

International Journal of Information Technology and Management

ISSN online: 1741-5179 - ISSN print: 1461-4111
<https://www.inderscience.com/ijitm>

Blockchain governance: reducing trusted third parties with Decred project

Marcelo Martins, Pedro Campos, Isabel Mota

DOI: [10.1504/IJITM.2025.10068956](https://doi.org/10.1504/IJITM.2025.10068956)

Article History:

Received:	12 April 2022
Last revised:	07 November 2023
Accepted:	19 April 2024
Published online:	28 January 2025

Blockchain governance: reducing trusted third parties with Decred project

Marcelo Martins

Faculdade de Economia,
Universidade do Porto,
4099-002 Porto, Portugal
Email: marcelo.martins@exploitedbunker.com

Pedro Campos*

Faculdade de Economia,
Universidade do Porto,
4099-002 Porto, Portugal
and
LIAAD – Laboratory of Artificial
Intelligence and Decision Support/INESC TEC, Portugal
Email: pcampos@fep.up.pt
*Corresponding author

Isabel Mota

Faculdade de Economia,
Universidade do Porto,
4099-002 Porto, Portugal
and
CEFUP – Center for Economics and Finance at UPorto, Portugal
Email: imota@fep.up.pt

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 investors. These stakeholders invest their coins, receive 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 means of exchange, trading it for goods or services or consuming other services provided by the blockchain as the digital notary. This paper 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 understand how blockchain technologies improve governance and avoid the tyranny of the majority. In order to reach our goal, we use multi-agent simulation and statistical modelling to verify to what extent Decred is capable of providing a predictable, scarce, trustworthy digital asset. We show that Decred increased blockchain security with its hybrid proof-of-work+proof-of-stake (PoW + PoS) security mechanism, making an attack more expensive.

Keywords: governance; blockchain; Decred; bitcoin; security; e-voting; proof-of-work; PoW; proof-of-stake; PoS; consensus; money; cryptoassets; cryptocurrencies.

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

Reference to this paper should be made as follows: Martins, M., Campos, P. and Mota, I. (2025) ‘Blockchain governance: reducing trusted third parties with Decred project’, *Int. J. Information Technology and Management*, Vol. 24, Nos. 1/2, pp.162–189.

Biographical notes: Marcelo Martins has an MBA in Business Management (2009–2011) and MBA in Finance (2013–2015), both at IBMEC, Brazil, and Master’s in Innovation Economics and Management from the University of Porto (Faculty of Economics). He is currently a Senior Application Security Engineer at Philip Morris International | CISSP-ISSMP, -ISSAP, CCSP, CISA, CISM, CRISC, PMP, AWS-Security, AWS-AdvancedNetworking. His past experience includes Decred, Feedzai, Modulo and other jobs as a n independent consultant.

Pedro Campos holds a PhD in Business and Management Studies, and Bachelor in Applied Mathematics. He is an Associate Professor at the University of Porto, School of Economics and Management, and currently the Director of the Methodology Unit at Statistics Portugal. He is also the Deputy-Director of the International Statistical Literacy Project. He is a researcher at LIAAD, the Laboratory of Artificial Intelligence and Decision Support of INESC TEC. He published more than 50 papers in peer-review journals and supervised more than 80 students in their Master and PhD thesis. His main fields of research are data science and agent-based modelling.

Isabel Mota is an Assistant Professor at the School of Economics and Management, University of Porto (Portugal) and a full researcher at the Center for Economics and Finance at UP (CEF.UP). Her academic background includes a Master’s and PhD in Economics at the University of Porto. She has publications in national and international journals, such as the *Papers in Regional Science and Computational Economics*, among others. Her current research interests include development economics, regional economics, and game theory, where she published a book on *Games, Strategy and Information*.

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 and 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).

Cryptocurrencies represent digital payment systems that operate independently of banks for transaction validation. The majority of these digital currencies function within decentralised networks powered by blockchain technology. One key characteristic of cryptocurrencies is their lack of dependence on central entities for issuance, making them conceptually resistant to government intervention or control.

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.

Cryptocurrencies have been rapidly evolving, and there has been new developments, changes, and recently new features have been introduced to the broader cryptocurrency landscape, particularly regarding security measures. Major cryptocurrencies such as Bitcoin use proof of work (PoW) to validate transactions and secure the network, although this mechanism raises concerns about energy consumption and computation expenditures. Proof of stake (PoS) is an alternative consensus mechanism which delegates control of the network to owners of the token. This mechanism has grown in popularity among digital coins because it implements a more energy efficient algorithm (Milunovich, 2022).

In this paper we investigate how the 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. Decred is considered important for several reasons, primarily due to its unique features and contributions to the broader blockchain and cryptocurrency ecosystem. It deals with a hybrid consensus mechanism PoW + PoS seeking to improve decentralisation, security, and governance by involving both miners and stakeholders in decision-making. Besides, Decred has a strong community involvement, since it fosters a sense of ownership among participants and encourages active engagement in the project’s development and decision-making processes. Overall, Decred’s combination of innovative technology, decentralised governance, community engagement, and commitment to security and privacy make it an important cryptocurrency within the broader blockchain landscape.

In order to reach our goal, we use multi-agent simulation and statistical modelling to answer the following question: is Decred capable of providing a predictable, scarce, and trustworthy digital asset? We use publicly available data from Decred and bitcoin blockchains between February 08, 2016 and February 10, 2020, and apply ‘InvalidationGame’, a Python script developed for this analysis, to simulate PoW and proof-of-work + proof-of-stake (PoW + PoS) attacks with the intent to show the difference in time and cost of such attacks.

Since 2021, and because of both the Covid pandemic and the war in Ukraine, which have caused supply chain problems, and also because the Fed raised interest rates, we observed a depreciation of bitcoin because in times of turbulence agents seek refuge in the dollar. Other cryptocurrencies were also impacted by both the covid lockdown and the Ukraine war. Moreover, as other currencies such as Decred are correlated with Bitcoin, investors prefer the most dominant market currency in periods of instability. For these reasons, prices for cryptocurrencies decreased sharply. Given the instability in the markets, we avoided to analyse the period after 2020.

This topic is particularly relevant because it discusses how to improve governance and avoid the tyranny of the majority in the context of blockchain technologies. At a time when cryptocurrencies are challenging the monetary system, despite their instability, Decred's study aims to contribute to a deeper understanding of this cryptocurrency and to help understand how investing in cryptocurrencies can depend on their social, security and economic characteristics.

Following this introduction, Section 2 starts with a brief explanation of the technologies behind the blockchain and the governance of money. Section 3 introduces the Decred Project and discusses how Decred improves the governance of consensus rules. Section 4 presents the findings of this research using simulations and statistical modelling and Section 5 concludes.

