Extortion of a Staking Pool in a Proof-of-Stake Consensus Mechanism

Alpesh Bhudia*, Anna Cartwright†, Edward Cartwright‡, Julio Hernandez-Castro§, Darren Hurley-Smith*
* Royal Holloway, University of London, † Oxford Brookes University, ‡ De Montfort University, § University of Kent

2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS) | 978-1-6654-8356-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/COINS54846.2022.9854946

***Abstract*—Cryptocurrencies to date, most notably Bitcoin, have primarily relied on a proof-of-work system to validate and process transactions on the blockchain. Proof-of-work systems have, however, several limitations, such as enormous energy demands, and so are likely to be replaced by proof-of-stake systems. These systems use a mechanism that does not rely on mining power but the amount of stake owned by a node, allowing randomly selected validators to create blocks and verify blocks created by other validators. Proof-of-stake systems naturally result in staking pools where in a third party organisation operates validators on behalf of investors who have staked in the currency. Given they have oversight for a large amount of staked currency, staking pools are a prime target for malicious actors. In this paper we explore the economic implications of an attack on a staking pool. We pay particular attention to how the staking pool and clients could resolve an extortion attack by a malicious actor who has accessed relevant signing keys.**

***Index Terms*—game theory, blockchain, PoS, ransom attacks**

I. Introduction

Cryptocurrencies have now become an accepted way for financial investors to diversify their portfolio [28], [38]. As demonstrated by Bitcoin (a peer-to-peer version of electronic cash introduced in 2008) they also have the potential to become a routine form of payment across the world [29]. In January 2021, the market capitalisation of cryptocurrencies reached $1 trillion for the first time, while the latest valuation has exceeded over $2 trillion [36]. There also now exist over 6000 cryptocurrencies [14]. Most cryptocurrencies rely on a decentralised ledger known as the blockchain. This allows all transactions across a peer-to-peer network to be secured by cryptography [26]. For a blockchain to function effectively on a global scale, the public ledger needs to be able to securely, achieve common agreement on a single data value among distributed processes or systems. This is achieved through the implementation of a consensus algorithm which defines a set of rules that all nodes in the network must follow to add new blocks to the chain.

Most consensus algorithms to date, like Bitcoin, rely on proof-of-work (PoW). In the PoW algorithm, miners (participating nodes in the network) solve computationally rigorous puzzles to validate and create new blocks of transactions in the cryptocurrency's blockchain [7]. Miners are rewarded (with cryptocurrency) if they are the first to find a valid solution to the puzzle. Miners compete, therefore, using physical scarce resources in the form of electricity and dedicated mining equipment to solve puzzles and earn currency. PoW has many undesirable consequences. For instance, it means that mining is only profitable in countries with the lowest price for electricity [16]. Mining is also highly inefficient in terms of energy use and duplication of effort [37]. PoW is not, therefore, a viable way for blockchain and cryptocurrencies to work in the long term.

Many new and existing cryptocurrencies, such as Ethereum, are migrating from Bitcoin's legacy PoW system to proof-of-stake (or a hybrid approach, such as Decred [22]) [20], [23], [25]. In a proof-of-stake (PoS) system owners of block creation is performed by *validators* who have *staked* currency as collateral. In return for participating in the block creation and validation process, validators receive crypto rewards. A PoS system has many advantages, including reduced energy use and the avoidance of duplication of effort. In allowing anyone with sufficient stake to become a validator, the system can also be more decentralised than PoW has turned out to be.

A potential drawback of a PoS system is that it creates new opportunities for malicious actors. While there are cases of Bitcoin being stolen [17], PoW has proved to be relatively secure. A PoS system is, by its very nature, more vulnerable to attack because currency is staked as part of validation. This inevitably results in more risk. For instance, in Ethereum 2.0, a validation key needs to be in constant use online to perform validation activities, and theft of that key would allow a malicious actor to force financial losses (through loss of stake) on the validator. More generally, a malicious actor could disrupt a validator's actions and, thereby, disrupt the accumulation of staker rewards. If PoS is to be the dominant form of system, it is essential that security implications are fully investigated.

