal authority of government. It explores the limits to the state and seeks to develop a more diverse view of state authority and its exercise." (Rhodes, 2007, p. 4). This section approaches governance from a private perspective, but the following sections will also approach the public governance.

In a peer-to-peer network blocks are broadcasted and may not reach all nodes. Nodes consider the longest chain as the valid one and will work to increase it. If a node receives two different blocks, they work on the first, keeping the other in case it becomes the longer chain. Not all nodes are miners, only those that work to extend the longer chain by validating the blocks. Other nodes just keep a copy of the distributed ledger (Nakamoto, 2008).

In a decentralised network, where nodes do not know each other, changes in consensus rules, like the block size, happen through block signalling. Miners use online messaging boards to agree on a binary signal to be carried inside blocks in a range, looking to build majority. In case of majority, the changes are implemented and kept in the longest chain, thus the time and electricity spent will be rewarded (Nakamoto, 2008).

The minority must choose to accept the majority's changes or 'hard fork'. Because the nodes keep a copy of the blockchain, they have all the history. A blockchain hard forking keeps the history of blocks and transactions until that point, but deliberately start working on a chain that will not be accepted by the majority because of its rules and characteristics, thus creating another network that will have its own utility value and coins that will have different market value and name. Bitcoin governance is solely based on proof-of-work as the decision-making tool and Figure 2 depicts a blockchain fork on Bitcoin network.

Figure 2 – Bitcoin network right after the Bitcoin Cash "fork"



Source: own elaboration

Blockchain governance may also be captured by the mining equipment producer, a player that has economic incentives to control how the blockchain rules should change, steering decisions towards its preferred direction. This is the case for Bitmain Technologies, a private Chinese company that dominates the ASIC-based cryptocurrency mining hardware industry, with approximately 75% of the global market share, and also the largest player in the mining pool services market. "Bitmain fully owns and operates two of the largest mining pools, AntPool and BTC.com, and is also the main investor in another large mining pool,

ViaBTC. Many of the other large mining pools are also business partners of Bitmain. (…) By acquiring a large share of the pool services market, the equipment producer has a disproportionate influence on the governance of the blockchain." (Ferreira, Li, & Nikolowa, 2019).

2.6. Privacy and fungibility

Considering the provisions in the General Data Protection Regulation (GDPR) for data minimisation, pseudonymisation and anonymisation, specifically article 5 (1), points (b) and (c), personal data shall be collected and processed with legitimate purposes and limited to what is necessary (European Parliament, 2016). At the same time, governments increase the processing of personal data to control political contributions, foreign donations, to fight terrorism, money laundering, and increase taxation and avoid money evasion. "Merchants must be wary of their customers, hassling them for more information than they would otherwise need" (Nakamoto, 2008, p. 1), because of regulations and to prevent frauds.

Blockchains allow the exchange of digital assets minimising or completely avoiding the processing of personal data by relying on public key cryptography to prevent frauds, which increasing privacy but reducing the control enforced on the individuals by the government. Privacy solutions involve running a local copy of the blockchain and also of the block explorer, a web application capable of graphically displaying blockchain data in human readable format, because web servers and applications can log IP addresses and allow the geolocation of users. Blockchain transactions can also be routed through the Tor network, also called 'deep web', an encrypted and log-free network of individuals, allowing for transactions, e-voting and political contributions in dictatorships and struggling countries. The mixing technologies coded in blockchains allow for the scrambling of transactions into smaller amounts, mixing several different inputs before they are output in a wallet, providing fungibility and significantly reducing the probability of identification.

2.7. Blockchain beyond the digital money

Although blockchains are usually related to digital money, the technology allows other applications like digital notary, transparent procurement and accountability and e-voting.

Identity and timestamping machine

In 2007, Estonia developed a blockchain technology that "makes it impossible to change the data already on the blockchain." With timestamping, "history cannot be rewritten by anybody and the authenticity of the electronic data can be mathematically proven." Timestamping works by creating a hash of an information an anchoring this hash into the blockchain. This way anyone can prove that an information or document already existed at some point in time, like a digital notary. Estonia claims that hackers, system administrators, and not even government itself could untraceably manipulate the data (Enterprise Estonia, 2019).

Government procurement and innovation programmes

Fraud and abuse of taxpayers' money in government procurement and innovation programmes are common and it is not possible to determine how much taxpayers' money is wasted every year. A 2018 OECD report shows that 42% of the employees of SOEs (State-Owned Enterprises) participating in a survey answered that corrupt or irregular practices took place in their company in the previous three years. Because SOEs account for approximately 22% of the world's largest enterprises, this problem cannot be understated (OECD, 2018). It continues explaining that the greatest obstacles facing SOEs are related to human behaviour and relationships. The first three obstacles in order of appearance are: a lack of a culture of integrity in the political and public sector; a lack of awareness among employees of the need for, or priority placed on, integrity; and opportunistic behaviour of individuals (OECD, 2018).

Transparency minimises the problem of information asymmetry, but it can't solve the agency problem or reduce conflicts of interests and power imbalances created by the human behaviour. For these problems, e-voting might be helpful.

2.8. E-voting and new models of governance

Power imbalances and information asymmetries between governments and citizens have historically led to profound social inequality and hierarchical power structures, often making it an arduous task to achieve non-dominating ideals. Corrupt governments and dictatorships can always use the system and rules against the citizens: "voting rules can intensify existing risks in the system that include the complexity of voting rules, the cost of voting, the limited hours of in-person voting, outdated voting machines, voter registration

problems, challenges with mail-in voting, delays in counting ballots and the potential for administrative errors that invalidate or – perhaps even worse – indicate a vote for a candidate other than the one the voter intended". Some of these problems can be mitigated with blockchain technology, because it maintains a timestamped immutable audit trail implementing checks and balances throughout the electoral process. It is possible verify the vote, which decision was taken and when, without linking a voting transaction to a particular voter (Johnson, 2019, p. 343).

Public and private governance depend on choices like direct versus representative democracy. Public governance depends on locally provided public goods (funded by a general tax paid by residents) and positive cross-boundary externalities. The preferences for public consumption and higher taxation depend on the capacity of the participant in free-riding other regions or participants. In the case of private governance, it depends on the private treasury, how it is funded and what it funds (Redoano & Scharf, 2004).

Blockchain-based governance can solve and replace centralised organisations and the problem of scale, where the State and representative democracy have been a solution so far, used to reach consensus and coordination between heterogeneous or distant groups of people, bridging the gap for mutual interactions. But governments are exposed to risks like lack of transparency, corruption, regulatory capture, misuse of power and authoritarianism, due to concentration of power, which leads to another problem: 'Quis custodiet ipsos custodes?' (Who will watch the watchmen?) (Atzori, 2015, p. 6).

As part of an anti-government phenomenon in Western democracies during the last decade, public governance has evolved to become more collaborative, decentralised and multi-stakeholder to "address the growing need to experiment an entrepreneurial model of leadership, finding innovative solutions to the mismanagement of State and bureaucracy across the traditional organizational and institutional boundaries" (Atzori, 2015, p. 13). Several countries are already using blockchain-based solutions to improve governance and voting trust:

Switzerland

The issuance of a blockchain-based government identity, certified by the City of Zug, started on 15 November 2017 and is called uPort. The app links a unique and unchangeable crypto address to the local user wallet. It aimed to expand its reach to other public services, like e-voting, bike renting, book borrowing, tax declarations or parking payments (European

Commission, 2019). The e-voting trial started on 25 June 2018 and was a success, involving citizens that put their voices forward in a consultative vote via smartphone on an invented issue (Meyer, 2018).

Estonia

The Estonian blockchain records the ownership of securities as reported by the Central Securities Depository (CSD). The system issues voting right assets and voting token assets for each shareholder. Voting tokens (Proof-of-Stake mining) can cast their votes on meeting agenda items if the tokens own voting rights (Nasdaq, 2017).

Thailand

In a live e-voting process held from 1-9 November 2018, Thailand's Democrat Party elect its leaders in a primary election and became the first political party to use blockchain technology to allow more than 120 000 party faithful to cast their votes in a transparent way (Nasdaq, 2018).

Brazil

VotoLegal app used Decred blockchain not to record votes but to register campaign donations and keep candidates accountable, tracking the donation figures and who the donor was (AppCívico, 2018). Decred Project will be inquired in the next section.

3. Decred Project

Decred is an open, progressive, and self-funding cryptocurrency with a system of community-based governance integrated into its blockchain. Decred is bound by a set of rules, which include guiding principles, a system of governance – Politeia – and a funding mechanism – the network fund (Decred Project, 2016).

3.1. Decred fundamentals and issuance

Decred blockchain server (dcrd) is a fork from Bitcoin blockchain server (btcd) from btcsuite Bitcoin package, created by Decred developers previously to Decred existence. Source code forking is different from blockchain forking, depicted in Figure 2 on section 2.5. A source code fork means that a copy of the original code was made (Martins, 2018).

Decred issuance

On 08 Feb 2016, on block #1, 1 680 000 DCR were pre-mined: 840 000 DCRs (50%) were distributed among developers as a form of payment and the other 840 000 were distributed via airdrop, with 282.63795424 DCR sent to each one of 2 972 email addresses who subscribed to the airdrop list, a form of distribution that developers created so that since the beginning there would be a circulation of DCRs (supply and demand), diluting the participation of the initial developers (Martins, 2018). Equation 3.1 shows how total Decred issuance is calculated. On Decred creation, on 08 Feb 2016, each mined block could reward the participants (PoW and PoS miners and the treasury) with a maximum total of 31.19582664 DCR. After every 6 144 blocks, the issuance is exponentially reduced a factor of $(100/101)^n$, a process repeated 400 times until June 2039. By this date, this issuance cycle, added to the initial 1 680 000 pre-mined DCRs, is supposed to issue[8] an estimated amount of 20 638 308 DCRs (Martins, 2018).

$$1\,680\,000 + \sum_{n=0}^{399} 6\,144\ x\ 31.19582664\ \left(\frac{100}{101}\right)^n = 20\,638\,308.20752631 \qquad (3.1)$$

Source: (Martins, 2018)

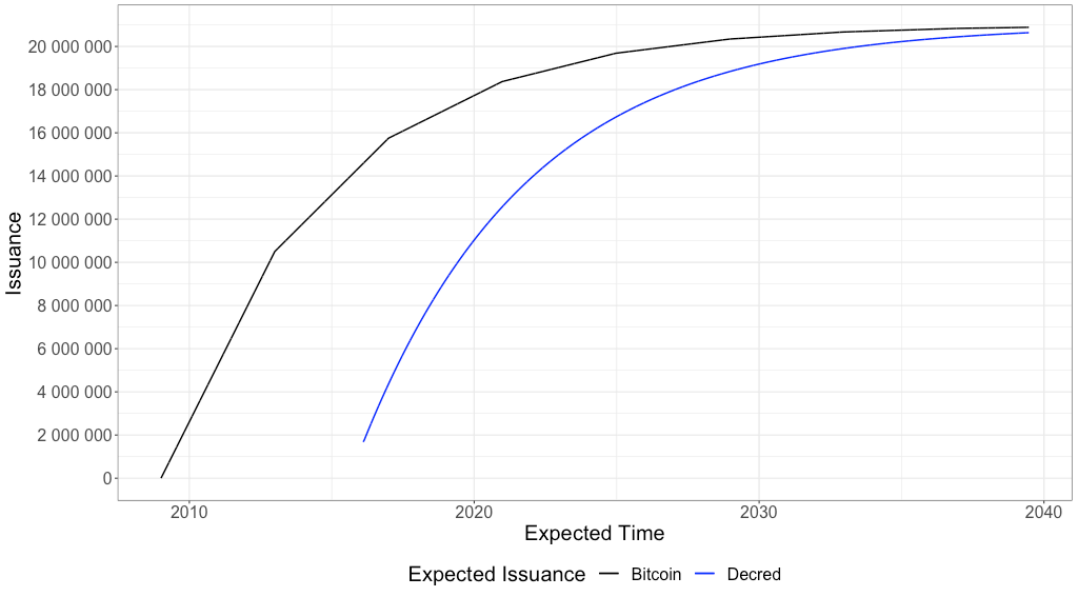
[8] Available at https://docs.decred.org/advanced/issuance/, last accessed 10 July 2020.

Bitcoin and Decred will issue each one almost 21M coins in their blockchains, but estimates show that Decred will have issued all of its coins by September 2120, with an upper supply limit of 20 999 999.99800912, while Bitcoin will still be 'printing money' until 2140. Equation 3.1 shows an estimate for Decred after reducing its block reward 400 times, approximately every 21.33 days, while Bitcoin takes almost 4 years to reduce by half its issuance of money (every 210 000 blocks, as shown in equation 3.2 below), an event called 'halving' which has a great impact in crypto financial markets. Figure 3 shows a comparison between their supply growth curves (based on equations 3.1 and 3.2) and it is noticeable that Decred curve has a smoother reduction in its issuance.

$$\sum_{n=0}^{32} 210\,000\ x\ \frac{50}{2^n} = 20\,999\,999.97690000 \qquad (3.2)$$

Source: Modified from (Bitcoin Community, 2017)

Figure 3 – Bitcoin and Decred estimated supply growth curves until June 2039



Source: own elaboration

3.2. Blockchain security

There is no good governance without security. If the rules are vague or cannot be correctly enforced, if the consensus mechanism does not prevent actors from playing a dominant role, if the voting system is insecure or if there is no transparency, accountability, and anonymity, it is not possible to guarantee the integrity of electoral outcomes (Johnson,

2019). Without the correct checks and balances there is no governance or democracy. Also, knowing that there is 'no free lunch' and that running a distributed ledger system that helps reduce uncertainties and voting irregularities comes with a cost, the incentives must be clear and well-balanced to avoid dominance and public distrust. This is why scarcity (money issuance and inflation) and rewards are central issues, especially for public permissionless blockchains.

Proof-of-Work/Proof-of-Stake (PoW/PoS) hybrid mining

PoW/PoS hybrid mining is critical to the understanding of the security mechanism of Decred blockchain, so a brief introduction is necessary. For consensus mechanisms that use only PoW a number of issues may arise, like denial of service via mining empty or artificially small blocks; censorship by ignoring certain transactions or addresses; and miners blocking or forcing consensus changes. There are disputes between miners, who want to centralize mining to increase their decision-making power and their profit to the detriment of the ecosystem; large companies and brokers, who seek to improve business-supporting features to increase their profit; and users and investors, who use the network for store of value and means of exchange. PoW mining can be seen as a single authentication factor for the consensus system, where it is usually executed by a small number of entities that do not necessarily represent the rest of the system participants. Although this process is fundamentally decentralized, practical issues lead the PoW mining process to be very centralized, similar to trusted third-party systems, like banks (Martins, 2018).

PoS mining creates a second-factor authentication, validating PoW mining decisions. Long-term stakeholders, those who wish to keep the coins, can vote on proposed changes to the network and their tickets validate the blocks mined via PoW. PoW miners get 60% of block reward, PoS miners receive collectively 30% and the remaining 10% goes to the treasury, also called the 'network fund'. With PoS mining the coins are temporarily locked in the blockchain in exchange for tickets that have voting power.

The first phase involves a majority of PoW miners and PoS stakeholders upgrading their software to the latest version. For PoW, 95% of 1 000 last blocks must be in the latest version and for PoS, 75% of the votes in a 2 016-block interval must be the latest vote version (Decred Project, 2020). When the proposals are ready to be voted they show up at users' software and miners and investors can choose how they will vote when they mine a block, or their ticket is drawn.

A deterministic pseudorandom lottery mechanism draws 5 tickets every block. Tickets vote on the validity of the previous block and are rewarded (in DCRs). A minimum of 3 tickets is necessary to validate the block and they are rewarded only if they actually cast their vote. The coins remain locked for 20 days, on average, but it could take as long as 143 days and 0.5% of the tickets expire after 143 days and do not get to vote and be rewarded, although the coins are released back but the fee paid to buy the ticket is not returned. Every block can contain up to 20 ticket purchases and prices are adjusted on 288-block windows to reduce[9] the chance of large stakeholders buying huge amounts of tickets (Decred Project, 2020).

Network fund to reduce conflicts of interest

A source of funding is necessary to maintain a solid and steady development. This source of funding might be the developers, public donations or a private company and it makes a difference when assessing the possibility of conflict of interest, the agenda of each organisation and their objectives behind the funding.