2 The technology behind the digital money

In this section, we address the technology behind the digital money, introducing the concept of blockchain, PoW, and the models of governance.

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. It is also known as 'the protocol of trust' that aims to decentralise as a security measure. Blockchain is a distributed and shared database of records and data, whose function is to create a global index for all the transactions that take place in a given market. It works like a ledger, only in a public, shared and universal way, allowing mechanisms of consensus and trust in direct communication between two parties, i.e., without the intermediary of third parties. It is constantly growing as new blocks are added to it by a new group of people.

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. 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

PoW is an important concept, as it describes a consensus mechanism that requires a significant amount of computing effort from a network of devices. PoW 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 (Nakamoto, 2008).

PoW is essentially one-CPU-one-vote. The longest chain has the greatest PoW 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

(Nakamoto, 2008). One important issue related to PoW is the environmental concerns due to its energy consumption. The energy consumed by PoW cryptocurrencies can have a significant carbon footprint, especially when a significant portion of the mining operations relies on fossil fuels. Regions with a high percentage of coal or other non-renewable energy sources in their power grids tend to have a larger environmental impact.

Sapkota and Grobys (2020) compare energy consumption in different consensus protocols and observe that PoW consensus is the most energy-consuming protocol while PoS consume considerably less energy.

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 working on the block, spending electricity on 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), with environmentally disastrous impacts. 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 (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. Nakamoto solved the issue of inflation by implementing a mechanism that gradually decreases the rate at which new bitcoin units are created over time. This mechanism is fundamental to the bitcoin protocol and is known as the ‘bitcoin halving.’ By implementing the bitcoin halving, Nakamoto created a system that ensures a controlled and diminishing rate of new bitcoin creation, thus addressing concerns related to inflation that are common in traditional fiat currencies. This scarcity and diminishing inflation are often cited as key reasons for bitcoin’s appeal as a store of value and a digital gold-like asset.

2.4 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”. In a decentralised network, 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 a majority. In case of a 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’. A blockchain hard forking keeps the history of blocks and transactions until that point, but deliberately starts 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 coins that will have a different

market value and name. Bitcoin governance is solely based on PoW as the decision-making tool.

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 et al., 2019).

3 The Decred project

Decred is an open, progressive, and self-funding cryptocurrency with a system of community-based governance integrated into its blockchain (Decred Project, 2016). On 08 February 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 2972 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).

3.1 Blockchain security

Blockchain security is paramount to implement good governance otherwise stakeholders' decisions could be reverted. In fact, 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). 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.

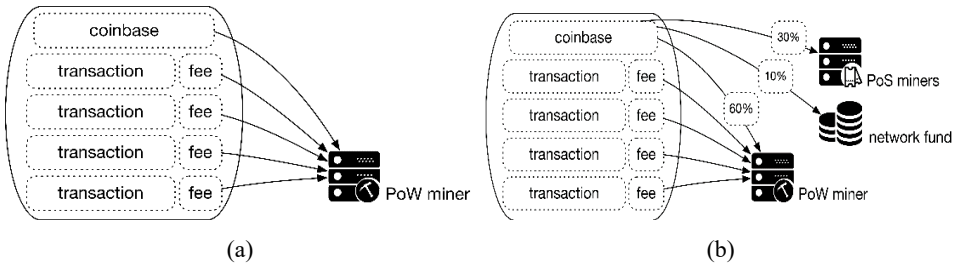
3.1.1 Proof-of-work/proof-of-stake hybrid mining

PoW/PoS hybrid mining is critical to the understanding of the security mechanism of the 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 centralise 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 decentralised, practical issues lead the PoW mining process to be very centralised, similar to trusted third-party systems, like banks (Martins, 2018).

PoS mining creates a second-factor authentication, validating PoW mining decisions (see Figure 1). 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 (Decred Project, 2020).

Figure 1 PoW vs. PoW/PoS (a) proof-of-work (PoW) (b) proof-of-work (PoW)/proof-of-stake (PoS)



Source: own elaboration

3.1.2 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.

To avoid relying on outside sources and agendas, the Decred project chose not to ask for the taxpayers’ money using innovation programmes nor started an ICO to be financed by third parties. Instead, the Decred project finances itself with 10% of every block reward. The realism of this solution depends on several factors, including the adoption and use of the Decred blockchain, the value of DCR, and the effectiveness of the project’s governance model.

3.1.3 The 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’^{1,2} for an attacker.

3.2 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 and 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 et al., 2018). Decred project implements the well-known on-chain³ governance, to maintain consensus rules⁴, as well as an off – chain governance, using the Politeia governance platform and a timestamping client/server architecture.

4 Assessing blockchain governance

The main goal of this study is to analyse how the Decred project has implemented security measures and is capable of improving blockchain governance. The following sections show details about how Decred improves security, how it 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.

This research uses publicly available data from the Decred and bitcoin blockchains between 08 February 2016 and 10 February 2020. For Decred, the data was obtained from PostgreSQL database used in dcrdata,⁵ the free, open source block explorer. For bitcoin, the data was obtained from Blockchain.com. Price information in USD was obtained from Yahoo Finance.^{6,7}

For Section 4.1, the probability distribution used inside the script was obtained from querying the above PostgreSQL database. For Section 4.2, the calculations used data obtained from the sources above. For Section 4.3, 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.

4.1 Security and the opportunity cost of an attack

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:

- 1 rent the equipment
- 2 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 an attack may devalue those coins, increasing the risk for the attacker.

Equation (1) 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. Equation (2) 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.

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

$$P(y) = \sum_{k=0}^{N/2} \binom{N}{k} y^{N-k} ((-y) \cdot p)^k \quad (1)$$

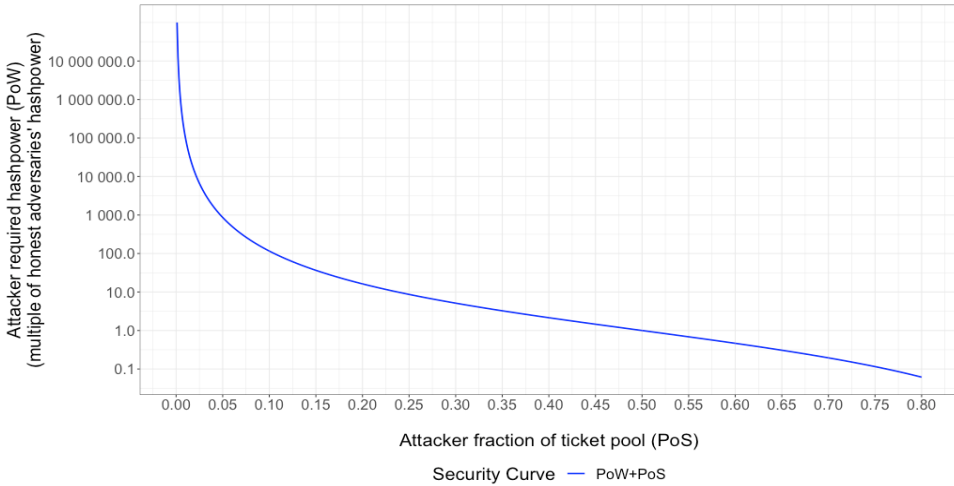
Source: Stafford (2019)

