Consensus Model & Incentive Model

Table of Contents

What is Consensus?

By consensus, we mean that a general agreement has been reached. Consider a group of people going to the cinema. If there is no disagreement on a proposed choice of film, then a consensus is achieved. If there is disagreement, the group must have the means to decide which film to see. In extreme cases, the group will eventually split.

What is a Consensus Mechanism?

The term 'consensus mechanism' is often used colloquially to refer to 'proof-of-stake', 'proof-of-work' or 'proof-of-authority' protocols. However, these are just components in consensus mechanisms that protect against Sybil attacks. Consensus mechanisms are the complete stack of ideas, protocols and incentives that enable a distributed set of nodes to agree on the state of a blockchain.

A consensus mechanism is what keeps decentralized networks secure. Nodes must agree on the current state before updating the blockchain. This automated process prevents errors and secures the network against threats such as double-spending or Sybil attacks, where malicious actors manipulate the network with fake nodes.

Distributed consensus is entirely automated, and it is executed as programmed. This way, users trust the technology, rather than a third party, for the integrity of a blockchain. As a result, the consensus mechanism’s logic and implementation must be flawless.

Bitcoin, the first mainstream blockchain, adopted the Proof of Work consensus mechanism in 2009. Thereby making Proof of Work one of the first consensus mechanisms. But other more innovative consensus algorithms have been introduced over time.

Types of Consensus Mechanisms

There are different kinds of consensus mechanism algorithms, each of which works on different principles.

While Proof of Work (PoW) is one of the earliest consensus algorithms, which works based on game theory. Many popular blockchains adopted it, including Bitcoin, Litecoin, and Dogecoin. This consensus mechanism is discussed in details in of Unit 2: The First Protocol: Bitcoin Blockchain (2.5 section).

Now first have a basic understanding of Proof of Stake.

Proof of Stake (PoS)

To help address the limitations of the PoW consensus mechanism and reduce the number of computational resources required to maintain the blockchain network, the Proof-of-Stake (PoS) concept was introduced. Proof-of-Stake concept was originally introduced by Sunny Kind and Scott Nadal in 2012. While PoW and PoS both share the same goal of reaching blockchain consensus, the process they take is quite different. Rather than expending resources to solve for a computationally intensive proof, participants only prove they have staked coins. PoS "validators" take on the role of "miners," but instead of running crypto mining machines, they are only required to hold and "stake" a certain amount of PoS digital tokens or coins in order to participate in the validation process. In PoS, new blocks are referred to as "minted" or "forged" rather than "mined."

Stake is typically the amount of cryptocurrency that a participant in a blockchain network has invested in the network via various methods, such as sending it to a specific address or locking it via a special transaction type. It is possible for stakes to go rogue and validate erroneous transactions. Nonetheless, some protocols have implemented incentive mechanisms to discourage such behavior. For example, in the Ethereum PoS model, malicious validators are punished by having their staked cryptocurrencies confiscated and being prohibited from staking in the future.

The methods by which the blockchain network uses the stake might vary, and each option includes trade-offs of its own. As an illustration, a few approaches being used in live blockchain networks include delegate systems, multi-round voting, coin ageing systems, and random selection of staked users. In all these variants of the PoS model, the cryptocurrency is typically no longer liquid for other purposes while being staked in the system.

In the long term, in the PoS model, the proportion of a stakeholder's stake to the total sum of cryptocurrency staked on the blockchain network influences the likelihood that they will publish a new block. Therefore, users who have a larger stake are more likely to propose new blocks. Since the PoS eliminates the need for validators to continuously purchase and upgrade hardware, achieving Sybil resistance requires almost no energy consumption, and reward mechanisms vary based on the validators' network roles. In the current Ethereum PoS model, for instance, the rewards for block proposals, sync committee members, and attestation are highly variable based on the number of Ether staked and the participation rate. These networks are designed so that all the cryptocurrency has already been distributed to users, as opposed to being generated at a constant rate.

Advantages

Fast Block Creation Time. Unlike PoW in Bitcoin, where block creation can last up to 10 minutes, PoS systems create new blocks within seconds. This makes transactions faster.

High Throughput. Since PoS has a faster block creation time, it can process more transactions quickly.

Energy Efficiency. PoS is way more energy efficient than other computational-intensive models such as PoW. In fact, research confirms that PoS uses 99% less energy compared to PoW. The validators do not need to solve any puzzle; the algorithm will pick them to validate based on their staking power.

Scalability (But Less Than Pow). PoS is a scalable consensus algorithm that can handle increasing transactions without compromising speed. However, it is less scalable than PoW.

Independence from Special Hardware. Becoming a validator in Proof of Stake is easier because it requires no special hardware. Apart from staking, the prospective validator only needs a CPU and storage devices. The lowered bar of entry encourages more participation.

Disadvantages

Suffering From Centralization. There can be centralization in a PoS setting since the major criterion is having enough native assets to stake. If a person or group of people can get a lot of native assets and become validators, they can influence the consensus sessions of the blockchain.

Lower Cost of Misbehaving in Blockchain Networks. Some PoS blockchains are relatively inexpensive to set up. As a result, the validators do not have so much to lose in case they are sanctioned for misconduct. For example, a prospective validator on Cardano must stake a minimum of 25,000 ADA, which is only around $9,600.

