**Distributed Ledger Technology Systems**

jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/distributed-ledger-technology-systems/#.YNGyTmgzaUl

* A Note On Native Assets - A DLT system’s native assets are the primary digital asset(s), if any, specified in the protocol. They are by definition endogenous to the system. These assets are typically used by the protocol to regulate record production, pay transaction fees on the network, conduct ‘monetary policy’, or align incentives. For example, Ethereum’s ETH token is its native asset, although the Ethereum blockchain also hosts a wide range of other user-defined tokens (using the ERC20 standard, for example). Native assets generally play a system-critical role in the functioning of the system as they are an essential component of the complex economic incentive design.
* Early open DLT systems exclusively used PoW as a Sybil prevention mechanism. PoW makes it computationally difficult (i.e. costly and time-consuming) to produce new records but easy for others to verify them. In contrast, emerging PoS-based systems use staking of endogenous resources (e.g. native asset) in order to choose the next record producer. PoW systems are resource-intensive but are robust as long as the number of participants is large and sufficiently distributed. In contrast, PoS systems are less resource-intensive than PoW systems, but are also generally vulnerable to ‘nothing-at-stake’ and ‘grinding’ attacks, among others.
* Incentivised Transaction Processing - Incentivised transaction processing refers to the explicit and implicit incentives present in the system to encourage record producers to engage in transaction processing by creating and proposing records. These incentives can be of different nature (e.g. monetary, legal, social) and can be expressed directly by protocol rules (e.g. block rewards in native asset) or by external factors (e.g. contractual agreements established between participants). Many DLT systems use a combination (Table 9). This distinction matters when categorising DLT systems. Open systems such as Bitcoin tend to be secured via economic incentive designs that make use of an endogenous network resource (native asset) as an economic coordination mechanism to align incentives. Dependent systems may use the native token of the system they are dependent upon. In contrast, closed networks with known and vetted participants generally rely on preestablished authority relations through mutual contractual obligations.
* Incentives. Bitcoin and Ethereum are secured through economic incentives: miners have intrinsic monetary incentives in the form of the block subsidy (i.e. newly minted native token units) and transaction fees (denominated in the native token). Record producers in these systems operate on the basis of economic incentives summarised by the Bitcoin white paper as follows: ‘He ought to find it more profitable to play by the rules [...] than to undermine the system and the validity of his own wealth’. As a result, exclusive focus of record producers on economic self-interest ensures a smooth functioning of the system.
* Open networks all require a native asset (generally referred to as cryptocurrency) that is being used as an economic coordination mechanism to align incentives of system participants to work towards a common goal: the native asset plays an essential role in incentivising record producers to process transactions.

**2nd Global Enterprise Blockchain Benchmarking Study**

<https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-enterprise-blockchain-benchmarking-study/>

* DLT systems can be public and permissionless: anyone is free to join, use, and leave the network as well as participate in the network consensus without having to ask for permission. Because these systems have dynamic membership (i.e. the number of peers on the network is unknown and subject to change), they rely on a combination of economic incentives via their native token and game theory in order to properly function and remain secure.
* *Consortium-led* networks should adopt a suitable commercial model that avoids favouring founding members and early adopters too much if others are to be encouraged to join.

**3rd Global Cryptoasset Benchmarking Study**

<https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study/>

* The emergence of governance tokens and new incentive mechanisms are examples of experimental approaches designed to make DeFi protocols less dependent on centralised control.

**DeFi Beyond the Hype. The Emerging World of Decentralized Finance**

<https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf>

* While strictly speaking not required, most DeFi services incorporate token-based incentive structures for important objectives such as liquidity and governance. As shown in Figure 2, these typically involve digital asset holders locking up assets in order to receive payments (similar to earning interest on a certificate of deposit) and DeFi users paying in fees (analogous to interest rates) to access assets from the resulting pool.
* Common mechanisms include lock-up yields that pay interest for immobilizing digital assets in pools, where they serve as liquidity or collateral for a DeFi service; liquidation fees that pay market-makers a percentage of the value of under-collateralized, liquidated loans; and liquidity mining that pays the interest in the form of tokens issued by the DeFi service itself. Because of DeFi’s composable, programmatic architecture, these mechanisms can be further integrated into structures such as yield farming, which optimizes returns from liquidity mining and lock-up yields by automatically moving funds across DeFi services. The earnings rate may be determined in several ways, including a pro-rata share of transaction fees, parameters set through the protocol’s governance process, or a bonding curve that rewards earlier participation.
* The idea of using tokens to incentivize decentralized network growth is not new. It is the essential to the consensus system of Bitcoin and other cryptocurrencies. Coinbase co-founder Fred Ehrsam outlined in 2016 how tokens could be used to help solve the proverbial chicken and egg problem of bootstrapping new networks and marketplaces.7 In the 2017 initial coin offering (ICO) bubble, however, tokens were often sold to speculators who flipped them for a quick profit, providing little functional benefit to the networks.8 DeFi provides a new opportunity for token models that reward long-term focused participants. The provision of capital is not just a payment to fund future protocol development and reward insiders; it is a direct contribution to DeFi activities such as trading, lending, stablecoin collateralization, and insurance. More liquidity increases the value of the network, and some of that value flows back to the liquidity providers. However, well-designed incentive structures and careful attention to leverage and volatility are needed to address risks.
* One of the major applications of DeFi incentive structures is governance. Tokens issued in connection with liquidity mining or related mechanisms often provide governance rights for the DeFi service. Token-holders can vote on proposed changes to protocols, or on defined parameters such as interest rates or collateralization ratios. The scope of decisions that can be made by token holders other than the developers varies. These tokens are tradeable on certain exchanges, with their value in theory tied to the activity level of the issuing DeFi service.
* In addition to its role in incentivizing activity, token-based governance provides a mechanism for further decentralization of DeFi services. As developers cede more control around essential decisions to token holders, their power over the protocol decreases. In many current DeFi projects, token-holder votes can instruct designated signers to change certain protocol values. A further level of decentralization requires multiple designated private keys (an arrangement known as multisig) to make modifications. The endpoint of this process occurs when developers establish a Decentralized Autonomous Organization (DAO) which executes the governance decisions of token votes as automated smart contracts, which no one has special power to countermand. With the benefits of decentralized governance come risks as well. For example, an attacker might use the governance system to impose policies that allow it to drain funds, with no effective means of recourse.
* In mid-2020, an anonymous developer forked the Uniswap software to create SushiSwap. It added a *governance* token, SUSHI, whereby the community votes on major changes to the protocol. A portion of trading fees across the platform are paid out to SUSHI token holders. The potential for value accrual in SUSHI tokens, in addition to liquidity provision, attracted substantial interest in SushiSwap. Uniswap subsequently created a UNI governance token. Uniswap’s cash flows do not yet accrue to the UNI token holders, but Uniswap has announced plans to do so.
* *Am I just concerned with staking to reach consensus? not governance staking? Staking to provide liquidity?*

**What Is Proof-of-Stake (PoS)?**

A blockchain consensus mechanism involving choosing the creator of the next block via various combinations of random selection and wealth or age of staked coins or tokens.

“The Proof Of Stake algorithm uses a pseudo-random election process to select a node to be the validator of the next block, based on a combination of factors that could include the staking age, randomization, and the node’s wealth.”

Each blockchain network may use a different way of calculating staking rewards.

Some are adjusted on a block-by-block basis, taking into account many different factors. These can include:

* how many coins the validator is staking
* how long the validator has been actively staking
* how many coins are staked on the network in total
* the inflation rate
* other factors

For some other networks, staking rewards are determined as a fixed percentage. These rewards are distributed to validators as a sort of compensation for inflation. Inflation encourages users to spend their coins instead of holding them, which may increase their usage as cryptocurrency. But with this model, validators can calculate exactly what staking reward they can expect.

A predictable reward schedule rather than a probabilistic chance of receiving a block reward may look favorable to some. And since this is public information, it might incentivize more participants to get involved in staking.

<https://www.stakingrewards.com/journal/what-is-staking>

Am I drawing conclusions about how it will work on hashgraph based on blockchain examples?

<https://www.nichanank.com/blog/2018/6/4/consensus-algorithms-pos-dpos>

* The goal of all consensus algorithms is for nodes in the network to come to an agreement on the correct transaction history – what they take as the source of truth.
* To motivate participants in the network to behave appropriately, there should be incentives and rewards for "correct" behavior. There may also be a punishment system for those who act against the interests of the network.

In blockchains, code and economics are intrinsically interlinked. When designing a consensus protocol, you want to align your cryptoeconomics such that when an individual participant optimizes personal gain, they optimize the collective outcome of the system as well.

* First ever mention – bitcointalk
* In early implementations of proof-of-stake networks e.g. Peercoin, there are only rewards (transaction fees) for producing valid blocks but no penalties for simultaneously creating blocks on multiple chains. – nothing at stake
* Dpos, pos pros cons trade offs

**Cryptocurrencies without Proof of Work** (Iddo Bentov, Ariel Gabizon, Alex Mizrahi) 2014

* Pure PoS
* PPCoin (Peercoin) and its problems (rational forks;;nothing at stake?;;double-spend(bribe) attack; timeweight
* PPCoin had v0.2, v0.3
* Present CoA that solves them. Follow the satoshi, protocol, punishment, freezing, selfish mining
* Dense-coa, identities not known far in advance

<http://earlz.net/view/2017/07/27/1904/the-missing-explanation-of-proof-of-stake-version>

* Pow, drawbacks
* PoW provides no incentive to use or keep the tokens,… Proof of Stake was invented to solve many of these problems by allowing participants to create and mine new blocks (and thus also get a block reward), simply by holding onto coins in their wallet and allowing their wallet to do automatic "staking"
* PoSv1 (peercoin)-> PoSv1 (blackcoin)-> Proof of Stake Version 3 (qtum, blackcoin)

**Blockchain Without Waste: Proof-of-Stake** (Saleh) 2021

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3183935>

* A permissionless blockchain lacks a central authority and thus attainment of consensus is a nontrivial (significant) issue for such a blockchain.
* What blockchain is, how it works, consensus.
* PoW and how it works, energy consumption problem; Economic limitations of PoW.
* PoS as an alternative, eliminates computational arms race; PoS literature
* PoS - Follow-the-Satoshi (FTS) algorithm, protocol
* Nothing-at-stake problem is actually not valid for PoS (a validator imposes a cost on herself if she updates the blockchain in a manner that persists disagreement) (persistent disagreement lowers the coin price -Bitcoin 2013 example).
* The above does not mean that PoS generates consensus. Conditions under which it does are presented. To generate consensus more easily, PoS protocols should impose minimum stake requirements and maintain low block reward schedules.
* Restricting access to update the blockchain to sufficiently large stakeholders induces an equilibrium that generates consensus expediently. This result arises because the cost of updating the blockchain in a manner that persists disagreement increases with a validator’s stake. That cost increases in a validator’s stake because, as previously referenced, persisting disagreement reduces coin value and stake references the number of coins held. For a sufficiently large stakeholder, the cost of persisting disagreement outweighs the benefit from the block reward and thus a sufficiently high minimum stake requirement to update the ledger generates an equilibrium in which validators coordinate on generating consensus. (Ethereum Casper has minimum stake)
* sufficiently low block rewards help generate consensus. Devaluation of coins due to adding to the shorter branch(fork), should outweigh block rewards, to encourage consensus. zero block reward generates consensus without a restriction on the set of stakeholders that may update the blockchain. sufficiently modest block reward schedule implies that disagreement resolves eventually with probability one within any equilibrium. A modest block reward schedule requires that block rewards offered to validators for updating the ledger be kept small.
* The ability to generate consensus with low block rewards distinguishes PoS from PoW. The reason for this difference arises because PoS requires all validators to hold native coins. That requirement ensures that low block rewards shift validator incentives toward maximizing the value of native coins, which, in turn, encourages validators to seek consensus.
* Some PoS implementations (e.g., Ethereum’s Casper) combat the Nothing-at-Stake problem with explicit punishment schemes. Those implementations require the ability for one branch to detect behavior on other branches, but Brown-Cohen, Narayanan, Psomas, and Weinberg (2018) establish that detection of the Noting-at-Stake problem requires making PoS vulnerable to the DoubleSpending Attack.9 Consequently, developing a PoS incentive structure that overcomes the Nothing-at-Stake problem without explicit punishment is important, and this paper does precisely that by providing restrictions on PoS protocol design parameters that overcome the Nothing-at-Stake problem.
* Nxt blockchain employs a PoS protocol with a zero block reward. Nxt’s online blockchain explorer provides no indication of prolonged forks.16 Moreover, Nxt’s developers assert, “the Nxt network does not experience long blockchain forks, and the low block reward does not provide a strong profit incentive” so that the Nothing-at-Stake strategy is “currently not practical.”
* Digital Signature Scheme (DSS) - precludes validators from fraudulently stealing coins from users.
* Wealth concentration. Rosu and Saleh (2020): PoS does not induce wealth concentration.
* Double-spending attack: sufficiently large market capital enables a PoS blockchain to overcome the double-spending attack.
* Staking pools can increase demand (Cong et al. (2020)) -> market cap, and consequently security.

