Bitcoin mining competition (Assignment 2)

Muhammad Nauman Ali

Abstract—**Using the Proof of Work and Merkle tree as introduced by Satoshi Nakamoto in 2008[1], this article explains its implementation and details. This technology together with cryptography enables transactions to be secure and transparent without involving intermediate parties such as banks. It also discusses the environmental, security threats and scalability aspects of the proof of work (PoF).**

Introduction

Blockchain is a distributed digital ledger that securely and openly records transactions. It utilizes encryption to protect financial transactions and a distributed network of nodes to guarantee the immutability and integrity of the ledger. A list of transactions is contained in each block of the chain, and once a block has been added to the chain, it can not be changed. With applications ranging from financial transactions to supply chain management, this produces a transparent and auditable system.

Background

Public and Private Blockchain

These are the two different types of Blockchains that are being used for different purposes and have different features.

Public Blockchain :

A public blockchain is a decentralized network that anybody may access to participate in and examine the blockchain. Because it lacks a need for authorization, anybody on the network may build new blocks and validate transactions. Public blockchains include those used by Bitcoin and Ethereum, for instance. Public blockchains are protected by consensus techniques like proof-of-work (PoW), where miners compete to solve challenging mathematical puzzles to confirm transactions. Anyone may contribute processing power to the network and benefit from participating in the consensus process. Transparency and security are the two key advantages of public blockchains. The network is protected by a decentralized consensus process, and anybody may view transactions on it. Public blockchains' scalability and transaction speed are their key drawbacks. A decreasing number of transactions can be performed per second as more users join the network, which causes longer transaction times and increased transaction costs.

Private Blockchain:

A private blockchain, on the other hand, is a permissioned network that limits access to particular persons or organizations. The network owner must give their consent in order to join and examine the blockchain in this restricted system. Companies or organizations who want to maintain control over the network and its users frequently employ private blockchains. Because they are made for a lower volume of users and transactions, private blockchains are often quicker and more scalable than public blockchains. Due to network owners may regulate who can participate and access the blockchain, private blockchains can also display better degrees of privacy and security. Private blockchains' lack of decentralization and transparency is their biggest drawback. The networks are not completely decentralized since only one entity has control over them, and this puts them at danger of being manipulated by the network owners.

Whether to utilize a public or private blockchain ultimately depends on the use case and the needs of the company.
Public blockchains are better suitable for applications that require security and transparency, whereas private blockchains are better suited for those that require speed, scalability, and network control.

Merkle Tree

To verify the validity and integrity of massive data sets, blockchain technology and cryptography employ a tree-like data structure called a Merkle Tree. It works by building a hash tree out of all the data, where each leaf node's hash value corresponds to a particular piece of data. These leaf nodes' hashes are then added together in pairs to produce new parent nodes, which are then added together in pairs until only one root node is left. Any alteration of the data will result in a modification of the root node hash, making it simple to spot and halt fraudulent activity. The authenticity and integrity of the full collection of data are represented by the root node hash.

Mining in Proof of Work

In Proof of Work (PoW) blockchain networks, mining is the process through which new blocks are added to the blockchain by solving difficult mathematical problems. Mining, a key element of the PoW consensus method, is used to verify transactions, safeguard the network's security, and preserve its integrity. It takes a lot of computing power from a network of nodes (also known as miners) to solve a difficult mathematical puzzle. The first miner to decipher the code and authorize the transaction wins newly minted bitcoin as payment for what they've done. This reward motivates miners to sign up for the network and invest money in the processing power required to solve the hashing problem.

The process of solving the problem is referred to as proof of work because the miner must demonstrate that they have used a significant amount of computing labor to validate the transaction. The puzzle's amount of difficulty is determined by the network, and it is meant to increase as more miners sign up for the system in order to ensure a consistent stream of new blocks. As a result, throughout the mining process, no miner or group of miners may unjustly dominate the network.