Since 2014 entrepreneurs and scammers started using ICOs (Initial Coin Offering) to raise money to fund new cryptocurrency projects. It is estimated that 28.4 billion dollars were raised from January 2014 to August 2018. (Kalomeni, 2018). The term comes from the IPO (Initial Public Offering) and such projects suffer from conflicts of interest inherent to their funding model. "ICOs usually have two major problems: (1) on paper everything is possible; (2) to undertake is to build something first and then get the results, make a profit." (Martins, 2018). Several projects never came to life, others had only the first commit of code to the code repository and after the funds were raised, they were abandoned.

To avoid relying on outside sources and agendas, Decred Project chose not to ask for the taxpayers' money using innovation programmes nor started an ICO to be financed by third parties. Instead, Decred Project finances itself with 10% of every block reward.

PoW majority attack and the lack of 'skin in the game'

The majority attack, also called '51% hashpower attack', depends on an adversary being able to create blocks faster than the rest of the network (the honest nodes), maintaining

[9] PoS Voting General FAQ, questions 5 and 6, available at https://docs.decred.org/faq/proof-of-stake/general/, last accessed 14 July 2020.

the longest chain. The outcomes would be to create blocks without specific transactions allowing for the double-spending of a transaction previously spent by reversing the recent ledger history to defraud merchants, or carry out a denial-of-service attack by refusing to include transactions in the mined blocks, excluding participants from the network by denying them the ability to send or receive payments (Bentov, Lee, Mizhari, & Rosenfeld, 2014). This attack is feasible for wealthy adversaries and has great dependence on huge initial investment to acquire the mining equipment and on low fixed costs due to electricity and rent prices. Cloud-based attacks are not considered here because general purpose virtual machines do not calculate hashes efficiently as an ASIC mining device built for this specific purpose.

As stated in the previous section, a pure PoW system allows for bad decision-making: PoW miners can 'mine and sell', meaning that they can spend the reward in the next blocks or exchange it for fiat currency without being hurt in the long-term by the consequences of a bad decision made. With a pure PoW there is much less 'skin in the game', because miners can mine other coins that use the same PoW algorithm as their mining equipment.

Miners and the profit maximisation strategies

In Section 2 we explained that mining incentives can also be funded with transaction fees besides the block reward. To avoid the 'tragedy of the commons', a game theory problem where participants have an incentive to act selfishly to increase their own outcome in detriment of all other participants (Hardin, 1968), miners can select which transactions they will process based on the fees paid by the users. Otherwise, free riders would aim for no fee at all, which would reduce the incentives for miners to buy equipment and spend electricity validating the blocks, in the end reducing the number of participants and the security of the network, making everyone worse off than if they cooperated and paid their fees.

Each miner can select a minimum acceptable fee. They could cooperate to raise fees, but miners have an incentive to defect. Because mining is a capital-intensive business, and equipment prices, import taxes, building rents and electricity costs differ from place to place, miners operating with lower efficiency will have an incentive to accept lower fees in order to meet their point of equilibrium. If the miners select an excessively high fee, they may be left with only a handful of transactions and will have to bear the same processing costs to mine the block, so they have an incentive to choose the minimum acceptable fee that maximises their utility. During bear markets, when their coin exchange rate to fiat currency is even lower, they have to sell more coins to be able to break even. Wealthy miners operating with

higher efficiency have incentives to manipulate the markets and lower the coin value, and consequently the exchange rate, to drive other miners off the market by pushing their revenue below their fixed costs.

Pure Proof-of-Stake systems

Proof-of-Stake ledgers are based on the assumption that stakeholders will maintain the ledger's security because their stake will devaluate in case of distrust in the system. PoS attacks do not require initial investment in equipment and electricity costs. While PoW attacks may be noticed when an adversary publishes a block in the network competing with the honest nodes to form the longest chain, PoS attacks happen in silence, using private keys that control transactions to sign a block. The higher the stake (transactions or coins), more powerful is the attack (Bentov, Gabizon, & Mizrahi, 2016).

This 'silent attack', also called 'Costless Simulation', allows miners to perform a 'stake-grinding' attack, extending only blocks that will make them the signers of the next block and thus taking control of the blockchain or creating multiple blockchains because it is cheap to create 'history'. Because it is not possible to differentiate realtime from blocktime, new users cannot tell when those multiple versions of the blockchain were created: to them, all versions are true. Only existing nodes from before the attack would be able to distinguish those multiple versions of history (Poelstra, 2015).

Decred Project approach

Decred increases PoW security by adding PoS to the mining process. An attacker with a fraction of the tickets would require a number of times the hashpower of honest miners to take over the network. By comparison, an attacker that had the same hashpower of the honest nodes (50% of total hashpower) would still need also 50% of the tickets to successfully attack the network, which is a sizable 'skin in the game' for an attacker.

Theoretically, if the minority chain with only a small fraction of tickets had a number of times more hashpower, they could keep up with the majority chain although this is unrealistic because of the economic incentives. Spending a number of times more electricity to obtain the same outcome would turn the reward in 1/n (Collins, 2017).

Other attacks, like the Miner's Dilemma (Eyal, 2015), those perpetrated by governments, Denial-of-Service attacks, which are based on the isolation of honest nodes among dishonest nodes to facilitate double-spending, the Sybil attack (Eyal & Sirer, 2014),

where an adversary creates multiple identities or nodes, and incentives for miners not to propagate to other nodes the received transactions are out of the scope of this inquiry.

Karakostas et. al. tried to define the concept and measure the 'egalitarianism' of cryptocurrencies reward by evaluating Decred (PoW+PoS); Bitcoin, Litecoin, Ethereum, Monero (PoW); and the Ouroboros PoS algorithm from Cardano. They created a simulation[10] to evaluate minimum required investment size, coinbase rewards, electricity prices, block difficulty, ASIC device specifications and coin prices (Karakostas, Kiayias, Nasikas, & Zindros, 2019). Their findings show a result pointing that Proof-of-Stake blockchains are more 'egalitarian' in terms of minimum/multiple size of investment for a stakeholder.

For Decred, they conclude that "egalitarianism is harmed for capitals which are not multiples of ticket prices" but they did not account for Decred Ticket Splitting, which is currently in beta stage and allows multiple participants to buy a ticket spending a minimum of 5 DCRs (in contrast with ticket prices above 100 DCRs since January 2019). Voting rights "are assigned pseudorandomly to a single participant, based on the percentage of their contribution. i.e., if someone purchases 60% of a split ticket, they have a 60% chance of being selected as the voter for that ticket" (Decred Project, 2019). They argue that "perfect egalitarianism could in principle be achieved by making the ticket price approach 0", which in a 'one coin one vote' system would lead to a linear increase in votes and stakeholder power. In the end, they reach a conclusion that Ouroboros and Decred are more 'egalitarian' but they did not account for the previously discussed (in)security of pure Proof-of-Stake blockchains, like Ouroboros PoS algorithm from Cardano (Karakostas, Kiayias, Nasikas, & Zindros, 2019, p. 17).

Decred Privacy and Proof-of-Stake mining

Decred Privacy mechanism uses CoinShuffle++[11], a protocol used in the mixing process, which builds on top of the ticket purchasing transactions of PoS mining, allowing stakeholders to purchase tickets anonymously. Ticket purchases provide a steady flow of transactions that can be used to mix transaction inputs and completely anonymise the output addresses. Additional work is necessary to obfuscate transaction amounts, and this is why

[10] The source code is available at https://github.com/decrypto-org/egalitarianism, last accessed 27 June 2020.
[11] From "P2P Mixing and Unlinkable Bitcoin Transactions", available at https://eprint.iacr.org/2016/824.pdf, last accessed 06 June 2020.

smaller fixed denominations are used (Yocom-Piatt, 2019a). The ability to monitor the electoral process using a timestamped audit trail to verify the vote without identifying the voter can increase transparency and participation in the voting process (Johnson, 2019).

3.3. On-chain and off-chain governance and decentralisation

The decentralised nature of Bitcoin has already been challenged in the past in a block size dispute, where estimates showed that Chinese miners controlled 74.5% of the network through mining pools. In 2015, developer groups failed to reach consensus over the decision to increase the block size from 1MB to 8MB. While those in favour argued for scalability of the network, those against argued that it would be a huge security risk because it would exclude less powerful machines from handling the blockchain (De Filippi & Loveluck, 2016).

While on-chain governance involves rules and decision-making process encoded in the blockchain, off-chain governance involves all other decisions related to the development and management of a project (Reijers, Wuisman, Mannan, & De Filippi, 2018). Decred Project implements the well-known on-chain[12] governance, to maintain consensus rules[13], as well as an off-chain governance, using the Politeia governance platform and a timestamping client/server architecture.

Decred Timestamping

Timestamping is the base of the blockchain digital notary and of Politeia off-chain governance system and dcrtime is the client/server application that hashes the content of a file and anchors this hash in the blockchain, proving its existence at a point in time. If the selected file has already been hashed, dcrtime (frontend time client) will show information about that file. Otherwise, the file hash will be published in Decred blockchain in the next hour. Decred offers this functionality for free every hour at dcrtime (backend time server) website[14] and also provides the source code.

[12] Available at https://voting.decred.org/, last accessed 06 June 2020.
[13] Available at https://docs.decred.org/governance/consensus-rule-voting/overview/, last accessed 06 June 2020.
[14] Available at https://timestamp.decred.org/, last accessed 06 June 2020.

Politeia

Politeia[15] is the censorship-resistant blockchain-anchored public proposal system. Through Politeia anonymous users may propose changes to the development and management of the project, including initiatives to spend the network fund. They can use the platform to debate the proposals, but debates can take place anywhere on the Internet. Statistics[16] about proposals can be looked up on the block explorer. The platform and its proposal repository are open source and every proposal receives a token that can be used to prove censorship, in case an administrator needs to remove illegal or nonconforming content. Politeia uses dcrtime to timestamp a proposal and anchor it to the blockchain.

Decentralised Autonomous Organisation (DAO)

A Decentralised Autonomous Organisation (DAO) is a "code-based system with internal capital that lives on the blockchain and operates autonomously (…) through a set of code-based rules ("smart contracts") to automatically execute payments when certain conditions are met" (Reijers, Wuisman, Mannan, & De Filippi, 2018, pp. 5, 6).

Decred Project plans to create a DAO to enable direct sovereignty over the protocol for a truly decentralised organisation. A DAO can be implemented in two ways: through direct or delegated voting. Delegated voting is like representative democracy (with its well-known issues) and direct voting involves debating proposals, casting votes and living with the consequences of the decisions made. Through Politeia the individuals have a voice and participate in the DAO, having direct sovereignty (Yocom-Piatt, 2019b).

The next section will assess blockchain governance, including the mechanisms implemented by Decred Project to increase governance and security.

[15] Available at https://proposals.decred.org/, last accessed 06 June 2020.
[16] Available at https://dcrdata.decred.org/proposals, last accessed 06 June 2020.

4. Assessing blockchain governance

Blockchain security is paramount to implement good governance otherwise stakeholders' decisions could be reverted. A secure protocol depends on adequate blockchain architecture, secure hashing functions and cryptographic primitives, transparency, privacy and decision-making mechanisms. Good security controls must be cheap to implement and costly to attempt to bypass or violate as a way of deterring dishonest adversaries.

4.1. Methodology

This research uses publicly available data from Decred and Bitcoin blockchains between Feb 08, 2016 and Feb 10, 2020. For Decred, the data was obtained from PostgreSQL database used in dcrdata[17], the free, open source block explorer. For Bitcoin, the data was obtained from Blockchain.com. Price information in USD was obtained from Yahoo Finance[18,19]. For section 4.2, the probability distribution used inside the script was obtained from querying the above PostgreSQL database. For section 4.3, the calculations used data obtained from the sources above. For section 4.4, all data was obtained from dcrdata and Yahoo Finance and was processed using R.

Section 4.2 uses the InvalidationGame, a Python script developed for this analysis, to simulate PoW and PoW+PoS attacks with the intent to show the difference in time and cost of such attacks. Section 4.3 analyses the attacks from Capex and Opex perspective to understand how much does an attack cost in dollar figures. Section 4.4 analyses data from dcrdata database, testing several hypotheses to assess Decred governance (security, issuance predictability, scarcity, incentives, voting). Section 4.5 develops an OLS model and a regression tree and section 4.6 summarises the findings.

4.2. Simulation: the InvalidationGame

The security provided by the two-factor authentication mechanism of PoW+PoS implemented by Decred can be better understood in a simulation. For that purpose, it is developed the InvalidationGame[20], a Python script that simulates a double-spending attack

[17] dcrdata, available at https://github.com/decred/dcrdata, last accessed 16 July 2020.
[18] Bitcoin USD price, available at https://finance.yahoo.com/quote/BTC-USD/history?period1=1454716800&period2=1586131200&interval=1d&filter=history&frequency=1d
[19] Decred USD price, available at https://finance.yahoo.com/quote/DCR-USD/history?period1=1454716800&period2=1586131200&interval=1d&filter=history&frequency=1d
[20] InvalidationGame, https://github.com/mmartins000/invalidationgame, last accessed 31 May 2020.

to show the probability of success of an attack when perpetrated against a pure PoW blockchain and also against a PoW+PoS one. It is assumed to be a double-spending attack because attacks cost upfront money (PoW) and the adversary attacking the network must have economic incentives to execute the attack. A double-spending attack is an attempt to spend the same coin[21] more than once. The attacker would spend a coin in a regular transaction and then try to mine blocks that would exclude that transaction from the blockchain, creating a blockchain fork. The chain with more blocks, being 6 blocks a generally accepted number because of Bitcoin reference client, is the one considered the single source of truth because it is the result of the work of the majority of nodes (Bonneau, et al., 2015).

Other possible scenarios would be:

- the sabotage performed by wealthy adversaries, like governments;
- an adversary mining empty blocks

Stakeholders can withhold a miner's reward invalidating blocks even if the block conforms to the consensus rules of the network. This disincentivises bad behaviour such as miners mining empty blocks or attempting double-spending attacks. For double-spending attacks, two assumptions must be considered: first "we consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent." (Nakamoto, 2008, p. 7). The other is an opportunity cost because a greedy attacker with substantial hashpower would have to choose between trying to perform a double-spending attack or participating as an honest node and generate new coins. (Nakamoto, 2008, p. 4). The logic behind the InvalidationGame can be expressed by several functions that have been implemented based on the following algorithm pseudo code:

```
Main function:
    Run batch of simulations(sims)
```

[21] Actually, due to the ledger inner workings, the attacker tries to spend the same transaction more than once. A transaction corresponds to an amount of coins, like a check.

```
Run batch of simulations(sims):
    For each simulation:
        Calculate hashpower(hashpower percentages, stake percentages)
        Run simulation(number of simulation to run)

    Calculate validated and invalidated block averages
```

```
Calculate hashpower(hashpower percentages, stake percentages):
    For each adversary:
        Select random block IDs proportionate to hashpower percentage

    If this simulation involves PoS mining:
        Generate a pool of random tickets
        For each adversary:
            Select random tickets from the pool proportionate to stake percentages
            Remove selected tickets from the pool
```

```
Run simulation(number of simulation to run):
    While Calculate distance(number of simulation, number of current cycle) < 6:
        Mine block()
        For each adversary:
            Log mined blocks

    Calculate the number of mined blocks until 2- and 6-block distance were reached
    Calculate duration of the simulation
```

```
Mine block(number of simulation to run, cycle number):
    While no PoW winner found for this cycle:
        Select random block from a pool of blocks
        Verify which adversary has this random block in their block list
        Log the winner or winners
        If PoS mining:
            Draws how many tickets will be drawn based on historical proportions
            Draw the selected number of tickets
            Verify which adversary has each ticket
            Log the winner or winners
            If the same adversary won PoW and PoS, log a mined block (valid)
            Else log an invalid block (due to an attack)
```

```
Calculate distance(number of simulation to run, cycle number):
    Calculate the maximum distance between any two adversaries
    If calculated distance == 2 or 6:
        Log the number of blocks to reach this calculated distance
    Calculate probabilities of catching up for the lagging adversary
    Return calculated distance
```

Source: own elaboration

The results shown in Tables 1-3 come from the execution of the InvalidationGame and assume that A0 represents the honest adversaries while A1 represents an adversary trying to reverse a transaction (the double-spending attack), but it makes no difference to the calculations if the roles are inverted. Hashpower simulates the probability of mining a block while Stake simulates the percentage of PoS tickets. For all simulations it is assumed that the adversary just spent a transaction and started a double-spending attack.