**A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks** (Wenbo Wang et. Al) 2019

* The concept of PoS was first proposed by Peercoin [76] as a modified PoW scheme to reduce the energy depletion due to exhaustive hash queries. Peercoin proposes a metric of “coin age” to measure the miner’s stake as the product between the held tokens and the holding time for them. The Peercoin kernel protocol allows a miner to consume its “coin ages” to reduce the difficulty of a PoW puzzle.
* Follow-the-satoshi, Ouroboros, snow white, casper
* Incentive issues: Regarding the incentive compatibility of PoS, an informal analysis in [77] shows that being honest is a δ-Nash equilibrium20 strategy when the stakes of the malicious nodes are less than a certain threshold and the endorsers are insensitive to transaction validation cost. However, a number of vulnerabilities are also identified in PoS. In [155], the nothing-atstake attack is considered. In order to maximize the profits, a block leader could generate conflicting blocks on all possible forks with “nothing at stake”, since generating a PoS block consumes no more resource than generating a signature. A dedicated digital signature scheme is proposed to enable any node to reveal the identity of the block leader if conflicting blocks at the same height are found. Alternatively, a rule of “three strikes” is proposed in [33] to blacklist the stakeholder who is eligible for block creation but fails to properly do so for three consecutive times. In addition, an elected mining leader is also required to sign an auxiliary output to prove that it provides some extra amount tokens as the “deposit”. In case that this node is malicious and broadcasts more than one block, any miner among the consecutive block creation leaders can include this output as an evidence in their block to confiscate the attacker’s deposit. Such a scheme is specifically designed to disincentivize block forking by the round leader.
* Grinding attack

**A Survey of Distributed Consensus Protocols for Blockchain Networks** (Yang Xiao, Ning Zhang, Wenjing Lou , Y. Thomas Hou) 2020

https://arxiv.org/pdf/1904.04098.pdf

* Blockchain, consensus definitions, concerns associated with PoW
* PoS, PoA, PoET
* Appropriate incentives that will continue to encourage honest participation in the blockchain network is another key component of consensus protocol. Therefore, alternative block proposing schemes are often accompanied by a new incentive mechanism that promotes participation fairness and increases overall system sustainability (Peercoin [6], Bitcoin-NG [7], Ourosboros (Cardano) [8], Snow White [9], and EOSIO [10], POA Network [11])
* Various consensus mechanisms that have been proposed
* We call a consensus protocol crash fault tolerant (CFT) or Byzantine fault tolerant (BFT) if it can tolerate a certain amount of crash or Byzantine process failures while keeping normal functioning.
* the incentive mechanism is indispensable to permissionless blockchain networks especially those carrying a financial responsibility; however for permissioned blockchains in which participation is sanctioned as a privilege (similar to a traditional distributed computing system), it is not a must-have.
* Proof-of-Stake (PoS) originates from the Bitcoin community as an energy efficient alternative to PoW mining. In the simplest terms, a stake refers to the coins or network tokens owned by a participant that can be invested in the blockchain consensus process. From the security point of view, PoS leverages token ownership for Sybil attack mitigation. Compared to a PoW miner whose chance to propose a block is proportional to its brute-force computation power, the chance to propose a block for a PoS miner is proportional to its stake value. From the economics point of view, PoS moves a miner’s opportunity cost from outside the system (waste of computation power and electricity) to inside the system (loss of capital and investment gain)
* We identify four classes of PoS protocols: chain-based PoS, committee-based PoS, BFT-based PoS, and delegated PoS (DPoS). Chain-based PoS inherits many of the components of the Nakamoto consensus protocol such as information propagation, block validation, and block finalization (i.e. longestchain rule), except that the block generation mechanism is replaced with PoS. Committee-based PoS leverages a multiparty computation (MPC) scheme to determine a committee to orderly generate blocks. BFT-based PoS combines staking with BFT consensus which guarantees deterministic finality of blocks. DPoS employs a social voting mechanism that elects a fixed-size group of delegates for transaction validation and blockchain consensus on behalf of the voters.
* Chain-based PoS: Peercoin 2012, Nxt 2013, Bentov’s PoA (follow-the-satoshi)2014;

Committee-based PoS: Bentov’s CoA 2017, Ourosboros 2017, Snow White 2017, Ourosboros Praos 2017;

BFT-based PoS: Tendermint 2014 (Cosmos Hub network), Algorand 2017, Casper FFG 2017;

Delegated PoS (DPoS): BitShares 2.0 2015, Lisk 2016, EOS.IO 2017, Cosmos 2019;

* Explanations of how they work
* Chain-based PoS still relies on the hashing puzzle to generate blocks.
* committee-based PoS adopts a more orderly regime: determining a committee of stakeholders based on their stakes and allowing the committee to generate blocks in turns (A secure multiparty computation (MPC) scheme is often used to derive such a committee in the distributed network).
* Snow White executes a modified version of the sleepy consensus protocol [102], an 19 asynchronous consensus protocol that ensures the consensus safety in case of sporadic participation and committee reconfiguration.
* Cardano, the cryptocurrency platform that deploys Ouroboros, mandates that every committee member should own no less than 2% of total tokens in circulation. This effectively limits the committee size to 50, safeguarding an efficient consensus process.
* Algorand employs committee-based PoS for block proposing and Byzantine agreement for block finalization
* Vulnerabilities of PoS/ possible attacks
* Other emerging consensus protocols
* ON DESIGNING BLOCKCHAIN CONSENSUS PROTOCOL

**The public blockchain ecosystem: An empirical analysis** Felix Irresberger, Kose John, Peter C. Mueller, Fahad Saleh 2020/2021

https://papers.ssrn.com/sol3/Papers.cfm?abstract\_id=3592849

* Proof-of-Stake PoS constitutes one of the early alternatives to PoW. King and Nadal (2012) provide the first PoS proposal. PoS overcomes PoW’s need for exorbitant energy expenditure by removing PoW’s computationally complex puzzle from the consensus process. The first pure PoS protocol was employed on the Nxt blockchain in 2013. Under PoS, agents are randomly conferred the authority to validate the next block. The likelihood of being chosen depends on an agent’s “stake” which refers to an agent’s overall holdings of the native cryptoasset.
* Delegated Proof-of-Stake Both PoW and pure PoS blockchains have faced criticism for their alleged inability to process transactions quickly. A variant of PoS protocols known as Delegated Proof-of-Stake (DPoS) arose in response to this criticism. DPoS was first introduced by Daniel Larimer, the eventual founder of the blockchain EOS. Under DPoS, a fixed number of delegates, also called “witnesses,” validate new blocks. Holders of the native cryptoasset vote for delegates. Similar to PoS, the number of votes is assigned in proportion to holdings of the native cryptoasset. The relatively small and fixed number of delegates reduces the validating agent network size compared to traditional PoS protocols. This small network size, in theory, allows for faster transaction rates, as fewer agents have to converge on a common version of the ledger.
* Dapps
* Security, confirmation time,
* Our framework suggests that three blockchain characteristics drive user utility - scale, security, and adoption - and that only a few blockchains are not dominated by some other blockchain in terms of utility for some user. We empirically identify an exclusive set of seven such blockchains, and we refer to those blockchains as the blockchain frontier. Blockchain frontier: Bitcoin, Ethereum, Tron, EOS, Binance Coin, Stellar, Bitcoin Satoshi’s Vision

**SoK: Consensus in the Age of Blockchains** (Shehar Bano et al) 2019

* The consensus protocol enables a distributed network of nodes to agree on whether a data item should be added to the blockchain. A plethora of consensus protocols exist—ranging from classical consensus (e.g., Fault Tolerance and Byzantine Fault Tolerance protocols), through probabilistic consensus such as proof-of-work (PoW), to committee-based consensus that repurposes classical protocols to the blockchain setting.
* Incentives. Incentive compatibility refers to the mechanism designed to financially motivate nodes to participate in the consensus protocol. Typically this is achieved as nodes are rewarded with in-band coins (i.e., a block subsidy and transaction fees) for producing blocks. As a result, nodes will naturally compete amongst themselves as their reward is proportional to the number of blocks they can produce. Thus the network is intuitively a free-market as nodes are encouraged to purchase resources and compete amongst themselves, and it is self-sustaining as nodes will only compete while the in-band reward has intrinsic real-world value. Blockchains that use smart contracts require clients to include fees (e.g., ‘gas’ in Ethereum) to be paid to the nodes that execute the smart contracts. This not only helps to incentivize node participation, but also protects the system from overuse by discouraging clients from submitting long computations that monopolize system resources.
* Pos: ouroboros, Snow White, Ouroboros Praos
* Ouroboros and Ouroboros Praos distribute rewards among all the participants regardless of whether or not they win the election. Snow-White employs the incentive structure of Fruitchain
* Nothing-at-stake. One way of dealing with this is to introduce a penalty mechanism: a miner producing blocks on different forks is penalized by having part of their stake taken [Snow white]. Another mitigation against nothing-at-stake is to remove the opportunity for forks in the consensus protocol altogether as proposed by Algorand.
* Grinding attack, long-range attack (bribe) and how to solve them.
* (committee) Classical BFT protocols assume two kinds of players: cooperative and byzantine. This assumption works well in ‘closed’ group settings where nodes are controlled by the same entity or federation. However, permissionless blockchains need to provide incentives to nodes for active participation in consensus [57, 58, 67].. However, with no clear incentives, the cooperative committee members have nothing to gain from participating in the consensus, which introduces a third kind of player: a rational player that, for each action it performs, assesses its expected utility in terms of the rewards it will receive.
* This has led to the design of incentive-compatible consensus protocols, where incentives are built into the core of the protocol (e.g., Solidus [2]). Classical techniques such as rational cryptography [19, 43] and the BAR model [3] could be adapted to work here. Due to the unavoidable selfish behaviour observed in distributed systems, the BAR model was introduced to construct systems that can tolerate both Byzantine and rational players.

