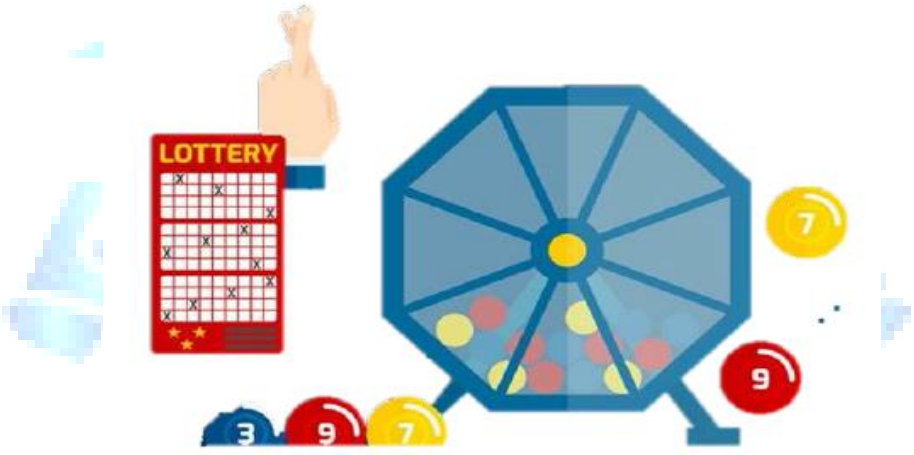
Proof of Elapsed Time

Introduction

- In this series of covering **consensus mechanisms** used by blockchain networks, today, we picked up Proof of Elapsed time (PoET). It is the algorithm behind Hyperledger permissioned blockchain network for businesses.
- details of the PoET algorithm along with its functioning. It also covers the difference between Proof of Work and Proof of Elapsed Time.

What is Proof of Elapsed Time (PoET)?

- PoET is a consensus algorithm used in a permissioned blockchain network to decide mining rights and next block miner. FYI, a permissioned blockchain network requires participants to prove their identity, whether they are allowed to join. Hence, it needs permission (or invitation) to join the decentralized network as a new participant (or node).
- The PoET algorithm was developed by Intel Corporation, the processor chip giant, in early 2016. Intel associated with Linux Foundation in the development of Hyperledger Sawtooth. They aimed to build a highly scalable private blockchain network.
- Intel introduced PoET as a time-lottery-based consensus algorithm secured by cryptography. The concept basically motivates the idealogy of giving equal chances of getting a reward like a lottery.



PoET Mechanism assigns an amount of time to each node in the network randomly. The node must sleep or do another task for that random wait time. Whichever node gets the

shortest waiting time wakes up and add their block to the network. Later, the new update information floods among other network participants.

The Proof of Elapsed time in blockchain needs to ensure 3 significant factors for this process to work:

- Ensure that the node or network participant **gets the random waiting time** indeed.
- Check if they are **not choosing the shortest waiting time on purpose**.
- Verify if the node has **completed the given waiting time** or not.

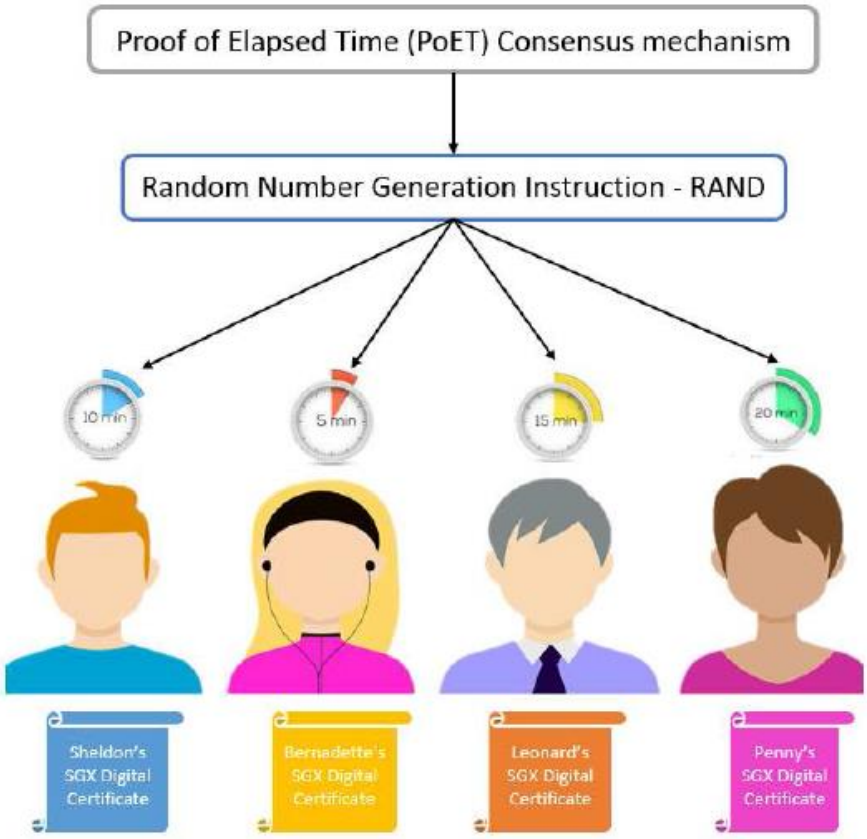
Let's dig a bit deeper into working on the Proof of Elapsed Time mechanism.