Tables 1 and 2 show two scenarios: in the first, adversary A0 has 90% of hashpower and A1 has a small amount (10%), and in the second, adversary A1 has about the same hashpower (55%) as the honest nodes represented by A0 (45%). In the first scenario it took, in average, 3.2771 blocks for an adversary to have a 2-block advantage over the other and 7.8240 blocks in average for a 6-block advantage, when the simulation ended. In the second the numbers were 6.7431 and 38.4911 blocks for 2-block and 6-block advantage. The numbers are higher in the second scenario because the adversaries have almost the same probability of mining a block (45% against 55%), taking longer for them to establish the generally accepted advantage of 6 blocks over the other.

The 2-block advantage is shown in an article (Grunspan & Pérez-Marco, 2019) that tries to demonstrate that the double-spending attack where the attacker has a relative hashrate $0 < q < ½$ is already unfeasible much sooner than the generally acceptable 6-block confirmation because it (generally) becomes unprofitable in 2 blocks, leading to the ruin of the attacker. The last line of the simulation output informs that the losing adversary is forgoing a block reward in valid blocks by trying to double-spend. Another cost, not mentioned in the tables, is the 'cost of doing business', that is the cost related to working on a block and having an adversary successfully mine it (and get the block reward).

Table 1 – Result of 100 000 90%/10% PoW simulated attacks

Number of simulations: 100000		Average: 0.0012 seconds, Total: 00:19:54	
Adversary	Hashpower	Simulations won	Simulations won
A0	90.00%	98681	98.681&
A1	10.00%	1319	1.319%
On average, 2-block and 6-block advantage reached in: 3.2771 and 7.8240 blocks			
Attack cost, on average: 0.7486 PoW block reward			

Source: own elaboration

Table 2 – Result of 100 000 45%/55% PoW simulated attacks

Number of simulations: 100000			Average: 0.0110 seconds, Total: 00:35:50
Adversary	Hashpower	Simulations won	Simulations won
A0	45.00%	26270	26.27%
A1	55.00%	73730	73.73%
On average, 2-block and 6-block advantage reached in: 6.7431 and 38.4911 blocks			
Attack cost, on average: 22.3953 PoW block rewards			

Source: own elaboration

While Tables 1 and 2 show the result of attacks in pure PoW blockchains, Table 3 shows an attack on a PoW+PoS blockchain, where the honest nodes (A0) have 45% of hashpower and 70% of PoS tickets. Although the dishonest adversary (A1) has more hashpower, the honest nodes have more tickets and will not validate blocks that contain double-spending transactions.

Table 3 – Result of 100 000 45%/55% PoW + 70/30 PoS simulated attacks

Number of simulations: 100000					Average: 0.077 seconds, Total: 04:03:16	
Adversary	Hashpower	Stake	Sims won	Sims won	Avg Invalid Blocks	Avg Valid Blocks
A0	45.00%	70.00%	84122	84.122%	1.6495	7.8575
A1	55.00%	30.00%	15878	15.878%	9.7451	1.8594
On average, 2-block and 6-block advantage reached in: 3.8929 and 10.7169 blocks						
Attack cost, on average: 1.8594 PoW block rewards, due to PoS invalidation						

Source: own elaboration

Table 3 shows that A1 forgo rewards for 9.7451 blocks in average due to blocks that were invalidated by the honest nodes. But the cost is even higher: some blocks mined (PoW) and validated (PoS) by A1 were left in an unextended blockchain fork because the honest nodes were able to extend their own chain in z blocks, and such chain has no block mined by A1 since the attack began. Hence the adversary also forgoes rewards for 1.8594 validated blocks, in average.

4.3. Security increases opportunity cost

A strong authentication mechanism increases the cost of an attack, which can be measured in dollar figures. To perform an attack against a PoW blockchain the attacker must i) rent the equipment; or ii) buy the equipment and build/rent the facilities and only then start an attack by spending electricity. An attack against a PoW+PoS blockchain includes also the cost of owning the coins (or cryptoassets) and such attack may devalue those coins, increasing the risk for the attacker.

Attacks can be internal or external: internal attacks happen when miners decide to perform an attack using current equipment. Because there is no central registration authority, individual miners would have to meet in forums or mining pools to reach consensus on such attack. Mining pools themselves could also be considered adversaries in case they decide to use the PoW they command to attack networks. An adversary may also rent mining devices to perform a short-term attack on a number of blockchains supported by the cloud mining provider. In an internal attack there is no increase in the number of equipment or total hashpower of the network. An external attack assumes that an adversary buys new equipment, thus increasing the processing power of the network. The adversary must account for the rapid depreciation of such devices, not only when it comes to product lifespan but also because new devices will render these devices inefficient.

Hashpower is estimated as shown in equation 4.1, taking the network difficulty informed by the blockchain protocol and the block time in seconds (600 seconds for Bitcoin, 300 seconds for Decred). Network difficulty measures how difficult it is to find the hash for a block under a certain target to keep blocks being generated within a certain amount of time.

$$Network\ difficulty\ x\ \frac{2^{32}}{block\ time} = Hashpower \tag{4.1}$$

Source: (Bitcoin Community, 2017)

As previously explained in section 3.2, subsection 'Decred Project approach', an attacker would require a combination of tickets and hashpower to obtain enough power to revert blocks mined by the honest nodes. Equation 4.2 shows how to calculate the probability of an attacker holding a majority of selected tickets knowing that the attacker controls fraction y of the tickets in the pool. In Decred network N is always 5 because every block draws a maximum of 5 tickets and k is the number tickets between N tickets the attacker might have. The participation ratio p will be assumed to be 1 because in Decred a majority of voters is usually online (Table 24 in section 4.4 has the numbers). Equation 4.3 calculates how much hashpower the attacker would need as a multiplier of the honest adversaries' hashpower given that the attacker has a probability P(y) of having a majority of tickets drawn. Figure 4 shows the Security Curve as a result of the PoW+PoS authentication mechanism.

Probability of an attacker holding a majority of selected tickets (PoS)

$$P(y) = \sum_{k=0}^{k<N/2} \binom{N}{k} y^{N-k}((1-y)\,.p)^k \tag{4.2}$$

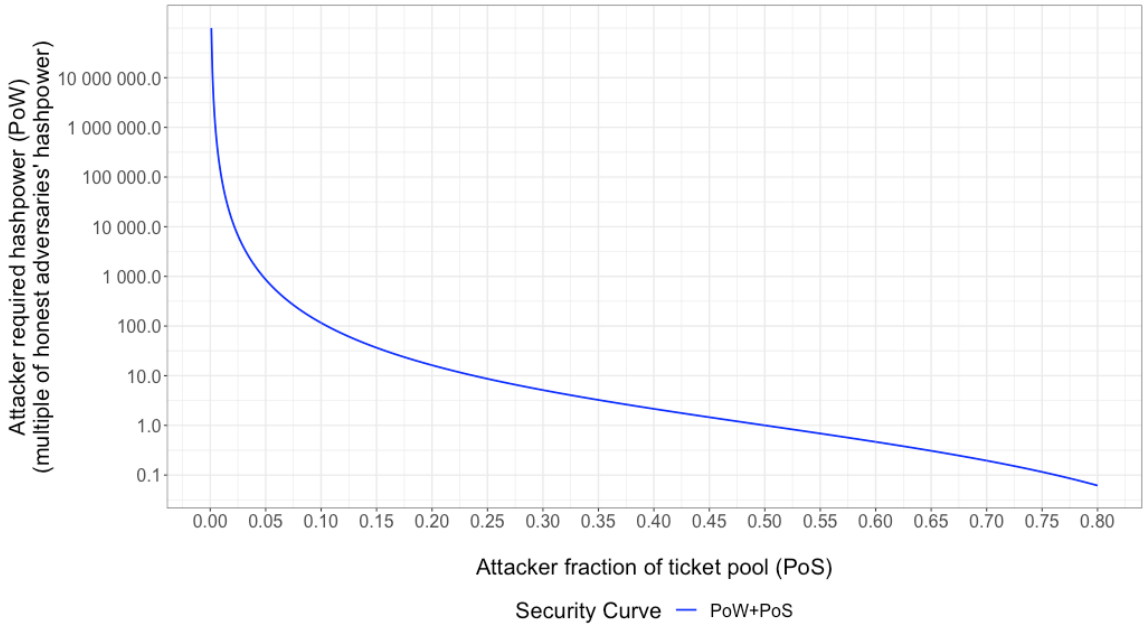
Source: (Stafford, 2019)

Attacker's required hashpower (PoW) to outpace the honest adversaries

$$x(y) = \frac{1}{P(y)} - 1 \tag{4.3}$$

Source: (Stafford, 2019)

Figure 4 – Security curve created by PoW+PoS combined authentication



Source: own elaboration

Any adversary with a combination of PoW+PoS power at the left of the security curve is considered safe to the security of the blockchain. As detailed in the beginning of this section, the following analysis assumes the point x=0.5, y=1.0 in the security curve, which means that the dishonest adversary has one time the hashpower of the honest adversaries (50% of the total) and 50% of all tickets in the pool (the 'majority attack').

External/internal attack

This section presents the cost of an external/internal attack where the adversary is 0% invested in either coin: the attacker buys equipment from vendors (external) and coins from traders or miners using fiat money (internal), both at market price and until the attacker reaches 50% of PoW equipment (increasing the number of equipment by a factor of 1) and 50% of the issued coins (Decred only) without increasing the exchange rate, which is an unrealistic assumption because it assumes that current ticket owners will sell half of their Decred otherwise the adversary would have to buy all Decred available (Decred not locked up in tickets, 49.84% of all issued coins on 10 Feb 2020) without skyrocketing its price.

The cost of an external PoW + internal PoS attack against Decred blockchain considers hashpower, coin price, current equipment, ticket price in DCRs (estimated as an internal attack), facility cost estimation and electricity price on 10 Feb 2020.

Table 4 – Decred Proof-of-Work equipment and network hashpower

(A) ASIC device: DCR5 (34 Th/s, 1 610W, USD 1 282)	34	Th/s
(B) Decred network hashpower on 10 Feb 2020	450 150	Th/s
(C = B / A) ASIC devices for 1x attack (more 450 150 Th/s)	13 240	unit
(D = 1 610W * C) ASIC devices will spend 1 610W * 13 240 units	21 316	kWh
(E = USD 1 282 * C) Cost to buy 13 240 DCR5 units	16 973 680	USD
(F = USD 0.05 * D) Cost of electricity in Iceland (USD 0.05/kWh)	1 066	USD/h
(G = 0.05 * (E + F)) Assuming facility cost (5% of device + electricity cost)	848 684	USD
(H = G / 720h) Facility cost per hour	1 179	USD/h

Source: own elaboration

Table 5 – Decred Proof-of-Stake cost of (internal) attack

(I) Ticket pool size in DCRs	5 558 457	DCR
(J = 0.5 * I) 50% PoS attack would require 50% DCRs in tickets	2 779 229	DCR
(K = 21.13 * J) Cost to buy 2 779 229 DCR at price USD 21.13	58 725 109	USD

Source: own elaboration

Table 6 – Total cost (PoW + PoS) of an attack against Decred on 10 Feb 2020

(K + E) Capex: USD 58 725 109 (PoS) + USD 16 973 680 (PoW)	75 698 789	USD
(F + H) Opex: 1 066 USD/h + 1 179 USD/h (PoW)	2 245	USD/h

Source: own elaboration

The cost of an external attack against Bitcoin blockchain considers hashpower, current equipment, facility cost estimation and electricity price on 10 Feb 2020:

Table 7 – Bitcoin Proof-of-Work equipment and network hashpower on 10 Feb 2020

(L) ASIC dev: Antminer S17+ (73 Th/s, 2 920W, USD 2 580)	73	Th/s
(M) Bitcoin network hashpower on 10 Feb 2020	107 525 520	Th/s
(N = M / L) ASIC devices for 1x attack (more 107 525 520 Th/s)	1 472 953	unit
(O = 2 920W * N) ASIC devices will spend 2 920W * 1 472 953 units	4 301 023	kWh
(P = USD 2 580 * N) Cost to buy 1 472 953 S17+ units: 1 472 953 * USD 2 580	3 800 218 740	USD
(Q = USD 0.05 * O) Cost of electricity in Iceland (USD 0.05/kWh)	215 052	USD/h
(R = 0.05 * (P + Q)) Assuming facility cost (5% of device + electricity cost)	190 010 937	USD
(S = R / 720h) Facility costs per hour	263 919	USD/h

Source: own elaboration

Table 8 – Total cost (PoW) of an attack against Bitcoin on 10 Feb 2020

(P) Capex (PoW)	3 800 218 740	USD
(Q + S) Opex: 215 052 USD/h (PoW) + 263 919 USD/h	478 971	USD/h

Source: own elaboration

Considering a external/internal majority attack (50% +1) and the information on Tables 9 and 10, Decred would be more expensive than Bitcoin to attack on 10 Feb 2020 if one of two conditions were true:

1) DCR price in USD (exchange rate) were 64.43 times the value at the time
2) Decred network size (hashpower) were 211 times the level at the time

If Decred network had the same hashpower as Bitcoin network, an external/internal attack on Decred network would cost 1.1355 times an external attack on Bitcoin network. If Decred network had the same hashpower as Bitcoin network and if Decred were priced at the same exchange rate as Bitcoin, an attack on Decred would cost 8.3277 times an attack on Bitcoin.

Table 9 – Decred and Bitcoin supply and exchange rates on 10 Feb 2020

Fiat exchange rate		Coin Supply	Exchange rate	
BTCUSD	9 856.61	18 209 137	466.4747	DCRBTC
DCRUSD	21.13	11 081 717	0.0021	BTCDCR

Source: own elaboration

Table 10 – Decred and Bitcoin network size (hashpower) in Th/s on 10 Feb 2020

Network size in Th/s on 10 Feb 2020		Network size in scale	
Decred	450 150 Th/s	0.0042	x Bitcoin size
Bitcoin	107 525 520 Th/s	238.8660	x Decred size

Source: own elaboration

Considering coin supply and exchange rates from Tables 9 and 10, the calculation results from Tables 6 and 8, and one very important restriction to this model that assumes that Decred stakeholders would sell up to 50% of their coins at market price, Table 11 shows that Bitcoin is more expensive to externally attack than Decred on 10 Feb 2020.

Table 11 – Most expensive blockchain to attack (external/internal) on 10 Feb 2020

Most expensive blockchain to attack on 10 Feb 2020:		
Decred (external/internal) 1-hour attack	0.0199	x than Bitcoin
Bitcoin (external) 1-hour attack	50.2067	x than Decred

Source: own elaboration

Internal/internal attack

An internal attack means that no additional mining devices are being added to the network. It could be current PoW miners performing a short-term attack on the network, but it is also possible to rent mining devices in the 'cloud'. 'Cloud' means companies that rent datacentre capacity as a service on the Internet where the customer pays only for used capacity (Opex) without the need to also build the datacentre, buy computing and networking devices (Capex) and pay to operate them (Opex). Nicehash[22] is one of these cloud mining companies renting processing power for some hashing algorithms. Crypto51[23] website calculates the cost of 1h attack for several PoW cryptocurrencies and how much hashrate

[22] Available at https://www.nicehash.com/, last accessed 19 Sep 2020.
[23] Available at https://www.crypto51.app/, last accessed 19 Sep 2020.

Nicehash cloud offers to perform a majority attack, allowing an adversary to pay only for the marginal cost of the hashrate. This website informs that Nicehash currently has 0% hashrate rental capacity for Bitcoin and Decred is not currently available in their list because it is a PoW+PoS cryptocurrency and PoS is one their recommended solutions to reduce the risk of a majority attack.

Although it is possible to rent PoW mining devices to perform attacks against almost any blockchain (assuming there is available hashrate for rental), Decred also requires the attacker to buy coins in order to acquire tickets (unless the attacker is willing/able to rent a multiple of the hashrate required to attack the network with less PoS voting power as shown in the Security Curve of Figure 4). Decred does not operate with a Delegated Proof-of-Stake (DPoS) system where the ticket owner can delegate its voting power to a mining pool or a Voting Service Provider (VSP), which could in turn override stakeholder's wishes and vote as it see fit, nor it would be possible to rent PoS voting power from ticket owners because of the pseudo random drawing mechanism.