Security in a PoS system is further complicated by the use of staking pools. A staking pool is a third-party business that brings together multiple stakers and performs validation activities on their behalf [21]. This appeals to stakers because they can earn rewards without having to act as validators. The staking pool can profit by taking a cut of validation rewards. It can be expected that most validation in a PoS will be performed by staking pools. In this paper we explore the consequences of an extortion attack on a staking pool. In such an attack the pool could be extorted for potential loss of stake to the pool's clients. As we discuss, there are various economic mechanisms the staking pool could use to resolve

We thank Justin Drake from the Ethereum Foundation for his support and feedback throughout this research.

such an attack.

We proceed as follow: In Section 2 we provide some background information on PoS. In Section 3 we discuss the economic implications of an extortion attack on a staking pool. In Section 4 we conclude.

II. Background

The specific ways in which a malicious actor could disrupt a staking pool will depend on the the currency and validation mechanism. In this section we, therefore, provide a high-level overview of how different PoS systems operate and the ways in which they can be disrupted. We begin by clarifying that there are two basic ways a malicious actor can disrupt a staking pool: slashing and/or reputation loss.

Many PoS currencies, including Ethereum, impose financial penalties on validators that are deemed to have acted against the chain [3], [5]. These penalties are designed to deter attacks on the currency and can be severe. Slashing is a process whereby a significant proportion of a validators stake is 'burned' if the validator is deemed to have behaved against consensus. Slashing is a mechanism to collectively police behaviour. Crucially, however, a malicious actor that has compromised a validator's signing key would be in a position to deliberately perform actions that would result in significant slashing penalties.

As we will discuss shortly, not all PoS currencies implement penalty or slashing strategies in their design. Exceptions include Cardano, Algorand, and Avalance. Here a malicious actor would not be able to directly threaten loss of stake through validation disruption. A successful attack would still, however, be in a position to impact the staking pool's ability to continue participating in the blockchain, thus reducing the flow of rewards [1], [10], [11]. In a competitive financial market, this would almost surely impact negatively on the reputation of the staking pool (or indeed currency) and lead to investors leaving. This would, in turn, impact on the profitability of the staking pool and may force its closure.

Depending on the design of the PoS, the disruption caused by a malicious actor could incur both slashing penalties and reputation loss. It can also impact differently across stakeholders. For instance, an investor in a staking pool potentially faces loss of stake. In this case they risk losing a portion of their investment. Less consequential, but still important in a competitive financial marketplace, is that the flow of rewards to the investor could be less than envisaged, or less than alternative market opportunities. In this case the investor risks opportunity cost losses for foregone profit. The pool operator risks loss of reputation which will impact on their ability to make profit from validation. In essence they risk an undermining of their business model. As we discuss in the economic modelling, a malicious actor may strategically gain from differentiating between types of victims, e.g. investor versus pool operator, to use extortion most effectively.

A. Proof-of-stake

The first cyrptocurrency to adopt the PoS mechanism was Peercoin (PPC) created by Sunny King and Scott Nadal in 2012 [24]. Many cryptocurrencies have followed, in an attempt to solve the problem of PoW mining's high energy consumption [4], [27]. In PoS, validators stake their coins which serves as an economic incentive to act in the network's best interests. On the basis that a validator would not devalue its own assets, stakeholders accept the responsibility to maintain the security of the blockchain. To become a validator, the coin owner must stake specific amounts of coins. The exact amount varies depending on the cryptocurrency. For example, in Ethereum 2.0, a minimum of 32 ETH is required, whereas, in Algorand, it is 1 or more ALGO coins [18].