How does the Proof of Elapsed Time (PoET) Algorithm work?

- The **time-lottery concept allows everyone in the network an equal chance of winning** the reward and being able to forge a new block to the network. The **PoET controller** maintains a stopwatch for each participating node. It ensures their waiting time ended, and now they can forge a new block. When the node wakes up, it submits the block and a cryptographic test to the PoET controller for verification.
- A newly proposed block selects if the controller approves the newly proposed block by the first woken up node. Else it gets discarded. And then, the selection process of assigning waiting time starts again.

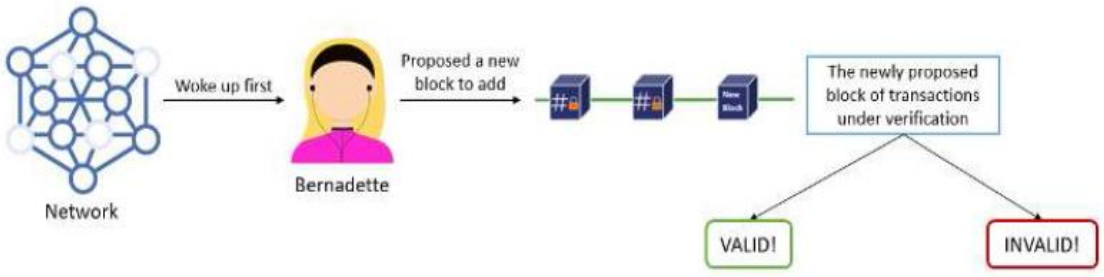
Selection Process

- First, each participating node has to share its certificate by Intel Software Guard Extension (SGX), which ensures its validity to generate a new block in the network. After that, they are eligible to get a timer object.
- The numbers assigned to each node as a timer object (waiting countdown time) by Intel's random number generation instruction, RAND. It generates difficult to detect random numbers.
- Now, the time object given to each participating node activates.



Generation Process

- After the time object ends and the node wakes up, it's eligible to forge a new block to the network.
- The active node generates the hash (using a hash function like SHA-256) of its block of transactions and submits it for acceptance. It doesn't require showing computation work done by the node.
- Afterward, the update gets flooded to the network.



Therefore ends the iteration of mining a new block in a permissioned blockchain network using the PoET consensus mechanism.

Proof of Work (PoW) VS Proof of Elapsed Time (PoET)

- Proof of Work (PoW) **demands computation work** from nodes (or miners) to become eligible for adding a new block. On the other hand, **PoET randomly selects** the among participating nodes by distributing waiting time objects. Here, each node is equally eligible to mine a new block.
- PoET is way more time and **energy-efficient** than PoW. It is backed by one of the renowned technology giants, Intel corporation, which makes it more trusting and reliable.

Benefits of Proof of Elapsed Time (PoET)

Following are the advantages of the PoET consensus mechanism:

- PoET can go up to a million transactions per second.
- It is highly energy-efficient and easily scalable.
- It's a block generation consensus algorithm, unlike proof of stake (PoS).
- PoET is for privately controlled spaces like business organizations.
- It ensures the same opportunity for network participants with time object and activation.
- As it's a permissioned blockchain network, the process of selecting validators ensures network security against cyber-attacks.

Limitations of Proof of Elapsed Time (PoET)

Following are the disadvantages of the PoET consensus mechanism:

- PoET is a permissioned and closed network, unlike Bitcoin and Ethereum.
- The mechanism highly depends on tools by Intel technology which might raise compatibility issues with other tools later.
- In Conclusion

Proof of Burn (PoB) in Blockchain

Introduction

The Blockchain network uses a consensus mechanism to ensure that all participants agree to a new update on the network. Such as adding a new block of transactions to the network, deciding the network rights, etc. Therefore, to ensure the continuity of the network algorithm needs to be established.

What is Proof of Burn (PoB)?