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

$$x(y) = \frac{1}{P(y)} - 1 \quad (2)$$

Source: (Stafford, 2019)

Figure 2 security curve created by PoW+PoS combined authentication (see online version for colours)



Source: Own elaboration

Figure 2 shows the security curve as a result of the PoW + PoS authentication mechanism. 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. Also, note that the point $(x = 0.5, y = 1.0)$ in the security curve 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. This is called the ‘majority attack’, or ‘51% hashpower attack’, a situation when a powerful and wealthy adversary is able to acquire the same processing capacity as the honest nodes.

We use publicly available data for mining devices regarding Capex and Opex to estimate an attack against Decred and bitcoin. The adversary has two options:

- 1 an external/internal attack, which means buying equipment on the market and coins from the stakeholders
- 2 an internal/internal attack that accounts for rental of cloud mining devices and acquisition of Decred to buy tickets.

4.1.1 External/internal attack

We start by estimating the cost of an external/internal attack where the attacker buys equipment from vendors (external) and coins from traders or miners using fiat money (internal). This scenario is unrealistic because 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.

The cost of an external PoW + internal PoS attack against the 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 February 2020 (Table 1, Table 2, Table 3).

Table 1 Decred proof-of-work equipment and network hashpower

(A)	ASIC device: DCR5 (34 Th/s, 1610W, USD 1282)	34	Th/s
(B)	Decred network hashpower on 10 February 2020	450,150	Th/s
(C = B/A)	ASIC devices for 1x attack (more 450,150 Th/s)	13,240	unit
(D = 1610W * C)	ASIC devices will spend 1610W * 13,240 units	21,316	kWh
(E = USD 1282 * 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)	1066	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 2 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 3 Total cost (PoW + PoS) of an attack against Decred on 10 February 2020

(K + E)	Capex: USD 58,725 109 (PoS) + USD 16,973 680 (PoW)	75,698,789	USD
(F + H)	Opex: 1066 USD/h + 1179 USD/h (PoW)	2245	USD/h

Source: Own elaboration

The cost of an external attack against the Bitcoin blockchain considers hashpower, current equipment, facility cost estimation and electricity price on 10 February 2020 (Table 4, Table 5):

Table 4 Bitcoin proof-of-work equipment and network hashpower on 10 February 2020

(L)	ASIC dev: Antminer S17+ (73 Th/s, 2920W, USD 2580)	73	Th/s
(M)	Bitcoin network hashpower on 10 February 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 = 2920W * N)	ASIC devices will spend 2920W * 1,472,953 units	4,301,023	kWh
(P = USD 2 580 * N)	Cost to buy 1,472,953S17+ units: 1,472,953 * USD 2580	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 5 Cost (PoW) of an attack against Bitcoin on 10 February 2020

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

Source: Own elaboration

We estimate that considering current hashpower and price in USD, an external/internal attack on the Decred network would cost 0.0199 times an external attack on the bitcoin network. Using the same metrics, an external attack on Bitcoin costs 50 times more than an attack on Decred (Table 6).

Table 6 Most expensive to attack (external/internal) on 10 February 2020

Most expensive to attack	1 hour	
Decred (external/internal)	0.0199	x than Bitcoin
Bitcoin (external)	50.2067	x than Decred

Source: Own elaboration

4.1.2 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). Nicehash⁸ is one of these cloud mining companies renting processing power for some hashing algorithms. Crypto51⁹ website calculates the cost of 1h attack for several PoW cryptocurrencies and how much hashrate 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 2).

Table 7 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 8 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 7 Total cost of internal/internal attacks on 10 February 2020

(K)	Decred Capex: USD 58,725,109 (PoS)	58,725,109	USD
(F + H)	Decred Opex: 1066 USD/h + 1178 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 8 Most expensive to attack (internal/internal) on 10 February 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 8 shows that Decred is over 120 times more secure than bitcoin for 1-hour attacks on 10 February 2020, meaning Decred is more expensive to internally attack than bitcoin.

Note that these computations only include the cost of an internal attack, not its rewards. Moroz et al. (2020) explain 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. (2020) show in equation (3) that in a competitive miner economy (under certain conditions of hashrate price and availability), the cost spent on 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:

$$P_b = \text{hash perblock} \times \text{cost per hash}$$

For e blocks, the cost of length e attack – block rewards for e blocks is null:

$$eP_b - eP_b = 0 \tag{3}$$

Source: adapted from Moroz et al. (2020)

Moroz et al. (2020) argue 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 (cost to perform an attack minus the block reward for a successful attack) shown in equation (3), any profit from the attack (the double-spending) will make the profit greater than the net cost of the attack. 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.

For Hasu et al. (2019) 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.

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, the InvalidationGame¹⁰ has been developed¹⁰ a Python script that simulates a double-spending attack to show the probability of success of an attack when perpetrated against a pure PoW blockchain and also against a PoW + PoS one (the logic behind the InvalidationGame can be synthesised on the algorithm pseudo code in Appendix 1). 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 coin¹¹ 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 six 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:

- 1 the sabotage performed by wealthy adversaries, like governments
- 2 an adversary mining empty blocks.

The results shown in Table 9 and Table 10 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.

Considering the scenario where the dishonest adversary has slightly more power than the honest nodes (50% + 1 of PoW devices and PoS tickets), Table 9 and Table 10 show the result of 100, 000 simulations for this setup for both attack scenarios. We may observe that the PoW simulation took 32 min 25 secs while the PoW + PoS simulation took 7 h 02 min, which shows the increase in cost to attack such networks (e.g., Decred).

Table 9 Result of 100,000 49.99%/50.01% PoW simulated attacks

<i>Number of simulations: 100,000</i>				<i>Average: 0.2092 seconds, Total: 07:02:19</i>		
<i>Adversary</i>	<i>Hashpower</i>	<i>Stake</i>	<i>Sims won</i>	<i>Sims won</i>	<i>Avg. invalid blocks</i>	<i>Avg. valid blocks</i>
A0	49.99%	49.99%	49,785	49.7850%	18.7086	17.9623
A1	50.01%	50.01%	50,215	50.2150%	18.6579	18.0050
On average, 2-block and 6-block advantage reached in: 4.9870 and 36.9674 blocks						

Notes: For A1, the attack cost, on average: 18.0050 PoW block rewards, due to PoS invalidation.