Comparison to Proof-of-Work

The following table outlines the basic distinctions/similarities between Proof of Work (PoW) and Proof of Stake (PoS)

Distinctions/ similarities	PoW	PoS
Application	Permissionless	Permissionless/permissioned
Block proposal	Miners	Validators
Cost required	Cost of hardware i.e., Asics/GPU plus energy	Cost to acquire crypto/coins
Finalizing a malicious block	Hacker would require 51% of computing power i.e., hash rate	Hacker would require 66% of staked coin for adding a malicious block
Forking	Naturally discourages by consensus	Can't be prevented naturally

Implementations	Bitcoin, Litecoin, Monero, Zcash etc.	Ethereum 2.0, Solana, Tezos, Cardano, Algorand, Celo etc.
Increase in security	Increases with increase in hash rate	More Staking in exchange for rewards
Key advantage	Two layers of security are established by the upfront expenditure of the hardware and ongoing energy costs	Owing to its advantages in energy efficiency, PoS blockchain allows ordinary users to take part in the validation process by staking the coins
Key disadvantage	High energy consumption and a concern with e-waste are driven by improvements in chip speed and efficiency achieved in every few years	Since there is no ongoing cost involved with validating the blocks, centralization at Coin staking level is one of the main issues with its weaker level of security than PoW
Key resource required	Energy/electricity	Crypto/coins
Rewards	Coinbase plus transaction/network fees	Transaction/network fees
Transaction finality	Probabilistic	Probabilistic/immediate
Trust model	Untrusted	Untrusted/semi-trusted

Proof-of-Stake comes with benefits over Proof-of-Work:

- better energy efficiency – there is no need to use lots of energy on proof-of-work computations
- lower barriers to entry, reduced hardware requirements – there is no need for elite hardware to stand a chance of creating new blocks
- reduced centralization risk – proof-of-stake should lead to more nodes securing the network
- because of the low energy requirement less ETH issuance is required to incentivize participation
- economic penalties for misbehavior make 51% style attacks more costly for an attacker compared to proof-of-work
- the community can resort to social recovery of an honest chain if a 51% attack were to overcome the crypto-economic defenses.

While PoW and PoS are by far the most prevalent in the blockchain space, there are other consensus mechanisms such as:

Delegated Proof of Stake (DPoS)

Daniel Larimer adapted the PoS mechanism to design the DPoS model in 2014. Popular blockchains such as Cosmos and Tron use a variation of PoS called DPoS. Not all who lock some specified amounts of native assets can become validators. Instead, some selected delegates—better called "witnesses"—perform the decision-making on behalf of the others. The stakers have the power to elect the witnesses to represent them. In case of misconduct, the stakers can also vote to technically "impeach" them. The DPoS has a democratic outlook and design.

Practical Byzantine Fault Tolerance (pBFT)

The Byzantine Generals Problem describes the complexity of reaching an agreement if there are disloyal generals. The pBFT consensus mechanism is a secure model that can withstand dishonest validators. It reaches a consensus when there is ⅔ agreement from the honest nodes. Hyperledger, Fabric, and other prominent blockchains are utilizing this mechanism. However, the security of pBFT will be breached if the dishonest nodes are more than ⅓ of all the nodes in the network. The nodes in pBFT are divided into primary and secondary nodes. The primary nodes are the leader nodes, while the secondary nodes are the backup nodes. The primary nodes are changed at every consensus round.

Proof of Weight (PoWeight)

Six MIT researchers, led by Yossi Gilad, developed a consensus for the Algorand blockchain. Their prime motivation is discovering an algorithm model that solves the Byzantine Generals' Problem. They discovered a consensus algorithm based on weight fraction and christened it Proof of Weight. Each user in this mechanism exists in weights, and how much they have in their accounts determines their weight. The algorithm picks committee members randomly among the users based on their weight. This randomness checkmates the possibility of having one or many dishonest users. Honest users must have up to ⅔ of the total money in the network. Otherwise, dishonest nodes can take over. Although the design of PoWeights might look similar to PoS, each is different. The users only have to have tokens in PoWeights and do not need to lock or stake them.

Proof of Capacity (PoC)

Another popular name for Proof of Capacity is Proof of Space. Stefan Dziembowski and Sebastian Faust formally introduced it in 2015. Burstcoin was the first project to utilize this algorithm. Miners need to prove that they have the storage capacity to mine crypto. The most recommended storage device in the instant case is a hard disk. The miner needs to get ready before the mining kicks off. They get ready by plotting nonces. A miner can only create as many nonces as they have space for. The network frequently broadcasts puzzles. Any miner who has the closest hash in their nonce wins the puzzle.

Proof of Authority (PoA)

There must be thorough due diligence on the miners for a blockchain to be ultimately secure. Some consensus mechanisms skip this process and fall into the hands of dishonest miners. Proof of Authority, a consensus mechanism in which validators stake their identity, fixes this loophole in its design. Firstly, the real-life identity of each validator is ascertained within a PoA consensus model. The network managers will check how trustworthy the prospective validator

is. This also makes it easy to track any validator in case of foul play. Secondly, each validator must stake a certain amount of assets as a sign of commitment. Basically, PoA validators stake their reputation and their coins.

Proof of Importance (PoI)

NEM blockchain introduced the Proof of Importance consensus algorithm to improve the Proof of Stake mechanism. First, the Proof of Stake mechanism makes validators lock up their assets and not transact with them. Secondly, it only rates validators based on their stakings. Proof of Importance goes beyond that. The algorithm rates a node based on 3 variables:

- How much is in an account?
- How often does the account transact with others within the protocol?
- What is the volume of each transaction?

These 3 questions form how the importance of an account or node will be. The Proof of Importance mechanism encourages network participants to hold assets and transact with them.

Sybil Resistance & Chain Selection

Proof-of-work and proof-of-stake alone are not consensus protocols, but they are often referred to as such for simplicity. They are actually Sybil resistance mechanisms and block author selectors; they are a way to decide who is the author of the latest block. Another important component is the chain selection (aka fork choice) algorithm that enables nodes to pick one single correct block at the head of the chain in scenarios where multiple blocks exist in the same position.

Sybil resistance measures how a protocol fares against a Sybil attack(opens in a new tab). Sybil attacks are when one user or group pretends to be many users. Resistance to this type of attack is essential for a decentralized blockchain and enables miners and validators to be rewarded equally based on resources put in. Proof-of-work and proof-of-stake protect against this by making users expend a lot of energy or put up a lot of collateral. These protections are an economic deterrent to Sybil attacks.

A chain selection rule is used to decide which chain is the "correct" chain. Bitcoin uses the "longest chain" rule, which means that whichever blockchain is the longest will be the one the rest of the nodes accept as valid and work with. For proof-of-work chains, the longest chain is determined by the chain's total cumulative proof-of-work difficulty. Ethereum used to use the longest chain rule too; however, now that Ethereum runs on proof-of-stake it adopted an updated fork-choice algorithm that measures the 'weight' of the chain. The weight is the accumulated sum of validator votes, weighted by validator staked-ether balances.

