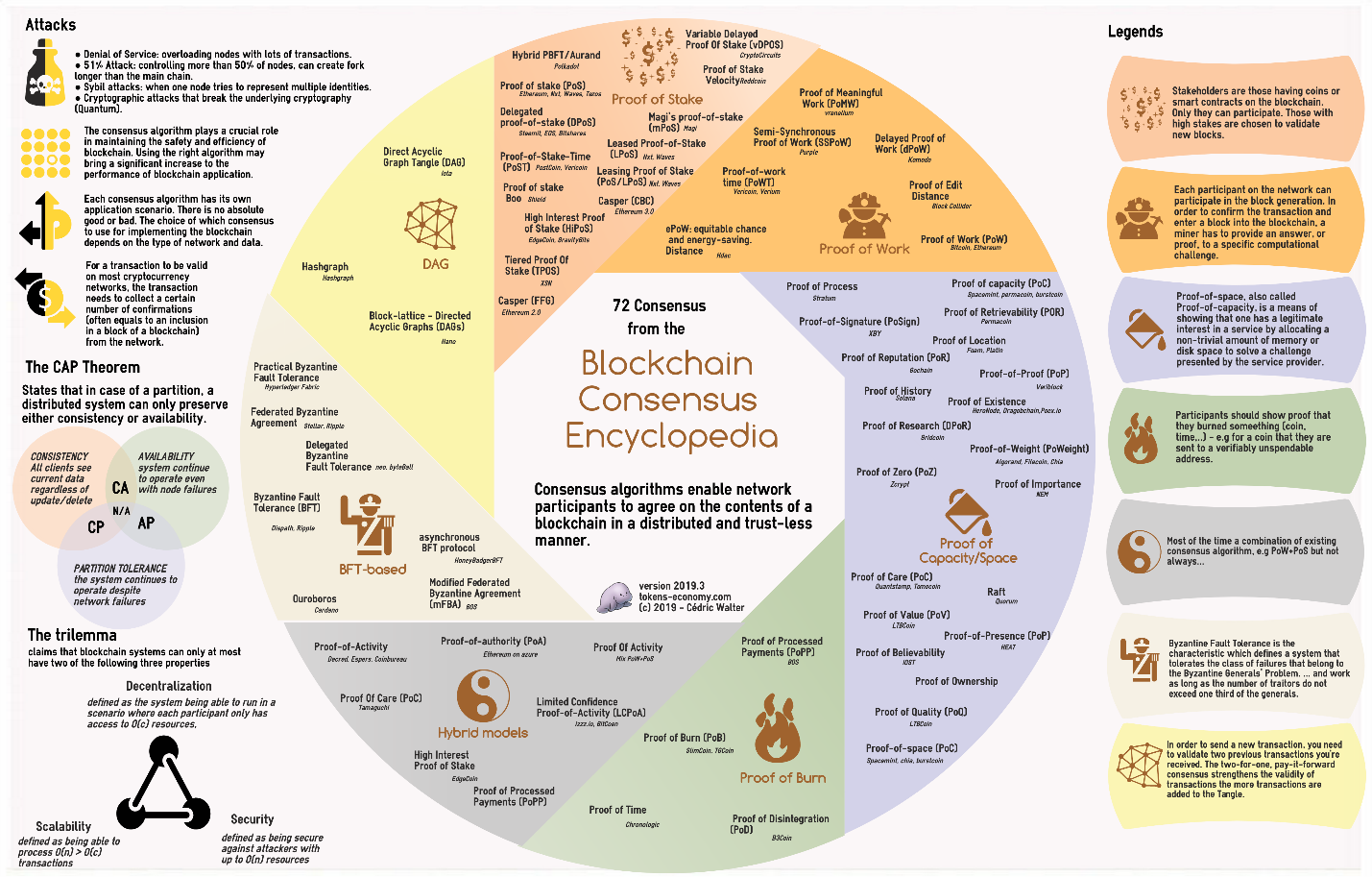
Consensus



Chain-based Proof-of-Work

PoW was originally invented as a means to combat spam (see hashcash) if you make it computationally expensive to send email then spamming would be cost prohibitive while still being almost free for a normal user to send email.

Bitcoin, which made the blockchain technology popular, developed the so-called Proof of Work (PoW) algorithm. In principle, each participant on the Bitcoin network can participate in the block generation. In order to confirm the transaction and enter a block into the blockchain, a miner has to provide an answer, or a proof, to a specific challenge. Miners use PoW to validate transactions and mining new coins, but its main goal is to block potential cyber-attacks or suspicious activities within the network.