Source: Own elaboration

Table 10 Result of 100,000 49.99%/50.01% PoW+PoS simulated attacks

<i>Number of simulations: 100,000</i>				<i>Average: 0.2092 seconds, Total: 07:02:19</i>		
<i>Adversary</i>	<i>Hashpower</i>	<i>Stake</i>	<i>Sims won</i>	<i>Sims won</i>	<i>Avg. invalid blocks</i>	<i>Avg. valid blocks</i>
A0	49.99%	49.99%	49,785	49.7850%	18.7086	17.9623
A1	50.01%	50.01%	50,215	50.2150%	18.6579	18.0050
On average, 2-block and 6-block advantage reached in: 4.9870 and 36.9674 blocks						

Notes: For A1, the attack cost, on average: 18.0050 PoW block rewards, due to PoS invalidation.

Source: Own elaboration

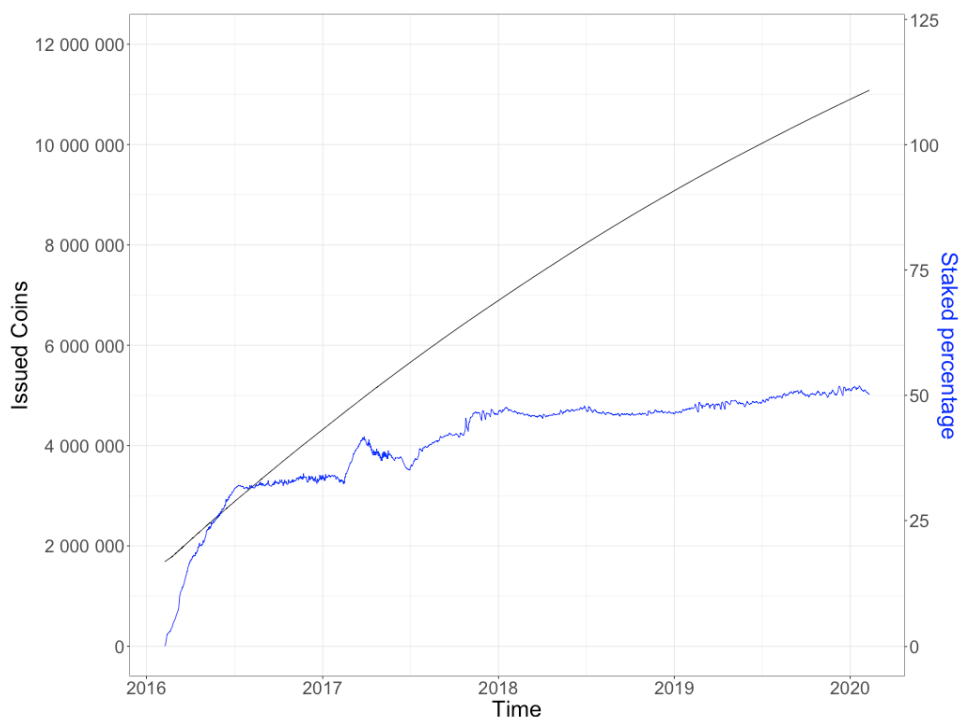
4.3 Testing governance hypotheses

The period of time investigated in this section comprises the launch of the Decred network on 8 February 2016, where the genesis block (name given to the first block) was mined, and 10 February 2020, four years after the first exchange rate in USD available in Yahoo Finance.¹² February 2020 also avoids significant market impacts that may be related to COVID-19 pandemic.¹³ The data was extracted from *dcrdata*, Decred's own block explorer, from Yahoo! Finance and Blockchain.com website and is available at Decred Governance Data Analysis Github code repository,¹⁴ along with the R and SQL scripts used to extract and process the data.

Hypothesis 1 The Decred staked percentage is related to coin issuance

The staked percentage corresponds to the amount of coins locked up in tickets. Figure 3 and Table 11 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.

Figure 3 Issued Decred coins and staked percentage (see online version for colours)



Source: Own elaboration

Table 11 Correlation between issued Decred coins and staked percentage

<i>Selected sample from</i>		<i>All time</i>	<i>> 10 February 2017</i>
N		1,464	1,096
Pearson's Correlation		0.8994	0.9045
Significance test	p-value	< 2.2e-16	< 2.2e-16

Source: Own elaboration

Hypothesis 2 The 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 waiting for the price possibly to go back up.

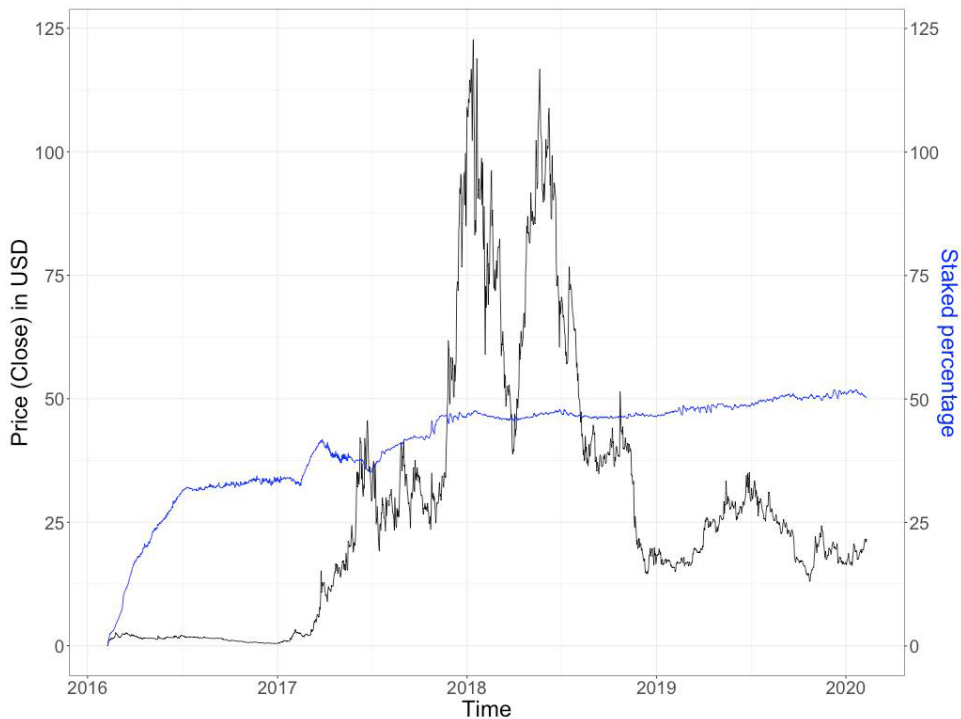
Figure 4 and Table 12 show Decred price in USD and the staked percentage of issued Decred coins. One year after the project was launched, on 10 February 2017, 33% of all issued coins were locked up in tickets and this number increased to 50% on 10 February 2020. In summary

- 1 additional coins are issued every day
- 2 investors keep showing long-term interest in the project, locking up their coins for up to 143 days to get a reward
- 3 this reward goes down as time goes by, because the reward drops by circa 1% every 21.33 days.

