TCS332 Fundamental of Information Security and Blockchain

Proof of work (PoW)

B. Tech CSE III Semester

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE

Graphic Era (Deemed to be University), Dehradun, India

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

Overview

- Proof of work (PoW) is a mining algorithm.
- It requires a not-insignificant but feasible amount of effort in order to prevent the malicious uses of computing power, such as launching denial of service attacks.
- Following its introduction in 2009, Bitcoin became the first widely adopted application.
- Proof of work forms the basis for many other cryptocurrencies as well, allowing for secure, decentralized consensus.

Overview

- Proof of work (PoW) is a decentralized consensus mechanism that requires members of a network to put effort into **solving an arbitrary mathematical puzzle** to prevent anybody from cheating the system.
- Proof of work is used widely in cryptocurrency mining for validating transactions.
- Due to proof of work, Bitcoin and other cryptocurrency transactions can be processed peer-to-peer in a secure manner without the need for a trusted third party.
- Proof of work at scale requires huge amounts of energy, which only **increases as more miners join** the network.

Overview

- Bitcoin is a digital currency that is underpinned by a kind of distributed ledger known as a "blockchain."
- This ledger contains a record of all bitcoin transactions, arranged in sequential "blocks," so that no user is allowed to spend any of their holdings twice.
- In order to prevent tampering, the ledger is public, or "distributed"; an altered version would quickly be rejected by other users.

Overview

- Proof of work (PoW) is a form of cryptographic zero-knowledge proof in which one party (the prover) proves to others (the verifiers) that a certain amount of computational effort has been expended for some purpose.
- Verifiers can subsequently confirm this expenditure with minimal effort on their part.
- The concept was invented by Cynthia Dwork and Moni Naor in 1993.

Rules to follow

- Miners earn bitcoin rewards for every block for which they find the solution. This is what drives them to mine in the first place.
- This monetary reward also drives them to follow the rules -not double-spending their money, for instance.
- Say Alice the Miner finds a winning hash for a block.
- If Alice submits the solution with the block but breaks rules within the block -say, spends coins more than once - the rest of the Bitcoin network will reject Alice’s block.
- Alice will lose all the bitcoin he should have won.
- The threat of losing the bitcoin rewards keeps miners honest.

Why PoW

- In most digital currencies, this problem is easy to solve. The bank that is in charge of the system keeps track of how much money each person has. If Alice sends Bob $1, then the bank deducts $1 from Alice and gives $1 to Bob.
- But in cryptocurrency, there isn’t such an intermediate entity. Proof-of-work provides a solution.

Cryptocurrencies use proof-of-work

- Bitcoin
- Ethereum
- Bitcoin Cash
- Litecoin
- Monero

Problems and issues with PoW

- **High energy use:**
- Bitcoin uses as much energy as all of Switzerland because of proof-of-work.
- And its energy use is increasing as more miners join the hunt for bitcoins, though some of this is powered by renewable energy.

Problems and issues with PoW

51% attacks:

If one mining entity is able to accumulate 51% of Bitcoin's mining hashrate, it can then go against the rules temporarily, double-spending coins and blocking transactions.

Problems and issues with PoW

- **Mining centralization:**
- Proof-of-work is all about creating a currency without one single entity in charge.
- However, in practice, the system is somewhat centralized, with just **three mining pools controlling almost 50% of Bitcoin's computational power.**
- Therefore, developers should try to resolve these issues.