BLOCKCHAIN

Unit3: Class 4

Slide 4

- First, PoA was proposed by a group of developers in March 2017 (the term was coined by Gavin Wood) as a blockchain based on the Ethereum protocol. The term was proposed in 2017 by Ethereum co-founder and former CTO Gavin Wood.
- It was developed primarily as a solution to the problem of spam attacks on Ethereum's Ropsten test network. The new network was named Kovan and is a primary test network available to all Ethereum users today.
- Best suited for private, permissioned blockchains. PoA blockchains have a collaborative consensus algorithm. Transactions and blocks are validated by approved accounts, known as validator. The validator nodes run consensus software, allowing them to put transactions in blocks. The process is automated and does not require validators to be constantly monitoring their computers.
- Proof-of-Authority (PoA) assigns a set of trusted nodes (authorities) to process transactions and build new blocks. New blocks need to be signed by the majority of authorities.
- Great performance, fast transactions, high throughput
- This system is best used for test networks that are used to test applications before they are deployed on public networks.

Slide 4

- In PoA, rights to generate new blocks are awarded to nodes that have proven their authority to do so.
- These nodes are referred to as **"Validators"** and they run software allowing them to put transactions in blocks.
- Process is automated and does not require validators to be constantly monitoring their computers but does require maintaining the computer uncompromised.
- PoA is suited for both private networks and public networks, like POA Network, where trust is distributed.
- PoA consensus algorithm leverages value of identities, which means that block validators are not staking coins but their own reputation instead.
- PoA is secured by trust on the identities selected.

Slide 5
The conditions may vary from system to system, the PoA consensus algorithm is usually reliant upon:

- valid and trustworthy identities: validators need to confirm their real identities.
- difficulty to become a validator: a candidate must be willing to invest money and put his reputation at stake. A tough process reduces the risks of selecting questionable validators and incentivize a long-term commitment.
- a standard for validator approval: the method for selecting validators must be equal to all candidates.

Slide 6
Pros:

- High transaction rate.
- Far more sustainable than algorithms like Proof of Work which require computational power.
- High risk tolerance if 51% of the nodes are not acting maliciously.
- Interval of time at which new blocks are generated is predictable. For PoW and PoS consensuses, this time varies.

Cons:

- PoA is not decentralized but is just an effort to make centralized systems more efficient.
- PoA validators are visible to anyone. Knowing validators identities could potentially lead to third-party manipulation.

PoA is used by PoA Network, Ethererum Kovan test net and Vechain

Examples:

- POA Network – https://poa.network
- Ethereum Rinkeby Testnet – https://www.rinkeby.io

Slide 7

Proof of Elapsed Time (PoET)

- PoET is a competitive consensus algorithm that is often used by permissioned blockchain to decide mining rights on the system.
- permissioned blockchain requires any prospective participant to identify themselves before they can join.
- It was developed for sawtooth lake project on Hyperledger.
- It was built to run in a secure area of the central processor of Computer called a trusted execution environment (TEE)

Hyperledger Sawtooth

Proposed by Intel, as a part of Hyperledger Sawtooth – a blockchain platform for building distributed ledger applications

Slide 8

For this to work, two requirements must be verified.

- First, did the lottery winner actually choose a random wait time?
    - Otherwise, a participant could intentionally choose a short wait time in order to win.
- Second, did the lottery winner actually finish waiting the specified amount of time?

PoET over Trusted Environments

- How will one verify that the proposer has **really waited** for a **random amount of time**?
    - Utilize special CPU instruction set – *Intel Software Guard Extension* (SGX) – a trusted execution platform.
    - SGX allows applications to run *trusted code* in a protected environment. For PoET, the trusted code is what ensures that these two requirements are satisfied keeping the lottery fair**.**
    - The trusted code is private to the rest of the application
    - The specialized hardware provides an attestation that the trusted code has been set up correctly

Joining the network

- A new participant downloads the trusted code for the blockchain.
- On initialization, the trusted code creates a new keypair.
- Participant sends a SGX attestation (which includes the trusted code's public key) to the rest of the network as part of a *join* request.

Participating in the lottery

- Participant obtains a signed *timer* object from the trusted code.
- Participant waits for the time specified by the timer object.

  - Participant obtains a certificate (signed by the trusted code's private key) that the timer has completed. Participant sends this certificate to the rest of the network along with the new block for the blockchain.

- Lottery based system that randomly selects a node from pool of validating nodes. The probability of a node being selected increases in line with how much processing resource the node has contributed to that blockchain.
- PoET allows you to control cost of consensus process. It is great for internal projects or ones where all the participants are known. It can be used to build decentralized applications.
- PoET relies on a trusted execution environment (TEE)
- Supported by modern CPUs from Intel, AMD and ARM.
- No cryptographic puzzle (like in PoW algorithms).
- PoET ensures blocks get produced in a random lottery fashion.
- Generates securely the next block + a proof of the waiting time inside the TEE
- The proof of waiting time can be verified by all other nodes.
- Problem: a small subset of compromised nodes can compromise the entire system

Slide 9

  - The working of the POET algorithm is as follows.

Each participating node in the network is required to wait for a randomly chosen time period, and the first one to complete the designated waiting time wins the new block.

Each node in the blockchain network generates a random wait time and goes to sleep for that specified duration.

The one to wake up first – that is, the one with the shortest wait time – wakes up and commits a new block to the blockchain, broadcasting the necessary information to the whole peer network The same process then repeats for the discovery of the next block

Slide 10

How will one verify that the proposer has really waited for a random amount of time?

- The PoET algorithm is for **permissioned** blockchain networks.
- A special verification is required from a node when it tries to *join* the network.
- This verification is achieved using Intel's **Software Guard Extension (SGX)** technology which was first introduced in 2015.
- It creates an *attestation* for a piece of code and protects the code from external access.

Slide 11

Process

The network operates in the following way:

1. A node downloads the PoET code and generates an attestation (key) for the code using SGX.
2. The node forwards this key when requesting to join the network. The nodes that are already a part of the network verify this key.
3. The new node now has its own *timer object* which is initialized to a random value. This randomness is guaranteed by the code protection offered by SGX.
4. All nodes are initialized with a random time; the first one to expire gets to be the winner. This means that it creates a new block, attaches it to the current blockchain, and gets the reward. Then, the nodes are initialized again.

Slide 12

PoET is a substantial improvement in the efficiency of proof of work systems. Simultaneously, it also provides a great solution to the "Random Leader Selection Problem" without being resource intensive or requiring complex staking mechanics and incentive structures necessary with proof of stake consensus.

PoET is also an excellent consensus mechanism for permissioned networks, which is why it is the go-to consensus mechanism for Hyperledger Sawtooth. On top of that, it scales efficiently and can be used as a "plug and play" model for testing environments with Hyperledger Sawtooth.

Disadvantages

SGX is a lauded and innovative technology, but recent developments are clearly a cause for concern regarding its use with PoET consensus. Intel will likely be able to fix the issue regarding the critical vulnerability, but the disadvantage here is the obvious and necessary reliance on a specialized hardware's security.

Not only that, but SGX is manufactured entirely by Intel, so the reliance of the consensus model extends to Intel as a company, a third party. The notion of such a reliance runs against the new paradigm that cryptocurrencies are attempting to achieve with blockchain networks, removal of trust in intermediaries.

4.4 Pros

- Low cost of upkeen
- Scalable to operation

4.5 Cons

- Needs specialized hardware
- Must know participants in the network

- PoET is used by Hyperledger- sawtooth lake project.