On the other hand, the slight increase in the staked percentage between February 2017 and February 2020 (period selected due to the curve shown on Figure 4) does not explain the price variation during the same period. Additional questions should consider if

- 1 price could increase in case of reduced offer of Decred in the market
- 2 price could decrease if the market understands that there is not enough Decred liquidity to be regularly used as currency
- 3 staked percentage could increase or decrease if the price respectively decreases or increases, 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 4 Decred price and staked percentage (PoS security) (see online version for colours)



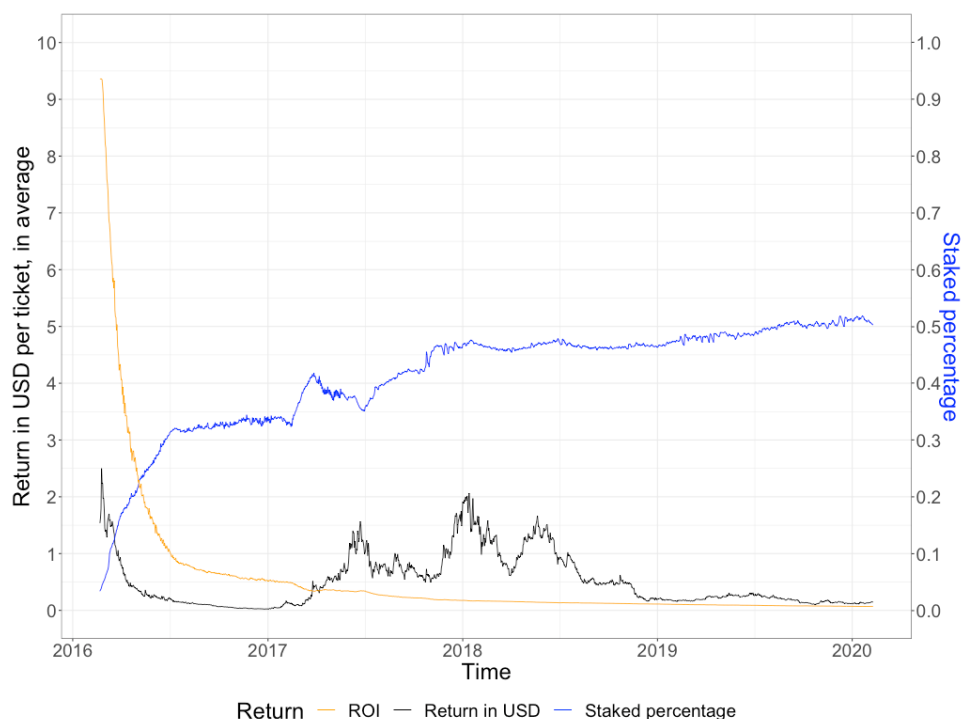
Source: Own elaboration

Table 12 Correlation between Decred price and staked percentage

Selected sample from		> 10 February 2016	> 10 February 2017
N		1,462	1,096
Pearson's correlation		0.4970	0.123
Significance test	p-value	0.0176	1

Source: Own elaboration

Figure 5 and Table 13 explore the correlation between the percentage of staked coins and the return in USD per ticket, on average, to investigate a relation between a possible drop in return and the incentives the investors have to keep staking.

Figure 5 Return in USD per ticket and staked percentage (PoS security) (see online version for colours)

Source: Own elaboration

Against the expectations, the return in USD shows a weak inverse correlation with the staked percentage, indicating that even with 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 February 2016 with a ROI of 93.59% and ends on 10 February 2020 with 0.69%. It means that on 21 February 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, on average.

Table 13 Correlation between return in USD per ticket and staked percentage

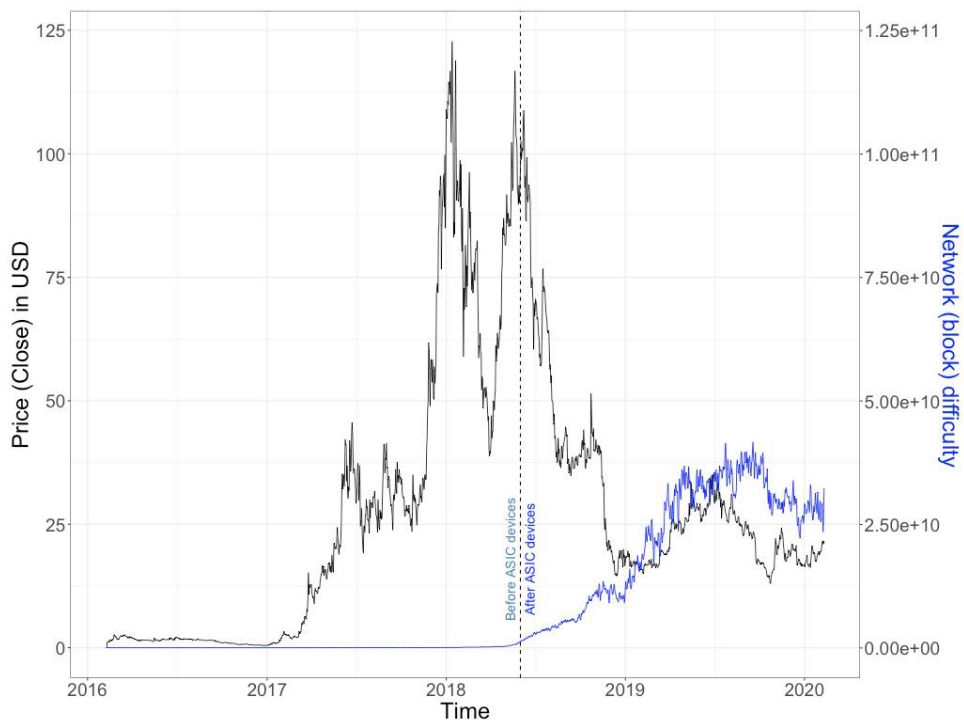
Selected sample from		> 21 February 2016	> 10 February 2017
N		1,450	1,083
Pearson's correlation		-0.0711	-0.3177
Significance test	p-value	1	1

Source: Own elaboration

Hypothesis 3 PoW security is related to price

As shown in Section 4.1, an increase in cryptocurrency security could increase the perceived value and drive its price up. Investors might also turn off mining devices if the cryptocurrency price is not enough to cover the costs of running them to provide security to the network, driving its price down. Figure 6 and Table 14 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 6 Decred price and network difficulty (PoW security) (see online version for colours)



Source: own elaboration

Table 14 Correlation between Decred price and network difficulty

<i>Selected sample from</i>		<i>All time</i>	<i>< 30 Dez 2018</i>	<i>> 01 Jan 2019</i>
N		1,464	1,058	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

Hypothesis 4 Decred founders' expenditure is related to price variance

Speculation (or panic) happens in the markets when founders, or an entity the market assumes as the founder, sell coins mined at the beginning of the project. It recently happened¹⁵ to a bitcoin unspent transaction (coins) mined in 09 February 2009, where 40 BTC were spent. To understand the scenario when it comes to Decred founders' pre-mined coins, Table 15 shows the percentage and amount in DCR from the founders' and airdroppers' pre-mine on block #1 spent until 10 February 2020.