There are several variations of PoS systems currently in existence, a few prominent ones shown in Table I. As you can see there are various solutions to achieve effective, resource-efficient network governance, including: Pure PoS (PPoS), Delegated PoS (DPoS), Hybrid Proof of Stake (HPoS), Nominated PoS (NPoS), and Liquid PoS (LPoS). PoS systems vary on a number of dimensions. In Table I we focus on penalties for inactivity (i.e. the validator not performing actions), slashing for perceived malicious activity against the currency (e.g. if a validator agrees with a bad block, a portion of their stake funds is slashed), and the expected flow of financial rewards for validation. We briefly discuss four prominent examples of PoS.

1) Algorand: Algorand implements a unique variation of proof of stake based on a new Byzantine Agreement protocol. It is known to be a highly democratised form of PoS with a low minimum staking requirement of 1 ALGO coin to participate in and secure the network. The project was launched in 2019 with an aim to accelerate transaction speed and reduce the time it takes to process/finalise the transactions on its network. The system uses algorithmic randomness to select a validator (verifier) from a set of validators who is responsible for constructing the next block of valid transactions. The most notable feature in Algorand is that all block rewards are proportionally distributed to all coin owners (must hold a minimum of 1 coin and the reward is based on the amount staked) rather than only to the validators. The protocol lacks the mechanism to punish dishonest validators on the network,

TABLE I
Summary of key features in prominent PoS blockchains

	Type	Min Stake	Slashing	Penalty*	Rewards†
Algorand	PPoS	✓	✗	✗	10.05%
Cardano	DPoS	✗	✗	✗	5.07%
Cosmos	PoS	✓	✓	✓	14.22%
Ethereum 2.0	HPoS	✓	✓	✓	4.81%
Polkadot	NPoS	✓	✓	✓	14.02%
Solano	DPoS	✓	✓	✓	5.79%
Tezos	LPoS	✓	✓	✓	5.3%

* Penalty occurred for inactivity or incorrect attestations.
† An estimate staking rewards a validator could earn per year based on [34].

i.e. slashing, which is not deemed a requirement since it is impossible to fork the blockchain due to how the Algorand consensus process works [13], [20].

2) Cardano: Cardano implements a delegated-proof-of-stake (DPoS) based on Ouroboros [23], allowing ADA coin owners who have no desire to run their own validator nodes and participate in the network to transfer all or some of their stake to another stake pool and be rewarded for the amount staked [33]. The DPoS system is one of the fastest blockchain consensus mechanisms, and it can handle a higher number of transactions than the PoW system. In addition, the system allows all coin holders to play a role in influencing network decisions. Similarly to Algorand, Cardano also does not have any mechanism to punish dishonest validators. Instead, its security is based around an opportunity cost of losing rewards and reputation [18].

3) Ethereum 2.0: Ethereum is slowly transitioning from PoW to PoS consensus mechanism, improving the network's security and scalability. A minimum of 32 ETH per validator is required to become a validator, a relatively large amount that means many investors will opt to join a staking pool. As you can see in Table I, Ethereum 2.0 uses slashing and penalties to discourage malicious or 'lazy' validators. The slashing penalty can be anything from 3% of the stake to the whole stake depending on the extent of other recently slashed balances [6]. A slashed validator is also forced to exit, which may take time depending on the size of the exit queue.

4) Tezos: Tezos is a self amending blockchain with similar features to Ethereum, such as a smart contract. It uses the *liquid* proof of stake approach that allows the coin owners to withdraw their stake from a validator (baker) at any time with no lock-up period, unlike Ethereum. In addition, the delegated funds never leave the owner's wallet but rather delegate their rights to a validator to participate in the blockchain on their behalf and collect rewards [8].

B. Slashing and Penalties

In PoS consensus algorithms [Table I], penalties and slashing for malicious activities can play a crucial role in maintaining the integrity of the blockchains. In addition, it also promotes security, honest network participation and availability of the validators. The slashing penalties vary across different blockchains. The two main reasons for enforcing the slashing penalty are i) to make the validator behave responsibly; ii) to make an attack on the network expensive and unattractive. The two common cases when the validator can be charged are: during downtime (validator absent from signing transactions) and double signing (validator signs two or more blocks at the same height) [18].

