University of Malta

Master of Science in Blockchain and Distributed Ledger Technologies

DLT5003: Introduction to Blockchain, DLTs and Cryptocurrencies

Assignment 1 Part 2 (PoW)

Date Submitted: 17th February 2023
Student: Karsten Guenther 0295697M (ICT Stream)
Lecturer: Prof. Joshua Ellul

Proof-of-Work

The Proof of Work (POW) consensus mechanism is a method used in some blockchain networks to reach consensus and validate transactions. The idea behind POW is to require participants, known as miners, to perform a computationally expensive task in order to add new blocks to the chain.

In a POW system, miners compete to solve a mathematical puzzle that is designed to be difficult to solve but easy to verify. The puzzle requires a significant amount of computational power to solve, which is why miners need to invest in specialized hardware to compete. The first miner to solve the puzzle earns the right to add the next block to the chain and receives a reward in the form of newly created cryptocurrency.

Once a block is added to the chain, it is considered to be verified and immutable, meaning it cannot be changed or deleted without consensus from the network. Other miners can quickly verify the new block's solution, so the network can continue to operate securely and efficiently.

The difficulty of the mathematical puzzle is adjusted periodically to ensure that new blocks are added to the chain at a consistent rate. This also helps to prevent the creation of too many new coins too quickly, which could lead to inflation.

Advantages of using a Proof of Work (PoW) consensus mechanism:

Security: PoW is a highly secure consensus mechanism. Its computational requirements make it difficult and costly for attackers to gain control of the network and manipulate the blockchain.

Decentralization: PoW is a decentralized consensus mechanism that relies on nodes in the network to validate transactions and add new blocks to the blockchain. This means that no single entity can control the network.

Fairness: PoW is designed to be fair, as all nodes in the network have an equal chance of adding new blocks to the blockchain. This means that no node has an unfair advantage over others.

Resilience: PoW is a resilient consensus mechanism that can withstand attacks and disruptions to the network. This is because the nodes in the network work together to ensure that the blockchain is secure and accurate.

Compatibility: PoW is compatible with a wide range of systems and platforms, which makes it a versatile consensus mechanism for a variety of use cases.

Disadvantages of using Proof of Work (PoW) as a consensus mechanism, including:

Energy consumption: PoW algorithms require significant amounts of computational power, which translates to high energy consumption. This has been a major concern, as the environmental impact of cryptocurrency mining has become increasingly apparent.

Centralization: As the computational power required for mining increases, it becomes more difficult for individuals to participate in the mining process. This has led to the concentration of mining power in the hands of a few large mining pools, which can potentially lead to centralization and control by a few entities.

Hardware requirements: Mining with a PoW algorithm often requires specialized hardware, such as ASICs (Application-Specific Integrated Circuits), which can be expensive to purchase and maintain.

Security risks: In a PoW system, an attacker with more than 50% of the mining power can potentially execute a 51% attack, allowing them to modify transactions and potentially double-spend coins.

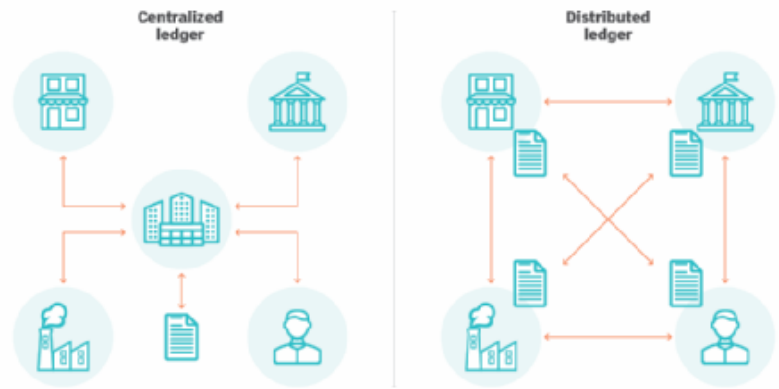
Slow transaction speeds: The computational power required for mining can result in slower transaction speeds, which can limit the scalability of the blockchain.

Miner incentives: PoW algorithms rely on miners to validate transactions and maintain the network, and they are incentivized to prioritize their own profits over the network's long-term health. This can lead to short-term decision making and potential conflicts of interest.

Proof of work in detail:

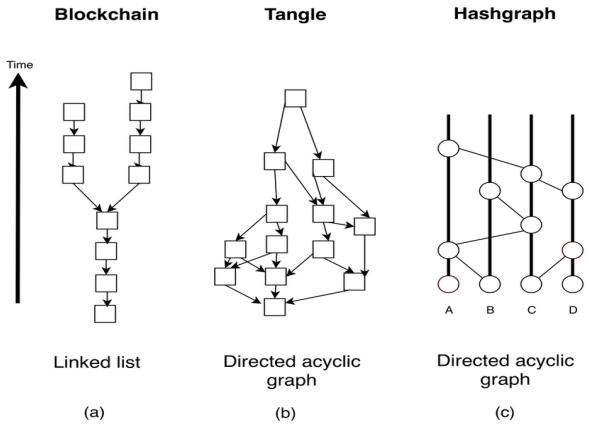
A blockchain is a distributed database that is maintained by a network of computers, also known as nodes. It is designed to be secure, transparent, and resistant to modification. The most famous use case for a blockchain is as the underlying technology for cryptocurrencies, such as Bitcoin.