Ethereum Consensus Model: Proof-of-Stake (PoS) Explained

Proof-of-stake (PoS) underlies Ethereum's consensus mechanism. Ethereum switched on its proof-of-stake mechanism in 2022 because it is more secure, less energy-intensive, and better for implementing new scaling solutions compared to the previous proof-of-work architecture.

Critics of Proof-of-Stake argue that it could provide a small set of centralized entities, like staking pools and institutional investors, with too much power over the network. While debate over the merits of this criticism continues, the Ethereum network's efforts to adopt Proof-of-Stake indicate that maintaining decentralization is possible.

What is Ethereum's Proof-of-Stake (PoS)?

Proof-of-stake is a way to prove that validators have put something of value into the network that can be destroyed if they act dishonestly. In Ethereum's proof-of-stake, validators explicitly stake capital in the form of ETH into a smart contract on Ethereum. The validator is then responsible for checking that new blocks propagated over the network are valid and occasionally creating and propagating new blocks themselves. If they try to defraud the network (for example by proposing multiple blocks when they ought to send one or sending conflicting attestations), some or all of their staked ETH can be destroyed.

Validators

To participate as a validator, a user must deposit 32 ETH into the deposit contract and run three separate pieces of software: an execution client, a consensus client, and a validator client. On depositing their ETH, the user joins an activation queue that limits the rate of new validators joining the network. Once activated, validators receive new blocks from peers on the Ethereum network. The transactions delivered in the block are re-executed to check that the proposed changes to Ethereum's state are valid, and the block signature is checked. The validator then sends a vote (called an attestation) in favor of that block across the network.

Whereas under proof-of-work, the timing of blocks is determined by the mining difficulty, in proof-of-stake, the tempo is fixed. Time in proof-of-stake Ethereum is divided into slots (12 seconds) and epochs (32 slots). One validator is randomly selected to be a block proposer in every slot. This validator is responsible for creating a new block and sending it out to other nodes on the network. Also in every slot, a committee of validators is randomly chosen, whose votes are used to determine the validity of the block being proposed. Dividing the validator set up into committees is important for keeping the network load manageable. Committees divide up the validator set so that every active validator attests in every epoch, but not in every slot.

How a transaction gets executed in Ethereum PoS?

The following provides an end-to-end explanation of how a transaction gets executed in Ethereum proof-of-stake.

1. A user creates and signs a transaction with their private key. This is usually handled by a wallet or a library such as ether.js, web3js, web3py etc but under the hood the user is making a request to a node using the Ethereum JSON-RPC API. The user defines the amount of gas that they are prepared to pay as a tip to a validator to encourage them to include the transaction in a block. The tips get paid to the validator while the base fee gets burned.
2. The transaction is submitted to an Ethereum execution client which verifies its validity. This means ensuring that the sender has enough ETH to fulfil the transaction and they have signed it with the correct key.
3. If the transaction is valid, the execution client adds it to its local mempool (list of pending transactions) and also broadcasts it to other nodes over the execution layer

gossip network. When other nodes hear about the transaction, they add it to their local mempool too. Advanced users might refrain from broadcasting their transaction and instead forward it to specialized block builders such as Flashbots Auction. This allows them to organize the transactions in upcoming blocks for maximum profit.

4. One of the nodes on the network is the block proposer for the current slot, having previously been selected pseudo-randomly using RANDAO. This node is responsible for building and broadcasting the next block to be added to the Ethereum blockchain and updating the global state. The node is made up of three parts: an execution client, a consensus client and a validator client. The execution client bundles transactions from the local mempool into an "execution payload" and executes them locally to generate a state change. This information is passed to the consensus client where the execution payload is wrapped as part of a "beacon block" that also contains information about rewards, penalties, slashings, attestations etc. that enable the network to agree on the sequence of blocks at the head of the chain.
5. Other nodes receive the new beacon block on the consensus layer gossip network. They pass it to their execution client where the transactions are re-executed locally to ensure the proposed state change is valid. The validator client then attests that the block is valid and is the logical next block in their view of the chain (meaning it builds on the chain with the greatest weight of attestations as defined in the fork choice rules). The block is added to the local database in each node that attests to it.
6. The transaction can be considered "finalized" if it has become part of a chain with a "supermajority link" between two checkpoints. Checkpoints occur at the start of each epoch and they exist to account for the fact that only a subset of active validators attest in each slot, but all active validators attest across each epoch. Therefore, it is only between epochs that a 'supermajority link' can be demonstrated (this is where 66% of the total staked ETH on the network agrees on two checkpoints).

Finality

A transaction has "finality" in distributed networks when it is part of a block that can't change without a large amount of ETH getting burned. On proof-of-stake Ethereum, this is managed using "checkpoint" blocks. The first block in each epoch is a checkpoint. Validators vote for pairs of checkpoints that it considers to be valid. If a pair of checkpoints attracts votes representing at least two-thirds of the total staked ETH, the checkpoints are upgraded. The more recent of the two (target) becomes "justified". The earlier of the two is already justified because it was the "target" in the previous epoch. Now it is upgraded to "finalized".

To revert a finalized block, an attacker would commit to losing at least one-third of the total supply of staked ETH. Since finality requires a two-thirds majority, an attacker could prevent the network from reaching finality by voting with one-third of the total stake. There is a mechanism to defend against this: the inactivity leak. This activates whenever the chain fails to finalize for more than four epochs. The inactivity leak bleeds away the staked ETH from validators voting against the majority, allowing the majority to regain a two-thirds majority and finalize the chain.

Crypto-Economic Security

Running a validator is a commitment. The validator is expected to maintain sufficient hardware and connectivity to participate in block validation and proposal. In return, the validator is paid

in ETH (their staked balance increases). On the other hand, participating as a validator also opens new avenues for users to attack the network for personal gain or sabotage. To prevent this, validators miss out on ETH rewards if they fail to participate when called upon, and their existing stake can be destroyed if they behave dishonestly. Two primary behaviours can be considered dishonest: proposing multiple blocks in a single slot (equivocating) and submitting contradictory attestations.