Table 12 assumes an internal PoW attack for both Bitcoin and Decred with an internal PoS attack for Decred (which will not increase the number of locked DCRs in tickets), in the same unrealistic assumption that current ticket owners will sell half of their Decred at market price, and Table 13 shows how many times one blockchain is more secure than the other considering an internal attack and using a ratio of the total cost of attacks:

Table 12 – Total cost of internal/internal attacks on 10 Feb 2020

(K) Decred Capex: USD 58 725 109 (PoS)	58 725 109	USD
(F + H) Decred Opex: 1 066 USD/h + 1 178 USD/h (PoW)	2 244	USD/h
(F + H + K) Decred Total 1-hour attack cost	58 727 353	USD
(24 *(F + H) + K) Decred Total 1-day attack cost	58 778 965	USD
(120 *(F + H) + K) Decred Total 5-day attack cost	58 994 485	USD
(Q + S) Bitcoin Opex: 215 052 USD + 263 904 USD (1-hour attack)	478 971	USD/h
(24 * (Q + S)) Bitcoin Total 1-day attack cost	11 495 304	USD
(120 * (Q + S)) Bitcoin Total 5-day attack cost	57 476 522	USD

Source: own elaboration

Table 13 shows that Decred is more expensive to internally attack than Bitcoin on 10 Feb 2020.

Table 13 – Most expensive to attack (internal/internal) on 10 Feb 2020

Most expensive to attack	1 hour	1 day	5 days	
Decred (internal/internal)	122.6115	5.1133	1.0264	x than Bitcoin
Bitcoin (internal)	0.0081	0.1956	0.9743	x than Decred

Source: own elaboration

Table 13 shows only the cost of an internal attack, not its rewards. Moroz explains[24] the game rewards by introducing the work of Budish where the attacker has access to hashrate rental market, which could render the attack free, cheap or impossible, depending on rental prices and availability (Budish, 2018). Moroz et al. demonstrate in Equation 4.4 that in a competitive miner economy (under certain conditions of hashrate price and availability), the cost spent in an attack is cancelled by its block rewards, driving the attack cost to zero. Then, being able to execute a 'free' attack, the attacker's profit derives from the double-spend.

Reward per block = Total expenditure to mine a block

$$P_b = hash\ per\ block\ x\ cost\ per\ hash$$

For e blocks: (4.4)

Cost of length e attack – Block rewards for e blocks = 0

$$eP_b - eP_b = 0$$

Source: Modified from (Moroz, Aronoff, Narula, & Parkes, 2020)

Moroz et al. conclude arguing that the security of a PoW blockchain comes from making the net cost attack greater than its profit, but with a net cost attack of zero shown in Equation 4.4, any profit will be greater. PoW blockchain security becomes then closely related to the difficulty (or impossibility) of renting large hashrates due to unavailability of such amounts or price slippage in rental market.

In the same line of argument, Auer argues that in the long run all pure PoW blockchain security will be low because they will depend exclusively on transaction fees when block rewards will be low or non-existent, and these transaction fees will only be high in times of

[24] "Double-Spend Counter-Attacks: Threat of Retaliation in PoW Systems", available at https://www.youtube.com/watch?list=PLKCUhIiFc_PfT_9IlARL2LZmXaAIthE_n&v=lKd-AoDyFlA, last accessed 19 Sep 2020.

network congestion (Auer, 2019). We may conclude that with less honest miners, it will be easier to reach majority by renting mining hashrate for blockchains that share hashing algorithms. This argument is used by Hasu et al. to suggest a highly contentious 1% annually perpetual coin issuance, which instead of adding inflation and decreasing purchasing power would actually increase purchasing power and reduce uncertainty over miner revenues by adding security through miner incentives (Hasu, Prestwich, & Curtis, 2019).

For Hasu et al. a successful attack might reduce the price of the underlying digital asset and thus miners are incentivised not to lease mining hardware to potential attackers while at the same time, depending on their skin in the game, holders are more likely to pay the cost of a social coordination (to counterattack). Instead, Lovejoy provided empirical data[25] that argues the opposite of the generally accepted expectation that prices would drop: for less prominent coins, the media exposure may have outweighed the loss of confidence keeping their prices levelled (or even higher) a month after the attack, but it is not possible to assume the same outcome for more prominent coins, like Bitcoin, where their value may derive from an expectation of security from these attacks (Lovejoy, 2020). This expectation of security counterarguments the hypothesis of buying Decred to acquire tickets, perform the double-spend attack and then try to sell Decred at a price close to buy price due to market slippage, possible devaluation caused by the attack and because tickets may take as long as 143 days to be drawn.

Using the same argument of skin in the game used by Hasu et al., and extending Budish model (Budish, 2018), Moroz et al. showed that the victim may also retaliate, if there is available hashrate capacity for rental, because the victim has more at stake (the value of the original transaction) than the attacker (Moroz, Aronoff, Narula, & Parkes, 2020). These arguments help show the strength of the PoW+PoS security mechanism.

Majority attack simulation

Considering the scenario presented at the beginning of this section, where the dishonest adversary has slightly more power than the honest nodes (50% +1 of PoW devices and PoS tickets), Tables 14 and 15 show the result of 100 000 simulations for this setup for both attacks scenarios. The PoW simulation took 32min25secs while the PoW+PoS simulation took 7h02min, which indicates the increase in cost to attack such networks.

[25] "51% attacks", available at https://dci.mit.edu/51-attacks, last accessed 19 Sep 2020.

Table 14 – Result of 100 000 49.99%/50.01% PoW simulated attacks

Number of simulations: 100000		Average: 0.0120 seconds, Total: 00:32:25	
Adversary	Hashpower	Simulations won	Simulations won
A0	49.99%	50037	50.0370%
A1	50.01%	49963	49.9630%
On average, 2-block and 6-block advantage reached in: 7.0091 and 55.0898 blocks			
Attack cost, on average 36.0709 PoW block rewards			

Source: own elaboration

Table 15 – Result of 100 000 49.99%/50.01% PoW+PoS simulated attacks

Number of simulations: 100000				Average: 0.2092 seconds, Total: 07:02:19	
Adversary	Hashpower	Stake	Sims won	Sims won	Avg Invalid Blocks	Avg Valid Blocks
A0	49.99%	49.99%	49785	49.7850%	18.7086	17.9623
A1	50.01%	50.01%	50215	50.2150%	18.6579	18.0050
On average, 2-block and 6-block advantage reached in: 4.9870 and 36.9674 blocks					
For A1, the attack cost, on average: 18.0050 PoW block rewards, due to PoS invalidation					

Source: own elaboration

4.4. Testing governance hypotheses

After December 2017 the cryptoasset markets sustained a severe devaluation in face of fiat currencies. Because cryptoassets have different characteristics (affinity demand, scarcity, issuance rules, governance model, hashpower security, technology, development activity and expectations), the demand curve is different on each case.

A few hypotheses related to Decred Project governance could be tested:

- Hypothesis 1: Decred staked percentage is related to coin issuance
- Hypothesis 2: Decred staked percentage is related to price variance
- Hypothesis 3: PoW security is related to price
- Hypothesis 4: Privacy participation is related to Decred price variance
- Hypothesis 5: Observed coin issuance is related to expected coin issuance
- Hypothesis 6: Tickets are drawn as expected in the official documentation
- Hypothesis 7: Decred founders' expenditure is related to price variance
- Hypothesis 8: Decred price variance is related to Bitcoin price variance
- Hypothesis 9: Decred voting turnout is higher on consensus rules

The period of time investigated in this section comprises the launch of Decred network on 08 Feb 2016, where the genesis block (name given to the first block) was mined, and 10

Feb 2020, four years after the first exchange rate in USD available in Yahoo Finance[26]. Feb 2020 also avoids significant market impacts that may be related to Covid-19 pandemic[27]. The Figures and Tables in this section show correlation of data, which does not imply causality. The data was extracted from dcrdata, the Decred own block explorer, from Yahoo! Finance and Blockchain.com website and is available at Decred Governance Data Analysis Github code repository[28], along with the R and SQL scripts used to extract and process the data.

Table 16 shows the first assessments made before testing the hypotheses. The average block per day is important for the network to keep the pace in terms of coin issuance and transaction processing while the average daily ticket pool size shows if the ticket pricing algorithm is working as expected, making the tickets more expensive when demand is high and lowering the price when demand drops. Having the observed values close to the expected ones show that the blockchain is working as defined by the consensus rules. These numbers will be used in the coming assessments.

Table 16 – Decred blockchain expected and observed results

From 08 Feb 2016 to 10 Feb 2020	Expected	Observed
Average block per day	288	288.5479
Average daily ticket pool size	40 960	41 257.3012

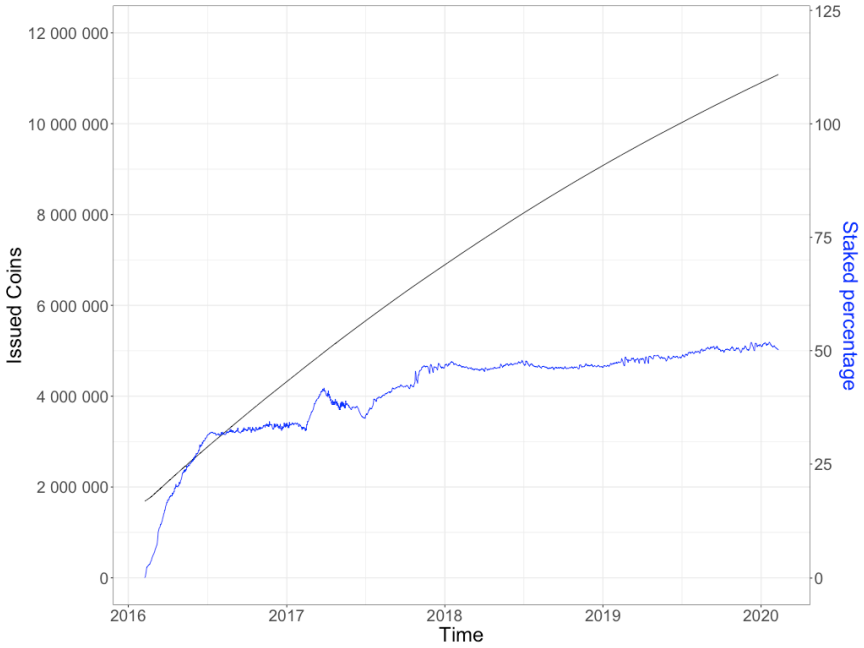
Source: own elaboration

Hypothesis 1: Decred staked percentage is related to coin issuance

The staked percentage corresponds to the amount of coins locked up in tickets. Figure 5 and Table 17 show a strong correlation between coin issuance and staked percentage, indicating that even though more coins are issued, stakeholders keep buying tickets, which drives up ticket price, and then participate in the governance process being financially rewarded for it.

[26] DCRUSD exchange rates, available at https://finance.yahoo.com/quote/DCR-USD/history?period1=1454716800&period2=1586131200&interval=1d&filter=history&frequency=1d, last accessed 10 July 2020.
[27] "Bitcoin Jumps to Highest Level Since March's Coronavirus Crash", available at https://www.bloomberg.com/news/articles/2020-04-23/bitcoin-jumps-to-highest-level-since-march-s-coronavirus-crash, last accessed 10 July 2020.
[28] Decred Governance Data Analysis, https://github.com/mmartins000/decred-gov-data-analysis, last accessed 12 Sep 2020.

Figure 5 – Issued Decred coins and staked percentage



Source: own elaboration

Table 17 – Correlation between issued Decred coins and staked percentage

Selected sample from		**All time**	**> 10 Feb 2017**
N		1464	1096
Pearson's Correlation		0.8994	0.9045
Significance test	p-value	< 2.2e-16	< 2.2e-16

Source: own elaboration

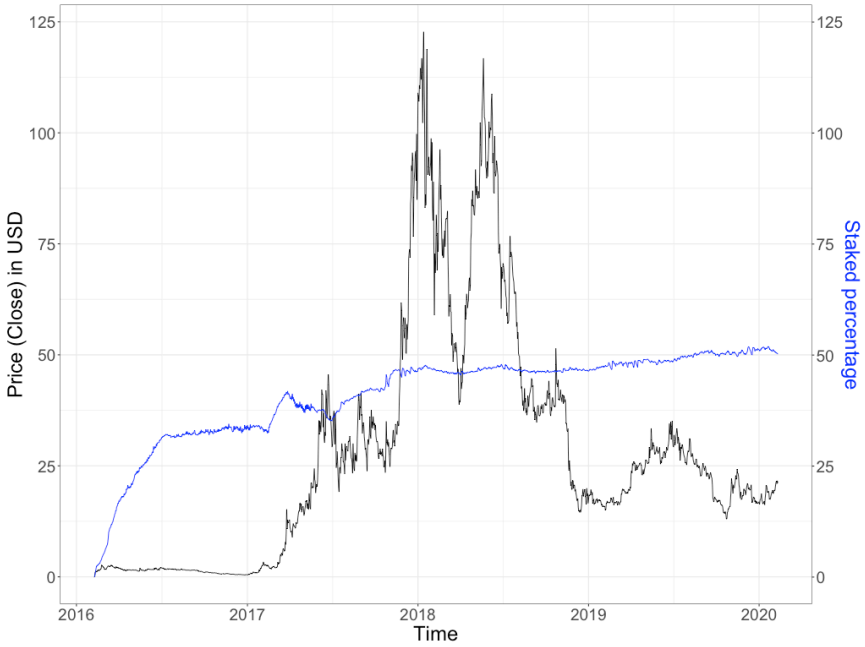
Hypothesis 2: Decred staked percentage is related to price variance

Because stakeholders get a reward from the governance process, and because the cryptocurrency market as a whole suffered a severe devaluation in the end of 2017, it is possible that investors that bought Decred when the price was higher now have an incentive to buy tickets and receive a reward while wait for the price to go back up, possibly.

Figure 6 and Table 18 show Decred price in USD and the staked percentage of issued Decred coins. One year after the project was launched, on 10 Feb 2017, 33% of all issued coins were locked up in tickets and this number increased to 50% on 10 Feb 2020. In summary, i) additional coins are issued every day, ii) investors keep showing long-term interest in the project, locking up their coins for up to 143 days to get a reward, and iii) this reward goes down as time goes by, because the reward drops by circa 1% every 21.33 days,

as shown in Figure 3 in section 3.1. On the other hand, the slight increase in the staked percentage between Feb 2017 and Feb 2020 (period selected due to the curve shown on Figure 6) does not explain the price variation during the same period. Additional questions should consider if i) price could increase in case of reduced offer of Decred in the market or ii) price could decrease if the market understands that there is not enough Decred liquidity to be regularly used as currency or iii) staked percentage could increase or decrease if the price decreases or increases, respectively, because stakeholders might want to take a profit if the price increases, or stake more if the price decreases and sell later when/if the price rebounds.

Figure 6 – Decred price and staked percentage (PoS security)



Source: own elaboration

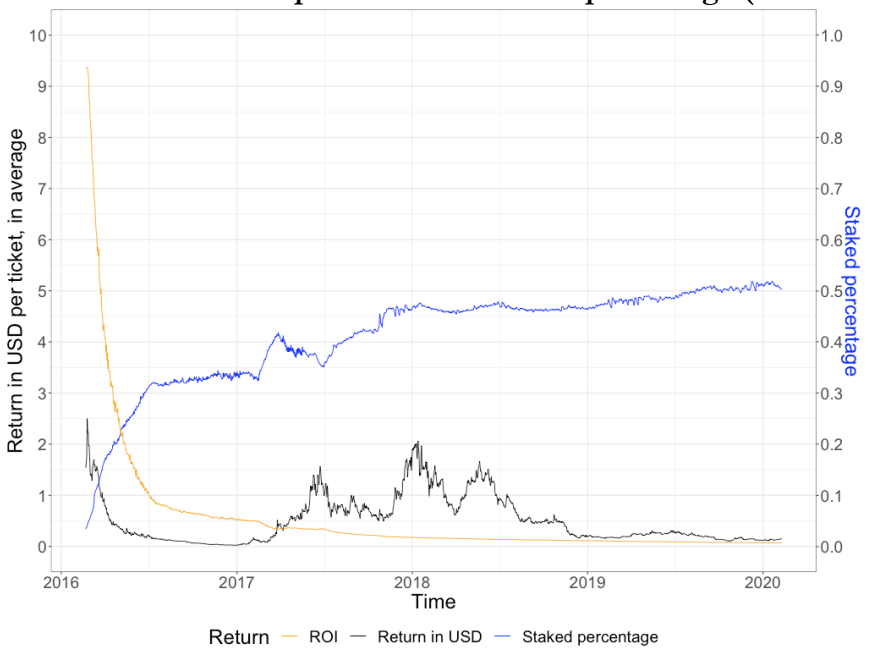
Table 18 – Correlation between Decred price and staked percentage

Selected sample from		**> 10 Feb 2016**	**> 10 Feb 2017**
N		1462	1096
Pearson's Correlation		0.4970	0.123
Significance test	p-value	0.0176	1

Source: own elaboration

Figure 7 and Table 19 explore the correlation between the percentage of staked coins and the return in USD per ticket, in average, to investigate a relation between a possible drop in return and the incentives the investors have to keep staking.