- **In the Proof of Burn (PoB) algorithm, miners reach a consensus by burning the coins. It's a process in which crypto coins get permanently eliminated from regular circulation.** In such cases, the burning of coins mechanism is used to validate transactions. Hence, **the more coins a miner burns, the higher the chances of adding the block to the network.**
- In comparison to the proof of Work (PoW) system, **PoB reduces energy consumption**. Moreover, compared with proof of stake (PoS) systems, **PoB doesn't need miners to stake coins** to add a new block to the network.
- There are various versions of Proof of Burn in blockchain, with the most acknowledged version being **Iain Stewart**'s algorithm. He's also the inventor of the Proof of Burn consensus mechanism.
- Here, **the concept of "burning the coins" means investing the native coins in virtual mining rigs (mining powers)**. It allows miners with the most virtual mining rigs or a miner who invested the most coins – to add his new block of transactions to the network. Hence, the number of burnt coins shows miners' commitment to the network.

How does the PoB Algorithm work?

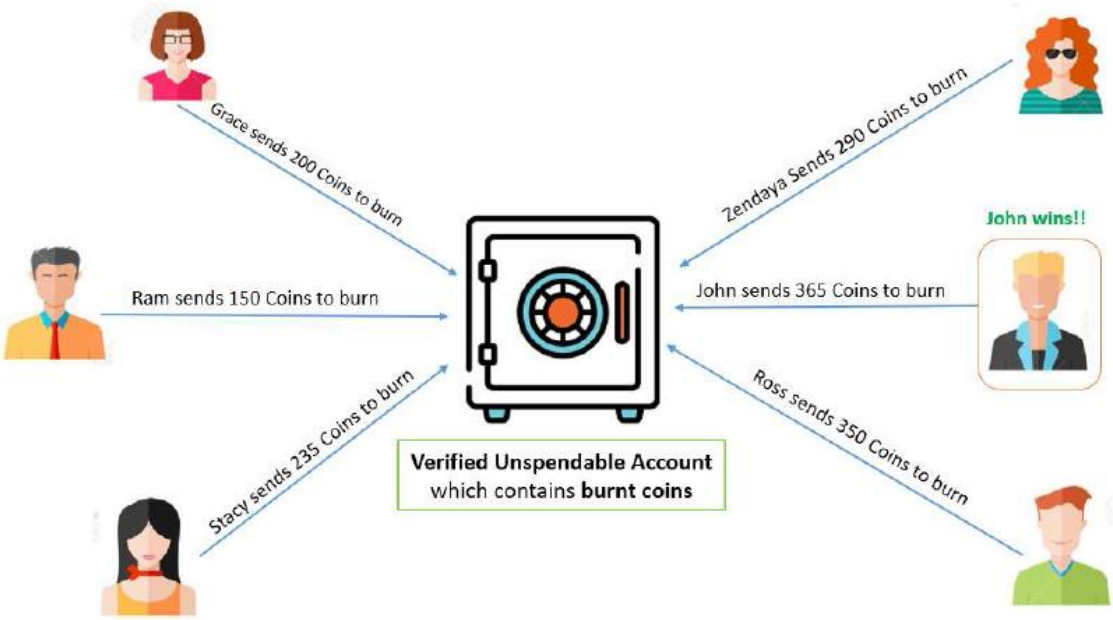
First, let's begin with how do the miners burn the coins?

Here, the miners transfer some amount of coins to an unspendable address or an escrow account. These publicly verified unspendable accounts are randomly created with no private keys associated. Once coins get received by burn address/accounts, it becomes useless and inaccessible. Eventually, the burnt coins in the account are used for strengthening the security of the network.

Let's take an example to understand the working of proof of Burn (PoB)?

We have 6 miners, each having their own block of transactions. As per the process, the miners have to burn some amount of coins to get an opportunity to add their block to the network.

See the below diagram. Each miner sends some of their coins to the burn address or unspendable escrow account.



John wins as he burns the maximum number of coins. Hence, he gets the chance to add his block of transactions to the network.

Moreover, the block added by John will be verified by other network validators. If the block is found invalid, then the second-highest (Ross) gets the chance to add a new block.

Wouldn't this approach be unfair for early adopters in the network?

Proof of Burn in blockchain promotes the **periodic burning of coins to avoid partiality among new and old network participants**. It means the virtual power of mining reduces each time a new block gets mined. Moreover, it motivates miners to make regular transactions instead of just one-time investments.

Now let's jump to the pros and cons of using the PoB approach.

Benefits of PoB

Following are the advantages of Proof of Burn in blockchain:

- Less power and energy consumption.
- Motivates miners to make regular transactions using cryptocurrency.

- PoB is more sustainable and doesn't need hardware for heavy computation.
- Used for long-term commitments

Limitations of PoB

Following are the disadvantages of Proof of Burn in blockchain:

- It's not an initial consensus algorithm. It requires a number of wealthy participants to burn their coins in the network.
- PoB has not been proven to be applied on massive networks.
- It takes more time to validate the block of transactions. Hence, a bit slower mechanism.