The amount of ETH slashed depends on how many validators are also being slashed at around the same time. This is known as the "correlation penalty", and it can be minor (~1% stake for a single validator slashed on their own) or can result in 100% of the validator's stake getting destroyed (mass slashing event). It is imposed halfway through a forced exit period that begins with an immediate penalty (up to 1 ETH) on Day 1, the correlation penalty on Day 18, and finally, ejection from the network on Day 36. They receive minor attestation penalties every day because they are present on the network but not submitting votes. This all means a coordinated attack would be very costly for the attacker.

Fork Choice

When the network performs optimally and honestly, there is only ever one new block at the head of the chain, and all validators attest to it. However, it is possible for validators to have different views of the head of the chain due to network latency or because a block proposer has equivocated. Therefore, consensus clients require an algorithm to decide which one to favor. The algorithm used in proof-of-stake Ethereum is called LMD-GHOST, and it works by identifying the fork that has the greatest weight of attestations in its history.

Proof-of-Stake and Security

The threat of a 51% attack still exists on proof-of-stake as it does on proof-of-work, but it's even riskier for the attackers. An attacker would need 51% of the staked ETH. They could then use their own attestations to ensure their preferred fork was the one with the most accumulated attestations. The 'weight' of accumulated attestations is what consensus clients use to determine the correct chain, so this attacker would be able to make their fork the canonical one. However, a strength of proof-of-stake over proof-of-work is that the community has flexibility in mounting a counter-attack. For example, the honest validators could decide to keep building on the minority chain and ignore the attacker's fork while encouraging apps, exchanges, and pools to do the same. They could also decide to forcibly remove the attacker from the network and destroy their staked ETH. These are strong economic defences against a 51% attack.

51% attacks are just one flavour of malicious activity. Bad actors could attempt long-range attacks (although the finality gadget neutralizes this attack vector), short range 'reorgs' (although proposer boosting and attestation deadlines mitigate this), bouncing and balancing attacks (also mitigated by proposer boosting, and these attacks have anyway only been demonstrated under idealized network conditions) or avalanche attacks (neutralized by the fork choice algorithms rule of only considering the latest message).

Overall, proof-of-stake, as it is implemented on Ethereum, has been demonstrated to be more economically secure than proof-of-work.

Ethereum Staking: What it is and How to Stake?

What is Ethereum Staking?

Ethereum staking refers to participation in Ethereum's transaction validation process following its move to a proof-of-stake consensus protocol. When staking, users lock in, or "stake," tokens on the blockchain in order to earn validator opportunities that secure the network in exchange for rewards.

In 2022, Ethereum underwent a major transition known as the Merge, when its consensus mechanism switched from a proof-of-work protocol to a proof-of-stake protocol. To stake Ether means becoming a validator, one of the pillars of proof-of-stake protocols. A validator is an entity who participates directly in Ethereum network consensus by authenticating transactions, creating new blocks on the chain and monitoring for malicious activity. Validators support the Ethereum protocol first-hand, and get subsequent rewards for doing so.

Staking is quite different from concepts like investing, Arie Trouw, software engineer and co-founder at XYO Network, explained: While investing in Ethereum is as simple as buying Ether and letting it sit in a wallet as the price fluctuates, staking, on the other hand, allows a user to earn tokens with interest, participate in liquidity pools, lending, yield farming and derivatives.

How Does Ethereum Staking Work?

In short, kicking off Ethereum 2.0 staking and the validator process means a user must stake 32 ETH, then acquire validator privileges and program their staking node accordingly.

In particular, there are a few core technologies that make Ethereum staking work and are important components of the validator process: Validator keys and epochs.

Validator Keys

Validator keys are the key pair associated with each validator that's established, and are used to verify validators and associated blocks on the Ethereum chain. Validator keys consist of one public key and one private key, and are each represented as a separate string of random characters. The validator public key is used by the network to identify the validator and deal with reward collection, and is attached to the transaction data when ETH is deposited for the staking deposit contract. The validator private key is used to sign any on-chain actions as a validator, like block proposals and attestations.

EPOCHS

Once keys and a node are set up, a validator must then wait to be selected to authenticate a transaction in part of the block production process. These are completed in time slots — a fixed time interval of 12 seconds during which a block is formed.

As time slots accumulate, they accrue into epochs, which are groups of 32 separate time slots that are each respectively 12 seconds. This totals 384 seconds, or 6.4 minutes, to form one epoch

The first block of an epoch is known as a checkpoint, which is followed by 31 regular blocks. This process is important to understand algorithmically, since the hash encoding the regular

blocks from 2 to 32 refer to the first checkpoint block as its key base, creating a single chain that holds the epoch together.

To complete the validator process, each block within a time slot is voted for by one committee of validators, each having a minimum of 128 members. The maximum number of members is 2,048, however, anything more than that is considered redundant. These 128 (or more) members are automatically and randomly elected to the committee from the general pool of Ethereum validators, fixed for the epoch duration.

Furthermore, each committee is distributed over one-time slot, forming 32 committees per each epoch. While one of the committee members validates a block, the remaining members can vote for this initiative. This kind of voting is called block attestation, Eugene Zomchak, product owner at CoinLoan, a crypto marketplace and lending platform, said. If approved, the block will become part of the main chain. At the end of an epoch, validators from the common pool are shuffled to form new committees for the next epoch. In total, there are at least 4,096 members per committee across 32 committees, equaling 131,072 Ether per epoch, Zomchak estimated.

The process rinses and repeats in entirety, ranging from a few seconds to several hours depending on network congestion.

Ways to Stake Ethereum

There are three main ways to stake Ethereum on the protocol, giving users options on how they would like to earn rewards and go about the staking process as a whole.