Table 15 Decred founders' and airdroppers' pre-mine issuance and expenditure

<i>From 08 February 2016 to 10 February 2020</i>	<i>N</i>	<i>Issued</i>	<i>Spent</i>	<i>Spent (%)</i>	<i>Spent (%) in 2016</i>
Founders' pre-mine	174	840,000	353,290	42.06	31.34
Airdroppers' pre-mine	2972	840,000	549,165	65.38	50.1

Source: Own elaboration

Figure 7 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 13) 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 assumed to be the founders, whose knowledge of blockchain technologies and security is extensive. It is not possible to ascertain 2,972 different persons in the airdrop because one person might have subscribed many times using different email addresses.

Table 15 and Figure 7 show that some founders decided to stake from the project launch and some investors envisioned 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% per drawn ticket every 20 days, on average, when the ticket price was DCR 2, as shown in Figure 6.

Hypothesis 5 The Decred price variance is related to Bitcoin price variance.

Figure 7 Decred founders' pre-mine expenditure of original transactions (see online version for colours)



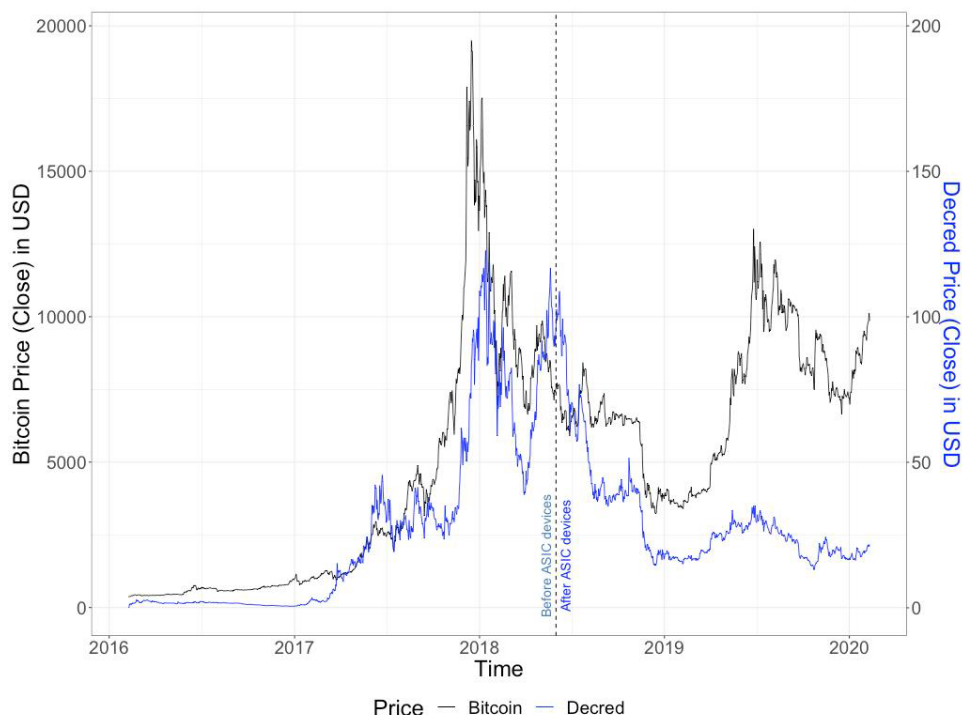
Source: Own elaboration

For the past years, empirical knowledge established that bitcoin and the alternative currencies tend to stay together for some periods of the year and go opposite ways on others. Figure 8 and Table 16 show that this was true for Decred and bitcoin until 01 Jun 2018, when the 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 February 2020, Decred and bitcoin exchange rates to USD were uncorrelated. As shown in Figure 8, bitcoin price movements do not seem to influence Decred price movements as it did before that date, when they were strongly correlated.

Table 16 Correlation between Decred and Bitcoin prices (close) in USD

Selected sample from	All time	< 30 May 2018	> 01 June 2018
N	1,464	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

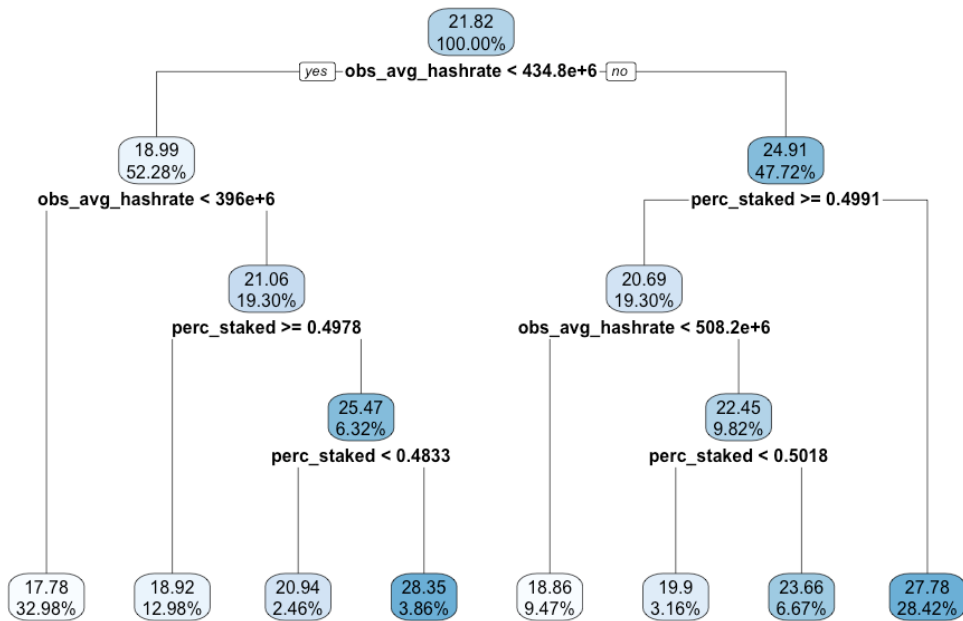
Figure 8 Decred and bitcoin prices (close) in USD (see online version for colours)

Source: Own elaboration

When this information is analysed together with Table 14 and Figure 6 that show 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 the 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-256¹⁶ and Decred uses BLAKE-256¹⁷.