**BAR fault tolerance for cooperative services** (Amitanand S. Aiyer et al.) 2005

* Byzantine, Altruistic, Rational

**Evolution of Shares in a Proof-of-Stake Cryptocurrency.** Ioanid Ro, Fahad Saleh. 2021

* Examine wealth concentration
* Do the rich always get richer by investing in a cryptocurrency for which new coins are issued according to a Proof-of-Stake (PoS) protocol? We answer this question in the negative: Without trading, the investor shares in the cryptocurrency are martingales that converge to a well-defined limiting distribution, hence are stable in the long run. This result is robust to allowing trading when investors are risk-neutral. Then, investors have no incentive to accumulate coins and gamble on the PoS protocol, but weakly prefer not to trade.
* Further, we show that when coin rewards are not increasing too fast, the investor shares are stable in a stricter sense: they remain fairly close to the initial value. Moreover, “poor” investors (i.e., those who start with a lower fraction of coins) end up with a more stable share distribution than “rich” investors.
* Modest rewards

**Formal Barriers to Longest-Chain Proof-of-Stake Protocols.** Jonah Brown-Cohen, Arvind Narayanan, Christos-Alexandros Psomas, S. Matthew Weinberg. 2018

* For instance, obtaining voting power in Proof-of-Stake has a monetary cost just as in Proof-of-Work: a coin cannot be freely duplicated any more easily than a unit of computation. However some aspects are fundamentally different. In particular, exactly because Proof-of-Stake is wasteless, there is no inherent resource cost to deviating (commonly referred to as the “Nothing-at-Stake” problem).
* In contrast to prior work, we focus on incentive-driven deviations (any participant will deviate if doing so yields higher revenue) instead of adversarial corruption (an adversary may take over a significant fraction of the network, but the remaining players follow the protocol). The main results of this paper are several formal barriers to designing incentive-compatible proof-of-stake cryptocurrencies (that don’t apply to proof-of-work).
* One of the key ingredients in successful cryptocurrencies is a random selection process that is Sybil-proof.
* Pow vs pos
* From a security perspective, it’s actually convenient that Proof-of-Work wastes resources: this guarantees that certain deviations (discussed in the next paragraph) from the intended protocol also cost additional resources, and are naturally disincentivized (this, of course, does not mean that deviations are never profitable). Pos falls on the protocol to disincentivize such behavior through clever reward schemes.
* Numerous recent works, both commercial and academic, aim to address this challenge (nothing at stake) with clever reward schemes
* pseudorandomness coming from the cryptocurrency
* obviously important that proposals be secure in the classical sense (network intrusion) before concerning oneself with incentives.
* Some works go further and provide incentive guarantees, proving that miners who strategically deviate from the prescribed protocol can only gain a small ε fraction of the total rewards [Snow white, Ouroboros]. Still, [Snow white] notes that it is preferable for known strategic deviations to be strictly disincentivized (and prove that their scheme achieves this for Nothing-at-Stake), and [ouroboros] observes that not all known deviations are captured by such claims (and prove that their scheme successfully disincentivizes double-spending).
* Preliminaries of how everything works, definitions
* Eclipse attack
* Longest-Chain Variants are particularly common within cryptocurrencies because of their robustness to Eclipse attacks. Even if the network is partitioned for an extended period, and both disjoint subsets produce completely different histories, the entire network will quickly converge to the higher-scoring history as soon as the subsets reunite. Alternative protocols based on Byzantine Consensus [6, 4] lack this property, and instead achieve finality. That is, once a user considers a block B to be included in the ledger, they will never consider valid any ledger that not including B. Indeed, in protocols with finality, if the network is partitioned for an extended period, progress will either stall, or the network will never reach consensus even after being reunited.
* Byzantine consensus protocols require some network connectivity assumptions in order to safely ignore messages sent too far in the past, and are less robust to Eclipse attacks
* Desirable properties of protocols: unpredictability, non-recency
* Selfish-mining, double-spending, nothing-at-stake
* without a provable deviation, we cannot “punish” suspected deviant miners without the risk of punishing honest but poorly-connected miners
* The Undetectable Nothing-at-Stake strategy never produces a provable deviation.
* Preventing predictable selfish mining is challenging, but some clever ideas exist in the literature. At a high level, Fruitchains [21], Ouroboros [17], and Tezos [14] design protocols where blocks need to be “supported” once mined (eligibility to support is also proportional to stake), so one would not only need a majority of blocks mined but also a majority of “support tokens(/fruit)” in a given window to successfully selfish mine. Both Snow White [9] and Ouroboros [17] provide proofs that any deviation from their prescribed protocol can only provide a small ε in additional mining rewards. However, [9] notes that it would be preferable for known attacks to be strictly disincentivized (more on this in Appendix C), and it remains open whether these reward schemes accomplish this.
* A simple defense specifically against predictable doublespend attacks is to accept long confirmation times. the authors of the Ouroboros [17] Protocol (which is predictable) suggest using confirmation times of 148 minutes to defend against double spend attacks by an attacker controlling 40% of the stake when blocks are created at a rate of one per minute (and this is consistent with our analysis).
* Undetectable Nothing-at-Stake… Algorand proposes a different approach: instead of using a longest-chain variant, it uses a Byzantine consensus protocol. Under some network connectivity assumptions, they show that the probability of a fork is negligible. As such, any deviant behavior that results in a fork (such as Undetectable Nothing-at-Stake) can be readily recognized as malicious, and safely ignored. Ethereum’s Casper [1] proposes a third solution that they call “dunkles”: punish every miner whose block winds up being orphaned (not a predecessor of the block maximizing S(A)). The high-level goal of this is to essentially copy the incentives from Proof-of-Work: if your block is orphaned, you still lose the electricity that went into mining it. By punishing the miner of every orphaned block, some honest miners will get punished just by bad luck, but it will also discourage attackers from mining off the longest chain. This seems like a promising direction, but there is currently no formal specification or rigorous evaluation of the proposal.
* Snow white, ouroboros
* No rewards
* Algorand
* Bentov-Gabizon-Mizrahi- Follow-the-satoshi
* GHOST

**Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism.** FAN YANG, WEI ZHOU, QINGQING WU, RUI LONG, NEAL N. XIONG, AND MEIQI ZHOU.

* PoW and PoS hybrid?
* The simulation experiments in blockchain system show that the proposed consensus algorithm is significantly more efficient than PoW and PoS, but slightly lower than DPoS. However, its degree of centralization remains far below that of DPoS. And through the downgrade mechanism, the proposed consensus algorithm can detect and downgrade the malicious nodes timely to ensure the security and good operation of system.
* To break the cycle of the competition in computing resources to generate blocks, DPoS introduces a voting mechanism based on PoS, and lower the time cost of generating a block to 3s
* DPoS divides the nodes in the blockchain system into three categories: witnesses, delegates, and workers. Witnesses are the core of the entire system and they were elected through resource voting by all nodes. The nodes winning the topN number of votes become the witnesses and take turns to generate blocks…higher degree of centralization.
* A downgrade mechanism is applied to quickly downgrade the malicious nodes and upgrade the reliable nodes to maintain the security and good operation of the system. (rewards> incentives?)
* Blockchain and how it works
* The consensus mechanism is a collaborative process algorithm that specifies how consensus is reached among all consensus nodes and identifies the validity of records. Members of the blockchain use it to negotiate whether the transaction is valid and make the account stay in sync. Each consensus node in the blockchain verifies and confirms the data according to the algorithm. After confirmed by a certain number of nodes, the valid data can be written into the blockchain [23]. At present, the most common consensus algorithms are: PoW, PoS, DPoS and PBFT. From the emergence of Bitcoin to today, there are more than 30 consensus algorithms, most of which are based on the above four consensus algorithms.
* PoS was firstly implemented by Sunny King’s Peercoin and its mining difficult is adjusted based on the number of stakes held by workers. Simply put, the more stakes you have, the easier it is to generate the block. Larimer designed the Delegated Proof of Stake (DPoS) and implemented it for the first time in its BitShares project [28]. The DPoS consensus process is divided into the earlier process of electing witness (i.e., block producers) and the later process of generating blocks. The witnesses are only responsible for witnessing the transaction, verifying the signature and timestamping the transaction, but not participating in the trading. They generate one block every 3s in turn, and if a witness did not complete the task at the specified time, it will be skipped and replaced by the next one. Each node on the network can vote for its own trusted witness, the more blockchain stakes he has, the higher possibility of him to be a witness. However, due to the mechanism that each witness node takes turns generating blocks, the identity of the witness is already known and always constant, which would make the blockchain system more vulnerable to collusion attacks.
* A major breakthrough in Tendermint [34] proposed in 2014 was the implementation of the first PBFT-based PoS consensus algorithm.
* In 2016, Micali proposed a fast Byzantine fault-tolerant consensus algorithm called AlgoRand [35]. The blockchain applying this algorithm uses the password lottery technique to select the verifier and leader of the consensus process, and reaches a consensus on the new block through its designed BA∗ Byzantine fault-tolerant protocol.
* PoS vs Pow.
* the voting enthusiasm of nodes in DPoS is not high, because a small number of vote holders occupy the vast majority of voting rights, resulting in the low influence from ordinary nodes even if they participate in voting. According to statistics in [20], more than 90% of shareholders have never participated in the vote. This has led to that the witnesses selected by a few votes’ holders becoming more and more fixed (i.e., as long as the witness does not act as a malicious node). And there are also a lot of security risks in the blockchain system because of the difficulty in dealing with malicious nodes [45]
* PBFT is mostly used in the consortium blockchain with a fixed number of nodes, but not applicable in a public blockchain with a large number of nodes because of its poor scalability.
* Some PoS-based consensus algorithms such as Tendermint, Ouroboros, and HoneyBadger attempt to solve the ‘‘Nothing at Stake’’ problem in the traditional PoS. Some PBFT-based consensus algorithms such as SCP, Algorand, and Elastico aim to enhance the scalability or security of the blockchain.
* Everything not as efficient as DPoS
* We introduce a downgrade mechanism to replace the malicious node as soon as it was found. On the one hand, when the witness node is found to be a malicious node, it falls into the candidate nodes set, and the rank of all existing witness nodes are decremented by one. On the other hand, the node with sequence number 1 in the set of candidate nodes is upgraded to the witness nodes set and ranked last in the witness nodes set. while the sequence number of all the remaining candidate nodes are decremented by 1, the malicious node is sorted at the end of the set of candidate nodes.
* The first is the idea of combining the advantages of PoW and DPoS to improve the original DPoS algorithm. We use the PoW to select a set of nodes with sufficient computational power instead of stakes to participate in the election. Secondly, we stipulate that each node has only one vote for randomly voting, which improves the fairness and decentralizes the right of generating blocks to avoid the collusion attack and improving the node activity of the entire blockchain system. Finally, this paper adopts the downgrade mechanism to quickly downgrade the malicious nodes to maintain the good operation and security of the system
* Hasn’t been applied in the existing busines environment

Table

Description automatically generated

**Table

Description automatically generated**

**Compounding of Wealth in Proof-of-Stake Cryptocurrencies.** Giulia Fanti, Leonid KoganSewoong OhKathleen RuanPramod ViswanathGerui Wang 2019