Solo Staking

Solo staking means being an individual validator on the Ethereum network. To solo stake, you must run and maintain an internet-connected Ethereum node using your own hardware and software, in addition to depositing 32 ETH. Being a validator means having machinery and internet strong enough to keep a node online at all times, otherwise the validator's ETH will be penalized. While solo staking is a significant responsibility, successful solo stakers earn rewards directly from the protocol instead of through third parties. They also have full control over the keys used to collect funds from ETH deposits and staking rewards.

Staking as a Service

Staking as a service, or "SaaS" in the Ethereum community, describes third-party services that run and maintain validator nodes on users' behalf. Users will still have to deposit 32 ETH to activate a validator, but delegate node operations to SaaS providers, usually for a cut of reward earnings. Staking as a service is often best for those who want to stake Ethereum but do not have the necessary hardware or knowledge to be a validator on their own. Staking as a service requires users to share their validator keys with their SaaS provider, leaving only partial control over node operations and fund access. However, this also means having a fully-maintained validator client to earn staking rewards from.

Pooled Staking

Pooled staking, or staking pools, involves multiple users contributing ETH together to reach the required 32 ETH deposit and activate one set of validator keys. Similar to staking as a service, pooled staking delegates validator node operations to a third-party, but can be done so

with a low amount of ETH. In many staking pools, users are given a liquidity token that acts as a receipt of staked amounts, which can be used as collateral on decentralized finance (DeFi) applications.

Pooled staking is the cheapest way to begin Ethereum staking, as many pools accept any amount of ETH to stake and reap rewards. Using a staking pool also doesn't require users to generate validator keys. Due to having several participants involved under a single validator, though, rewards are split and are usually smaller in value than other staking methods.

Risks of Staking Ethereum

- **Slashing and Validator Penalties**

When a validator operates maliciously or makes an incorrect on-chain attestation, this will result in slashed, or lost, earnings. This '"slashing insurance" is there to keep validators accountable, and is utilized to punish validators for inactivity or malicious actions.

Some violations that because slashing include proposing and signing two different blocks for the same slot or attesting to change the history of a block. If slashed, staked ETH will gradually be taken from the validator and they will be removed from the network.

- **Third-Party Vulnerabilities**

If using a staking as a service provider or staking pool, staked ETH is held by a third party and not kept privately by the staker. This makes earnings more susceptible to system theft, hacking or government intervention if the third party violates the law.

- **Market Volatility**

Staking any cryptocurrency comes with the possible change in token value as the market shifts. This can result in quick increases in reward earnings, but also quick decreases, so it's best to consider budget and willingness for investment risk before staking.

Ethereum Incentive Model

What are incentives?

An incentive is any design element of a system that influences the behaviour of system participants by changing the relative costs and benefits of choices those participants may make. Incentives include pay-for-performance reward systems that compensate individuals with money and they also include systems that incorporate no financial rewards at all.

What are incentives mechanisms/ models in Blockchain platforms?

The incentives and punishment mechanisms in a distributed system is vital for industry players to ensure network security and incentivize participants to act in a way that benefits the entire system. From miner rewards, to transaction fee-setting mechanisms, to token curated registries, to prediction markets, incentives are everywhere in blockchain platforms. Incentive design is a critical part of the overall economic design of effective blockchain platforms. It is the piece that builds on a platform's value proposition and structures the system for which the token of the platform will be designed. From an economics perspective, it is the core of the system.

Types of Incentive Mechanisms

Existing incentive mechanisms in blockchain can be divided into two categories according to incentive forms: monetary incentive and non-monetary incentive.

The **monetary incentive** is designed for regulating the behaviour of system entities from an economic perspective. It increases the utility of entities when they participate in the system by rewarding entities with money, thereby giving the entities motivation to join the system. The monetary incentive mechanisms employ economic balance to increase the cost of attacking or behaving selfishly to prevent attacks and encourage the entities to cooperate.

Existing **non-monetary incentive** can be further divided into credit-based incentive, reputation-based incentive, and gamified incentive.

Reputation-based incentives pay more attention to encouraging nodes to collaborate. The reputation-based incentives usually apply reputation values to regulate node behaviours. For example, setting reputation thresholds can motivate the nodes to behave cooperatively for keeping their reputation values at a high level.

Credit based approaches provide incentives by paying the cooperative users certain amount of credit or virtual money. Such approaches could be the most promising due to their explicit and flexible incentive methods; nevertheless, most credit-based incentive schemes either rely on a central trusted authority (that do not exist in P2P applications) or do not give an explicit digital currency system that is provably secure, leading to possible system collapses.

Both the credit-based incentive and the reputation-based incentive manage the relationships among system entities with trust. However, reputation stands for the comprehensive trust of a group in an individual, while credit emphasizes the subjective dependence of a trustor on a trustee. A large number of studies apply these two incentive mechanisms to prevent collusion between untrusted individuals.

The gamified incentive takes advantage of entities' psychological tendency to play games, provides the entities with a pleasant emotional experience in the process of completing system tasks, actively guides entities to behave as system design. In other words, gamified incentives employ the psychological factors of nodes to guide node behaviours. Gamified incentives provide nodes with a sense of accomplishment instead of real benefits such as money and reputation. Common gamified incentive mechanisms use points and badges as incentives.

Incentive Goals

Incentive mechanisms can be classified based on incentive goals. The incentive mechanisms can encourage nodes to participate in maintaining the safety and sustainability of a blockchain system. They can also prevent various attacks and mitigate blockchain weaknesses to make the system work in a normal and expected way. Therefore, incentive mechanisms play a crucial role in the blockchain system. Generally, there are two main types of incentive goals: incentive for system participation and incentive for cooperation with other nodes.

Participation. Blockchain requires the participation of a plethora of nodes to ensure security and decentralization. Existing system design naively holds an assumption that the nodes will actively participate as expected. However, the nodes are rational and profit-driven in practice, therefore, they need incentives to participate. The participation incentives is further classified

into Blockchain 1.0 and 2.0 according to the functions of system nodes. Specifically, the incentives for mining blocks, broadcasting blocks, sending historical blocks, and executing contracts. When discussing the incentive mechanisms in Blockchain 3.0 and blockchain-based incentive mechanisms, it refers to the participation incentives to participation in specific application scenarios.