C. Staking pool

A staking pool provides coin owner/s who have no intention of running their own validator nodes to delegate their participation rights to a third party, such as Binance, Everstake, and Coinbase, while retaining ownership of their assets. Consolidating resources increases the staking pool's voting power and their chances of validating blocks and receiving rewards. Further, it negates the stakeholder's need to worry about the technical implementation and maintenance of setting up and running a validating whilst making a passive income. In comparison to solo staking, the reward earned from staking pool is smaller due to i) the rewards split among many pool participants; ii) fees charged by the pool operator. This is illustrate in Table II [19], [21], [34].

TABLE II
SUMMARY OF KEY FEATURES IN THE POS STAKING POOLS PROVIDERS

	Min*	Lock Up†	Avg. Fee‡	Reward§
Algorand	✓	✗	-	2.55%
Cardano	✗	✗	5.39%	4.99%
Cosmos	✗	✓	7.68%	15.63%
Ethereum 2.0	✗	✗	10.89%	4.44%
Polkadot	✓	✓	4.86%	13.99%
Solano	✗	✓	9.73%	5.84%
Tezos	✗	✗	10.05%	1.96%

* Require a minimum no. of tokens to participate and start earning rewards.
† Period the stakeholder's tokens are not accessible while staking.
‡ The average commission rate of staking providers.
§ An estimate staking rewards stakeholder could earn per year based on [34].

III. ECONOMIC ANALYSIS

In this section we model the potential implications of an extortion attack on a staking pool. In the model time runs in periods $t = 0, 1, ...$ We take as given a a set of investors $N = \{1, ..., n\}$ who want to use PoS as a way to earn financial returns. Let $m_i(t)$ denote the amount of currency investor i has to invest at time t. Let $M(t) = \sum_i m_i(t)$ denote the total balance. There are a set of staking pools $K = \{1, ..., k\}$ who offer a service to investors whereby they take money, perform validation activities and offer a financial return. Let $N_k(t) \subset N$ denote the set of investors in staking pool k at time t and let $I_k(t) = \sum_{i \in N_k(t)} m_i(t)$ denote the total amount invested in staking pool k at time t.

We assume that under normal operations the staking pool will accumulate a return of α in each period from staker rewards. Thus, ceteris paribus, the investment grows from $I_k(t)$ to $(1 + \alpha)I_k(t)$. We assume that if the pool's validator's perform maliciously the staking pool will receive a penalty consisting of fixed penalty $\beta I_k(t)$ and 'special penalty' $\gamma I_k(t)/M(t)$. The fixed penalty is a portion of the amount invested while the special penalty is a function of the amount invested as a proportion of total balance. We do not rule out that $\beta = \gamma = 0$ meaning no penalty (as with Algorand and Cardano).

Staking pools compete across commission rates and 'quality of service' which would include security. We denote by c_k the commission charged by pool k. So, the staking pool makes revenue $c_k \alpha I_k(t)$ in period t. The investor receives return $(1 - c_k)\alpha$. Thus, in normal operations, $m_i(t + 1) = m_i(t)(1 + (1 - c_k)\alpha))$ if investor i invests in staking pool k. Investors

would, everything else the same, prefer a staker with a lower commission. They may, though, also value security and so may be willing to pay a higher commission if they believe this offsets the risk of losing stake. We assume that staking pool incurs cost F_k per period from operating the staking pool.