PoW network mining requires a lot of computation and energy, which may lead to high electricity costs and environmental problems. But it is a tried-and-true consensus method that has been used in a number of successful blockchain networks, including Bitcoin and Ethereum. The "hash puzzle," a difficult mathematical conundrum that needs producing a hash value that complies with particular constraints, is solved by miners using their computer power. The hash value must normally be lower than a specified threshold that is established by the network's difficulty.

Miners must attempt many solutions by changing the input data to the hash function until they discover one that complies with the requirements since the hash problem is meant to be difficult. This process is frequently referred to as "hashing" or "hashing power."When a miner successfully solves the hashing issue, the new block may then be broadcast to the network for confirmation and verification. After other nodes have confirmed the block's legitimacy on the network, they can subsequently add it to their copies of the blockchain. The rivalry amongst miners to crack the hash problem and add new blocks to the blockchain is what keeps the network safe and ensures that no one miner or group of miners can control the network.

Addition of new Blocks to the Blockchain

In order to add new blocks to a blockchain in a Proof of Work (PoW) network involves difficulty. The level of difficulty determines how difficult the math puzzle is that miners must solve in order to add a new block to the network. The difficulty level increases as the challenge becomes harder to solve and demands more computing power.

In the case of Bitcoin, the difficulty level of the network is modified to preserve a constant pace of block generation, which is normally every 10 minutes. As the network's processing capability improves, the amount of complexity required to sustain the block creation pace rises. Similar to the last illustration, if processing capacity decreases, the difficulty level must likewise decrease in order to sustain the rate of block production.

The difficulty level must be changed in order to preserve network security and prevent a single miner or small group of miners from taking over the network. If the difficulty level is set too low, it will be easier for miners to solve the puzzle and add new blocks, which will result in an increase in the number of blocks on the blockchain and maybe a security concern. It will be extremely difficult for miners to solve the problem if the level of difficulty is set too high, which might slow down block formation and possibly create a network slowdown. As a result, difficulty encourages mining, upholds network security, and ensures a steady pace of block genesis.

Architecture

In a blockchain network, the client and server work together to validate the blockchain. When the client requests information from the server, the server replies by providing it back to the client. The client uses this information to verify the authenticity and integrity of the blockchain. The client initially asks the server for the blockchain's current state. The height of the most recent block, a list of all transactions on the blockchain, and its hash are components of the state.

The server then sends the requested data back to the client. Additional details, such as the difficulty of the proof-of-work method or a list of network nodes, may also be provided by the server.

Overall, the client-server method of certifying the blockchain is crucial for ensuring the security and integrity of the blockchain network. All blockchain flaws may be found and fixed by the client and server working together to make sure all transactions are secure and legal.

Before being forwarded to the server for additional verification, a block must first be confirmed on the client side using a nonce.

The client initially produces a new block by gathering transaction data, creating a block header, and selecting a nonce value. The block header contains the timestamp, the Merkle root hash of the transactions, the hash of the block before it, and additional metadata. The block header is given the nonce, a random integer that may be changed to vary the block hash that is generated.

The client then applies the hash method and the current nonce value to hash the block header. If the produced hash meets particular criteria for example, begins with a specified number of zeros, it can be sent to the server for verification.

The server then rehashes the block header using the provided nonce value to do its own validation after receiving the block from the client. If the resultant hash meets the criteria for a legitimate block, the server adds the block to the blockchain and broadcasts it to other nodes in the network.

If the hash does not meet the criteria, the server rejects the block and notifies the client of the issue. The client can change the nonce value and carry on with the operation after locating a valid block.

The process of validating a block using a nonce on the client side and sending it to the server for validation is a crucial component of the consensus mechanism in blockchain technology, which ensures that all nodes in the network concur on the state of the blockchain and that transactions are validated in a secure and decentralized manner.

Implementation

Mining is the technique through which new blocks are added to a blockchain network using the Proof of Work algorithm. In this process, the miners compete with one another in order to solve a cryptographic puzzle that involves finding a nonce, that when coupled with block data and hashed, produces a hash that meets a specific difficulty target. The minor that finds this block first broadcast the block in the network and if that block is accepted by other participants the block is only then added to the blockchain.