Cooperation. Another immature assumption of existing blockchain systems is that all system nodes will strictly perform as system design. In practice, the profit-driven nodes will maximize their profits through various selfish or malicious behaviours, such as violating the system design and exploiting vulnerabilities for attacking the system. These behaviours could cause short-term or long-term threats to the system and harm the profits of other system nodes. To overcome this problem, one can introduce an incentive mechanism into the system to encourage node cooperation. Specifically, the cooperation includes two types of behaviours: strictly executing the system protocols and discouraging from initiating attacks.

Ethereum Incentive Model

Vitalik Buterin, the creator of ethereum, said that, not only do incentives play a key role in securing the blockchain, they are also the reason bitcoin soared to success when decades of previous attempts at peer-to-peer currency failed.

The rewards and punishment mechanisms in a distributed system is vital for industry players to ensure network security and incentivize participants to act in a way that benefits the entire system. Ethereum's model to network security serves as a prime example of the importance of cryptoeconomics, with its high nominal and real yields ranking among the top of major smart contract Layer 1s.

All actions on the Ethereum blockchain have gas fees. Fees make sure that all transactions are intentionally initiated and that smart contract code is safe, also we avoid infinite loops of computational wastage in code. Gas points specify the fees in standard values. They allow for independent cryptocurrency valuation and computation of transaction and computational fees. Just like fiat currency in stock markets, cryptocurrency also has market highs and lows. This however does not apply to gas fees; gas points don't change with the financial markets.

Operations on the blockchain such as loading from memory, storing to memory, transaction base fee, and creation of contracts all have varying gas costs. It is a fee structure. If fees specified in the fee structure are not met by a transaction, the transaction is rejected. This can be compared to sending a text without sufficient airtime. The text will not be delivered because of insufficient funds.

Ethereum Fee Schedule

APPENDIX G. FEE SCHEDULE

The fee schedule G is a tuple of 31 scalar values corresponding to the relative costs, in gas, of a number of abstract operations that a transaction may effect.

Name	Value	Description*
G_{zero}	0	Nothing paid for operations of the set W_{zero}.
G_{base}	2	Amount of gas to pay for operations of the set W_{base}.
$G_{verylow}$	3	Amount of gas to pay for operations of the set $W_{verylow}$.
G_{low}	5	Amount of gas to pay for operations of the set W_{low}.
G_{mid}	8	Amount of gas to pay for operations of the set W_{mid}.
G_{high}	10	Amount of gas to pay for operations of the set W_{high}.
$G_{extcode}$	700	Amount of gas to pay for an EXTCODESIZE operation.
$G_{extcodehash}$	700	Amount of gas to pay for an EXTCODEHASH operation.
$G_{balance}$	700	Amount of gas to pay for a BALANCE operation.
G_{sload}	800	Paid for a SLOAD operation.
$G_{jumpdest}$	1	Paid for a JUMPDEST operation.
G_{sset}	20000	Paid for an SSTORE operation when the storage value is set to non-zero from zero.
G_{sreset}	5000	Paid for an SSTORE operation when the storage value's zeroness remains unchanged or is set to zero.
R_{sclear}	15000	Refund given (added into refund counter) when the storage value is set to zero from non-zero.
$R_{selfdestruct}$	24000	Refund given (added into refund counter) for self-destructing an account.
$G_{selfdestruct}$	5000	Amount of gas to pay for a SELFDESTRUCT operation.
G_{create}	32000	Paid for a CREATE operation.
$G_{codedeposit}$	200	Paid per byte for a CREATE operation to succeed in placing code into state.
G_{call}	700	Paid for a CALL operation.
$G_{callvalue}$	9000	Paid for a non-zero value transfer as part of the CALL operation.
$G_{callstipend}$	2300	A stipend for the called contract subtracted from $G_{callvalue}$ for a non-zero value transfer.
$G_{newaccount}$	25000	Paid for a CALL or SELFDESTRUCT operation which creates an account.
G_{exp}	10	Partial payment for an EXP operation.
$G_{expbyte}$	50	Partial payment when multiplied by $\lceil \log_{256}(exponent) \rceil$ for the EXP operation.
G_{memory}	3	Paid for every additional word when expanding memory.
G_{txcreate}	32000	Paid by all contract-creating transactions after the *Homestead* transition.
$G_{txdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{txdatanonzero}$	68	Paid for every non-zero byte of data or code for a transaction.
$G_{transaction}$	21000	Paid for every transaction.
G_{log}	375	Partial payment for a LOG operation.
G_{logdata}	8	Paid for each byte in a LOG operation's data.
G_{logtopic}	375	Paid for each topic of a LOG operation.
G_{sha3}	30	Paid for each SHA3 operation.
$G_{sha3word}$	6	Paid for each word (rounded up) for input data to a SHA3 operation.
G_{copy}	3	Partial payment for *COPY operations, multiplied by words copied, rounded up.
$G_{blockhash}$	20	Payment for BLOCKHASH operation.
$G_{quaddivisor}$	20	The quadratic coefficient of the input sizes of the exponentiation-over-modulo precompiled contract.