A. Malicious attack

Suppose that an attacker obtains the validator signing keys of staking pool k at time t and so can enact malicious activities from there onwards. These malicious activities can take two related forms. First, they can enforce a penalty in period t of lost stake. The size of this penalty would be $P(t) = \beta I_k(t) + \gamma I_k(t)/M(t)$. Second, they could disrupt the accumulation of validator rewards and, in so doing, harm the reputation of the staking pool. We assume, given that the staking pool market is competitive, that the loss of reputation would be sufficiently severe to force the liquidation of the staking pool. Specifically investors would withdraw remaining stake meaning the staking pool misses out on future profits. We approximate the loss from foregone gains due to closure of the staking pool as at least $L(t) = c_k \alpha I_k(t)(1 + \delta + \delta^2 + ...) = \alpha I_k(t)/(1 - \delta)$ where $\delta < 1$ is a discount factor. This calculation takes into account that the staking pool loses commission from period t onwards.

The total financial loss to the staking pool from the attack would be $P(t) + L(t)$. The malicious actor could attempt to extort the pool operator based on this potential loss. Specifically, they could extort the pool operator to 'leave them alone' in a way that would be operationalized through a smart contract. The exact nature of the smart contract would need to depend on specific circumstances but could, for instance, be as follows: The pool operator deposits a ransom that is transferred to the malicious actor if and only if the validators are allowed to exit without any penalties or other disruption of validation activities. This would allow the pool operator to set up new, replacement validators and continue operations with only a minimum amount of disruption. The staking pool could, thus, potentially continue operation without any loss of reputation or loss of investors' stake.

In all likelihood the pool operator will not have access to sufficient reserves to cover a payment of $P(t) + L(t)$. This is because the staking pool is a financial intermediary that channels the investments of others. Moreover, the liability of losses $P(t)$ to stake will vary by contractual obligations. In some cases the staking pool will be constituted in a way that the pool operator is directly liable to recompense investors for any lost stake. In this case the pool operator stands to lose $P(t) + L(t)$. In some cases, however, the pool operator will be constituted in a way that the pool is not liable for lost stake (which is seen as an inherent risk). In this case the pool operator stands to lose $L(t)$ and any investor $i \in N_k(t)$ stands to lose $P_i(t) = P(t) \times m_i(t)/I_k(t)$ as given by their share of the penalty. We focus on this latter case.

B. Resolving the financial loss

We now consider the economic strategies open to the malicious actor and staking pool. Recall the malicious actor has the capability to inflict a total loss of $P(t) + L(t)$ on the staking pool k. This would result in losses of $L(t)$ for the pool operator and $P_i(t)$ for investors staked in the pool. We distinguish three broad strategies the malicious actor could employ:

1) The malicious actor demands a ransom of $R < P(t) + L(t)$ is paid by the staking pool operator or losses will be inflicted. In this case the challenge to raise sufficient money to pay the ransom is devolved to the pool operator. The operator could pay the ransom themselves (if $R < L(t)$) and/or can raise money from effected investors. If the malicious actor does not know the identity of investors then it is natural to ransom the pool operator.
2) The malicious actor demands a ransom of R is paid by investor i or losses will be inflicted. In this case the challenge to raise sufficient money to pay the ransom is devolved to the relevant investor. Again, the investor could pay the ransom themselves (if $R < P_i(t)$) and/or raise money from the pool operator and other investors. If the malicious actor knows the identity of a large investor in the staking pool then it may be natural to ransom that investor (e.g. if $P_i(t) > L(t)$ meaning the investor stands to lose more than the pool operator).
3) The malicious actor demands a ransom R_p from the pool operator and ransom R_i from individual investor $i \in N_k(t)$, where $R_p + \sum_i R_i < P(t) + L(t)$. Losses will be inflicted if and only if all ransom demands are met. In this case the malicious actor effectively signals the contribution that each affected party is obliged to pay. It would be incentive compatible for the victims to pay if $R_i < P_i(t)$ and $R_p < L(t)$. Note, however, that side payments between investors and the pool operator would still be possible.