Figure 7 – Return in USD per ticket and staked percentage (PoS security)



Source: own elaboration

Against the expectations, the return in USD shows a weak inverse correlation with the staked percentage, indicating that even the returns dropping the investors keep staking and participating in the governance process. The orange line represents the Return on Investment (ROI) and it measures the return in DCR for each ticket bought, considering the ticket price which is adjusted by the consensus rules to keep an average of 40 960 tickets in the ticket pool. The corresponding scale is in the right axis and starts in 21 Feb 2016 with a ROI of 93.59% and ends in 10 Feb 2020 with 0.69%. It means that in 21 Feb 2016, when the ticket price was DCR 2.00, the investors received a return of 93.59% (or DCR 1.8717) for each ticket bought, every 20 days, in average.

Table 19 – Correlation between Return in USD per ticket and staked percentage

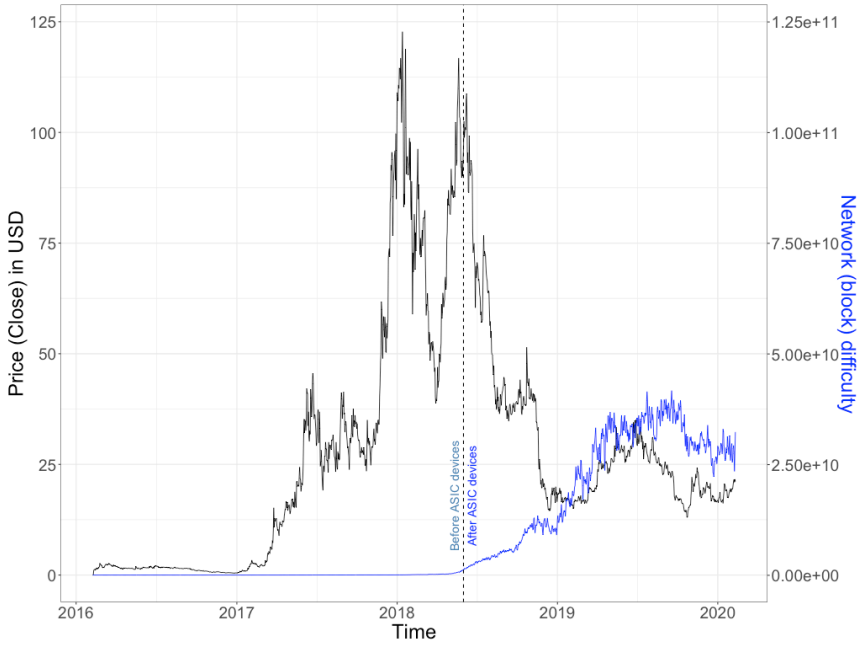
Selected sample from		> 21 Feb 2016	> 10 Feb 2017
N		1450	1083
Pearson's Correlation		-0.0711	-0.3177
Significance test	p-value	1	1

Source: own elaboration

Hypothesis 3: PoW security is related to price

Although there is not a unique method for cryptocurrency valuation, it is well-known in crypto financial markets that cryptocurrency value comes from its utility (or the utility investors derive from it) as in traditional money, as explained in section 2, not from its cost. As shown in section 4.3, an increase in security (or utility) could increase the perceived value and drive its price up. Investors might also turn off mining devices if cryptocurrency price is not enough to cover the costs of running them to provide security to the network, driving its price down. Figure 8 and Table 20 show weak correlation between this assumed relation, price and network difficulty for Decred, for selected samples from 2019 onwards. There is no correlation between such variables when the samples include the whole history or until 31 Dec 2018.

Figure 8 – Decred price and network difficulty (PoW security)



Source: own elaboration

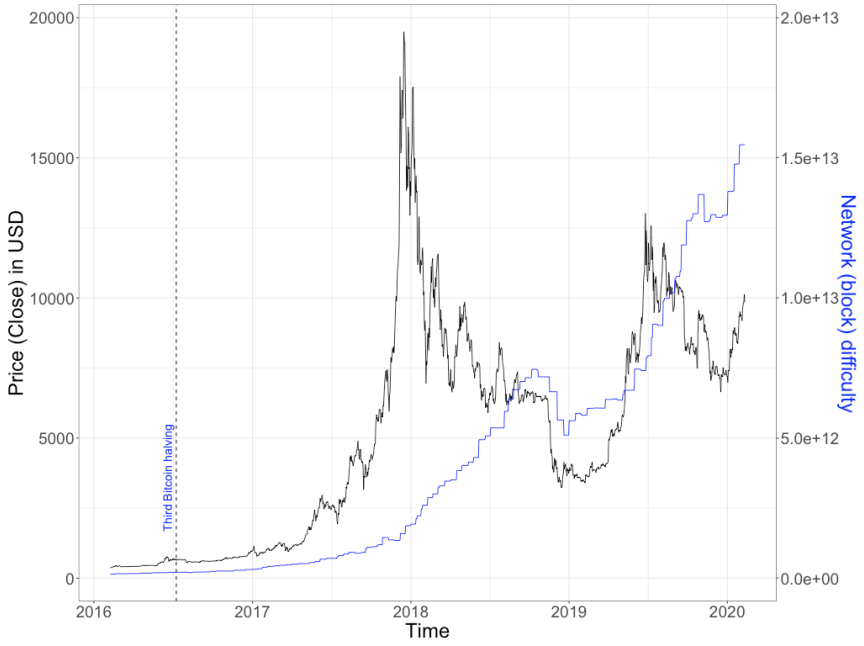
Table 20 – Correlation between Decred price and network difficulty

Selected sample from		All time	< 30 Dez 2018	> 01 Jan 2019
N		1464	1058	406
Pearson's Correlation		-0.0939	0.1138	0.5308
Significance test	p-value	< 2.2e-16	< 2.2e-16	0.0102

Source: own elaboration

Figure 9 and Table 21 also show a weak correlation between price and network difficulty for Bitcoin, no matter the period selected. The third Bitcoin 'halving' event, name given to the programmed periodic change that reduces in half the coin issuance, do not seem to have caused any impact, according to Figure 9, although at that time, the cryptocurrencies were unknown to most of the people and the market was not developed as it is today.

Figure 9 – Bitcoin price and network difficulty (PoW security)



Source: own elaboration

Table 21 – Correlation between Bitcoin price and block mining difficulty

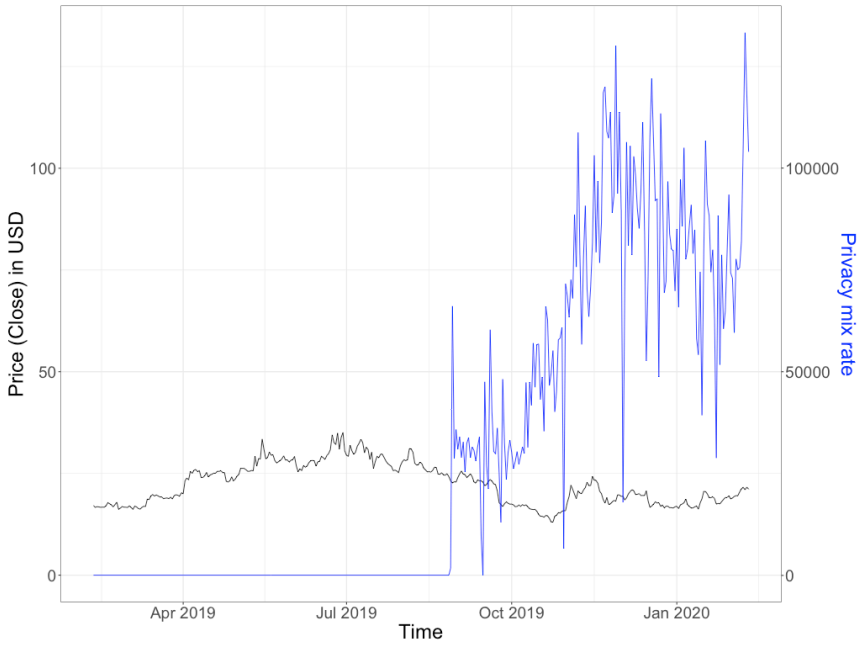
Selected sample from		All time	< 30 Dez 2018	> 01 Jan 2019
N		1464	1058	406
Pearson's Correlation		0.5924	0.5376	0.5486
Significance test	p-value	< 2.2e-16	< 2.2e-16	< 2.2e-16

Source: own elaboration

Hypothesis 4: Privacy participation is related to Decred price variance

In the cryptocurrency market, just like regular enterprise valuation, new features (or contracts) may be related to an increase in price, at least for a very short time, maybe only on release day. A decrease in price is also possible, with some investors selling their positions once the event happens, because it was already 'priced' before the event. Another explanation for a decrease in price would be a lack in governance transparency added by the privacy feature, because it is not possible to track founders' expenditure anymore and they might be heavily invested (staked) causing imbalances to the decision-making process, taking advantage on their initial position size (pre-mine). Figure 10 and Table 22 show a weak inverse correlation between Decred price (close) in USD and the release of the privacy feature.

Figure 10 – Decred price variance and coins in private transactions



Source: own elaboration

Table 22 – Correlation between Decred price (close) and privacy mix rate

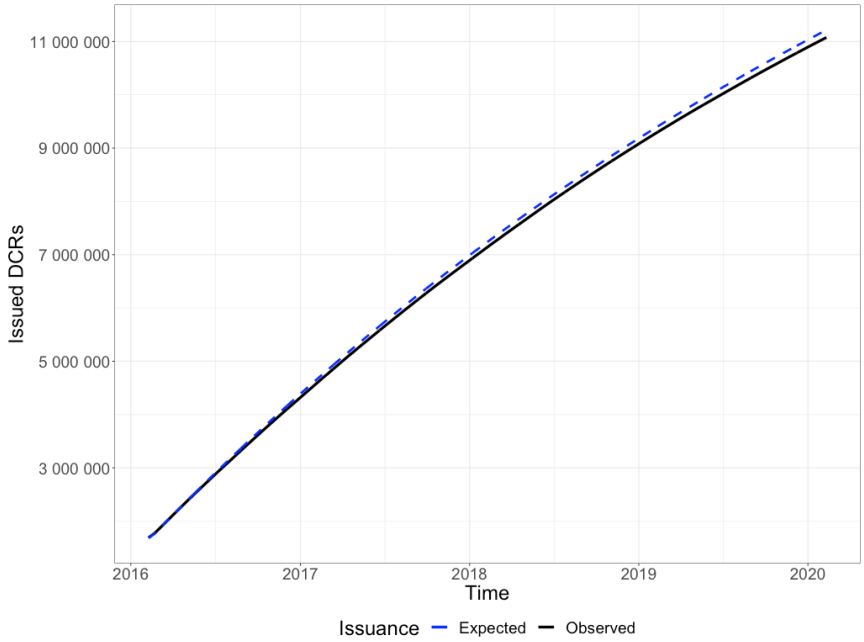
N		366
Pearson's Correlation		-0.5286
Significance test	p-value	< 2.2e-16

Source: own elaboration

Hypothesis 5: Observed coin issuance is related to expected coin issuance

The introduction of section 2 and section 2.3 detailed the properties of money, like scarcity, and argued that 'good and trustworthy coins' must be issued in a predictable manner and according to its value. Consensus rules in the protocol, kept in place by good governance, are responsible for the issuance of new coins, which are the incentive for miners to provide security to the blockchain and to stake coins in PoS tickets. Figure 11 and Table 23 show a perfect correlation between the expected coin issuance (dashed blue curve) defined in Decred blockchain consensus rules and the observed coin issuance (continuous black curve) from 08 Feb 2016 and 10 Feb 2020.

Figure 11 – Expected and observed Decred coin issuance



Source: own elaboration

Table 23 – Correlation between expected and observed Decred coin issuance

N		1464
Pearson's Correlation		1
Significance test	p-value	< 2.2e-16

Source: own elaboration

The difference between expected and observed coin issuance can be explained by Table 24, that shows the number of blocks with only 3 and 4 ticket votes. The blockchain protocol defines that a ticket drawn in one block must sign a transaction validating the next block, thus adding security to the network. Besides that, these stakeholders can vote in the

on-chain and off-chain proposals and for such are rewarded with 30% (6% for each of 5 tickets/votes per block) of coin issuance for that block. If the wallet (name given to the software that manages private keys that sign transactions) is offline when the ticket is drawn, it will not sign the transaction and will not be rewarded with new coins. This also reduces the PoW reward, which reaches 100% only when 5 voting tickets are mined.

Table 24 – Decred ticket voters per block

From 08 Feb 2016 to 10 Feb 2020	Count	Percentage
Blocks with 0 voting tickets	4 096	0.0097
Blocks with only 3 voting tickets	5 526	0.0131
Blocks with only 4 voting tickets	21 881	0.0518
Blocks with all 5 voting tickets	391 045	0.9254

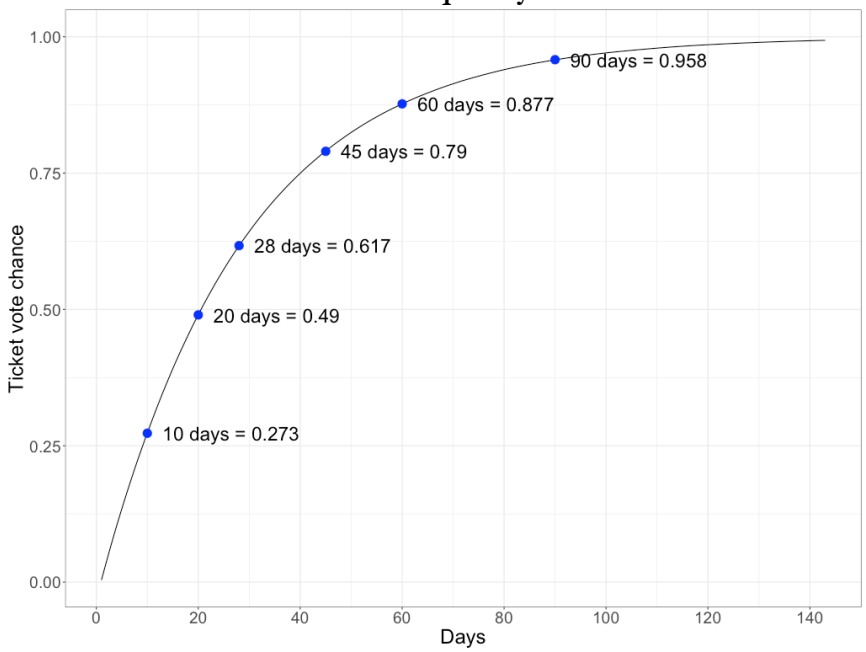
Source: own elaboration

Hypothesis 6: Tickets are drawn as expected in the official documentation

As explained before, predictability and scarcity play their role in the process of building a trustworthy coin. To keep stakeholders interested in the staking process, fundamental to governance, the voting chance must meet the expectations and the financial reward must be paid according to the consensus rules. The official Decred documentation[29] displays a chart with the probability of a ticket voting by day. Table 25 shows these expected values for ticket vote chance, as documented by the project, and the observed values from 08 Feb 2016 to 10 Feb 2020. Table 26 shows a very strong correlation between those values, which indicates that ticket vote chances, and investors rewards, happen in practice as described in theory. Figure 12 below shows the cumulative vote chance curve.

[29] Available at https://docs.decred.org/proof-of-stake/overview/, last accessed 10 July 2020.

Figure 12 – Observed cumulative frequency of Decred ticket vote chance



Source: own elaboration

Table 25 – Expected and observed cumulative Decred ticket vote chance

From 08 Feb 2016 to 10 Feb 2020	Expected	Observed
Chance of having the ticket voted in 10 days	0.296	0.273
Chance of having the ticket voted in 20 days	0.505	0.490
Chance of having the ticket voted in 28 days	0.626	0.617
Chance of having the ticket voted in 45 days	0.794	0.790
Chance of having the ticket voted in 60 days	0.879	0.877
Chance of having the ticket voted in 90 days	0.958	0.958
Chance of having the ticket expired (after 143 days)	0.005	0.007

Source: own elaboration

Table 26 – Correlation between expected and observed Decred ticket vote chance

N		7
Pearson's Correlation		0.9998
Significance test	p-value	< 2.2e-16

Source: own elaboration

Hypothesis 7: Decred founders' expenditure is related to price variance

Speculation (or panic) happens in the markets when founders, or an entity the market assume as the founder, sell coins mined at the beginning of the project. It recently happened[30] to a Bitcoin unspent transaction (coins) mined in 09 Feb 2009, where 40 BTC were spent. To understand the scenario when it comes to Decred founders' pre-mined coins, Table 27 shows the percentage and amount in DCR from the founders' and airdroppers' pre-mine on block #1 spent until 10 Feb 2020.