Ethereum Improvement Proposal 1559 Incentive Model

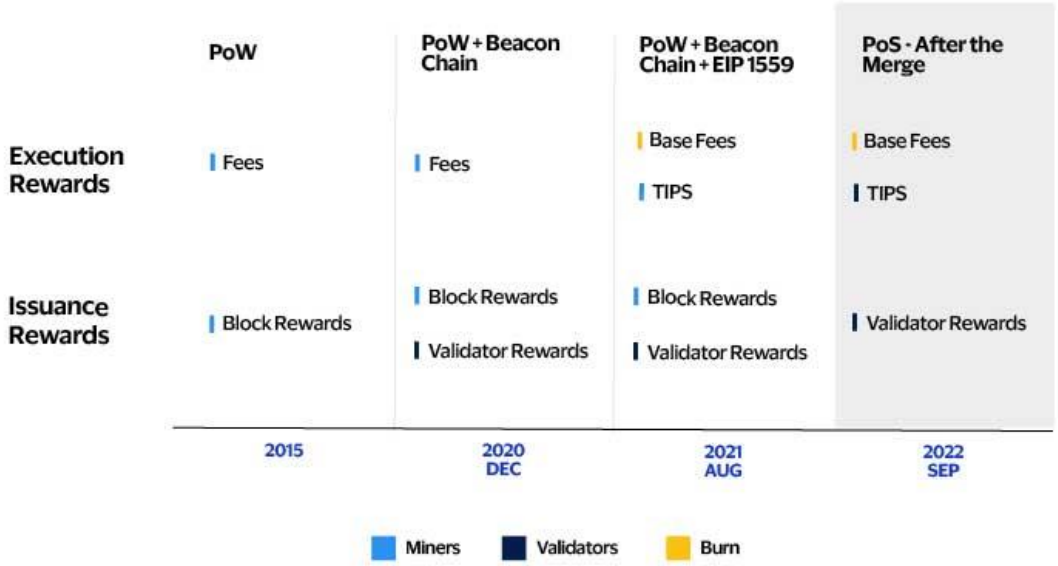
The Ethereum network has undergone significant changes in recent years, including the introduction of the EIP (Ethereum Improvement Proposal) 1559 via the London Hard Fork in August 2021. This proposal has drastically altered the Ethereum network's fee model and how it rewards network participants. The EIP 1559 fee model incentivizes network validators and regulates network traffic to help ensure that the Ethereum network functions efficiently. This event, the London Hard Fork, resulted in the network charging two types of fees: the base fee, which would be burned and be used to regulate the circulating supply of ETH, and the tip, which would incentivize network validators.

As we know that the process of executing transactions on the Ethereum network requires a gas fee. Gas is a measurement unit that quantifies the total computational effort an operation will require. For example, a money transfer is a simple operation that will generally require less gas than a DeFi-lending transaction that involves more complicated code execution. The transaction fee depends on the amount of gas needed for the computation and the unit cost of gas, which is a dynamic value in gwei (1 billion gwei = 1 ETH). The unit cost is based on two variables: the base fee and the tip. The base fee is dynamically determined by the size of the

last processed block to regulate the network traffic. This means if the previous block is larger than the target block size (15M gas), the network is busy, causing the base fee to increase. If the previous block is smaller than average, the opposite will happen. In other words, at times of network congestion, the base fee will be high and continue to rise until the congestion is relieved. The tip, on the other hand, is set by the user initiating the transaction and serves as a priority fee. Transactions with higher tips are processed before those with lower tips, giving users the ability to prioritize their transactions. The formula below explains the EIP 1559 fee model in simple terms.

EIP 1559 fee model: [Gas fee (in gwei) = Gas units × (Base fee + Priority fee)]

Overall, the EIP 1559 fee model provides a new mechanism for incentivizing network participants and regulating network traffic. The reduction of network rewards following The Merge (15th September 2022), combined with the introduction of this new fee model, results in a dynamic reward system.



Before The Merge, miners and validators were incentivized to earn around 13,000 ETH and 1,700 ETH per day, respectively. Post the Merge, block rewards and transaction tips are now directed to the validators; miners no longer need to be paid with new ETH. This reduces the rate of new ETH minted by almost 87 percent. When network activity increases, the ETH burn rate surpasses the issuance rewards that validators are paid. In such cases, the network data suggests that ETH issuance becomes negative, resulting in a deflation of ETH-circulating supply. These types of scenarios are common after The Merge because a threshold base fee of 16 to 18 gwei is sufficient for ETH to become deflationary, given the current number of validators.

Ethereum Rewards and Penalties

Ethereum incentivizes validators with rewards. To participate in Ethereum validation, node operators must first deposit ETH into a smart contract. They are then rewarded for running client software that verifies the validity of newly created blocks through the peer-to-peer (P2P) network. At a high level, validators are motivated by two types of rewards:

1. Issuance rewards that come from the consensus layer for performing tasks such as proposing the next block and attestations
2. Execution rewards, which come from the execution layer for processing and adding the blocks of transactions

Issuance rewards

Issuance rewards in the Ethereum network are a crucial part of the staking mechanism and incentivize validators to participate and maintain network security. These rewards are predictable, however, as the level of staked ETH increases, the rewards will decrease accordingly. The rewards are distributed to validators every 6.4 minutes, which is known as an epoch. The rewards that validators receive are multiplied by the "base reward," which acts as the foundation for all other rewards calculations. The "base reward" is determined by the validator's "effective balance" and represents the average reward that a validator can expect to receive under optimal conditions per epoch. The "effective balance" is a calculated value based on the current balance and is used to determine the size of the rewards or penalties a validator may receive. The "effective balance" can never exceed 32 ETH.

Proposal rewards

Proposers are randomly chosen validators who are compensated for proposing the Ethereum network's next block. Once chosen, the validator must produce a block for that slot (a slot lasts 12 seconds; there are 32 slots in an epoch). The other validators' beacon chain attestations are accumulated in the block, and the block producer is compensated with a portion of the inclusion rewards from the block's attestations. The block producer is awarded one-eighth of the inclusion reward, while validators whose attestations are included in the block are awarded seven-eighths.

Sync committee rewards

The sync committee is a group of validators on the Ethereum network who are responsible for ensuring the beacon chain's integrity and security. These validators are in charge of signing the header of each beacon chain slot, which is an essential facet of the consensus process. The sync committee is made up of 512 validators and rotates infrequently — every 256 epochs, or roughly every 27 hours — to ensure that light clients can identify sync committee members without having to keep the entire beacon chain state. A random selection of validators determine the membership of the sync committee, like that of the block proposals, for each period of 256 epochs. By participating in the sync committee, these validators are able to earn rewards for their work in securing the network.

Attestation rewards

Most validator rewards come from making attestations. Validators who vote (attest) on the current head of the chain and on checkpoints earn rewards. Attestations play a crucial role in establishing the finality of the blockchain, meaning that once the validators have attested to a checkpoint in an epoch, the prior transactions cannot be removed or altered. In the attestation process, every active validator is selected to make exactly one attestation per epoch. This means that the attestation rewards are the most frequent type of reward and contribute significantly to the overall yield of validators.