* Proof-of-stake (PoS) is a promising approach for designing efficient blockchains, where block proposers are randomly chosen with probability proportional to their stake. A primary concern in PoS systems is the “rich getting richer” effect, whereby wealthier nodes are more likely to get elected, and hence reap the block reward, making them even wealthier. In this paper, we introduce the notion of equitability, which quantifies how much a proposer can amplify her stake compared to her initial investment. Even with everyone following protocol (i.e., honest behavior), we show that existing methods of allocating block rewards lead to poor equitability, as does initializing systems with small stake pools and/or large rewards relative to the stake pool. We identify a *geometric* reward function, which we prove is maximally equitable over all choices of reward functions under honest behavior and bound the deviation for strategic actions;
* A central problem in blockchain systems is that of block proposal: how to choose which block should be appended to the global blockchain next. Many blockchains use a proposal mechanism by which one node is randomly selected as leader (or *block proposer*). This leader gets to propose the next block in exchange for a token reward—typically a combination of transaction fees and a freshly-minted *block reward*, which is chosen by the system designers.
* Pow inefficient, PoS as alternative
* Although the idea of PoS is both natural and energy-efficient, the research community is still grappling with how to design a PoS system that provides security while also incentivizing nodes to act as network validators. Part of incentivizing validators is simply providing enough reward (in expectation) to compensate their resource usage. However, it is also important to ensure that validators are treated fairly compared to their peers. In other words, they cannot only be compensated adequately on average; the variance also matters.
* Compounding/rich-get-richer effect
* Most cryptocurrencies today use a *constant block reward* function like Bitcoin’s, which remains fixed over a long timespan (e.g., years). We ask how a PoS system’s choice of block reward function can affect concentration of wealth, and whether one can achieve the PoW baseline stake distribution simply by changing the block reward function.
* We introduce an alternative block reward function called the *geometric reward function*, whose rewards increase geometrically over time. We show that it is the most equitable PoS block reward function, by showing that it is the unique solution to an optimization problem on the second moment of a time-varying urn process;
* We study the effects of strategic behavior (e.g. selfish mining) on the rich-get-richer phenomenon. We find that in general, compounding can exacerbate the efficacy of strategic behavior compared to PoW systems. However, these effects can be partially mitigated by carefully choosing the amount of block reward dispensed over some time period relative to the initial stake pool size.
* We show that cryptocurrencies that start with large initial stake pools (relative to the block rewards being disseminated) can mitigate the concentration of wealth, both for constant and geometric reward schemes.
* Stake pools
* Brunjes *et al.* also studies stake pools and how to incentivize their formation through the design of reward mechanisms.
* A second variance reduction approach changes the block reward allocation protocol; our work falls in this category. Two examples are Fruitchains [[20](https://link.springer.com/chapter/10.1007/978-3-030-32101-7_3#CR20)], which spread block rewards evenly across a sequence of block proposers, and Ouroboros [[15](https://link.springer.com/chapter/10.1007/978-3-030-32101-7_3#CR15)], which rewards nodes for being part of a block formation committee, even if they do not contribute to block proposal. Both of these approaches were proposed in order to provide incentive-compatibility for block proposers; they do not explicitly aim to reduce the variance of rewards. However, they implicitly reduce variance by spreading rewards across multiple nodes, thereby preventing the randomized accumulation of wealth. In our work, instead of changing how block rewards are disseminated, we change the block reward function itself.
* Although we do not consider BFT-based PoS protocols in this paper [[12](https://link.springer.com/chapter/10.1007/978-3-030-32101-7_3#CR12), [28](https://link.springer.com/chapter/10.1007/978-3-030-32101-7_3#CR28)], such protocols provide robustness to strategic behavior by forcing consensus on each block. Such protocols may also provide robustness to compounding, since block rewards can be shared among many nodes.
* We have also assumed in this work that users instantly re-invest rewards into the proposer stake pool, for two reasons. (1) In PoS systems where users explicitly deposit stake, existing implementations automatically deposit rewards back into the stake pool. For example, the reference implementation of Casper the Friendly Finality Gadget (a PoS finalization mechanism proposed for Ethereum) automatically re-allocates all rewards back into the deposited stake pool [[23](https://link.springer.com/chapter/10.1007/978-3-030-32101-7_3#CR23)]. (2) In other PoS systems, the stake pool is simply the set of all stake in the system, and is not separate from the pool of tokens used for transactions [[8](https://link.springer.com/chapter/10.1007/978-3-030-32101-7_3#CR8)]. Hence as soon as a proposer earns a reward, that reward is used to calculate the next proposer (modulo some maturity period);
* Block Reward Choices. Many cryptocurrencies use Bitcoin’s block reward schedule, which fixes the total supply of coins at about 21 million coins, and halves the reward every 210,000 blocks (≈4≈4 years)
* Several systems have adopted similar block rewards that are constant over long periods of time (e.g., Ethereum [[3](https://link.springer.com/chapter/10.1007/978-3-030-32101-7_3#CR3)], ZCash [[13](https://link.springer.com/chapter/10.1007/978-3-030-32101-7_3#CR13)], Dash [[7](https://link.springer.com/chapter/10.1007/978-3-030-32101-7_3#CR7)], Particl). In this paper, we revisit the question of how to choose r(n). A key observation is that r(n) must compensate nodes for the cost of proposing blocks. Many cryptocurrencies implicitly adopt the following maxim: *On short timescales, each block should yield the same block reward.*
* Rewards measured in tokens or fiat
* Equitability
* Selfish mining
* This work measures the concentration of wealth in PoS systems, showing that existing block reward functions (e.g., constant, decreasing rewards) have poor equitability. We introduce a maximally-equitable geometric reward function. The negative effects of compounding can be further mitigated by choosing the total block rewards for each epoch to be small compared to the initial stake pool size.

**Incentive compatible and anti-compounding of wealth in proof-of-stake** (Yilei Wang et al) 2020

* the basic regime in blockchain is consensus mechanism, which may keep in functional order if all participants have enough incentives
* the usage of constant reward function may cause compounding of wealth (i.e. equitability) in PoS
* geometric reward function
* we propose a new reward function based on geometric reward function by introducing random bonus mechanism. More concretely, each participant who has the privilege to create a new block may get extra bonus except for his rewards. We meticulously design positive bonus to assign enough incentives at the beginning of system so that participants are willing to take part into the consensus ­­­­mechanism. Note that the expectation of the whole bonus is zero. That means there exist some negative bonus, which will not impede the incentives since the rewards derived from reward function are large enough to neutralize the negative bonus. Our new reward function performs well in both world restraining the compounding phenomenon and guaranteeing incentive compatibility to acceptable extents.
* Equitability­­
* Solidus is an incentive compatible cryptocurrency on the basis of permissionless Byzantine consensus [20]. It injects incentives for almost each phase of the practical Byzantine consensus like get-epoch phase, elect phase, prepare phase and accept phase. The incentives also consist of negative ones such as penalties for malicious actions. On the other hand, Solidus can also mitigate selfish mining attacks.
* Ouroboros also considers incentives by rewarding nodes, who are members of a committee generating a new block [21].
* FruitChains is a new blockchain protocol, which introduce a notion of fairness [22]. It manages to reach optimal fairness level under the scenario of selfish mining attack since it undermines incentive compatibility [23]
* Evaluating inequality. Gini coefficient
* COULDN’T ACCESS FULL PAPER

[**https://eth.wiki/en/concepts/proof-of-stake-faqs**](https://eth.wiki/en/concepts/proof-of-stake-faqs) **(ethereum)**

* two major types: chain-based proof of stake and [BFT](https://en.wikipedia.org/wiki/Byzantine_fault_tolerance)-style proof of stake.
* Benfits of pos vs pow
* Because of the lack of high electricity consumption, there is not as much need to issue as many new coins in order to motivate participants to keep participating in the network. It may theoretically even be possible to have negative net issuance, where a portion of transaction fees is “burned” and so the supply goes down over time.
* discourage centralized cartels from forming and, if they do form, from acting in ways that are harmful to the network (eg. like [selfish mining](https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf) in proof of work).
* Ability to use economic penalties to make various forms of 51% attacks vastly more expensive to carry out than proof of work - to paraphrase Vlad Zamfir, “it’s as though your ASIC farm burned down if you participated in a 51% attack”.
* Chain-based” proof of stake algorithms almost always rely on synchronous network models,
* Selfish mining
* nothing at stake. In many early (all chain-based) proof of stake algorithms, including Peercoin, there are only rewards for producing blocks, and no penalties. This has the unfortunate consequence that, in the case that there are multiple competing chains, it is in a validator’s incentive to try to make blocks on top of every chain at once, just to be sure
* The result is that if all actors are narrowly economically rational, then even if there are no attackers, a blockchain may never reach consensus. If there is an attacker, then the attacker need only overpower altruistic nodes (who would exclusively stake on the original chain), and not rational nodes (who would stake on both the original chain and the attacker’s chain), in contrast to proof of work, where the attacker must overpower both altruists and rational nodes
* some argue that stakeholders have an incentive to act correctly and only stake on the longest chain in order to “preserve the value of their investment”, however this ignores that this incentive suffers from [tragedy of the commons](https://en.wikipedia.org/wiki/Tragedy_of_the_commons) problems: each individual stakeholder might only have a 1% chance of being “pivotal” (ie. being in a situation where if they participate in an attack then it succeeds and if they do not participate it fails), and so the bribe needed to convince them personally to join an attack would be only 1% of the size of their deposit; hence, the required combined bribe would be only 0.5-1% of the total sum of all deposits.
* Strategies how chain based pos solve nothing at stake: (first way)slasher-punish if they create two blocks; (second) punish for creating blocks on a wrong chain;
* we can replicate the economics of proof of work inside of proof of stake. In proof of work, there is also a penalty for creating a block on the wrong chain, but this penalty is implicit in the external environment: miners have to spend extra electricity and obtain or rent extra hardware. Here, we simply make the penalties explicit. This mechanism has the disadvantage that it imposes slightly more risk on validators (although the effect should be smoothed out over time), but has the advantage that it does not require validators to be known ahead of time.
* Stake grinding in Nxt and Peercoin. Solved by: require validators to deposit their coins well in advance, and not to use information that can be easily manipulated as source data for the randomness. The first is to use schemes based on [secret sharing](https://en.wikipedia.org/wiki/Secret_sharing) or [deterministic threshold signatures](https://eprint.iacr.org/2002/081.pdf) and have validators collaboratively generate the random value. The second is to use cryptoeconomic schemes where validators commit to information (ie. publish sha3(x)) well in advance, and then must publish x in the block; …… Hence, all in all, many known solutions to stake grinding exist; the problem is more like [differential cryptanalysis](https://en.wikipedia.org/wiki/Differential_cryptanalysis) than [the halting problem](https://en.wikipedia.org/wiki/Halting_problem) - an annoyance that proof of stake designers eventually understood and now know how to overcome, not a fundamental and inescapable flaw.
* 51% attack equivalent
* Capital lock up.
* in PoW, we are working directly with the laws of physics. In PoS, we are able to design the protocol in such a way that it has the precise properties that we want - in short, we can optimize the laws of physics in our favor.
* Centralization concerns
* One strategy suggested by Vlad Zamfir is to only partially destroy deposits of validators that get slashed, setting the percentage destroyed to be proportional to the percentage of other validators that have been slashed recently. This ensures that validators lose all of their deposits in the event of an actual attack, but only a small part of their deposits in the event of a one-off mistake. This makes lower-security staking strategies possible, and also specifically incentivizes validators to have their errors be as uncorrelated (or ideally, anti-correlated) with other validators as possible; this involves not being in the largest pool, putting one’s node on the largest virtual private server provider and even using secondary software implementations, all of which increase decentralization.