Miner

In cryptocurrency networks, “miners” are special nodes that perform the PoW calculation on a set of transactions plus the hash of the previous block to generate the next block in the blockchain. Since the block contains the hash of the previous block, changing a historical block would require regenerating all of the subsequent blocks. Regenerating all the hashes would be computationally intensive – tính toán chuyên sâu and would require a lot of energy – and energy isn’t free. It would also be time consuming. The process of proving work and generating blocks is called ”mining”. Miners are rewarded for this work with newly minted coins adding to the total supply.

Nodes

Nakamoto consensus to determine the next head block; that is, at its core: "Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously- đồng thời, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one."

Algorithm

1. Transactions are bundled together in form of blocks.

2. Miners verify the transactions within the blocks as legitimate.

3. Miners then solve a mathematical problem known as the proof-of-work problem.

4. A reward is then given to the first person to solve the problem.

5. Verified transactions are stored in the public blockchain

Attacks

With a PoW coin the miners don't need to own an investment in the coin that they are attacking, so there might be an incentive for them to run a 51% attack.

Pros

Oldest and safest

Transaction fees not mandatory

Easy to verify solutions

Difficulty of finding solutions can be precisely quantified

Provably inseparable from the block it secures

Cons

Poor performance

PoW uses an enormous amount of computing power, which, in itself lowers incentive

It is also vulnerable to attack, as a potential attacker would only need to have 51% of the mining resources (hashrate) to control a network, although this is not easy to do.

Reducing block rewards

Proof of Work restricts the inputs to the structure of given blockchains mining algorithm. In Bitcoin’s case this would have to be a nonce, and in Ethereum’s case the input must be a random integer, a nonce, and a seed hash of the block.

Proof of Meaningful Work (PoMW)

While the basic idea, to protect the Blockchain by proving that a certain amount of computation was invested to create every single block, is worth being preserved, the current implementation, using purely artificial computational tasks (hashing), with the sole goal of burning “enough” energy, is much too wasteful to be used productively and scales very badly. Proof of Meaningful Work keep the good idea, but implement it using meaningful computation tasks, so that the energy invested in the proof of the miners’ computational strength is used for calculations that support public scientific research projects

Pros

Decrease wasted energy. The needed energy will be used for socially responsible projects in the fields of healthcare, science, ecological – sinh thái protection and more

Cons

attack of more than 50% of the total computing power.

**Hybrid Proof of Work (HPoW)**

HPoW still uses PoW but modifies it so it isn’t profitable and, as a result, creates an entire cryptocurrency network that can run on energy efficient, easy to set-up, low-cost computers or cloud services. HPoW removes the profit incentive – khuyến khích for miners because the mining reward is so low. In fact, mining farms would actually lose money if they tried to mine Lynx, meaning they will leave Lynx to the individuals who want to solve the sustainability – sự bền vững problem. This takes control away from mining farms and pools and puts it squarely into the hands of individuals (solo miners) who want to build upon and use Lynx. HPoW supports network maintenance by incentivizing – khuyến khích and empowering those who want to use Lynx. With every new solo miner that connects, the network becomes more secure by reducing the risks associated with a centralized and hierarchical cryptocurrency network. This security is achieved through redundancy: the more individual nodes on the network, the stronger the network becomes. If an individual node or miner fails, or if an entire region of nodes fail due to widespread power outages or war, the network is still secure because mining rigs are plentiful.

Taken together, the three business rules result in “Hybrid Proof of Work” (HPoW) 1. A single miner can’t win a block more than once every 30 minutes. 2. The miner’s reward address balance must be greater than or equal to a required fluctuating minimum amount of Lynx to win a block. 3. By using random selection, the fastest miners are not always guaranteed to win the block reward.

**Proof of Work time (PoWT)**

Proof-of-Work-Time (PoWT) is a novel approach to forming a consensus by introducing a variable blocktime that scales with mining power, where the blockchain speeds up with power increases. This better scales the blockchain, increases transaction speed with power and allows for auto-adjusting more profitable mining. Difficulty dependent blocktime (Max ~6.2 minutes, minimum 15 seconds).

**Delayed Proof of Work (dPoW)**

Delayed Proof of Work (dPoW) is a hybrid consensus method that allows one blockchain to take advantage of the security provided through the hashing power of a secondary blockchain. This is achieved through a group of notary nodes that add data from the first blockchain onto the second, which would then require both blockchains to be compromised – bị tổn hại to undermine the security of the first.

**Proof of Edit Distance**

Algorithm

Edit distances are a class of algorithms that score how close two strings are to each other. For instance the *an Edit Distance* for “ETH” and “ETC” is “0.8222” where two identical strings would score a “1”. There are many algorithms also in the string similarity space including the *Levenshtein Distance*, *Smith-Waterman Gotoh* *Distance,* and the *Ratcliff-Obershelp Distance.*

Using Proof of Edit distance for forging new blocks

Miners compete to find a string that when hashed in a normalization process is above a minimum distance threshold. This string could then be the hash of an intermediary-blockchain and the header hash for the next block.