In a blockchain, every node has a copy of the entire database, and they all work together to add new blocks of data to the chain. Each block contains a set of transactions that have been verified and validated by the network of nodes. Once a block has been added to the chain, it is very difficult to change or delete any of the data in that block. This makes the blockchain an excellent tool for creating a secure and tamper-proof ledger of transactions.

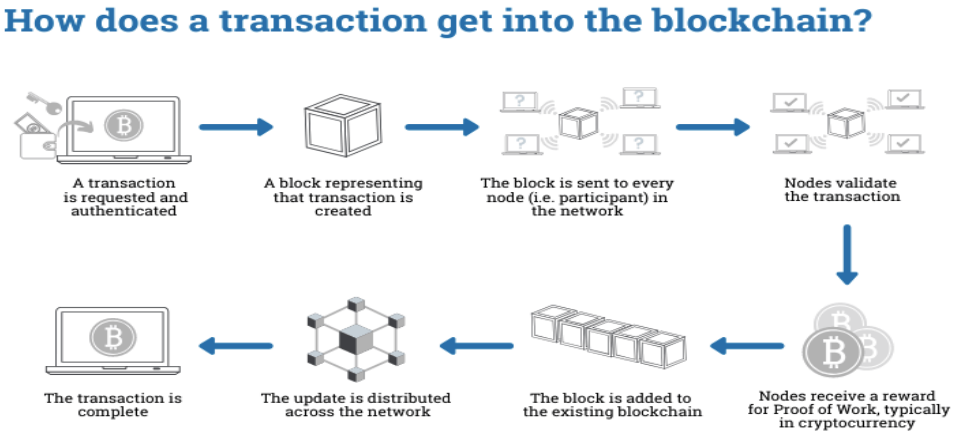


The process of adding a new block to the chain is known as "mining" in the case of Bitcoin and other proof-of-work cryptocurrencies. The mining process in a blockchain is a crucial part of maintaining the integrity and security of the network. Mining involves verifying and adding new blocks to the blockchain, which contains a record of all transactions that have taken place on the network.

In a proof-of-work (PoW) blockchain, like Bitcoin, the mining process involves solving complex mathematical problems using computational power. Miners compete to solve these problems, and the first miner to solve the problem and add a new block to the blockchain is rewarded with a certain amount of cryptocurrency, typically in the form of transaction fees and newly minted coins.



The mathematical problems that miners must solve are designed to be difficult and resource-intensive, requiring significant computational power. The purpose of this is to prevent any one miner or group of miners from controlling the network and making unauthorized changes to the blockchain.



To begin mining, a miner needs to download the blockchain and install specialized software that communicates with the rest of the network. The software allows the miner to receive new transactions and broadcast the solved block to other nodes on the network.

Once a miner has verified that a transaction is valid, they will add it to a block and start the mining process by attempting to solve a cryptographic puzzle. After receiving a transaction, a miner first checks its validity by verifying that the digital signature is valid and that the transaction does not result in a double spend. The miner does this by checking the transaction against the blockchain's transaction history and current state.

If the transaction is valid, the miner includes it in a block along with other valid transactions. The miner then performs a computationally intensive process called hashing on the block's contents, creating a hash that meets the difficulty target set by the network. This difficulty target is what makes the mining process competitive and ensures that no single miner can easily add a block to the blockchain.

The cryptographic puzzle in a proof-of-work system typically involves finding a hash that meets certain requirements, such as being below a certain target value. The hash function used is designed to be computationally difficult to reverse, so the only way to find a valid hash is through trial-and-error.

To solve the puzzle, the miner takes the block header, which includes the transactions to be included in the block, and combines it with a random number called a "nonce". This combined data is then hashed using a cryptographic hash function. If the resulting hash meets the specified requirements, the miner has found a valid solution and can broadcast the new block to the network.

If the hash does not meet the requirements, the miner must increment the nonce and try again. This process is repeated until a valid hash is found. The probability of finding a valid hash is determined by the difficulty level, which is adjusted periodically to ensure that blocks are added to the blockchain at a consistent rate.

Once the miner has found a valid hash, they broadcast the new block to the network, and other nodes in the network verify the block to ensure that it meets the protocol rules. If the block is accepted, it is added to the blockchain, and the miner who found the valid hash is rewarded with the block reward in the form of cryptocurrency.

Once a block has been mined and added to the chain, it is broadcast to all the other nodes on the network. These nodes validate the new block by checking that all the transactions within it are legitimate and have not been tampered with. Once a block has been validated by the network, it becomes a permanent part of the blockchain and cannot be changed.

Because the blockchain is a distributed database, there is no central authority that controls it. Instead, the network of nodes works together to maintain the integrity of the blockchain. This means that the blockchain is very resistant to tampering and attacks.