<https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/>

* Nothing at stake problem, peercoin, slasher

**Economics of Proof-of-Stake Payment Systems** (Giulia Fanti, Leonid Kogan, Pramod Viswanath) 2018/2020

* Bitcoin and its drawbacks
* On its own, PoS does not specify a consensus protocol. For example, it is unclear how to securely implement PoS proposer election in the first place, as well as how to use the results of that procedure.
* because individual token holdings in the PoS stake systems determine the allocation of rewards within the system, as we discuss in our PoS primer below, tokens effectively confer cash flow rights on their holders – they can therefore be valued using standard valuation methods.
* token valuation plays an additional role in PoS: it gives a quantitative measure of the security of the system. Because of the way PoS systems are architected, higher token values imply better security
* effect of valuation bubbles on network security
* The primary expense for PoS participants is the fact that they must 3 deposit tokens as collateral in order to reap rewards; This observation allows us to tie PoS cryptocurrency valuations to fiat quantities through the opportunity cost of holding tokens.
* implications of valuation dynamics for network security
* Block confirmation : in Algorand, confirmation occurs after every block, and the guarantee is ultimately probabilistic; the block can only be overturned with a fixed, low probability, assuming that at least 2/3 of participants are honest (Chen and Micali, 2016). In other PoS cryptocurrencies (e.g., Ethereum v2.0), confirmation is executed via a separate finalization procedure that is run by a (possibly separate) set of nodes called validators. Typically, once a block is finalized, it and all prior blocks cannot be reverted without the nodes responsible for the change incurring significant penalties through a process called slashing.
* In PoS systems, a common approach to proposer election relies on verifiable random functions (VRFs) (Qtum, Peercoin, BlackCoin, Particl, Cardano (?), and Algorand (Chen and Micali, 2016))
* In chain-based protocols, such as those using PoSv3 (e.g, Qtum, Particl), forking is much more common; this happens both because of network delays (a proposer may not know about the most recent block) and the fact that multiple proposers may be elected at the same time. In chain-based protocols, proposers typically append their block to the longest chain known to the proposer at the time.
* For our purposes, the details of block proposal matter primarily because of how they affect the incentives in the system. For instance, in chain-based protocols, proposers are rewarded for creating blocks that end up in the final longest chain. These rewards manifest in two ways: block rewards and transaction fees.
* Block rewards, transaction fees definitions
* Although finalization is not yet widespread, it is being considered for adoption in a few major cryptocurrencies. Ethereum, for instance, has proposed a finalization mechanism in its roadmap (Buterin and Griffith, 2017), and major cryptocurrencies like Ripple and Stellar provide similar finality guarantees (Mazieres, 2015)
* Slashing *(slashing destroys coins of bad nodes-> increases token value-> honest nodes are better off).*
* In Ethereum’s finalization protocol, Casper the Friendly Finality Gadget (FFG), 4% of the slashed funds are given to the node that reports the misbehavior, and the remaining 96% is burned so that nobody can spend it.
* Casper FFG imposes a lower limit on the deposit to become a validator; at the time of writing, this minimum was 1500 ETH, close to $190,000. Hence, any misbehavior would result in the validator losing a substantial sum of money.
* Notice that although slashing is described in the context of finalization, the concept can also be used to protect against other kinds of misbehavior. For example, one could require proposers to deposit stake, and slash proposers who propose multiple blocks at once.
* If consumers hold no token balances between transactions, any benefit validators derive from collecting 18 rewards in newly minted tokens is completely offset by the decline in the market value of tokens in their stake.
* Do rewards from minting new tokens devalue existing ones? (are rewards dilutive) (yes. By expanding the overall amount of available tokens, there is obviously an inflation or an overall value dilution ongoing, which can be neglected as long as you participate.)
* In the PoS system, attackers face a very different tradeoff: to execute the majority attack, one must gain a sufficient degree of majority in the validation pool, which requires holding a significant number of tokens. 8 The cost of the attack is that ones’ token holdings would be slashed (confiscated) based on the network security protocol. Majority attacks are only feasible if their economic benefits exceed the cost of executing the attack – hence, network security hinges critically on token valuation.
* More generally, high token valuation relative to the economic footprint of the network serves as a deterrent against majority attacks. While there may not exist a particular level of token valuation that guarantees network security (e.g., because the benefit of an attack may be unbounded, if the objective is to undermine the network), we can nonetheless obtain useful information by observing how various design features and events affect token values.
* Valuation bubbles
* Certain design feature may be introduced to help reduce the negative effect of valuation bubbles on validators’ willingness to stake tokens. For instance, one may lock in validators’ holdings over extended time periods, making it impossible for them to respond to highly transient valuation changes. In return, validators would then require a higher expected rate of return in equilibrium, to compensate them for the loss of liquidity. Understanding the net effect of such arrangements on network security, and network dynamics in general, is an important question for future research.
* raising the token supply rate while the size of the validator pool is deemed below the desired level, leads to a sharp increase in the validators’ rate of return, thus attracting more capital to the pool.
* current designs and proposals for PoS systems include various restrictions on validators, intended to curtail various types of network attacks by allowing network participants to penalize validators for recent violations of the network protocol.

**Reward Sharing Schemes for Stake Pools** (Lars Brünjes\* Aggelos Kiayias† Elias Koutsoupias‡ Aikaterini-Panagiota Stouka) 2020

* One of the main open questions in blockchain systems research is developing reward mechanisms that incentivize honest protocol execution and decentralization. Despite progress in the understanding of the security properties of PoS blockchains, designing a robust incentive mechanism that promotes decentralization remains open.
* the reward pool can be facilitated either via the creation of new cryptocurrency, the collection of transaction fees, or a combination thereof
* stake pools

**SoK: Lending Pools in Decentralized Finance** (Massimo Bartoletti) 2020

* Lending pools are inherently hard to design. Besides the typical difficulty of implementing secure smart contracts [2–4, 35], lending pools feature complex economic incentive mechanisms, which make it difficult to understand when a lending pool actually achieves the economic goals it was designed for. As a matter of fact, a recent failure of the oracle price feed used by the Compound lending pool platform led to $100M of collateral being (incorrectly) liquidated [19]. Indeed, most current literature in DeFi is devoted to study the economic impact of these incentive mechanisms [39, 40, 46–48, 50].

**SoK: Tools for Game Theoretic Models of Security for Cryptocurrencies** (Sarah Azouvi, Alexander Hicks) 2020

* the explicit consideration of incentives in the protocol design of cryptocurrencies (or “cryptoeconomics”) has become an important topic.
* Cryptocurrencies, on the other hand, explicitly define some incentives in the design of their system, for example in the form of mining rewards, suggesting that they could be properly aligned and avoid traditional failures. Unfortunately, many attacks related to incentives have nonetheless been found for many cryptocurrencies [45, 46, 103], due to the use of lacking models.
* Game theory (nash equilibrium)
* Because the security of most decentralized systems, like cryptocurrencies, is linked not only to the security of the protocols, but also to having a majority of participants following the rules, decentralization and incentives have to be considered.
* Decentralization
* Incentives are key to achieving an honest majority. Azouvi et al. [13] give an overview of the role incentives play in security protocols, including cryptocurrencies, highlighting the fact that achieving guarantees of equilibria on paper may not be meaningful in practice when the wrong assumptions and models are used
* Bitcoin, Ethereum
* Covert adversaries are somehow similar to adding a punishment to the utility function. Rational players do not want to be caught cheating as the punishment decreases their utility. In Aumann and Lindell’s setting the protocol detects the cheating, but in practice we need to incentivize participants to do so.
* the BAR model defined by Aiyer et al. [7] introduces three different types of players: Byzantine, altruistic (players that simply follow the rules) and rational players.
* In his draft work about incentives in Casper [30], Buterin introduces the griefing factor which is the ratio of the penalty incurred to the victim of an attack and the penalty incurred by the attacker. The idea of a griefing factor intuitively makes sense, as disputes in the real world can be resolved by fining a party according to the damages caused, and from a modelling point of view gives a quantifiable punishment that can be explicitly taken into account when computing equilibria. He also proves that following the protocol in Casper is a NE as long as no player holds more than a third of the deposit at stake.
* For example, mining rewards can be designed as part of a protocol to ensure some level of decentralization but the utility function of miners will also depend on their individual economic environment that the protocol cannot fix. In this case, relating the economics of miners to their relationship with the system could do more to ensure some level of decentralization than tweaking the rewards given out by the protocol.
* Pools

**Competitive Equilibria Between Staking and Onchain Lending** (Tarun Chitra) 2020

https://cryptoeconomicsystems.pubpub.org/pub/chitra-staking-lending-equilibria/release/6

* When the yield provided by these contracts is more attractive than the inflation rate provided from staking, stakers will tend to remove their staked tokens and lend them out, thus reducing network security.
* Our results illustrate that rational, non-adversarial actors can dramatically reduce PoS network security if block rewards are not calibrated appropriately above the expected yields of on-chain lending
* PoS and how it works
* As PoS algorithms inherently connect a decentralized network’s security with the capital cost of a digital asset, PoS protocols tie their security to the cost of capital rather than to the cost of a natural resource. Volatility in the cost of capital, which is usually higher than that of natural resources [8], can have adverse effects on capital commitments to PoS networks. The main result we show is that alternative sources of yield can drive staking token capital allocators to collectively drain a network’s security, akin to a bank run. In particular, we find that PoS in deflationary systems is unstable and unlikely to work, and that for more reasonable inflation rates, the effectiveness of PoS depends on the relationship between staking and lending rates
* Attacks
* Agent based simulations

**Incentives in Security Protocols** (Sarah Azouvi, Alexander Hicks, and Steven J. Murdoch) 2018

* Originating from the rejection of any centralised authority, these are a rare example of systems whose security inherently relies on incentive schemes, unlike the EMV protocol above. Transactions are verified and appended to the blockchain by miners incentivised by mining rewards and transaction fees defined in the protocol to encourage honest behaviour in a trustless, open system.
* Nash equilibria are not well suited for this context

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9028039>

Towards a New Reward and Punishment Approach for Blockchain-based System. 2019

* Incentives and consensus
* Rewards for everyone
* Punishment system. Distribute ‘slashed’ rewards amongst honest nodes. (are they focusing on pow?)

The short answer is that burning tokens gives value to everyone through distributed scarcity, whereas distributing it to remaining validators would encourage them to sabotage each other in an effort to get each other’s slashed tokens. ( (Two Point Oh: Explaining Validators) (

* Pow, pos, dpos
* traditional reward and punishment systems, existing ones in blockchain
* Most POW-based Cryptocurrency Blockchains (for instance, Bitcoin and its variants) reward the leader participant (elected miner via consensus algorithm) with newly generated tokens. This leader also collects transaction fees joining all transactions the block creates. In other words, each time a block is created, only one participant is doubly rewarded, and the effort of the other participants is wasted wrongly without any monetization or recognition from the Blockchain. To minimize losses and wasted energy, there are nodes that choose not to do the mining in an autonomous way, but they gather in pools to do the mining in a collective way. The manager of these mining pools distribute the awards among its members proportionally according to their contributions.
* The reward system for Blockchains based on DPoS is to reward the delegates, who are responsible for sharing them proportionally with their constituents.
* Blockchains based on the POS consensus algorithm already implement a punishment system that reduces the stake of nodes whose behavior is malicious. However, the recovered tokens are not paid directly to the participating nodes of the network.
* Why punishment is important. Systems based on our approach, possess a punishment system. this feature is fundamental to our approach since it is an effective method to dissuade fraudulent participants and force them to recover in confidence as quickly as possible. Moreover, the penalties provide a new source of income for the rest of the network.
* Despite the multitude and evolution of consensus mechanisms in operational Blockchains, the reward system has not experienced any significant renewal aimed at retaining participants by guaranteeing them, at least, a minimal income after each round of mining. The proposed approach aims to stabilize and secure Blockchain networks and make them more reliable, by encouraging efficient and honest nodes to actively participate while respecting the rules of the Blockchain protocol of which they are members. With this new method of reward and penalization, systems based on Blockchain technology can easily retain its participants by awarding them permanent and proportionate rewards according to their scores and conformity rate. The latter is calculated automatically to promote transparency and the credibility of the system implementing this approach and improving the retention rate of these participants.

**Sustainable Growth and Token Economy Design: The Case of Steemit.**2018

* Rewards and crypto economics more generally. In other words, the designer of the system should define “desirable behaviors” and provide fair rewards for each behavior, while also presenting what participants can do with the token. If designed well, desirable behaviors will then be reinforced
* Mechanism design is also applied in crypto-economics. For instance, Satoshi Nakamoto modeled Bitcoin using the concept of mechanism design. Specifically, Bitcoin was created with the goal of de-centralization, and “rewards” have been introduced as a substitute for a central organization that would maintain, manage, and expand the system [9]. Allowing the behaviors of individuals following their personal interests to also benefit the community they belong to, mechanism design is an extremely important concept to maintain and expand cryptocurrencies by blockchain technology
* If token value rises steadily, it is possible to retain existing users while attracting new ones and the community will be able to grow sustainably. Token price is determined by the supply and demand of the token on the cryptocurrency market. If token holders keep the tokens for a long period, the supply of tokens will decrease and its price will increase. Therefore, it is desirable to hold the tokens for a long time to reduce their velocity and increase their value [41–43]. However, if you hold tokens for too long, the transactional volume collapses to 0, which is not desirable. Therefore, it is important to induce users to hold tokens for an appropriate amount of time.