The Proof of Work technique is used by miners. The Proof of Work algorithm's hardness, which determines how difficult the cryptographic puzzle is to solve, is controlled by the blockchain network. The harder it is to get the correct hash value for the new block, the more processing power is needed. The network often adjusts the difficulty level to maintain a steady rate of block generation.

For the implementation of the algorithm, the following steps were followed.

The proofOfWork() function is used to implement the Proof of Work consensus algorithm. It calls the createBlock() function to generate a new block and then iterates through all possible nonce values until a hash is found that meets the target difficulty. The difficulty level is set by the DIFFICULTY constant, which represents the number of leading zeroes the hash must have to be considered valid.

The createBlock() function retrieves transactions from the network and constructs a new block with them. It sets the previous_block field to the hash of the last block in the chain and initializes the nonce to 0. The createBlock() function returns the new block, which is then used by the proofOfWork() function.

In the proofOfWork() function, the nonce is incremented with each iteration, and the block's hash is recalculated using the double_hash() function provided in the utils.cryptographic module. The resulting hash is then checked to see if it meets the target difficulty. If it does, the function stops iterating, the block's mined_by field is set to the miner's identity, and the creation_time field is updated to reflect the time it took to find the solution.

The signature field of the block is calculated by signing the block hash with the private key associated with the miner's public key. The resulting block is returned by the proofOfWork() function and is ready to be broadcast to the network.

For the Merkle tree implementation, the following approach was used:

The build_tree method constructs the Merkle tree by iterating over the transactions in data and hashing each one using a hash function. The resulting hashes are stored in the leaf_nodes list. The method then continues to build the Merkle tree structure by iteratively combining pairs of hashes into parent nodes until only a single root node remains. The method returns a dictionary containing the root hash of the Merkle tree.

Discussion

Proof of Work (PoW) is a consensus method used by blockchain networks to ensure the accuracy of transactions and prevent duplicate spending. PoW is well known for its high level of security. Miners are required by the blockchain because they add new blocks and validate transactions by cracking difficult mathematical riddles. This method defends the network from assaults since it would take a lot of computing power to take control of the network. PoW also enables a decentralized network as anybody with the necessary equipment may participate in the mining process.

This shows that the network has no single point of failure and is not controlled by a single entity. It motivates miners to participate in the network by rewarding them with freshly minted bitcoin for successfully adding a block to the blockchain. As a result, miners are being encouraged to keep up transaction validation and network security.

However, there are several shortcomings in the systems. PoW consumes a lot of energy in order to verify transactions and add blocks to the blockchain. Questions concerning the environmental implications of cryptocurrencies that employ PoW have been raised as a result of the impossibility of the energy usage to be sustained over the long run. With PoW, centralization and decentralization are both potential outcomes. More processing power and particular hardware are required as mining becomes more difficult. The network may eventually fall under their possible control as a result of the mining being concentrated in a small number of massive mining pools.PoW also has scalability issues since it takes so long to process transactions and add blocks to the network. This might result in longer transaction delays and higher transaction fees during times of heavy network traffic. PoW is a tried-and-true and safe consensus method overall, however there are serious problems with its scalability and energy usage. Delegated Proof of Stake (DPoS) and Proof of Stake (PoS) are two scalable and energy-efficient consensus methods being investigated by various blockchain networks.

Comparative Analysis

Proof of Stake (PoS):

Validators (also known as "stakers") employ the Proof of Stake consensus procedure, which necessitates that they stake their bitcoin holdings, in order to validate transactions and add new blocks. With increasing stake amount, the chance of being selected to validate the next block rises. Because transactions are authenticated without the need for miners to tackle difficult mathematical challenges, PoS utilizes less energy than PoW. Instead, it selects validators based on their network participation. PoS is hence less vulnerable to 51% attacks, in which one party seizes control of the vast majority of the network's processing capacity. However, a disadvantage of PoS is that it can result in a circumstance where the wealthiest validators have an unfair advantage.