Table 27 – Decred founders' and airdroppers' pre-mine issuance and expenditure

From 08 Feb 2016 to 10 Feb 2020	N	Issued	Spent	Spent (%)	Spent (%) in 2016
Founders' pre-mine	174	840 000	353 290	42.06	31.34
Airdroppers' pre-mine	2 972	840 000	549 165	65.38	50.1

Source: own elaboration

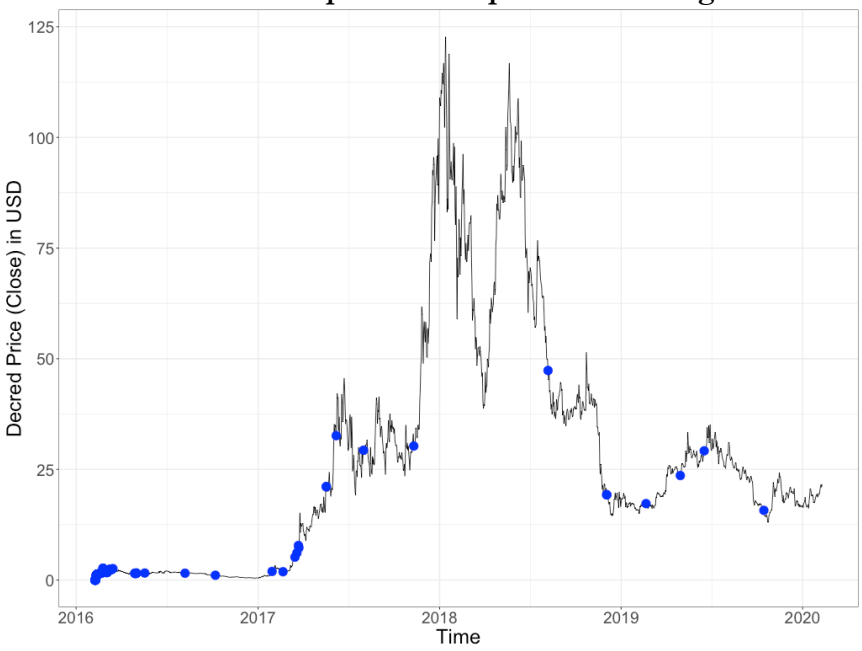
Figure 13 compares Decred price (close) in USD with the timeline of the expenditures. It is important to notice that expenditures include stake transactions and for those transactions, almost 100% of the original unspent transactions were spent buying tickets (staking). About 31,34% of founders' pre-mine were spent during 2016, mostly to buy tickets and the maximum exchange rate reached that year for Decred was USD 2.68. It is assumed that the 290 835 unspent DCR (issued minus spent DCR in Table 27) distributed to airdroppers are lost (lost private keys, adding to the scarcity of the coin) because those who got this amount of DCR for free (DCR 282.94 per airdropper) would have sold it at some point between 2017 year end and mid-year 2018, when the USD exchange rate increased several times. This is not to be assumed of the founders, whose knowledge of blockchain technologies and security is extensive. It is also not possible to ascertain 2 972 different persons in the airdrop because one person might have subscribed many times using different email addresses.

Table 27 and Figure 13 show that some founders decided to stake since the project launch and some investors envision governance issues caused by power imbalances due to founders possibly outvoting other stakeholders given their initial stake size and to the initial PoS block reward that started at DCR 1.8717 on block #4096, yielding a return of 93.59%

[30] "Crypto Faithful Flip Out on Speculation Satoshi Sold Bitcoin", available at https://www.bloomberg.com/news/articles/2020-05-20/crypto-faithful-freak-out-amid-speculation-satoshi-sold-bitcoin, last accessed 16 July 2020.

per drawn ticket every 20 days, in average, when ticket price was DCR 2, as shown in Figure 6.

Figure 13 – Decred founders' pre-mine expenditure of original transactions

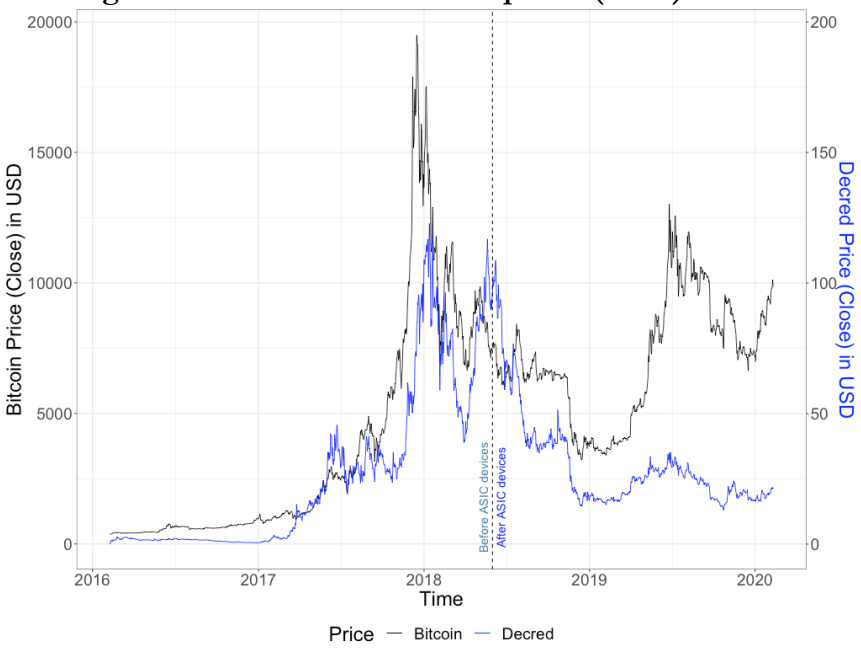


Source: own elaboration

Hypothesis 8: Decred price variance is related to Bitcoin price variance

For the past years, empirical knowledge established that Bitcoin and the alternative currencies tend to walk together for some periods of the year and go opposite ways on others. Figure 14 and Table 28 show that this was true for Decred and Bitcoin until 01 Jun 2018, when Decred ASIC devices hit the market, which may or may not be a significant event for this comparison. After 01 June 2018 and until 10 Feb 2020, Decred and Bitcoin exchange rates to USD are uncorrelated. As shown in Figure 14, Bitcoin price movements do not seem to influence Decred price movements as it did before that date, when they were strongly correlated.

Figure 14 – Decred and Bitcoin prices (close) in USD



Source: own elaboration

Table 28 – Correlation between Decred and Bitcoin prices (close) in USD

Selected sample from		All time	< 30 May 2018	> 01 June 2018
N		1464	844	620
Pearson's Correlation		0.7233	0.9156	0.0886
Significance test	p-value	< 2.2e-16	< 2.2e-16	< 2.2e-16

Source: own elaboration

When this information is analysed together with Table 20 and Figure 8, the correlation between Decred price and Decred network difficulty, it is possible to notice a relation between the timelines. The data shows that at some point between June 2018 (when Decred ASIC devices hit the market) and Jan 2019, Decred price was not correlated to Bitcoin price anymore, but to Decred network difficulty. One possible explanation for this event is the fixed cost of running the ASIC devices, which makes PoW miners the biggest sellers of coins. Bitcoin and Decred ASIC devices are different because of the one-way hashing algorithm used by the projects. Bitcoin uses SHA-256[31] and Decred uses BLAKE-256[32].

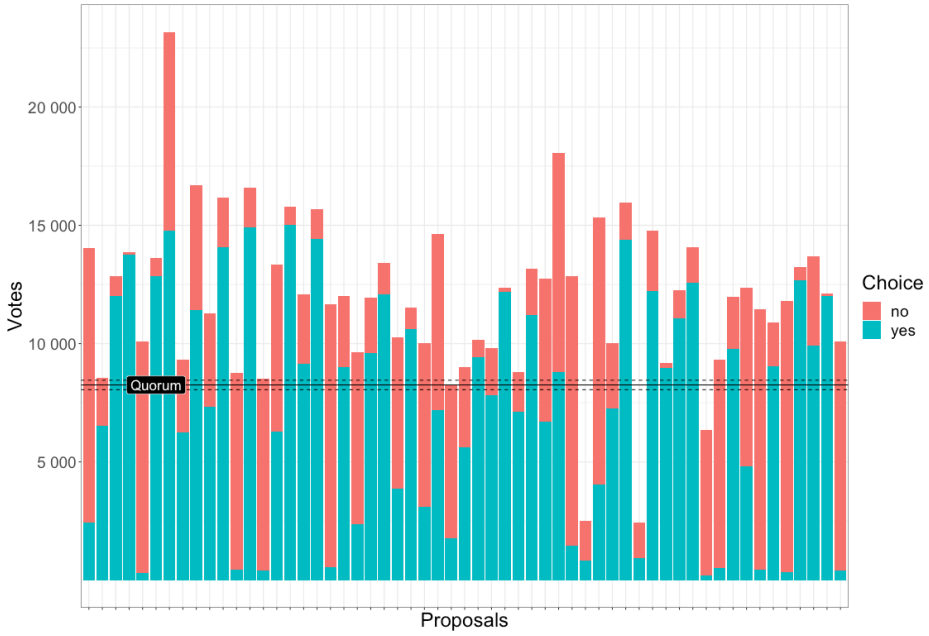
[31] NIST Hash Functions, available at https://csrc.nist.gov/projects/hash-functions, last accessed 16 July 2020

[32] BLAKE-256 hash function, available at https://docs.decred.org/research/blake-256-hash-function/, last accessed 16 July 2020

Hypothesis 9: Decred voting turnout is higher on consensus rules

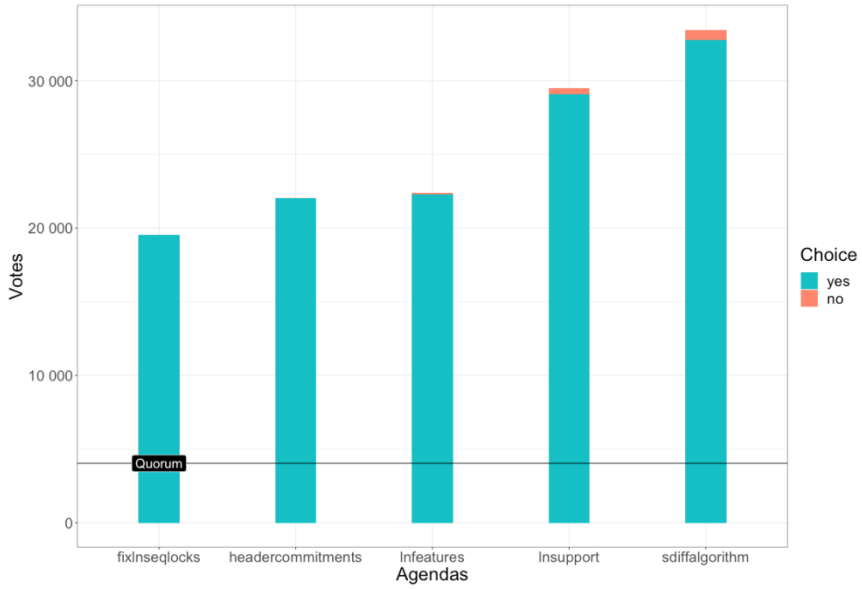
Decred stakeholders (PoS) seem to be more interested in long-term decisions, like the ones that change the consensus rules (on-chain governance) than project management and network funding decisions (off-chain governance). Figures 15 and 16 and Table 29 show PoS voting turnout and approvals for 57 off-chain and 5 on-chain governance proposals.

Figure 15 – Votes by proposal in Decred Politeia voting platform (off-chain)



Source: own elaboration

Figure 16 – Votes by proposal to change consensus rules (on-chain)



Source: own elaboration

While Figure 15 shows 3 proposals that did not reach quorum and other 5 that barely made it from a total of 57, Figure 16 shows that all 5 proposals had a higher average turnout and approval rate, which may also be an indicative of the opinion of stakeholders regarding the objectives being financed (off-chain proposals) or the quality of the proposals written by core developers (on-chain proposals) given that average disapproval rates of on-chain proposals were minimal compared to average disapproval rates of off-chain proposals.

The average voting turnout was calculated considering an average of votes 'yes' or 'no' cast per proposal divided by the average number of live daily pool tickets, shown in Table 29. This next Table also shows the average voting turnout and approval for both voting processes. For on-chain governance, while the approval percentages may seem low when compared to Figure 16 (only 67,99%, in average), the calculations consider the rate of votes 'yes' among 'no' and abstentions, with this last 'choice' deliberately not shown in Figure 16.

Table 29 – Observed turnout and approval percentage average

	Off-chain Gov.	**On-chain Gov.**
N Proposals	57	5
Average daily ticket pool size	41 257.3012	
Average voting turnout	0.2894	0.6153
Average proposal approval	0.5965	0.6799

Source: own elaboration

4.5. OLS model and regression tree

Table 30 shows an Ordinary Least Squares (OLS) model taking into consideration data from 01 Jan 2019 to 10 Feb 2020, where Decred price is the dependent variable. The quality of adjustment is good, as we can observe from R-squared and F-statistics. We may observe that Staked Percentage might have negatively influenced Decred price while Average Hashrate and Coin Issuance have a positive impact. Transaction Count and Transaction Sum seem to have no impact in Decred price. It might be interpreted as a sign that long-term investors must reduce their positions in staking to be able to transact Decred. Hashrate may increase price but may also be a sign that miners are turning off their devices when prices are too low.

Table 30 – OLS model: Decred Price (USD) as dependent variable

Residuals

Min	1Q	Median	3Q	Max
-9.6921	-2.0604	0.0554	2.2413	11.2513

Coefficients

	Coefficient	Std. Error	t value	Pr(>|t|)
Intercept	7.758e+01	9.471e+00	8.191	3.53e-15 ***
Coin Issuance	1.598e-03	5.555e-04	2.877	0.00423 **
Average Hashrate	4.330e-08	2.322e-09	18.646	< 2e-16 ***
Staked Percentage	-1.625e+02	1.736e+01	-9.362	< 2e-16 ***
Transaction Count	-3.820e-04	4.306e-04	-0.887	0.37557
Transaction Sum	1.003e-07	4.998e-07	0.201	0.84108

Significance: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

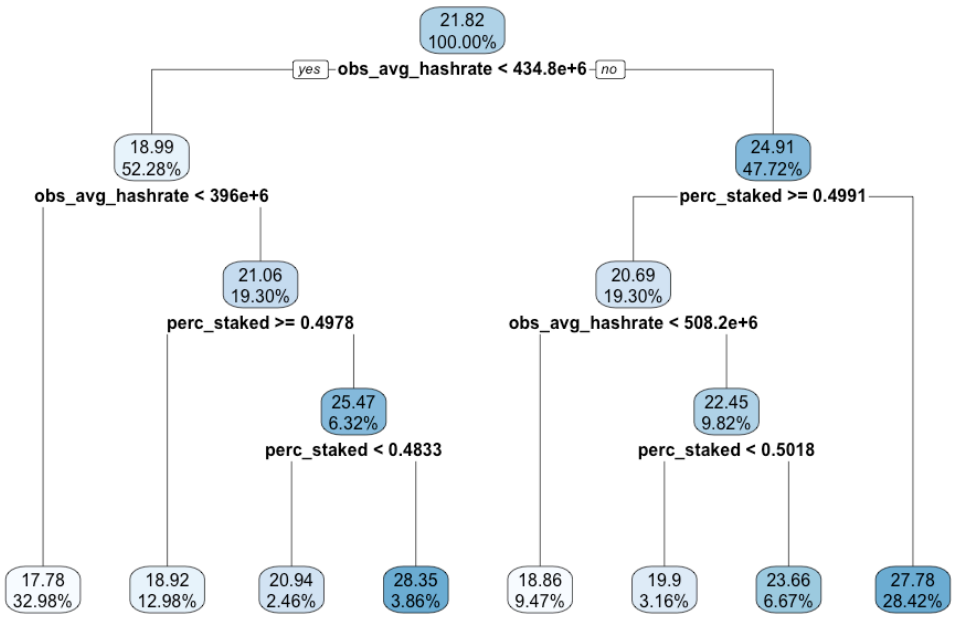
Residual standard error: 3.654, Degrees of freedom: 400
R-squared: 0.4803, Adjusted R-squared: 0.4738
F-statistic: 73.94 (p-value: < 2.2e-16)

Source: own elaboration

Figure 17 and Table 31 show the relation between price, average hashrate and staked percentage using a regression tree, a machine algorithm built through a process known as binary recursive partitioning, based on an iterative process that splits the data into partitions or branches (Breiman, Friedman, Olshen, & Stone, 1984). Lower prices were observed when the network had lower average hashrates and at the same time hashrates were higher, the staked percentage was diminishing when compared to maximum values. First, the data was divided in 70% training and 30% testing samples. Then, a hyperparameter model with 240 combinations of different values for minimum split of branches, maximum number of leaves and complexity parameter was generated. All models were tested and the values that produced the least amount of cross-validated error were chosen as the optimal model to generate the regression tree. The Mean Absolute Error calculated using the optimal model against the testing sample was 2.6096 and the Root Mean Square Error was 3.4690. Table 32 shows the importance each variable had in the calculations. We may conclude that average hashrate and staked percentage are the most important variables to try to understand price levels. The regression tree was optimised to select the number of tree leaves and levels to reduce the mean absolute error, and considered that coin issuance, transaction count and

transaction sum were irrelevant to predict price. The market showed some correlation regarding low hashrates and low prices and also high hashrates and staked percentage below 50%, and these patterns accounted for almost two thirds of observed prices between 01 Jan 2019 and 10 Feb 2020.