What affects the price movements in Bitcoin and

Ethereum?

What affects the price movements in Bitcoin and

Ethereum?

***What affects the price movements in Bitcoin and Ethereum?***

***https://onlinelibrary-wiley-com.libproxy.ucl.ac.uk/doi/epdf/10.1111/manc.12352***

* *We find solid evidence that the amount of active addresses is the most significant variable among others influencing price movements in Bitcoin and Ethereum.*
* *Granger causality*

[*https://ieeexplore-ieee-org.libproxy.ucl.ac.uk/stamp/stamp.jsp?tp=&arnumber=8090398&tag=1*](https://ieeexplore-ieee-org.libproxy.ucl.ac.uk/stamp/stamp.jsp?tp=&arnumber=8090398&tag=1)

* *The methodology used to conduct this study will make use of the statistical analysis of the 5 greatest drops in the value of Bitcoin against the US dollar. Whilst other currencies could be used the US dollar is used as the standard rate of currency in international markets for commodities as well as being the world’s foremost reserve currency. These suggest a fairer platform for comparison because the dollar is used as a benchmark for international markets and is less likely to suffer severe fluctuations itself which could lead to inaccurate readings. To further ensure that the fluctuations being investigated are due to activity in the Bitcoin market and not the dollar, each fluctuation will be checked against the exchange rate between Bitcoin and the Pound Sterling. If the value of Bitcoin is seen to have changed significantly against both the pound and the dollar it can safely be assumed that the fluctuation in value is a result of activity surrounding Bitcoin and not the other two currencies.*

***Returns and network growth of digital tokens after cross-listings***

[*https://reader.elsevier.com/reader/sd/pii/S0929119920302972?token=E61EDF442E0740ED8522AB514A0EAD4F56FCF4B5EC8EC41635E9779611A7757C00D54F5D2CDD55E73D7FE87CC99D8C6E&originRegion=eu-west-1&originCreation=20210718184407*](https://reader.elsevier.com/reader/sd/pii/S0929119920302972?token=E61EDF442E0740ED8522AB514A0EAD4F56FCF4B5EC8EC41635E9779611A7757C00D54F5D2CDD55E73D7FE87CC99D8C6E&originRegion=eu-west-1&originCreation=20210718184407)

* *Granger causality*
* *Cumulative abnormal returns*
* *Possibility of pump and dump affecting price analysis. As presented by Li et al. (2020), pump and dump schemes have occurred rather frequently in the crypto-ecosystem. These events last for only several minutes, with the run-up in price and increased trading volume being quickly reversed. These schemes are not associated with token issuer actions such as software upgrades, news announcements or cross-listings. While we cannot rule out the presence of pump and dump schemes within the period under analysis, their potential effect would be short lived given their docu-mented nature of reversal within the day of the event. Our index adjusted cumulative returns accumulate over a 28-day window*

*The Granger-causality test helps to examine if lagged values of one variable help to predict another variable. It shows the p-values associated with the F-test if relevant sets of coefficients are zero.*

*(can do both ways) stakers->price; price->stakers*

(grouped according to **A Survey of Distributed Consensus Protocols for Blockchain Networks** (Yang Xiao, Ning Zhang, Wenjing Lou , Y. Thomas Hou) 2020) check.

**CHAIN-BASED**

**Nxt** blockchain – first fully PoS, did they change things up eventually?

**Peercoin**

<https://www.youtube.com/watch?v=0v__lVdK-DI&ab_channel=ChronosCrypto>

* V0.9 increased rewards (June 8 2020/ 15.05.2020). V0.9 development cycle was about improving the economics of peercoin as cryptocurrency.
* Goals to raise annual PoS inflation rate closer to 1% target and boost participation of minters. To reach 1%, 100% of coins had to be minting and producing blocks (unrealistic) -> increases minting rewards to better track this goal.
* Coinage reward increase from 1% to 3 %.
* Add static reward. Continuous minting maximizes earning of static rewards.
* Overall 450% reward increase from v0.8 to v0.9.
* Coin age limit: 1 year accumulating coinage limit. Must mint a block that year, before coins can continue earning you rewards next year. Discourages inactive coins.

<https://university.peercoin.net/#/deflation-through-transaction-fee-burning>

The majority of proof-of-stake based blockchains have also chosen an economic model where minters are compensated from transaction fees. This however leads to uneven distributions of coins to minters as some blocks will contain more transaction fees while others have less.

<https://docs.peercoin.net/#/protocol-versions-changelog->

* The Minting process can only start after 30 days of coinage.

<https://www.stakingrewards.com/earn/peercoin/metrics>

* 46% participation

<https://peercoinpulse.medium.com/peercoin-inflation-adjustment-54bcb283afe4>

<https://talk.peercoin.net/t/update-48-upcoming-changes-to-peercoins-pos-reward-economics/10249>

<file:///C:/Users/Dasa/Downloads/PoS%20Reward%20Adjustment%20Developer%20Chat%20Log.html>

https://github.com/peercoin/rfcs/blob/master/text/0018-pos-reward/0018-pos-reward.md#detailed-design

PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake 2012

<https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf>

https://www.peercoin.net/

PPCoin had v0.2, v0.3,…..

(started as PoW + PoS)

One of the early appearances of Proof of Stake may be attributed to Sunny King and Scott Nadal in their 2012 paper for Peercoin. They describe it as a “peer-to-peer cryptocurrency design derived from Satoshi Nakamoto’s Bitcoin.”

The Peercoin network was launched with a hybrid PoW/PoS mechanism, where PoW was mainly used to mint the initial supply. However, it wasn’t required for the long-term sustainability of the network, and its significance was gradually reduced. In fact, most of the network’s security relied on PoS.

Proof-of-work and proof-of-stake both serve as means of distributing new coins.

A transaction fee prevents spam and is burned (instead of being collected by a miner), benefiting the overall network.

To recover from lost coins and to discourage hoarding, the currency supply targets growth at 1% per year in the long run. (wiki)

https://university.peercoin.net/#/11-economics-of-peercoin

<https://medium.com/peercoin/minters-get-richer-bdf1a1cd5674>

<https://peercoinpulse.medium.com/?p=d126e214dd66>

Bitcoin transaction fees, users compete with each other to get their transaction to be executed first, makes it expensive

Qtum, Particl

**COMMITTEE-BASED**

**CARDANO**

Based on peer-reviewed academic research,

1000 total stake pools. ….// Active Pools: 2,712

ADA is a native coin of the Cardano protocol

There are pool operators in the Cardano network that are responsible for minting new blocks. Their nodes operate 24/7 and randomly produce new blocks when they become slot leaders. These nodes process transactions.

Staking allows you to participate in minting new blocks without the need to have your computer permanently switched on. You, as an ADA coins holder, have decision power. You can choose a pool to which you want to delegate your coins. It means that your coins (your stake) will become a part of the total power (total stake) of the pool.

In pools there are Operators and delegators.

https://cardanians-io.medium.com/economic-and-incentive-model-behind-cardano-proof-of-stake-3e483a588043

* There is a limited number of ADA coins so they are naturally scarce. To be precise, there will be only 45,000,000,000 ADA coins. As far as there is a demand for the ADA coins the Cardano protocol has a digitally scarce resource that can be used to reward people for honest behavior.
* Cardano’s Proof-of-Stake is designed in a way that ensures high security and motivates to keep a high level of decentralization through economic and incentive models. Cardano has ADA coins that have a value so it can reward participants of network consensus for honest behavior and high-quality service. Moreover, it can motivate stake-holders to hold coins and thus maintain decentralization on a high level (.decision power is really distributed among many stake-holders)
* Incentivizee by newly minted ADA tokens for 10 years and then rely on transaction fees that have been accumulated??
* creates a natural demand for the ADA coins
* The incentive mechanism is modeled with an assumption of rationality of participants. Each participant acts selfishly to maximize their own return. Selfless participants are rare. Nearly all participants are self-interested and pursue strategies that reward them. The economic model, that is programmed directly in the protocol, defines rules and laws that are used to reward all participants that take part in making consensus. One of the core principles of game theory is that an ideal system is one where selfish participants, acting in their own best interests, are also, by design, acting in the best interests of the system.

<https://cryptoslate.com/cardano-ada-retains-its-spot-as-the-most-staked-crypto/>

<https://www.ibtimes.co.uk/cardanos-ouroboros-proving-proof-stake-can-work-wild-1663150>

* (2018) Kiayias said the Ouroboros incentives are still under active development. "We gave a thorough analysis of the capabilities of a covert adversary (one that is afraid to be caught cheating because of a penalty) compared to an adversary that is not afraid getting caught.
* "In general, incorporating penalties is a possibility, but it will only be used if it is completely justifiable within a thorough game theoretic model that includes Nash equilibrium and incentive compatibility analysis. We are actively developing this research now and soon we will have a white paper that explains how incentives will be implemented," he said

**Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol** (Aggelos Kiayias, Alexander, Russell Bernardo, David Roman Oliynykov)

https://link.springer.com/chapter/10.1007/978-3-319-63688-7\_12

* Short intro about proof of work requiring a lot of energy.
* Present proof of stake as an alternative.
* Cites security concerns associated with proof of stake.
* A fundamental problem for PoS-based blockchain protocols is to simulate the leader election process.
* Present a secure PoS protocol (Static and dynamic versions).
* How the proposed protocol addresses common attacks.
* Present a reward mechanism to incentivise the participants to the system.
* Delegation mechanism
* Comment on related work. Sleepy, Snow White, Algorand, Fruitchain (PoW).

<https://github.com/input-output-hk/cardano-docs/blob/master/docs/cardano/proof-of-stake.md> (follow-the-satoshi)

ouroboros praos

ouroboros genesis

**SLEEPY.**

2017 R. Pass and E. Shi, “The sleepy model of consensus,” in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2017, pp. 380–409.

<https://link.springer.com/chapter/10.1007/978-3-319-70697-9_14>

* Inspired by longest chain. Idea of nakamoto

**SNOW WHITE**

2019 Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure Proof of Stake. Phil Daian, Rafael Pass, Elaine Shi

https://link.springer.com/chapter/10.1007/978-3-030-32101-7\_2

* Comparison to other protocols incl Ethereum

**BFT-BASED**

**ALGORAND**

**ALGORAND** (Jing Chen, Silvio Micali) 2016/7

https://arxiv.org/abs/1607.01341

* Ledgers are the future.
* Btc – wasteful, scales poorly, concentrates power in very few hands.
* Algorand uses algorithmic randomness to select a set of verifiers who are in charge of constructing the next block of valid transactions. Selections are immune from manipulations, unpredictable until the last minute, universally clear. No different classes of users (e.g miners, ordinary users). Very small possibility of forking. Addresses legal and political concerns.
* Bitcoin and its problems
* Algorand work efficiently in permissionless and permissioned environments, withstands adversarial environments. The amount of computation required is minimal. A new block generated in less than 10 min and will never leave the blockchain. All power resides with the users
* Uses Byzantine Agreement protocol to reach agreement.
* Sleepy, Ouroboros reference
* …. Come back to this one

<https://www.youtube.com/watch?v=zNdhgOk4-fE&ab_channel=LexFridman>

* Algorand challenges blockchain trilemma (scalability, security, decentralization)
* PoW- not many can compete -> centralization; DPoS also centralized
* Game theory (1.30/1.32)
* Incentives are very hard to design because people are very complex creatures.
* Essentially algorand has no incentives, but the notion is believable. (1.34) epsilon utility equilibrium. No incentives -> good thing.