Other studies also analyse PoW and PoS. Cao et al. (2020) compare the consensus mechanisms in the blockchain and conclude that the consensus process is affected by the computation power. Han et al. (2023) compare PoW and PoS in terms of transaction settlement and, using historical data show that the optimal block time, average settlement time and average settlement fees, of the PoS are less than that of the PoW.

Sapkota and Grobys (2020) use portfolio analysis to explore whether energy is a fundamental economic factor affecting cryptocurrency prices. They conclude that cryptocurrencies employing PoW consensus protocols do not generate returns that are significantly different from those that incorporate PoS consensus protocols. They also show that cryptocurrencies that incorporate the hybrid version of these consensus protocols generate significantly higher average returns than others.

Figure 9 Regression tree with hashrate and staked percentage (see online version for colours)

Source: Own elaboration

4.4 Regression tree analysis

Figure 9 shows the relation between price, average hashrate and staked percentage using a regression tree, a machine algorithm built through a binary recursive partitioning based on an iterative process that splits the data into partitions or branches (Breiman et al., 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 into training and 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. We may conclude that average hashrate and staked percentage are the most important variables to explain 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 predicting 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 February 2020.

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 guns¹⁸ 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).

The 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 may 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 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 a voting system is the patent filed¹⁹ by the USA Postal Service (USPS) on 13 Aug 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. 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.

This research showed how secure blockchain technologies increase governance and avoid trusted third parties, providing security, transparency, incentives, change rules and network coordination. We explored first an external PoW/internal PoS attack scenario, where the attacker has to buy ASIC devices on the market but the coins would have to be bought from current stakeholders, and then an internal PoW/internal PoS attack, accounting for rental of cloud mining devices and acquisition of Decred to buy tickets. We showed 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). In addition, we developed a simulation script called *InvalidationGame* to show that the cost of performing such an attack in terms of time and forgone block rewards was much higher when performed against PoW + PoS networks.

We also used real blockchain data to analyse Decred governance and observed that:

- 1 Decred USD exchange rates were moderately correlated to Decred network difficulty (which increased after the release of ASIC devices as expected)
- 2 the staked percentage of Decred coins is related to the amount of issued coins but not to the USD exchange rate

- 3 that Decred founders have spent part of their original pre-mine transactions (coins), mostly buying tickets.

But Decred stakeholders do not seem to be concerned about being outvoted due to founder's increasing stake size given that

- 1 the staked percentage increased after privacy feature launch
- 2 the founders' pre-mine is well-known since before the project launch
- 3 founders' expenditure were public from the start until the privacy feature.

It should be said that since 2020, and due to both the pandemic and Ukraine war that induced severe supply chain problems, and also because the FED raised interest rates, a bubble developed as in times of turbulence agents seek refuge in the dollar. In addition, many currencies such as Decred have a strong correlation with bitcoin's price, and in times of insecurity, investors also rush from these currencies to bitcoin. For these reasons and since 2021, the price of cryptocurrencies has decreased. In a future study, the robustness of our results could be tested considering data after 2021.

We ended with a regression tree that explored the influence of average hashrate and staked percentage on price. It showed that PoW security has great influence on price, as lower prices happened when the network had lower hashrates (PoW security). Further research could include the use of this technology to improve the security of current voting machines and blockchain – based governance to solve and replace centralised organisations.

References

- Bank of England (2019) *What is Quantitative Easing?* Retrieved November 25, 2019, from Bank of England [online] <https://www.bankofengland.co.uk/monetary-policy/quantitative-easing> (accessed 1 December 2015).
- Bentov, I., Gabizon, A. and Mizrahi, A. (2014) *Cryptocurrencies without Proof of Work*, ArXiv, abs/1406.5694.
- Bentov, I., Lee, C., Mizrahi, A. and Rosenfeld, M. (2014) 'Proof of activity: extending bitcoin's proof of work via proof of stake', Casale, G. (Ed.): *ACM SIGMETRICS Performance Evaluation Review*, 8 December, Vol. 42, No. 3, Retrieved November 20, 2019.
- Bitcoin Community. (2017) *Genesis Block*, Retrieved November 26, 2019, from Bitcoin Wiki [online] https://en.bitcoin.it/wiki/Genesis_block (accessed 30 November 2017).
- Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A. and Felten, E.W. (2015) 'SoK: research perspectives and challenges for bitcoin and cryptocurrencies', *2015 IEEE Symposium on Security and Privacy*, IEEE, San Jose, CA, USA.
- Breiman, L., Friedman, J., Olshen, R. and Stone, C. (1984) *Classification and Regression Trees*, Wadsworth, Inc., New York.
- Budish, E. (2018) *The Economic Limits of Bitcoin and the Blockchain*, Retrieved September 19, 2020 [online] <https://faculty.chicagobooth.edu/eric.budish/research/Economic-Limits-Bitcoin-Blockchain.pdf> (accessed 5 June 2018).
- Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M. and Li, Y. (2020) 'Performance analysis and comparison of PoW, PoS and DAG based blockchains', *Digital Communications and Networks*, No. 2020, <https://doi.org/10.1016/j.dcan.2019.12.001>.
- De Filippi, P. and Loveluck, B. (2016) 'The Invisible politics of bitcoin: governance crisis of a decentralized infrastructure', *Internet Policy Review*, 17 October 2016, Vol. 5, No. 4.