Figure 17 – Regression Tree with Hashrate and Staked Percentage



Source: own elaboration

Table 31 – Regression Tree Rule Coverage

AvgPrice	Hashrate	Staked Percentage	Cover
17.78	< 395.9e+06		32.08%
18.86	434.7e+06 to 508.2e+06	>= 0.4991	9.47%
18.92	395.9e+06 to 434.7e+06	>= 0.4978	12.98%
19.90	>= 508.2e+06	0.4991 to 0.5018	3.16%
20.94	395.9e+06 to 434.7e+06	< 0.4833	2.46%
23.66	>= 508.2e+06	>= 0.5018	6.67%
27.78	>= 434.7e+06	< 0.4991	28.42%
28.35	395.9e+06 to 434.7e+06	0.4833 to 0.4978	3.86%

Source: own elaboration

Table 32 – Regression Tree, Variable Importance Score

Variable	Importance
obs_avg_hashrate	3675.12
perc_staked	3372.37
obs_coin_issuance	1137.87
tx_sum	1010.45
tx_count	642.22

Source: own elaboration

4.6. Discussion of results

Sections 4.2, 4.3, 4.4 and 4.5 show details about how Decred improves security, keeps predictable coin issuance, maintains scarcity, balances power and incentives between PoW and PoS miners and runs its governance through transparent but private voting on on-chain and off-chain proposals.

A few scenarios were considered for this analysis, being the most feared of them the 'majority attack', also called '51% hashpower attack', when a powerful and wealthy adversary is able to acquire the same processing capacity, or decision power, as the honest nodes. Although this scenario is extremely unrealistic for Decred, not only because it would consider an adversary buying (or renting) 13 240 units of DCR5 ASIC devices or equivalent processing power almost at once, which implies that these devices must be already built and for sale – or available for rent (otherwise, as with any other coin, if the purchase is done during the course of a few months, the devices might become inefficient with the release of newer and more capable devices or the honest adversaries might increase their share) and mostly because considering the issued Decred coins until 10 Feb 2020, shown in Table 9 of Section 4.3, the adversary would have two options: i) an internal attack, which means buying half of the coins the stakeholders locked up in tickets (which would in turn require them to stop staking and selling them at market price without slippage) for the dishonest adversary to lock them back into tickets to reach 50% of PoS voting power; or ii) buy almost all of the remaining unlocked Decred coins, which by 10 Feb 2020 amounted to 50.16% of all issued coins (49.84% is locked up in tickets, so the adversary would have to buy another 49.84% to have the same voting power), which implies first in finding them because not all coins are available for sale in online exchange platforms and second, in buying them all without skyrocketing its price (slippage).

Simulation: the InvalidationGame

Section 4.2 used a simulation script called InvalidationGame to demonstrate that the cost of performing such an attack in terms of time and forgone block rewards (had the attacker chosen to perform an honest work), which also translates into wasted electricity costs, is way higher when performed against PoW+PoS networks. Tables 2 and 3 showed how long an attack takes in average when PoS is added as a second factor of authentication to PoW. While 100 000 45%/55% pure PoW simulated attacks took 35 minutes to complete, a batch of 100 000 45%/55% PoW + 70%/30% PoS simulated attacks took 4h03m to run its course until a 6-block difference between adversaries. For the previously mentioned 'majority attack' scenario, Tables 14 and 15 show that the same 100 000 simulations took 32 minutes and 7h02m, respectively. In terms of cost and forgone block rewards it is important to notice that the 'attack cost' shown on Tables 3 and 15 calculate only successfully PoW mined blocks invalidated by PoS miners, not the work done on PoW blocks wasted when the adversary was able to successfully mine them, as shown on Tables 2 and 14. So, although not shown, the attack cost on those PoW+PoS simulations is much higher than those numbers. It is also important to note that the forgone reward happens when the honest nodes are able to compete and win the battle for the longest chain.

Security increases opportunity costs

Section 4.3 considered first an external PoW/internal PoS attack scenario although unrealistic as previously explained, which means the attacker would have to buy ASIC devices (and account for their depreciation and replacement) on the market increasing the total number of PoW devices but the coins would have to be bought from current stakeholders willing to sell at market price without slippage, keeping the staked percentage at the same level. Then an internal PoW/internal PoS attack was considered, accounting for rental of cloud mining devices (PoW) and acquisition of Decred to buy tickets (PoS). For this scenario, calculations showed that Decred was over 120 times more secure than Bitcoin for 1-hour attacks on 10 Feb 2020.

Considering the information presented on Tables 14 and 15, it would be reasonable to assume that while a PoW attack would cost an average of 36 block rewards forgone because the dishonest adversary decided to use the processing power to try to attack the network as shown in Table 14, a PoW+PoS attack would cost the average of 18 block rewards from invalidated blocks due to PoS mining as shown on Table 15 + the 36 PoW block rewards

from Table 14, because after mining a valid block through PoW mining, the adversary must have the block validated in PoS mining.

Tables 6 and 8 show the hourly cost to operate the 'majority attack' on Decred and Bitcoin, respectively. Because Decred network produces 12 blocks per hour and Bitcoin 6 blocks per hour, in average, and because of the number of block rewards forgone in an attack shown right above, an attack would take a few hours to complete, increasing its costs. An attack targeting Decred network would inflict an additional damage by leaving the dishonest adversary with coins locked up in tickets that shall devaluate when a successful (double-spending) attack becomes public.

Even extremely unrealistic because of the available Decred coins necessary to launch a PoS attack, section 4.3 shows that an external 'majority attack' on Decred is cheaper to attempt than on Bitcoin due to network size and USD exchange rates but Decred is more expensive to attack when considering the more plausible internal attack using rental hashrate market for PoW (internal) and coins acquired from current stakeholders for PoS (internal).

Testing governance hypotheses

Section 4.4 used real blockchain data to analyse Decred governance aspects and if price variance or staked percentage is somehow related to other factors, for example. When predictability and scarcity, introduced in sections 2 and 2.3 are evaluated, observed Decred blockchain data analysed on hypotheses 5 and 6 show that coins are issued with the expected predictability and tickets are voted and rewarded as predicted in the official documentation, which is fundamental to produce scarce, valuable, trustworthy coins.

According to the data analysed on hypotheses 3 and 8, Decred USD exchange rates were correlated to Bitcoin USD exchange rates until mid-year 2018, when Decred ASIC devices were released. Somewhere between that point in time and Jan 2019 the data shows that Decred USD exchange rates became moderately correlated to Decred network difficulty (which increased after the release of ASIC devices as expected).

Hypothesis 9 considered the voting participation as a means to evaluate on-chain and off-chain governance. The data compiled and displayed on Figures 15 and 16 and Table 29 indicate that Decred stakeholders have more interest in on-chain proposals, those able to change blockchain consensus rules and cause long-term impact on the project. These proposals, written by core developers, may be more relevant and also well-written than average which is a possible explanation for the higher approval rate.

The staked percentage of Decred coins is related to the amount of issued coins but not to the USD exchange rate, according to hypotheses 1 and 2. Table 17 shows a strong correlation between staked percentage and issued coins, which indicates that while new coins were issued according to the rules, stakeholders showed an increasing interest in participating in the governance and in being passively rewarded in PoS staking. Regarding USD exchange rates, Table 18 shows no correlation with staked percentage one year after project launch, period selected to disregard the initial staking starting on zero as possible outliers.

At last, hypotheses 4 and 7 showed that privacy launch and USD exchange rates have a weak inverse correlation and that Decred founders have spent part of their original pre-mine transactions (coins), mostly buying tickets, respectively. Putting these two arguments together, Decred founders could still be using the already spent transactions to increase their positions by being rewarded for PoS mining while using their initial weight on the project to make the decisions and it would not be possible to assert it due to the privacy feature. It is also not possible to account for the 2 972 airdrop subscribers, since they could include many subscriptions from the same person, including the founders. But Decred stakeholders do not seem to be concerned about this possibility given that i) the staked percentage increased after privacy feature launch; ii) the founders' pre-mine is well-known since before the project launch; and iii) founders' expenditure were public from the start until the privacy feature.

OLS model and decision tree

The influence of average hashrate and staked percentage in price are depicted in the OLS model, where the relation between the variables from 01 Jan 2019 to 10 Feb 2020 shows that a significant increase in average hashrate may double Decred price. The relation between average hashrate (PoW) and price indicates that PoW miners refrain from selling low and that PoW security has great influence in price, while the relation between demand for tickets (financial return + PoS voting power) and price possibly indicates that long-term investors are not willing to undo their positions in exchange for a small profit in the present while forgoing the opportunity to direct the project as they see fit and the risk of a much higher return on investment in the future. This relation between price, average hashrate and staked percentage is also shown in the regression tree, where the data shows that lower prices happened when the network had lower hashrates (PoW security).

5. Conclusions and further research

Orthodox economists are still sceptical regarding cryptocurrencies, attributing the value of money to men with guns (Krugman, 2018) or stressing the question of trust because "every currency is based on confidence that the hard-earned 'deposited' into it will be redeemable on demand" (Stiglitz, 2019), even though they are only redeemable in themselves and men with guns[33] could not hold the purchasing power of the Venezuelan bolivar. They believe "conventional money generally does its job quite well", that "using a bank account means trusting a bank, but by and large banks justify that trust" (Krugman, 2018) and that cryptocurrencies are used by "people who engage in nefarious activities" (Stiglitz, 2019).

This research showed how secure blockchain technologies increase governance and avoid trusted third parties, providing security, transparency, incentives, change rules and network coordination. Real-world use cases, forgotten by the aforementioned Nobel laureates, include unbanked people in poor countries[34], citizens of collapsing dictatorships[35], remittances in developing countries[36], refugees' access to food and cash[37], evasion of barriers to international payment systems and financial markets[38], avoidance of censorship and state control[39], avoidance of banks and third parties[40] and freezing of assets[41], property transactions[42], innovation hubs[43], digital notaries, to fight Covid hardships[44] and payments.

---

[33] "Venezuela's Latest Problem Is There Are Now Too Many Dollars", https://www.bloomberg.com/news/articles/2020-01-03/venezuela-s-latest-problem-is-there-are-now-too-many-dollars, last accessed 06 February 2020.
[34] "Can blockchain accelerate financial inclusion globally?", https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-blockchain-accelerate-financial-inclusion.pdf, last accessed 06 February 2020.
[35] "Bitcoin has saved my family", https://www.nytimes.com/2019/02/23/opinion/sunday/venezuela-bitcoin-inflation-cryptocurrencies.html, last accessed 06 February 2020.
[36] "Moving beyond remittances to help the world's poor", https://www.weforum.org/agenda/2019/08/cross-border-money-for-the-poor, last accessed 06 February 2020.
[37] "WFP Building Blocks", https://innovation.wfp.org/project/building-blocks, last accessed 29 June 2020.
[38] "Skirting U.S. sanctions, Cubans flock to cryptocurrency to shop online, send funds": https://www.reuters.com/article/us-cuba-cryptocurrency/skirting-u-s-sanctions-cubans-flock-to-cryptocurrency-to-shop-online-send-funds-idUSKCN1VX2H0, last accessed 06 February 2020.
[39] "Why China Is So Afraid Of Cryptocurrencies", https://www.forbes.com/sites/rogerhuang/2020/12/31/why-china-is-so-afraid-of-cryptocurrencies/, last accessed 06 February 2020.
[40] "Why are Venezuelans seeking refuge in crypto-currencies?", https://www.bbc.com/news/business-47553048, last accessed 06 February 2020.
[41] "Brazil tries shock therapy on inflation", https://www.chicagotribune.com/news/ct-xpm-1990-03-25-9001240707-story.html, last accessed 09 Aug 2020.
[42] "Chromaway property transactions – Sweden", https://publications.jrc.ec.europa.eu/repository/bitstream/JRC115049/blockchain_for_digital_government_online.pdf, last accessed 06 February 2020.
[43] "The World Bank is betting big on blockchain-based bonds", https://www.technologyreview.com/2018/08/10/141094/the-world- bank-is-betting-big-on-blockchain-based-bonds/, last accessed 29 June 2020.
[44] "UNICEF Cryptocurrency Fund": https://www.unicef.org/press-releases/unicef-cryptocurrency-fund-announces-its-largest-investment-startups-developing-and, last accessed 10 July 2020.

Even the large banks are creating their own private coins[45], in a movement that resembles Hayek's prediction previously explored in section 2. The International Monetary Fund (IMF) is also considering the issuance of a digital currency, a centralised one, as expected (Lagarde, 2018).

Cryptocurrencies avoid the personal data leakages[46] occurred to large banks, because they do not process personal data, only centralised exchange platforms do. Although banks claim they can refund customer's stolen money, so far they weren't able to 'refund' social security numbers and driver's licenses as explained by Decred Lead Developer Marco Peereboom (Web Summit, 2019). To counter this issue, Decred developers are working on a free, open source, decentralised exchange platform called DEX[47] to enable trustless exchange of blockchain assets through atomic swaps.

For the EU Blockchain Observatory and Forum, data privacy issues range "from reconciling blockchain's data sharing properties with the data protection provisions of the GDPR to addressing the legal status of smart contracts and digital assets." (European Commission, 2018). How would permissionless public blockchains comply with the right to erasure warranted in GDPR Article 17[48]? Or private or permissioned ones comply with the same right warranted by CCPA Section 1798.105[49]? Personal data should not be trusted in the hands of third parties and models have been proposed to reduce the trust and limit the access by data processors (Zyskind, Nathan, & Pentland, 2015).

The issue of fake news and disinformation in social media is not new, only the technology was upgraded. A NATO report on Russian gaslighting informs that after WWII "the USSR was not afraid to spread disinformation that clearly differed from reality; it used an integrated approach in distributing its propaganda through a variety of channels, ranging from educational institutions and scientific and reference literature to extensive use of the popular media" (Krumiņš, 2018). To fight Russian disinformation, Estonia created the

[45] "The end of Ripple?", https://www.forbes.com/sites/billybambrough/2019/02/15/the-end-of-ripple/, last accessed 06 February 2020.
[46] "More Than 100 Million Consumer Personal Data Leaked After A Massive Cloud Breach At Capital One": https://www.forbes.com/sites/jeanbaptiste/2019/07/30/more-than-100-million-consumer-personal-data-leaked-after-a-massive-cloud-breach-at-capital-one/, last accessed 06 February 2020.
[47] Source code is available at https://github.com/decred/dcrdex, last accessed 28 June 2020.
[48] EU General Data Protection Regulation (GDPR) is available at https://eur-lex.europa.eu/eli/reg/2016/679/oj, last accessed 06 February 2020.
[49] CCPA available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121, last accessed 14 July 2020.