In evaluating the merits of these three strategies from the perspective of the malicious actor we note that the situation facing the pool operator and investors is a collective action problem [30]. This is because any efforts by the pool operator, or an investor, to stop an attack have a spillover external benefit on other investors who also benefit from the attack being stopped. More specifically, the setting has the nature of a threshold public good game, wherein players (the pool operator and investors) need to collective contribute enough to cover the ransom demand and stop attack [9], [15]. The public good in this case is stopping an attack.

Experimental evidence suggests that it can be difficult to coordinate on the provision of a threshold public good [2], [15]. This can partly be explained by concerns over fairness [35]. In our context, the pool operator and investors may disagree over the 'fairest' way to split the cost of covering a ransom demand. The malicious actor would, therefore, want to design the game in a way that maximizes the chances of

TABLE III
PAYOFF IMPLICATIONS FOR INVESTOR 1 OF DEPOSITING THE RANSOM

Investor 1	Pool operator and investors $2,3$	
	All deposit	Not all deposit
Deposit	Lose R_1	Lose $P_1(t)$
Not deposit	Lose $P_1(t)$	Lose $P_1(t)$

the pool operator and investors being able to coordinate and effectively finance the ransom. We identify two mechanisms the malicious actor can use.

The first mechanism is to use individual ransom demands as in strategy (3) above. While this does not rule out side payments between investors, or investors believing the ransom split is unfair, it does provide a very clear guide to the pool operator and investors of the ransom amount they need to pay. This will reduce the risk of coordination failure. If the malicious actor does not know the identity of all the investors then they would be advised to restrict ransom demands to those they do know (and/or exert effort to discover the identity of investors). In practice this means the ransom demand is likely to be focused on the pool operator and the larger investors in the pool.

The second mechanism the malicious actor should use is a 'refund' if the total ransom demand is not met [12], [31], [32]. This can be written into the smart contract. Specifically, a smart contract can be written where the amount deposited by each affected party is common knowledge. If the total ransom demand is met then the malicious actor removes the threat, e.g. by letting the validators exit without penalty. If the total ransom demand is not met then the deposits are returned and the malicious actor takes action against the pool. This returning of deposits means the pool operator or investor has nothing to fear from depositing their ransom amount.

Using the two mechanisms above we can envisage the economic cost-benefit trade-off for the pool operator and investor. Suppose, for example, the malicious actor is able to identify 3 investors $i = 1, 2, 3$ and sets ransom demand $R_p < L(t)$ for the pool operator and ransom demands $R_i < P_i(t)$ for investors $i = 1, 2, 3$. The total ransom demand is $R = R_i + R_1 + R_2 + R_3$. In Table III we summarize the payoff scenarios for investor i. Given that $R_1 < P_1(t)$ it is a weakly dominant strategy for investor 1 to deposit the ransom. It is similarly a dominant strategy for the pool operator and other investors to also deposit the ransom. Thus, the malicious actor can secure a ransom in an incentive compatible way.

IV. CONCLUSIONS

Early crypto-currencies, including Bitcoin, have relied on an energy inefficient proof-of-work consensus mechanism. Proof-of-stake (PoS) consensus mechanisms are likely to become the norm as society moves away from PoW. While PoS resolves the inefficiencies associated with PoW it raises new security concerns. In particular, a PoS system, by its very nature, means that large amounts of money are at stake in performing routine blockchain validation activities. A malicious actor may want to exploit this opportunity for illicit gains. In this paper we have explored the economic consequences of a staking pool being subject to an extortion attack.

A malicious actor who has obtained the validation key of a staking pool can make two distinct threats. First, they can threaten to perform actions that would result in a slashing penalty. A slashing penalty would result in significant loss of stake for investors. Second, they can threaten to disrupt the flow of rewards to investors. This would impact on the reputation of the staking pool and, thus, result in investors withdrawing their stake, which negatively impacts on the profits of the staking pool operator. The exact nature of the threat will depend on the specifics of the PoS implementation. For instance, Cardano does not have slashing penalties and so this threat is removed. Cardano does, though, have an active marketplace in which the reputation of a pool operator will be important.[1]

We show that a malicious actor should distinguish between victims when attempting to extort. In particular, it is in the interests of the criminal to set differentiated ransom demands for affected victims (the pool operator, and investors) based on their potential loss. This allows the malicious actor to 'facilitate' victims paying the ransom by avoiding disagreement or miss-coordination between victims on how to resolve an extortion demand. Realistically the malicious actor would presumably target for extortion the pool operator and some of the larger investors in the pool. A smart contract could be written that allows payment of the ransom with security that the ransom will stop the threat of action against the staking pool. For instance, the smart contract may allow exit of the validators and a 'rest' of the staking pool.