Let Minimum Distance Threshold by “t”, String to find “B”, and Edit Distance Function “ED”. Such that for each blockchain header hash “h” satisfies:

ED( H(h), H(B) ) < t

Or in the case of merging two blockchains:

ED(H(h1),H(B)) < t && ED(H(h2),H(B)) < t === true

To find the new block in an intermediary-blockchain, the miner would iterate- lặp lại through a random charset or number, hashing strings until it finds a hash that is above the threshold for all of the blocks.

Pros

Any hash or string structure can be provided as an input which means that as long as the blockchain has unique hashes it can be easily added to the Proof of Edit challenge.

**ePoW: equitable chance and energy-saving.**

Hdac uses ePoW as a consensus algorithm for creating new blocks and connecting them to the blockchain. ePoW refers to “PoW based on equitable – tương đồng chance and energy-saving.” The Hdac algorithm considers these two as its basic philosophy.

The ePoW consensus algorithm can reduce the number of nodes participating in PoW and motivates the participation of multiple mining nodes. As a result, we intend to prevent energy waste due to excessive hashing power for mining competition and distribute equitable mining opportunities. reduces the mining monopoly by applying the block window concept. It reduces the wasteful energy consumed in the hash calculation by avoiding spontaneous – tự phát mining attempts during the block window application period once the mining is successful. If a node succeeds in mining, no new block can be mined during the block window application period. Even if a greedy node neglects - bỏ mặc this mechanism and succeeds in mining a new block, it will not be recognized as a valid block in the entire Hdac blockchain network, thus eliminating the need to try to find an invalid block.

The block hash must satisfy the data specification according to the degree of difficulty and should not be within a given block window (time spacing). This block window size can be expressed in the form of a time function, Ws = f(t). “F(t)” is a function that increases in proportion – tỉ lệ to time, and therefore the window size gradually increases with time. This means that there is a great opportunity for early participants, and over time, it becomes increasingly difficult for certain mining nodes to monopolize – độc quyền mining and more equitable distribution can be achieved.

The ePoW block window is a system that gives certain constraints – hạn chế on mining attempts after succeeding in mining in a certain PoW cycle. The block window size (Ws) is defined as, f(t) = [(N\*0.7) x (cumulative number of blocks currently (t))] / (cumulative block number for 10 years (tm)), and the node factor (N) is calculated from the list of recent successful mining nodes. The reason for the arrival time of the maximum block window size (Wm) being 10 years is because it is set to reach the point of more than 80% of the total block generation by that time.

**Semi-Synchronous Proof of Work (SSPoW)**

The consensus algorithm of Purple is called Semi-Synchronous Proof of Work, or SSPoW for short. It is a variation of Satoshi’s original Proof of Work model of consensus It’s design is to remove the bottleneck that the Proof of Work algorithm imposes - áp đặt on the transaction throughput of the network. This is done by decoupling – tách ra the choosing of validator nodes, which is done via Proof of Work from the actual transaction validation process. When a node finds a valid Proof of Work, it is advanced into the validator pool where it has an allocated period in which it can validate transactions. This is done asynchronously – không đồng bộ while the choice of validator nodes (PoW) is synchronous – đồng bộ . In this way, the consensus mechanism becomes semi- synchronous, greatly increasing the throughput of the network while providing a safety control mechanism which can be adjusted based on the current network conditions. The algorithm works by establishing a byzantine partial causal ordering on the network events that are sent between the validator nodes and by transforming it into a total order which is assured – yên tâm to be consistent – thích hợp as long as less than a third of the validators are either byzantine or unresponsive. However, the Total Ordering Algorithms assume that the communication medium between the nodes is reliable so it falls on the CA side of the CAP spectrum. Another step must be included in the algorithm in order to provide partition – vách ngăn tolerance – sức chịu đựng. Another step must be included in the algorithm in order to provide partition tolerance. Validator pool Transactions are validated by nodes that are in the validator pool. In order to participate in the validation process, nodes have to issue network events, in a deterministic order. A network event issued by a node contains pending transactions which the node wishes to include in the ledger. When nodes join the pool, they are placed on a circle which is represented by the interval [0, 1). Each validator in the pool owns a share of this circle which is represented by a sub-interval of [0, 1). The order in which the nodes are placed on the circle determines the order in which they are required to issue events. The node owning the lowest share of the interval is always required to be the first to issue an event. When a node joins the pool, the node with the largest share must give half of their share to the joining node. If a node leaves the pool, a node is deterministically chosen to receive the leaver’s share. Pending transactions are deterministically partitioned – phân vùng among all current validators in order to prevent two nodes from validating the same transaction. A validator node receives the transaction fees of all the transactions that it has processed as reward if it isn’t found to be byzantine or crashed.