Digital Embassy[50] project using KSI blockchain[51] technology. But fake news and disinformation come to one central issue: who has the power to assert the truth? The digital notary using blockchain, backed by good governance and strong security, may provide a solution to protect history. Solutions that use blockchain and smart contracts to check news (Qayyum, Qadir, Janjua, & Sher, 2019) and also that leverage Artificial Intelligence and Machine Learning to identify fake content (Hasan & Salah, 2019) have been proposed, but some of them end up being a high-tech version of the Ministry of Truth, depicted by George Orwell in his novel '1984' from 1949. In other cases, such decentralised applications may be targeted by bots and fake accounts, the current problem with fake news but upgraded to the blockchain.

Decred Project shows one way of implementing blockchain governance and plays its role in several of the use cases mentioned in the second paragraph of this section while adding a 'second-factor of authentication', simulated by the InvalidationGame, that depends on 'skin in the game'. Skin in the game is key to a good governance. While some economists venture a critique, and at the same time, spare no effort to defend a State that operates "an economy that socialized risk and privatized rewards of economies in a manner that enriched elites at the expense of everyone else" (Mazzucato, 2013, p. 193), as mentioned in the Introduction, Decred Project operates a governance model where one has to be invested to make the calls in a direct democracy, after debating with peer investors or fellow citizens and then live with the consequences of their choices (Yocom-Piatt, 2019b). After all, "if you have the rewards, you must also get some of the risks, not let others pay the price of your mistakes. If you inflict risk on others, and they are harmed, you need to pay some price for it" (Taleb, 2018, p. 11). Skin in the game explains why Decred Project funds itself and its innovations with the network fund, not with taxpayers' money from an 'Entrepreneurial State'.

Decred Project not only aims to provide an alternative to financial systems that depend on a trusted third party and to people that depend on the good will of giant financial institutions but also to show how e-voting my happen in a secure and transparent fashion. In 2018, the European Parliament mentioned e-voting as a possible use case in their Blockchain Resolution (European Parliament, 2018). E-voting systems need to be transparent, open source and extensively tested to provide a trustworthy digital identity

[50] Available at https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/, last accessed 29 June 2020.
[51] Available at https://e-estonia.com/solutions/e-governance/data-embassy/, last accessed 29 June 2020.

system, allowing voters to be registered and cast their votes anonymously, and reveal an automatic count while preserving voters' identity. The most recent attempt to succeed in building such voting system is the patent filed[52] by the United States Postal Service (USPS) on Aug 13, 2020 after a few setbacks before the US presidential election. The patent describes a "Secure Voting System" that mixes blockchain and mail, where a registered voter receives a computer readable code by mail and confirms their identity. In the voting process, the system separates the voter's identity and publishes the vote in the blockchain. Previously in 25th of April of the same year, the Utah Republican Convention successfully used blockchain for its election process[53] with a large turnout. Almost a week after that, in Apr 30, 2020, US Senate staff suggested on a staff memorandum[54] that the Senate could consider blockchain as a remote voting tool, citing the example of Estonia, if they could eliminate the threat of a '51 percent attack'. E-voting systems could help reduce power imbalances and information asymmetry, ensure that only eligible voters participate and increase voter's turnout and trust in elections and democracy.

[52] US Patent Application Publication no. US 2020/0258338 A1, Secure Voting System, available at https://pdfaiw.uspto.gov/.aiw?docid=20200258338&SectionNum=1&IDKey=7A4F4EA40D1F&HomeUrl=http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1%2526Sect2=HITOFF%2526d=PG01%2526p=1%2526u=/netahtml/PTO/srchnum.html%2526r=1%2526f=G%2526l=50%2526s1=20200258338.PGNR.%2526OS=%2526RS=, last accessed 29 Aug 2020.

[53] Utah Republican Convention Uses Blockchain Voting Service, available at https://www.forbes.com/sites/robertanzalone/2020/04/29/utah-republican-convention-uses-blockchain-voting-service/#39d925edcfee, last accessed 29 Aug 2020.

[54] PSI Staff Memorandum, available at https://www.portman.senate.gov/sites/default/files/2020-04/2020.04.30%20PSI%20Staff%20Memorandum%20-%20Remote%20Senate%20Process%20-%20Final_0.pdf, last accessed 30 Aug 2020.

Appendix

Appendix 1: The source code of the subproject named 'InvalidationGame', written in Python, to simulate the PoW+PoS authentication security mechanism presented in sections 4.2 and 4.3, is available at https://github.com/mmartins000/invalidationgame.

Appendix 2: The source code of the subproject named 'Decred Governance Data Analysis', written in SQL for data extraction and in R for data processing, figure and regression tree generation presented in sections 4.4 and 4.5, is available at https://github.com/mmartins000/decred-gov-data-analysis.

References

AppCívico. (2018). Voto Legal Blockchain Explorer. Retrieved November 20, 2019, from Voto Legal: https://blockchain.votolegal.com.br/

Atzori, M. (2015, December 1). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? Retrieved December 5, 2019, from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713

Auer, R. (2019). Beyond the doomsday economics of "proof-of-work" in cryptocurrencies. Bank for International Settlements, Monetary and Economic Department. Bank for International Settlements.

Bank of England. (2019). What is quantitative easing? Retrieved November 25, 2019, from Bank of England: https://www.bankofengland.co.uk/monetary-policy/quantitative-easing

Bentov, I., Gabizon, A., & Mizrahi, A. (2016, August 31). Cryptocurrencies Without Proof of Work. Financial Cryptography and Data Security, pp. 142-157.

Bentov, I., Lee, C., Mizhari, A., & Rosenfeld, M. (2014, December 8). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. (G. Casale, Ed.) ACM SIGMETRICS Performance Evaluation Review, 42(3). Retrieved November 20, 2019

Bitcoin Community. (2017, November 30). Genesis block. Retrieved November 26, 2019, from Bitcoin Wiki: https://en.bitcoin.it/wiki/Genesis_block

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015 IEEE Symposium on Security and Privacy. San Jose, CA, USA: IEEE.

Breiman, L., Friedman, J., Olshen, R., & Stone, C. (1984). Classification and regression trees. Wadsworth, Inc.

Budish, E. (2018, June 5). The Economic Limits of Bitcoin and the Blockchain. Retrieved September 19, 2020, from https://faculty.chicagobooth.edu/eric.budish/research/Economic-Limits-Bitcoin-Blockchain.pdf

Collins, D. (2017, November 24). Detailed Analysis of Decred Fork Resistance. Retrieved February 06, 2020, from Reddit: https://www.reddit.com/r/decred/comments/7f9ie1/detailed_analysis_of_decred_fork_resistance/

De Filippi, P., & Loveluck, B. (2016, October 17). The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure. Internet Policy Review, 5(4).

Decred Project. (2016). Decred Constitution. Retrieved November 20, 2019, from Decred Project: https://docs.decred.org/governance/decred-constitution/

Decred Project. (2019). Ticket Splitting. Retrieved from Decred Documentation: https://docs.decred.org/proof-of-stake/ticket-splitting/

Decred Project. (2020). Proof-of-Stake (PoS) Voting. Retrieved February 09, 2020, from Decred Docs: https://docs.decred.org/proof-of-stake/overview/

Elliott, F., & Duncan, G. (2009, January 3). Chancellor Alistair Darling on brink of second bailout for banks. Retrieved November 20, 2019, from The Times: https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h

Enterprise Estonia. (2019). KSI blockchain. Retrieved from https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

European Commission. (2018, October 16). Blockchain and the GDPR. Retrieved November 20, 2019, from EU Blockchain Obervatory and Forum: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

European Commission. (2019). Blockchain for digital government. Luxembourg: Publications Office of the European Union. Retrieved from EU Science Hub: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government

European Parliament. (2016). EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679. Retrieved November 25, 2019, from Eur-Lex: https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament. (2018, October 03). Distributed ledger technologies and blockchains: building trust with disintermediation. Retrieved February 06, 2020, from European Parliament: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_EN.html?redirect

European Parliament. (2019, March). Leveraged finance: a supervisory concern in the Banking Union? Retrieved November 25, 2019, from European Parliament: http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634369/IPOL_BRI(2019)634369_EN.pdf

Eyal, I. (2015, July 20). The Miner's Dilemma. 2015 IEEE Symposium on Security and Privacy (pp. 89-103). San Jose, CA: IEEE. Retrieved February 08, 2020, from https://ieeexplore.ieee.org/abstract/document/7163020

Eyal, I., & Sirer, E. (2014, November 09). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. Financial Cryptography and Data Security. FC 2014, 8437(Lecture Notes in Computer Science), 436-454.

Facebook. (2019). The Libra Association. Retrieved November 24, 2019, from Libra: https://libra.org/en-US/association-council-principles/#libra_association_council

Ferreira, D., Li, J., & Nikolowa, R. (2019, March 25). Corporate Capture of Blockchain Governance. European Corporate Governance Institute (ECGI) - Finance Working Paper No. 593/2019.

Friedman, M. (1960). A Program for Monetary Stability. Fordham.

Friedman, M. (2002). Capitalism and Freedom. The University of Chicago Press.

Friedman, M., & Goodhart, C. A. (2003). Money, Inflation and the Constitutional Position of the Central Bank. Retrieved November 25, 2019, from Institute of Economic Affairs: https://iea.org.uk/publications/research/money-inflation-and-the-constitutional-position-of-central-bank

Grunspan, C., & Pérez-Marco, R. (2019, Dez 12). On probability of Nakamoto double spend. Retrieved Feb 12, 2020, from Arxiv: https://arxiv.org/abs/1912.06412

Hardin, G. (1968). The Tragedy of the Commons. Science, 162(3859), pp. 1243-1248.

Hasan, H. R., & Salah, K. (2019). Combating Deepfake Videos Using Blockchain and Smart Contracts. IEEE Access, 7, pp. 41596-41606.

Hasu, Prestwich, J., & Curtis, B. (2019, October). A model for Bitcoin's security and the declining block subsidy. Retrieved September 19, 2020, from https://uncommoncore.co/wp-content/uploads/2019/10/A-model-for-Bitcoins-security-and-the-declining-block-subsidy-v1.05.pdf

Hayek, F. A. (1990). Denationalisation of money: The argument refined (3rd ed.). The Institute of Economic Affairs.

Hayek, F. A. (2009). A Commodity Reserve Currency. In F. A. Hayek, A Tiger by the Tail (pp. 41-43). The Institute of Economic Affairs and the Ludwig von Mises Institute. Retrieved November 26, 2019, from A Tiger by the Tail: https://iea.org.uk/publications/research/a-tiger-by-the-tail-the-keynesian-legacy-of-inflation

Johnson, D. (2019, September 18). Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values? European Journal of Risk Regulation, 10(2), 330–358.

Kalomeni, M. (2018, September 27). The ICO market is not collapsing. It's maturing. Retrieved November 24, 2019, from Elementus: https://elementus.io/blog/ico-market-august-2018/

Karakostas, D., Kiayias, A., Nasikas, C., & Zindros, D. (2019). Cryptocurrency Egalitarianism: A Quantitative Approach. International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019), Article No 7; pp. 7:1-7:21.

Krugman, P. (2018, July 31). Transaction Costs and Tethers: Why I'm a Crypto Skeptic. Retrieved February 06, 2020, from The New York Times: https://www.nytimes.com/2018/07/31/opinion/transaction-costs-and-tethers-why-im-a-crypto-skeptic.html

Krumiņš, G. (2018). Soviet Economic Gaslighting of Latvia and the Baltic States. Defence Strategic Communications, 4(Spring 2018), pp. 49-78.

Lagarde, C. (2018, November 14). Winds of Change: The Case for New Digital Currency. Retrieved February 06, 2020, from International Monetary Fund: https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency

Lovejoy, J. (2020, May). An Empirical Analysis of Chain Reorganizations and Double-Spend Attacks on Proof-of-Work Cryptocurrencies. Retrieved September 19, 2020, from https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/5f08d13a1cd5592cb330a0d0/1594413374526/LovejoyJamesP-meng-eecs-2020.pdf

Martins, M. (2018, July 24). The origin of Decred. Retrieved November 20, 2019, from Stakey Club: https://stakey.club/en/the-origin-of-decred/

Mazzucato, M. (2013). The Entrepreneurial State. Anthem Press.

Menger, C. (2007). Principles of Economics (5th ed.). (J. Dingwall, & B. F. Hoselitz, Trans.) Vienna, Austria: Ludwig von Mises Institute.

Menger, C. (2009, November 17). On the Origins of Money. Ludwig von Mises Institute. Retrieved November 30, 2019, from Mises Institute.

Meyer, D. (2018, July 03). Blockchain Voting Notches Another Success—This Time in Switzerland. Retrieved February 05, 2020, from Fortune: https://fortune.com/2018/07/03/blockchain-voting-trial-zug/

Moroz, D. J., Aronoff, D. J., Narula, N., & Parkes, D. C. (2020). Double-Spend Counterattacks: Threat of Retaliation in Proof-of-Work Systems. Cryptoeconomic Systems 2020. Cambridge, MA, USA: MIT.

Nakamoto, S. (2008, October 31). Bitcoin: A peer-to-peer electronic cash system. Retrieved November 22, 2019, from Nakamoto Institute: https://nakamotoinstitute.org/bitcoin/

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton, Oxford, USA, UK: Princeton University Press.

Nasdaq. (2017, January 23). Is Blockchain the Answer to E-voting? Nasdaq Believes So. Retrieved February 05, 2020, from Nasdaq: https://www.nasdaq.com/articles/blockchain-answer-e-voting-nasdaq-believes-so-2017-01-23

Nasdaq. (2018, November 13). Thailand Uses Blockchain-Supported Electronic Voting System in Primaries. Retrieved from Nasdaq: https://www.nasdaq.com/articles/thailand-uses-blockchain-supported-electronic-voting-system-primaries-2018-11-13

OECD. (2018, August 27). State-Owned Enterprises and Corruption: What Are the Risks and What Can Be Done? Retrieved November 27, 2019, from OECD: https://www.oecd.org/corporate/SOEs-and-corruption-what-are-the-risks-and-what-can-be-done-highlights.pdf

Poelstra, A. (2015, March 22). On Stake and Consensus. Retrieved from Satoshi Nakamoto Institute: https://nakamotoinstitute.org/static/docs/on-stake-and-consensus.pdf

Qayyum, A., Qadir, J., Janjua, M. U., & Sher, F. (2019, July-August). Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News. IT Professional, 21(4), pp. 16-24.

Redoano, M., & Scharf, K. A. (2004, March). The political economy of policy centralization: direct versus representative democracy. Journal of Public Economics, 88(3-4), 799-817.

Reijers, W., Wuisman, I., Mannan, M., & De Filippi, P. (2018, December 18). Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies. TOPOI: International Review of Philosophy, 37(17). Retrieved from Springer Link: https://link.springer.com/article/10.1007/s11245-018-9626-5

Rhodes, R. A. (2007, April 17). Understanding Governance: Ten Years On. Organization Studies, pp. 1-22.

Stafford, B. (2019). Parametrized cost of attack as a measure of Decred network security.

Stiglitz, J. (2019, July 02). Thumbs Down to Facebook's Cryptocurrency. Retrieved February 20, 2020, from Project Syndicate: https://www8.gsb.columbia.edu/articles/chazen-global-insights/thumbs-down-facebook-s-cryptocurrency

Taleb, N. (2018). Skin in the Game: Hidden Asymmetries in Daily Life. Random House.

Thatcher, M. (1983, October 14). Speech to Conservative Party Conference. Retrieved November 22, 2019, from Margaret Thatcher Foundation: https://www.margaretthatcher.org/document/105454

Wall Street Journal. (2018, April 5). Where are They Now: Profiles of the Biggest Figures From the Financial Crisis. Retrieved November 22, 2019, from Wall Street Journal: https://graphics.wsj.com/image-grid/fcprofiles/

Web Summit. (2019, November). Can you really trust your bank? Web Summit 2019. Lisbon, Portugal: Web Summit.

Yocom-Piatt, J. (2019a, August 28). Iterating Privacy. Retrieved February 09, 2020, from Decred Blog: https://blog.decred.org/2019/08/28/Iterating-Privacy/

Yocom-Piatt, J. (2019b, November 19). Cointelegraph. Retrieved February 20, 2020, from Secrets They Missed at DevCon: What It's Really Like in a Working DAO: https://cointelegraph.com/news/secrets-they-missed-at-devcon-what-its-really-like-in-a-working-dao

Zyskind, G., Nathan, O., & Pentland, A. (2015, July 20). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops (pp. 180-184). San Jose, CA, USA: IEEE. Retrieved November 27, 2019, from IEEE Security and Privacy Workshops: https://ieeexplore.ieee.org/abstract/document/7163223