In evaluating the future of PoS systems it is vital to consider the threat of malicious activity against staking pools. In identifying and analysing that threat we hope to promote awareness on the need of both pool operators and investors to carefully evaluate security. Pool operators need to run robust and secure systems in which risks are mitigated. Similarly, investors should evaluate the security of a pool operator and weigh that against the fee or commission the pool operator charges. The early days of PoS may potentially see a 'race to the bottom' in which a free market with low entry costs results in relatively insecure pool operators with low fees thriving. This would open the door for criminals to attack. While security standards will subsequently rise as investors and pool operators 'learn by mistake' we consider it vitally important to try and preempt and avoid such a painful exercise.

ACKNOWLEDGMENT

This project was partly supported by Ethereum Foundation Grant #FY21-0378 'Game theoretic modelling of a ransomware attack on validators in Ethereum 2.0'. The research of Alpesh Bhudia is supported by the EPSRC and the UK

[1] See, for example, https://developers.cardano.org/docs/operate-a-stake-pool/marketing-stake-pool/

government as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/P009301/1).

REFERENCES

[1] ADAGO. Cardano stake pool compromised. [Online] Available: https://twitter.com/AdagoPool/status/1351781426094632965. Accessed: 07/04/2022.

[2] F. Alberti and E. J. Cartwright, "Does the endowment of contributors make a difference in threshold public-good games?" *FinanzArchiv/Public Finance Analysis*, pp. 216–239, 2015.

[3] J.-P. Aumasson, D. Kolegov, and E. Stathopoulou, "Security review of ethereum beacon clients," *arXiv preprint arXiv:2109.11677*, 2021.

[4] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Ieee, 2018.

[5] BeaconScan. Validators slashing — mainnet beacon chain ethereum 2.0 explorer. [Online] Available: https://beaconscan.com/slots-slashed. Accessed: 08/04/2022.

[6] J. Beck, "Rewards and penalties on ethereum 2.0 [phase 0]," [Online] Available: https://consensys.net/blog/codefi/rewards-and-penalties-on-ethereum-20-phase-0/, accessed: 14/06/2022.

[7] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in *International conference on financial cryptography and data security*. Springer, 2016, pp. 142–157.

[8] Blockdaemon. How tezos staking works. [Online] Available: https://blockdaemon.com/docs/protocol-documentation/tezos/how-tezos-staking-works/. Accessed: 09/04/2022.

[9] C. B. Cadsby and E. Maynes, "Voluntary provision of threshold public goods with continuous contributions: experimental evidence," *Journal of public economics*, vol. 71, no. 1, pp. 53–73, 1999.

[10] Cardano. Keep your core node safe. [Online] Available: https://forum.cardano.org/t/spos-do-not-repeat-my-mistakes-keep-your-core-node-/37766. Accessed: 10/04/2022.

[11] Cardano. skey got compromised - staking & delegation / operate a stake pool. [Online] Available: https://forum.cardano.org/t/what-to-do-after-the-node-skey-got-compromised/33617. Accessed: 09/04/2022.

[12] E. Cartwright and A. Stepanova, "The consequences of a refund in threshold public good games," *Economics Letters*, vol. 134, pp. 29–33, 2015.

[13] J. Chen and S. Micali, "Algorand," *arXiv preprint arXiv:1607.01341*, 2016.