- Decred Project (2016) *Decred Constitution*, Retrieved November 20, 2019, from Decred Project [online] <https://docs.Decred.org/governance/Decred-constitution> (accessed July 2020).
- Decred Project (2019) *Ticket Splitting*, Decred Documentation [online] <https://docs.Decred.org/proof-of-stake/ticket-splitting> (accessed July 2020).
- Decred Project (2020) *Proof-of-Stake (PoS) Voting*, Retrieved February 9, 2020, Decred Docs [online] <https://docs.Decred.org/proof-of-stake/overview> (accessed September 2020).
- Elliott, F., and Duncan, G. (2009) *Chancellor Alistair Darling on Brink of Second Bailout For Banks*, Retrieved November 20, 2019, The Times [online] <https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h>. (accessed 3 January 2009).
- Enterprise Estonia (2019) *KSI Blockchain* [online] <https://e-estonia.com/solutions/security-and-safety/ksi-blockchain> (accessed September 2020).
- European Commission (2019) *Blockchain For Digital Government*, Publications Office of the European Union. Retrieved from EU Science Hub, Luxembourg [online] <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government>.
- European Commission (2018) *Blockchain and the GDPR*, Retrieved November 20, 2019, EU Blockchain Observatory and Forum [online] https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (accessed 16 October 2018).
- European Parliament (2016) *EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679*, Retrieved November 25, 2019, Eur-Lex [online] <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed September 2020).
- Ferreira, D., Li, J., and Nikolowa, R. (2019) *Corporate Capture of Blockchain Governance*, , March 25, European Corporate Governance Institute (ECGI) – Finance Working Paper No. 593/2019.
- Han, K., Choi, J.H., Choi, Y., Lee, G.M. and Whinston, A.B. (2023) ‘Security defense against long-term and stealthy cyberattacks’, *Decision Support Systems*, Vol. 166, p.113912, <https://doi.org/https://doi.org/10.1016/j.dss.2022.113912>.
- Hardin, G. (1968) ‘The tragedy of the commons’, *Science*, Vol. 162, No. 3859, pp.1243–1248.
- Hasu, Prestwich, J. and Curtis, B. (2019) *A Model For Bitcoin’s Security and the Declining Block Subsidy*, Retrieved September 19, 2020 [online] <https://uncommoncore.co/wp-content/uploads/2019/10/A-model-for-Bitcoins-security-and-the-declining-block-subsidy-v1.05.pdf> (accessed October 2019).
- Johnson, D. (2019) ‘Blockchain-based voting in the US and EU constitutional orders: a digital technology to secure democratic values?’, *European Journal of Risk Regulation*, 18 September, Vol. 10, No. 2, pp.330–358.
- Krugman, P. (2018) *Transaction Costs and Tethers: Why I’m a Crypto Skeptic*, February 6, 2020, from The New York Times: <https://www.nytimes.com/2018/07/31/opinion/transaction-costs-and-tethers-why-im-a-crypto-skeptic.html> (accessed 31 July 2018).
- Martins, M. (2018) *The Origin of Decred*, Retrieved November 20, 2019, Stakey Club [online] <https://stakey.club/en/the-origin-of-Decred> (accessed September 2020).
- Milunovich, G. (2022) ‘Assessing the connectedness between Proof of work and proof of stake/other digital coins’, *Economics Letters*, Vol. 211, No. 110243.
- Moroz, D.J., Aronoff, D.J., Narula, N. and Parkes, D.C. (2020) ‘Double-spend counterattacks: threat of retaliation in proof-of-work systems’, *Cryptoeconomic Systems 2020*, MIT, Cambridge, MA, USA.
- Nakamoto, S. (2008) *Bitcoin: A Peer-To-Peer Electronic Cash System*, Retrieved November 22, 2019, Nakamoto Institute [online] <https://nakamotoinstitute.org/bitcoin/> (accessed 31 October 2008).

- Reijers, W., Wuisman, I., Mannan, M. and De Filippi, P. (2018) 'Now the code runs itself: on-chain and off-chain governance of blockchain technologies', *TOPOI: International Review of Philosophy*, Vol. 37, No. 17, Springer Link [online] <https://link.springer.com/article/10.1007/s11245-018-9626-5> (accessed September 2020).
- Rhodes, R.A.W. (2007) 'Understanding governance: ten years on', *Organization Studies*, Vol. 28, No. 8, pp.1243–1264.
- Sapkota, N. and Grobys, K. (2020) 'Blockchain consensus protocols, energy consumption and cryptocurrency prices', *Journal of Energy Markets*, Vol. 13, No. 4, pp.117–139, DOI: 10.21314/JEM.2020.221.
- Stafford, B. (2019) *Parametrized Cost of Attack as a Measure of Decred Network Security*.
- Stiglitz, J. (2019) *Thumbs Down to Facebook's Cryptocurrency*, Retrieved February 20, 2020, Project Syndicate [online] <https://www8.gsb.columbia.edu/articles/chazen-global-insights/thumbs-down-facebook-s-cryptocurrency> (accessed 2 July 2019).

Notes

- 1 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 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 et al., 2014).
- 2 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 to the 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 had cooperated and paid their fees.
- 3 <https://voting.Decred.org> (accessed 6 June 2020).
- 4 <https://docs.Decred.org/governance/consensus-rule-voting/overview/> (accessed 6 June 2020).
- 5 dcrdata [online] <https://github.com/Decred/dcrdata> (accessed 16 July 2020).
- 6 Bitcoin USD Price [online] <https://finance.yahoo.com/quote/BTC-USD/history?period1=1454716800&period2=1586131200&interval=1d&filter=history&frequency=1d> (accessed July 2020).
- 7 *Decred USD Price* [online] <https://finance.yahoo.com/quote/DCR-USD/history?period1=1454716800&period2=1586131200&interval=1d&filter=history&frequency=1d> (accessed July 2020).
- 8 <https://www.nicehash.com> (accessed 19 September 2020).
- 9 <https://www.crypto51.app> (accessed 19 September 2020).
- 10 InvalidationGame [online] <https://github.com/mmartins000/invalidationgame> (accessed 31 May 2020).
- 11 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.
- 12 DCRUSD exchange rates [online] <https://finance.yahoo.com/quote/DCR-SD/history?period1=1454716800&period2=1586131200&interval=1d&filter=history&frequency=1d> (accessed 10 July 2020).

- 13 *Bitcoin Jumps To Highest Level Since March's Coronavirus Crash* [online] <https://www.bloomberg.com/news/articles/2020-04-23/bitcoin-jumps-to-highest-level-since-march-s-coronavirus-crash> (accessed 10 July 2020).
- 14 *Decred Governance Data Analysis* [online] <https://github.com/mmartins000/Decred-gov-data-analysis> (accessed 12 September 2020).
- 15 *Crypto Faithful Flip Out on Speculation Satoshi Sold Bitcoin* [online] <https://www.bloomberg.com/news/articles/2020-05-20/crypto-faithful-freak-out-amid-speculation-satoshi-sold-bitcoin>, (accessed 16 July 2020).
- 16 NIST Hash Functions, available at <https://csrc.nist.gov/projects/hash-functions>, last accessed 16 July 2020
- 17 BLAKE-256 hash function, available at <https://docs.decred.org/research/blake-256-hash-function/>, last accessed 16 July 2020
- 18 *Venezuela's Latest Problem Is There Are Now Too Many Dollars* [online] <https://www.bloomberg.com/news/articles/2020-01-03/venezuela-s-latest-problem-is-there-are-now-too-many-dollars> (accessed 06 February 2020).
- 19 *US Patent Application Publication no. US 2020/0258338 A1, Secure Voting System* [online] <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.PG.NR.%2526OS=%2526RS=>, (accessed 29 August 2020).

Appendix 1

Algorithm pseudo code

Main function:

Run batch of simulations(sims)

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

Source: Own elaboration

Algorithm pseudo code (continued)

```

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