**ETHEREUM (CASPER)**

<https://hackingresear.ch/economic-incentives/>

* Interest model

<https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-economics/>

* The Ethereum 2.0 upgrade will bring with it a switch from Proof of Work to Proof of Stake. This means instead of miners competing for a block reward, validators will be paid to perform assigned rules and secure the network. It's vitally important to get the economics of staking right so that the network stays healthy and secure.If the incentive to stake is too low, the network will not get the minimum amount of validators needed to maintain consistent cross-shard communication. If the incentive is too high, the network is overpaying for security and inflating at a rate that is detrimental to the economics of the network as a whole.
* Lockup
* Risks

<https://www.youtube.com/watch?v=3x1b_S6Qp2Q&ab_channel=LexFridman>

* Align incentives
* Byzantine, PoW, PoS
* Phase 0: proof of work and PoS separately
* Casper FFG combines them

<https://www.youtube.com/watch?v=XW0QZmtbjvs&ab_channel=LexFridman>

* PoS consensus mechanism by which nodes in the network agree on which transactions came in and in which order, make sure that once block is accepted it cannot be reverted
* Why need PoS, PoW(30 min): civil resistance. Why one person one vote would not work.
* Pow - Cost of energy and cost of hardware.
* PoS launched in December, not coming to consensus about anything at this point

<https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#finality>

Proof-of-stake is the underlying mechanism that activates validators upon receipt of enough stake. For Ethereum, users will need to stake 32 ETH to become a validator. Validators are chosen at random to create blocks and are responsible for checking and confirming blocks they don't create. A user's stake is also used as a way to incentivise good validator behavior. For example, a user can lose a portion of their stake for things like going offline (failing to validate) or their entire stake for deliberate collusion.

Unlike proof-of-work, validators don't need to use significant amounts of computational power because they're selected at random and aren't competing. They don't need to mine blocks; they just need to create blocks when chosen and validate proposed blocks when they're not. This validation is known as attesting. You can think of attesting as saying "this block looks good to me." Validators get rewards for proposing new blocks and for attesting to ones they've seen.

If you attest to malicious blocks, you lose your stake.

The threat of a 51% attack still exists in proof-of-stake, but it's even more risky for the attackers. To do so, you'd need to control 51% of the staked ETH. Not only is this a lot of money, but it would probably cause ETH's value to drop. There's very little incentive to destroy the value of a currency you have a majority stake in. There are stronger incentives to keep the network secure and healthy.

Stake slashings, ejections, and other penalties, coordinated by the beacon chain, will exist to prevent other acts of bad behavior. Validators will also be responsible for flagging these incidents.

<https://consensys.net/blog/blockchain-explained/what-is-proof-of-stake/>

<https://ethereum.org/en/eth2/staking/>

* Proof-of-stake is managed by the Beacon Chain.
* Ethereum will have a proof-of-stake Beacon Chain and a proof-of-work mainnet for the forseeable future. Mainnet is the Ethereum we've been using for years.
* During this time, stakers will be adding new blocks to the Beacon Chain but not processing mainnet transactions.
* Ethereum will fully transition to a proof-of-stake system once the Ethereum mainnet merges with the Beacon Chain.
* A miner upgrade will follow to enable withdraw of staked funds.

<https://ethos.dev/beacon-chain/>

Validators also police each other and are rewarded for reporting other validators that make conflicting votes, or propose multiple blocks.

Validators are rewarded the most when their attestation is included on-chain at their assigned slot; later inclusion is a decaying reward.

Incentives; rewards and penalties description.

Validators can also “voluntary exit” after serving for 2,048 epochs, around 9 days. Can’t withdraw the stake right away.

C**asper the Friendly Ghost: A "Correct-by-Construction" Blockchain Consensus Protocol**

<https://www.youtube.com/watch?v=ELU6hCL3HoA&ab_channel=CyberInitiative>

* Sharding – splitting up work in a distributed system to scale its capacity (fundamentally has more than 1 part) ->there cnnot be a sharded binary consensus protocol (bit cannot be sharded)
* Sharded consensus protocol
* …

**Casper the Friendly Finality Gadget** (Vitalik Buterin and Virgil Griffith) 2017

<https://arxiv.org/pdf/1710.09437.pdf>

* Two schools of thought in PoS design: chain-based PoS and Byzantine fault tolerant PoS. Repurposing BFT algorithms for proof of stake was first introduced by Tendermint.
* Casper follows this BFT tradition, though with some modifications.
* If a validator violates a rule, we can detect the violation and know which validator violated the rule. Accountability allows us to penalize malfeasant validators, solving the “nothing at stake” problem that plagues chain-based PoS. The penalty for violating a rule is a validator’s entire deposit. This maximal penalty is the defense against violating the protocol. Because proof of stake security is based on the size of the penalty, which can be set to greatly exceed the gains from the mining reward, proof of stake provides strictly stronger security incentives than proof of work.
* Proof of stake’s security derives from the size of the deposits, not the number of validators,
* Dynamic validator sets
* 2/3 of validators (by deposit) need to cast votes
* Slashing conditions (<https://medium.com/@VitalikButerin/minimal-slashing-conditions-20f0b500fc6c>)
* The long range attack
* To resolve catastrophic crashes (disconnect from the network): Inactivity leak
* Imperfections of Casper
* Future workpapers will explain and analyze the financial incentives within Casper and their consequences. A particular economic problem related to such automated strategies to block attackers is proving upper bounds on the ratio between the degree of disagreement between different clients and the cost incurred by the attacker.

**Incentives in Ethereum's hybrid Casper protocol (**Vitalik Buterin, Daniël Reijsbergen, Stefanos Leonardos, Georgios Piliouras) 2020

<https://onlinelibrary.wiley.com/doi/epdf/10.1002/nem.2098?saml_referrer>

* One of the main alternatives to PoW is virtual mining or proof of stake(PoS).7-9In PoS, the right to propose a block is earned by locking—or depositing—tokens on the blockchain, which hasno inherent energy cost.
* What casper ffg is, hybrid casper
* This addresses two of the classical challenges that affect PoS protocols19,20: the nothing-at-stake problem through the slashing mechanism that penalizes misbehavingviolators21and long-range attacks through a modified fork-choice rule that prioritizes (and never automatically reverts)finalized checkpoints over PoW.22
* We show that the scheme is incentive compatible in the sense that participants are incentivized to follow the protocol, and we investigate its impact on the basic properties of liveness and safety.
* In hybrid Casper FFG, some nodes assume the role of validators. Nodes can become validators by locking/staking tokens on the PoW chain, thus creating a deposit. Validators need to wait a long period after depositing before being allowed to withdraw. In the benchmark setting,22this is 15 000 epochs, ie, around 120 days.
* Finality
* Rewards and penalties mechanism.
* According to Casper's payments scheme, validators who vote correctly during an epoch are rewarded, and validators who do not are penalized. This is achieved by adjusting the validators' deposits depending on their own voting behavior, ie, on whether they are voting or not, and on the performance of the protocol as a whole, ie, on what total fraction of validators vote correctly and whether that is enough to justify and finalize checkpoints. correct voting;non voting; conflicting/incorrect voting;
* Incorrect or missing votes are not punished as harshly as conflicting votes, as there are several faulty behaviors that can cause a validator  to fail to produce a valid vote.
* The difficulty with fault attribution in the case of missing/incorrect votes (which in general suffers from the problemof speaker/listener fault equivalence42) creates a tension between preventing harm and fairness, ie, between sufficientlypenalizing malicious validators and adequately incentivizing honest validators to participate.
* Slashing. Any validator is able to call the slash function with the data for two potentially offending vote messages as its argu-ments. If the slash call is found to be valid, then the offending validator's deposit is partially or entirely taken away(slashed) and the sender receives 4% of the validator's deposit as a “finder's fee.” In the Casper contract, the degree to which the validator's deposit is shrunk dependsto the total amount slashed recently across the protocol—the reasoning is to punish more harshly when there is a higherrisk that two conflicting checkpoints with the same height will be finalized.
* We assume that the protocol consists of two main types of nodes: block proposers who propose blocks on the underlying chain and validators who vote for checkpoint blocks
* …liveness, safety
* Incentive compatibility.
* REWARDS:
  + setting the reward too high makes the protocol expensive to operate.
  + Setting the reward too low means that fewer people will be willing to deposit, which in turn implies that the protocolis more centralized and less secure.
  + Setting rewards too low also increases the possibility of discouragement attacks,54where an attacker either performs a censorship attacks or finds a way to cause high latency (eg, by splitting the network), causing validators to lose money; the threat of this may encourage validators to leave or discourage them from joining
* PENALTIES:
  + setting the penalty factor too high implies improved liveness, ie, faster recovery from situations in which more than one third stop voting properly.
  + Setting the penalties too high, however, also implies higher risks for validators and bigger losses even if they accidentall yare not able to stay online.
* DEPOSIT SIZE:
  + setting the deposit size dependence higher means that validators can make a larger profit by performing censorship orDoS attacks against other validators
  + Setting the deposit size dependence too low means that the protocol does not automatically adjust the interest ratedepending on how risky potential validators perceive depositing to be, as argued in Choi.55
  + Users are looking for not just low issuance and high security, but also stability of the level of issuance and security.Having rewards decrease as the total deposit size increases (ie, setting p high) accomplishes the former g oal trivially,and the latter goal by “trying harder” to attract validators when the total deposit size is small. However, low values of pmean that from the perspective of a single validator, the interest rate is stable (eg, if you deposit when the interest rateis 5%, you know that this will not drop dramatically even if a large sum is deposited by other validators)
* Several approaches can be taken to limit the number of participating validators. The intended approach by Ethereum was to impose a fixed minimum deposit size of 1500 ETH. Alternative approaches would be to not accept new deposits beyond a hard limit of N validators, to only accept votes from the N validators with the highest deposit size, or to dynamically adjust the minimum deposit size based on the number of validators. Accurate predictions of the impact of the minimum deposit on the number of validators require economic modeling that is outside the scope of this paper. As for other PoS-based blockchain platforms: in EOS, 21 delegates57chosen by the stakeholders control the consensus algorithm,whereas Cardano aims for 100(0) stake pools.58,59
* All schemes will involve a trade-off: although heavy penalties for offline validators improve liveness and safety, they also negatively affect honest participants who suffer from unavoidable network or computer failures.

https://eth.wiki/en/concepts/casper-proof-of-stake-compendium

**Upgrades to the ethereum network could turn crypto staking into a $40 billion industry by 2025, JPMorgan says**

<https://markets.businessinsider.com/news/stocks/ethereum-upgrades-crypto-staing-industry-boom-jpmorgan-ether-2021-7>

* The staking industry - in which users earn cryptocurrency by putting up their own tokens to validate transactions - is currently worth around $9 billion, JPMorgan analysts, led by Kenneth Worthington, said in a note on Wednesday.
* JPMorgan's analysts praised the staking model and its opportunities for investors. "We see the ability to earn a positive real return as one of the factors driving the cryptocurrency market to become more mainstream," they said.

However, the analysts said there are risks. One is that staking locks up a user's cryptocurrency holdings for a period. Prices could tumble, but the user would be unable to sell. Another is that users could fall victim to fraud if staking on unreliable networks.

**More than $13 billion worth of ether has been staked on ethereum 2.0 as momentum builds behind the network overhaul**

https://markets.businessinsider.com/news/stocks/ether-eth-ethereum-2-network-upgrades-staking-jpmorgan-2021-7

* More than $13 billion has now been staked on the ethereum 2.0 network, as interest grows.
* Users put forward a "stake" and gain the right to validate transactions and earn more coins.
* Ethereum users are almost always required to stake 32 ether before they can become validators on the network and earn coins in return, meaning there were likely more than 190,000 validators as of Monday.

