BLOCKCHAIN

Unit3: Class 5

Slide 3

- **Proof of space** (**PoSpace**), also called **Proof-of-capacity** (**PoC**) or **Proof-of-storage**
- It is a means of showing that one has a legitimate interest in a service (such as sending an email) by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider.
- Like proof of work, except that instead of computation, storage is used.
- Proof of space is seen as a fairer and greener alternative due to the general-purpose nature of storage and the lower energy cost required by storage.
- Several theoretical and practical implementations of PoSpace have been released and discussed, such as SpaceMint and Burstcoin.

Slide 4

PoSpace in Cloud

- PoSpace is also being used in cloud storage technologies in which the peers contribute their free disk space and get service proportionately.
- Peers can also get paid if they let their free space to be used by peers that need more space.
- Eg: Storj is a PoSpace based cloud storage
- ***Explanation:*** **Proof-of-space** (**PoSpace**), also called **proof-of-capacity** (**PoC**), is a means of showing that one has a legitimate interest in a service (such as sending an email) by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider.
- The concept was formulated by Dziembowski *et al.* in 2015.
- Proofs of space are very similar to proofs of work, except that instead of computation, storage is used.
- Proof-of-space is related to, but also considerably different from, memory-hard functions and proofs of retrievability.
- A proof-of-space is a piece of data that a prover sends to a verifier to prove that the prover has reserved a certain amount of space.
- For practicality, the verification process needs to be efficient, namely, consumes a small amount of space and time.
- For soundness, it should be hard for the prover to pass the verification if it does not actually reserve the claimed amount of space.
- One way of implementing PoSpace is by using hard-to-pebble graphs.
- The verifier asks the prover to build a labeling of a hard-to-pebble graph.
- The prover commits to the labeling.

- The verifier then asks the prover to open several random locations in the commitment.
- Proofs of space are a fairer and greener alternative due to the general-purpose nature of storage and the lower energy cost required by storage.

Slide 5

Concept

- PoSpace is a piece of data that a prover sends to a verifier to prove that the prover has reserved a certain amount of space.
- Verification process needs to be efficient, namely, consume a small amount of space and time.
- It should be hard for the prover to pass the verification if it does not actually reserve the claimed amount of space.
- One way of implementing PoSpace is by using hard-to-pebble graphs.
- The verifier asks the prover to build a labeling of a hard-to-pebble graph.
- The prover commits to the labeling. The verifier then asks the prover to open several random locations in the commitment.
- Proof of Capacity and Proof of Space blockchains have collaborative consensus, where nodes that are securing transactions – these can be called 'farmers"- allocate a non-trivial amount of their memory or disk space.
- Almost anyone can become a "farmer" and this allows for greater decentralization of the network.

Slide 5 &6

PoC miners use a 2-step system

- Plotting
    - Plotting consists of creating a random solution, known as a plot, through the Shabal cryptographic algorithm and storing it on a miner's hard drive.
    - Plotting is the process of generating plot files, which are just files storing a large number of pre-computed hashes.
    - Each *plot* file contains one of more groups of 8192 hashes, these groups are called *nonces.*
    - A nonce is exactly 256KiB in size (8192 x 32 bytes per hash). Additionally, each nonce is divided into 4096 pairs of hashes, the pairs are referred to as *scoops*.
    - Each nonce can also be identified by its index number, ranging from 0 to 2^64.

- The plotting process takes the miner's burst address as an input, which ensures that plot files can only be used by a single miner.

- Mining
    - Once the plot files have been generated, the actual mining process can take place.
    - The miner will first fetch the relevant information from the wallet for the current block, this includes a 32 byte hash called the "generation signature" from the previous block, the block height (index of the current block), and something called the "base target" which is calculated based on the last 24 blocks and can be considered as the "difficulty level" of the block.
    - Mining consists of miners reaching the solution, and whoever reaches it first, gets to mine the next block.

5.1 Difference between PoW and PoSpace

- Instead of using your processing power to compete to secure the blockchain, you use your leftover memory.
- Farmers not fighting to secure blocks.

PoSpace is green and scalable consensus like PoS, but instead of needing to own and hold cryptocurrency, you can use resources you already have and are not currently using.