[14] Coinmarketcap. All cryptocurrencies list. [Online] Available: https://coinmarketcap.com/all/views/all/. Accessed: 14/04/2022.

[15] R. T. Croson and M. B. Marks, "Step returns in threshold public goods: A meta-and experimental analysis," *Experimental Economics*, vol. 2, no. 3, pp. 239–259, 2000.

[16] O. Delgado-Mohatar, M. Felis-Rota, and C. Fernández-Herraiz, "The bitcoin mining breakdown: Is mining still profitable?" *Economics Letters*, vol. 184, p. 108492, 2019.

[17] A. Extance, "Bitcoin and beyond," *Nature*, vol. 526, no. 7571, p. 21, 2015.

[18] G. Fanti, L. Kogan, and P. Viswanath, "Economics of proof-of-stake payment systems," in *Working paper*, 2019.

[19] H. Gersbach, A. Mamageishvili, and M. Schneider, "Staking pools on blockchains," *arXiv preprint arXiv:2203.05838*, 2022.

[20] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proceedings of the 26th symposium on operating systems principles*, 2017, pp. 51–68.

[21] P. He, D. Tang, and J. Wang, "Staking pool centralization in proof-of-stake blockchain network," *Available at SSRN 3609817*, 2020.

[22] C. Jepson, "Dtb001: Decred technical brief," *Available at https://cryptorating.eu/whitepapers/Decred/decred.pdf*, 2015.

[23] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annual international cryptology conference*. Springer, 2017, pp. 357–388.

[24] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, no. 1, 2012.

[25] J. Kwon, "Tendermint: Consensus without mining," *Draft v. 0.6, fall*, vol. 1, no. 11, 2014.

[26] D. Mechkaroska, V. Dimitrova, and A. Popovska-Mitrovikj, "Analysis of the possibilities for improvement of blockchain technology," in *2018 26th Telecommunications Forum (TELFOR)*. IEEE, 2018, pp. 1–4.

[27] S. Motepalli and H.-A. Jacobsen, "Reward mechanism for blockchains using evolutionary game theory," in *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2021.

[28] M. A. Naeem, I. Mbarki, and S. J. H. Shahzad, "Predictive role of online investor sentiment for cryptocurrency market: evidence from happiness and fears," *International Review of Economics & Finance*, vol. 73, pp. 496–514, 2021.

[29] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[30] M. Olson, *The logic of collective action*. Harvard University Press, 2009, vol. 124.

[31] T. R. Palfrey and H. Rosenthal, "Participation and the provision of discrete public goods: a strategic analysis," *Journal of public Economics*, vol. 24, no. 2, pp. 171–193, 1984.

[32] A. Rapoport and D. Eshed-Levy, "Provision of step-level public goods: Effects of greed and fear of being gypped," *Organizational Behavior and Human Decision Processes*, vol. 44, no. 3, pp. 325–344, 1989.

[33] S. M. S. Saad and R. Z. R. M. Radzi, "Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos)," *International Journal of Innovative Computing*, 2020.

[34] StakingRewards. Earn passive income with crypto — staking rewards. [Online] Available: https://www.stakingrewards.com/. Accessed: 09/04/2022.

[35] E. Van Dijk and H. Wilke, "Coordination rules in asymmetric social dilemmas: A comparison between public good dilemmas and resource dilemmas," *Journal of Experimental Social Psychology*, vol. 31, no. 1, pp. 1–27, 1995.

[36] W. M. VanDenburgh and R. B. Daniels, "Pragmatic realities of bitcoin and crypto-investing," *The CPA Journal*, 2021.

[37] H. Vranken, "Sustainability of bitcoin and blockchains," *Current opinion in environmental sustainability*, vol. 28, pp. 1–9, 2017.

[38] W. Zhang and P. Wang, "Investor attention and the pricing of cryptocurrency market," *Evolutionary and Institutional Economics Review*, vol. 17, no. 2, pp. 445–468, 2020.