Execution rewards

Execution rewards are given to validators for executing transactions and performing related tasks in the Ethereum network's execution layer. These rewards differ from issuance rewards as they are highly variable and depend on the level of activity on the blockchain and the demand for blockspace. Unlike issuance rewards, which are largely dependent on the blockchain's staking level, execution rewards are purely dynamic and subject to external factors and opportunities.

1. **Tips - Priority fees**

As discussed, the implementation of EIP 1559 has helped lead to the full burn of base fees and the introduction of tips as a source of income for validators. A tip is an additional fee paid by users to fast-track their transaction and have it confirmed before others. This fee serves as an economic incentive for validators to prioritize the given transaction and include it in the next block. By paying a tip, users can ensure that their transaction is processed in a timely manner, which can be especially important in cases where speed is a priority.

2. **MEV**

MEV refers to the maximum amount of value that validators can extract from producing blocks through specific techniques such as front-running, back-running, decentralized exchange arbitrage, liquidations, sandwich attacks and NFT (Non-Fungible Token) MEV. This value is created by manipulating the order of transactions and fees, beyond the standard block rewards and gas fees. Independent network participants known as "searchers" are responsible for extracting a significant portion of MEV. Validators can also receive a share of MEV as

searchers offer high gas fees in exchange for a higher likelihood that their profitable transactions will be included in a block.

Only validators who are running what is known as "MEV boost" client software can access MEV rewards. MEV boost is an optional service for Ethereum PoS validators that allows them to increase their APR (annual percentage return) by outsourcing their block production duties to the highest bidder. When setting up MEV boost, validators can choose from which relays to accept blocks. Currently, there are 10 major MEV boost relays, including Flashbots, Ultrasound, BlockNative, Manifold and Eden.

Penalties

It is also crucial to understand the repercussions of acting maliciously or deviating from protocol regulations in the Ethereum network, which can compromise the security of the blockchain and its finalization. To uphold network safety and stability, Ethereum has implemented various disciplinary measures, including slashing, inactivity leaks and penalties, to reprimand validators who partake in such harmful or non-conformant behavior. Incentivizing validators on the Ethereum is similar to a double-edged sword. On one hand, validators are offered a prize for safeguarding the network, but on the other, they face consequences for falling short of their responsibilities. This carrot-and-stick approach encourages validators to strive for responsible and secure participation in the network.

- Slashing involves removing a portion of a validator's staked ETH as punishment for violating protocol regulations, such as submitting conflicting attestations for the same checkpoint or proposing two conflicting blocks at the same height. This can result in substantial losses and expulsion from the protocol.
- Inactivity leaks, on the other hand, are a mechanism that gradually decreases the staked ETH of inactive validators, encouraging them to remain active and participate in the network. This is designed to restore finality in the event that a large number of validators permanently fail.
- Penalties also apply to validators who fail to meet their obligations, such as their attestation duties. These penalties result in small amounts of stake being lost and are implemented to align the incentives of all participants toward maintaining the network's security and integrity.

Liquid Staking Derivatives and Staking Model for Ethereum

Liquid staking is a method that enables users to stake their assets without locking them up, offering improved capital efficiency and liquidity. In the context of Ethereum, liquid staking derivatives are synthetic assets that mirror the value of staked ETH, providing more flexibility than regular staking methods. In addition to the various rewards that validators can derive from consensus and execution tasks, there has been a growing interest in liquid staking derivatives for ETH in recent times. Regular staking typically requires a validator to lock up a minimum quantity of tokens (32 ETH in the case of Ethereum), which can be a barrier to entry for smaller participants who may not have the minimum number of tokens required. Operating a validator also requires technical knowledge to ensure smooth system operation and prevent the

possibility of slashing. Additionally, with Ethereum, ETH tokens deposited directly to the staking contract were locked up until the Shapella Upgrade, which was finalized on 12th April 2023. Liquid staking helps unlock greater capital efficiency on staked ETH, improve accessibility to staking participation by allowing users to stake less than 32 ETH, and enable users to avoid lockups in favour of a more liquid version of ETH. Due to the capital efficiency provided by liquid staking derivatives, Ethereum's staking ratio has increased, with 18.1 million ETH staked on the beacon chain, accounting for 15.6% percent of the total ETH supply as of April 3rd, 2023.

Considering the current network demands, staking returns on Ethereum can be expected to be between four and six percent on average. In the near term, these returns can rise above 10 percent and reach the low teens if there is a high demand for block space. This is because when demand for block space is high, validators can earn higher rewards for including transactions in a block. However, as withdrawals are enabled and more market participants seek to stake their ETH, this will result in a lower staking yield as the rewards are distributed among more validators in the long run.

Summing Up

Key points about Ethereum (PoS)

- Energy efficient compared to Proof of Work
- Requires staking 32 ETH to become a validator
- Addresses "nothing at stake" and long-range attack vulnerabilities
- Offers new earnings potential from staking rewards & fees
- Risks wealth inequality if only large holders can participate
- May increase centralization with few large staking pools
- Penalizes malicious actions to align incentives
- Requires extensive real-world testing to optimize

In conclusion, the Casper transition brings profound possibilities along with risks that require mitigation. Crafting the right incentives around staking, decentralization, honesty, and equitable access will determine whether it fulfils Ethereum's aspirations for the future. The community must collaborate closely to ensure Casper strikes the right balance. And they must continue iterating even after launch. If done thoughtfully, Casper can open the door to mass blockchain adoption.

Understanding the incentives and punishment mechanisms in a distributed system, is vital for industry players to ensure network security and incentivize participants to act in a way that benefits the entire system. Ethereum’s model to network security, with its high nominal and real yields ranking among the top of major smart contract Layer 1s.

References:

https://usa.visa.com/solutions/crypto/consensus-mechanisms.html

https://ethereum.org/da/developers/docs/consensus-mechanisms/pos/

usa.visa.com/solutions/crypto/cryptoeconomics.html