It is fairer and greener alternative to other blockchains. They can be used to build applications and transfer value.

Slide 7

Pros:

- *Similar to PoW but uses space instead of computation. Thus much environmental friendly.*
- *Can be used for malware detection, by determining whether the L1 cache of a processor is empty (e.g., has enough space to evaluate the PoSpace routine without cache misses) or contains a routine that resisted being evicted.*
- *Can be used for anti-spam measures and denial of service attack prevention.*

Cons:

- *Incentivization can be an issue.*

PoSpace and PoC are used by Burstcoin, Chia and SpaceMint

Slide 9

Proof of Burn (PoB)

- Most PoB systems have non competitive consensus algorithm. Transactions are validated by elected nodes.
- These nodes check to see if the fee has been paid. User pays the fee by burning some cryptocurrency.
- Burning means sending their cryptocurrency to an address where it can never be retrieved.
- With in the Factom blockchain this action grants the user the ability to publish a transaction.
- This transaction can be about anything and has been used to secure things land titles, birth records and data feeds on IoT devices.
- It was proposed as a more sustainable alternative to the PoW consensus algorithm.
- Essentially, Proof of Burn looks like a Proof of Work algorithm but with reduced rates of energy consumption.
- The block validation process of PoB-based networks does not require the use of powerful computational resources and does not depend on powerful mining hardware (like ASICs).
- Instead, cryptocurrencies are intentionally burned to “invest” resources in the blockchain, so the candidate miners are not required to invest physical resources.
- In PoB systems, miners invest in virtual mining rigs (or virtual mining power).
- In other words, by performing coin burns, users can demonstrate their commitment to the network, gaining the right to “mine” and validate transactions.
- Since the process of burning coins represents virtual mining power the more coins a user burns in favor of the system, the more mining power he/she has and, thus, the higher the chances to be chosen as the next block validator.

Slide 10

How does PoB works?

- The process of burning coins consists of sending these to a public verifiably address where they become inaccessible and useless.
- Typically, these addresses (aka. eater addresses) are randomly generated without having any private key associated with them.
- Naturally, the process of burning coins reduces the market availability and creates an economic scarcity, causing a potential increase in its value.

- Coin burning is another way of investing in the security of the network.
- One of the reasons Proof of Work blockchains are secure is the fact that miners need to invest lots of resources in order to finally be profitable.
- Similar to PoW. But instead of investing electricity, labor work, and computational power, PoB blockchains are supposed to be secured by the investment made through coin burns and nothing else.
- PoB systems will provide block rewards to miners and within a certain period, the rewards are expected to cover the initial investment of the burned coins.
- There are different ways of implementing the Proof of Burn consensus algorithm. While some projects perform their PoB mining through the burning of Bitcoins, others achieve consensus by burning their own native coin.

Slide 11

Coinburn

- Miners should show proof that they have *burned* some coins
- Sent them to a verifiably un-spendable address
- Expensive just like PoW, but no external resources are used other than the burned coins
- PoW vs PoB – Real resource vs virtual/digital resource
- PoB works by burning PoW mined cryptocurrencies

Slide 12

Pros

- Cheap to use
- Scalable to all types of applications.

- One argument made for proof-of-burn is that it encourages a long-term commitment and time horizon for a project. This theoretically creates greater price stability for the coin as long-term investors are less likely to sell or spend their coins.

- Proof-of-Burn is also said to be better than proof-of-work at ensuring coins are distributed in a fair, decentralized manner. Contrast this with proof of work mining, where we've all seen how the rise of ASIC mining pools can cause greater centralization of mining.

Cons

- Centralization.
- Limited functionality

- While proof-of-burn proponents say it doesn't use resources, critics claim that proof-of-burn does involve resource waste in as much as the resources used to generate the burnt coins is wasted.
- There is also a problem similar to that seen in proof-of-stake consensus, where those who have a lot of coins continue to amass an even greater number of coins. It's the rich get richer problem.
- Proof-of-burn has also been called a high risk protocol, as there is no guarantee that a user will ever recover the full value of the coin being burned

Proof of Burn is used by Slimcoin, TGCoin and Factom**.**