**TENDERMINT (COSMOS)**

pBFT + DPoS(Delegated Proof-of-Stake)

internet of blockchains solution

Kwon, J. Tendermint: Consensus without mining (2014). https://cdn.relayto.com/media/files/LPgoWO18TCeMIggJVakt\_tendermint.pdf

* Repurposing BFT algorithms for proof of stake was first introduced by Tendermint.

Cosmos, for example, has “hard slashing” for anyone who double-signs or is offline for a significant period of time. This mechanism ensures that validators are indeed actively participating in the consensus in a consistent manner.

**DPoS**

“A DPoS-based blockchain counts with a voting system where stakeholders outsource their work to a third-party. In other words, they are able to vote for a few delegates that will secure the network on their behalf.”

Centralized?

Bitshares -- first

Polkadot – migrated to PoS on 18 June 2020

Binance coin

EOS

Tron

Tezos L.M Goodman. Tezos A self-amending crypto-ledger white paper

<https://www.stakingrewards.com/journal/state-of-tezos-staking>

* effects of  introduction of custodial staking on large exchanges like Coinbase
* Since the Carthage network upgrade in March 2020, rewards have become more dynamic.
* A common misconception about Tezos is that all staked coins are out of circulation, i.e. they cannot move or be sold next block. In fact, only baker deposits, fees, and rewards for the past 14 days are locked (frozen). The total amount of frozen capital across all bakers is at most 6.2% (52.4M XTZ) in deposits and 0.2% (1.6M XTZ) in rewards.
* Tezos went through three generations of growth. We call them the Early Backers (Jun’18 – Mar’19), the 2019 Boomers (Apr’19 – Oct’19), and the Brrrr Generation (Nov’19 – now)
* interface

<https://tzstats.com/docs/api#tezos-api>

<https://blockwatch.cc/databases/blockchains> - btc, Litecoin, doge, tezos data (paid?)

*Who went from PoW to staking? Who made changes around staking or rewards?*

*Check blackcoin as there is v2*

Fanti, Kogan, and Viswanath (2020) study valuation of a PoS cryptocurrency;

Irresberger et al. (2020) highlight the recent growth of PoS cryptocurrencies empirically;

NEO (AntShares) - delegated Byzantine Fault Tolerance

Ungrouped by me Pos:

NEM <https://nemplatform.com/wp-content/uploads/2020/05/NEM_techRef.pdf>

Blackcoin

* Blackcoin has a simpler concept; your stake is simply the amount of the cryptocurrency in your wallet that you have assigned as your stake.
* Blackcoin is a cryptocurrency that was released in early 2014 and also functions on a pure proof-of-stake consensus mechanism. Again, it’s a relatively small cryptocurrency by value and not widely used.

Blackcoins Pavel Vasin. Blackcoins proof-of-stake protocol v2, 2014. https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf

<https://www.dummies.com/education/finance/cryptocurrency-mining-and-proof-of-stake-algorithms/>

* Attacks
* Pros cons

**SoK: Understanding BFT Consensus in the Age of Blockchains**

<https://eprint.iacr.org/2021/911.pdf>

* Ouroboros,
* Algorand

<https://www.stakingrewards.com/journal/is-staking-really-profitable>

* Importance of participation: if the coin fails to maintain a reasonable daily volume, it might get delisted from exchanges (example Bean Cash delisted from Bittrex) and your whole investment can go to zero.
* Tezos profitability

*Participation -> attract users now to ensure they are there when use cases are established.*

<https://www.stakingrewards.com/journal/will-defi-and-staking-merge>

* Lock up, slashing
* Tezos
* Liquid staking and effect on incentives (report)

<https://www.stakingrewards.com/journal/10-key-take-aways-from-the-staking-ecosystem-case-study>

* Interface importance
* education

<https://medium.com/digishares/tokenomics-and-staking-a5e58a27b180>

One of the ways token-based platforms are addressing these issues are through the introduction of staking. Staking is different to Proof-of-Stake (POS) and Distributed Proof-of-Stake (DPOS). POS and DPOS are consensus mechanism within blockchain, designed for validating transactions and producing blocks whereas staking is a method through which various incentives are provided for achieving different goals, such as validating a block in a blockchain. In order to ensure that a correct block is produced in a blockchain, staking is used to incentivize users to produce correct blocks and earn rewards, thus avoiding the risk of losing staked tokens due to incorrect validation of blocks. In this sense, staking is used within the POS and DPOS consensus mechanism to encourage good behaviour.

The rewards are structured so that the longer a user holds their tokens, the higher reward it will receive. The argument for rewarding users who hold their tokens is to gain price stability

The act of burning tokens reduces the supply of tokens, and assuming that demand is constant or increasing, the price of token will increase.

It allows platforms to address the velocity problem because with every transaction, the circulation of tokens is increased. With higher velocity, the token price is pressured to fall, because there is an inverse relation between price and velocity. With the introduction of staking, not all tokens will be available for transactions. If it is required to stake, the staked tokens will be out of circulation with every transaction. With every transaction, the circulation of tokens is increased and as well as the staked tokens. This reduces velocity since due to staking, some tokens are held, while some tokens are being transacted. With the inverse relation between price and velocity, the reduced velocity due to staking prevents the price to fall.

Fruitchain incentive structure – for pow originally. penalties

PoW provides no real incentive (ok price appreciation might be considered one but it is not imbedded in the incentive mechanism) to keep mined tokens. Miners sell tokens-> price goes down. Pos on the other hand does(to keep staking more and compound rewards)… *Bitcoin has experienced a remarkable increase in both the price of the token and the network hash rate. Intuitively, higher prices should provide stronger incentives for miners and increase the provision of computing resources. In turn, a more secure network should reduce users’ uncertainty about attacks and fraud, increasing the demand for the DN token and its price*

“what’s the incentive scheme to attract non speculative users (the ones that would not just dump the tokens in the market)”. [usually imbedded in pos protocols. ?small rewards, compounding, the more you have the better, etc]

Cosmos, for example, has “hard slashing” for anyone who double-signs or is offline for a significant period of time. This mechanism ensures that validators are indeed actively participating in the consensus in a consistent manner.

projects may introduce additional staking promotions (such as Algorand) that last for specific periods, thus further incentivizing new users, while also changing the rewards calculus

<https://figment.io/resources/misunderstanding-yield-and-inflation-in-proof-of-stake-networks/>

* token holder dilution rate (often referred to as inflation). *“PoS Networks do*not*have an Inflation Rate. Rather they have a*Token Holder Dilution Rate*.”*
* *“PoS networks do not have a yield. Rather token holders receive a Share of Staking Rewards.”*
* you are receiving a portion of the new tokens minted. Again, it is relative ownership/participation in the network that is changing for token holders.

By staking you are (hopefully) maintaining or even increasing your relative participation in the network. How much depends largely on overall staking rates as token awards only go to those who are staking.

* Staking rewards — and the possibility of slashing — are a set of incentives that encourage token holders and validators to secure a PoS blockchain. In return, they maintain or grow their relative share of token holdings in the network. Staking creates the “skin in the game” necessary for good behavior such as running nodes in the network and discouraging bad behaviors like failing to remain online or double signing.

Staking rewards do NOT exist to provide an income stream to token holders. Think instead, “by staking I can increase my network participation (ownership if you like) by 0.3% over the following year” or “if I do not stake, my relative participation/ownership in the network will be diluted by 1.5% over the next 12 months”.

The economic rationale for staking a PoS token is not to receive “yield” (it doesn’t exist) but because you believe that by doing so you will be growing your relative interest in the network and also contributing to significant token appreciation.

* Note: All of above assumes that a network’s staking awards are being solely generated by minting new tokens as part of a set of staking incentives.

Can users abuse the incentive system?

In contrast to that, people who are not bonding their token to the network will have easy access to them which means ultimately liquidity. But they will not participate in the constant stream of new token distribution and will over time reduce their ownership in the network.

permissioned permissionless?

PoS critisizm

<https://halshs.archives-ouvertes.fr/halshs-00945053/document>

<https://download.wpsoftware.net/bitcoin/old-pos.pdf>

Stellar

Since its network inception, Stellar (XLM) has offered what it terms inflation, a steady 1% inflation rate to the supply on the whole network, which allows its network to maintain low transaction fees, as stakers collect the inflation rewards weekly at 12 AM GMT every Tuesday.Stellar’s inflation rewards were initially designed to be easy to obtain, but not too high of an interest rate to dilute the total value of supply of the network. The initial intention was to simultaneously attract new platform users, as well as encouraging an active usage of the coin by introducing opportunity costs for merely hoarding coins.However, Stellar has recently proposed an upgrade that, if ratified, may eliminate its inflation, citing a failure of fostering development and rewarding of positive actors within the Stellar ecosystem. Instead, Stellar has rolled out some unique airdrops, such as the one to Keybase users and Github users, targeting developers and decentralized technology users. 2019

NEO/GAS – two coin model

This token economic model was unique for two reasons - firstly, it created a new system in which block rewards would not dilute the coin that provides the ability to earn the block rewards. Secondly, the model allowed for a separation between a pure utility token and a token whose value is derived from the ability to produce or earn the utility token.

Inflation – lex podcast guy (…from first principles)

btc rewards

The attacker’s incentives to carry out such an attack of course depend on exactly how minng rewards are distributed, but it is clear that globally predictable selfish mining allows the attacker to produce a greater fraction of blocks on the longest chain. For standard reward schemes this is indeed profitable

Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. On the instability of bitcoin without the block reward. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 154–167. ACM, 2016.

Ittay Eyal and Emin G¨un Sirer. Majority is not enough: Bitcoin mining is vulnerable. In International conference on financial cryptography and data security, pages 436–454. Springer, 2014.

no.

<https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf>

scalable bitcoin-ng

A Model of Cryptocurrencies Michael Sockiny Wei Xiongz January 2021

Proof-of-Stake Longest Chain Protocols: Security vs Predictability Vivek Bagaria

**SOLIDUS? PROOF OF WORK**

Solidus is an incentive compatible cryptocurrency on the basis of permissionless Byzantine consensus [20]. It injects incentives for almost each phase of the practical Byzantine consensus like get-epoch phase, elect phase, prepare phase and accept phase. The incentives also consist of negative ones such as penalties for malicious actions. On the other hand, Solidus can also mitigate selfish mining attacks.

Solidus: An Incentive-compatible Cryptocurrency Based on Permissionless Byzantine Consensus (Ittai Abraham et al) 2017

**Demystifying Incentives in the Consensus Computer** (Loi Luu et al) 2015

<https://dl.acm.org/doi/pdf/10.1145/2810103.2813659>

* Verifiers dilemma
* The problem we look at in this work is independent of the underlying consensus algorithm used in the network as the verifier’s dilemma arises in any cryptocurrency that has high block’s verification cost.
* In this paper, we introduce a verifier’s dilemma demonstrating that honest miners are vulnerable to attacks in cryptocurrencies where verifying transactions per block requires ***significant computational resources***

**Token Economics in Real Life: Cryptocurrency and Incentives Design for Insolar’s Blockchain Network**

[**https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9321727**](https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9321727)

* Simulation techniques references

**Where do we stand in cryptocurrencies economic research? A survey based on hybrid analysis** Aurelio F. Bariviera∗

Another gap in the literature is how ~~mining~~ protocols could affect price. It is well known that cryptocurrencies use different protocols to maintain network consensus3 . To the best of our knowledge there is no paper considering the influence of consensus protocols in **price formation, returns or volatility**.

*Avalanche, Binance Smart Chain, NEAR, Solana*