Byzantine Fault Tolerance (BFT):

Consensus algorithms of the BFT family are designed to tolerate the failure of a specific number of network nodes. A preset number of nodes must agree on a transaction's authenticity before the network will accept it in quorum-based BFT algorithms. Therefore, compared to PoW or PoS algorithms, BFT algorithms are more resilient to attacks and malfunctions. BFT can be slower and more difficult than other consensus methods since it requires many rounds of communication between nodes to reach consensus.

Proof of Storage (PoStorage):

Proof of Storage is a consensus method that stores and verifies data using network nodes rather than by solving difficult mathematical problems. Nodes show their storage capacity by providing a cryptographic proof that they are storing a specified quantity of data. PoStorage consumes less energy than PoW, but it requires a lot of storage, which might be a problem in some situations. PoStorage is also vulnerable to Sybil attacks, where a perpetrator creates a large number of fictitious nodes to increase the amount of storage they have access to. Overall, each consensus-building method has benefits and drawbacks. PoW is secure but energy-intensive, PoS is secure but energy-efficient, BFT is robust but challenging to implement, and PoStorage is secure but susceptible to Sybil attacks. The consensus method to be utilized is chosen based on the specific needs of the blockchain network and the goals of its creators.

Environmental effect of Proof of Work

As the name of the algorithm suggests, the Proof of Work, can be criticized for its environmental impact. Some of the criticisms are discussed in this section.

Energy Consumption:

For Proof of Work to solve the cryptographic problem and add new blocks to the blockchain, a significant amount of energy is needed. Its energy use is primarily caused by the powerful computers that miners need to validate transactions. Blockchain networks using the Proof of Work have a large carbon footprint due to their high energy usage. The majority of the energy used by miners is produced from non-renewable resources that have an impact on climate change. Proof of Work blockchains consume a lot of energy; according to some estimates, the Bitcoin network alone uses more energy than numerous countries. The environment is significantly impacted and climate change is accelerated by this excessive energy consumption.

Electronic waste:

Amount of Mining requires specialized equipment, but it soon becomes obsolete when new, more efficient mining equipment is invented. This produces a significant quantity of electronic waste, which is difficult to recycle and might have a harmful impact on the environment.

Centralization:

Due to its significant energy and computational requirements, Proof of Work mining is difficult for people or small businesses to participate in. The network's computing power is thereafter controlled by a limited number of important mining pools to a large extent. One such solution is to choose the Transition to other consensus mechanisms like Proof of Stake and Proof of Authority. Despite the fact that each of these solutions has drawbacks of its own, but they are more environmentally responsible alternatives.

In order to address the concerns of this algorithm different solutions can be proposed. Switching to sustainable energy sources like solar or wind etc is one way to lessen the environmental impact of Proof of Work blockchain networks. The energy efficiency of mining equipment can also be improved. Manufacturers can create chips that use less energy, while miners can improve their equipment to use less energy.

As an alternative, Electronic hardwares might be recycled and used again. By modifying it for new uses or developing gear that is easier to update when new technology becomes available, several firms are looking at methods to recycle and reuse mining equipment.

Security threats to Proof of Work

Although Proof of Work has been in use for more than ten years now and is a proven consensus process, still there are security risks. Some of the security risks are discussed in this section.

The 51% attack is among the most important security issues for the Proof of Work blockchain networks. In this case, a single entity or group holds more than half of the network's processing capacity, giving them the authority to regulate the network and possibly reverse transactions. Blockchain networks should try to maintain a large pool of miners to reduce this danger. Bitcoin also has a difficulty adjustment mechanism in place that makes it more challenging for a single party to control the network.

The Sybil attack also poses a security risk to the Proof of Work blockchain networks. To gain control of the network in this scenario, the attacker generates numerous false identities. The attacker may be able to modify transactions if they have complete control over a lot of the nodes. Blockchain networks can use Proof of Stake in order to reduce this risk by requiring players to confirm their identity before taking part in the consensus process.

Last but not least, transaction malleability is when an attacker changes the transaction ID to produce a new transaction that appears legal but is actually invalid. Double spending may result from this. Blockchain networks that use Schnorr signatures, which boost transaction security and lessen the danger of transaction malleability, can put mechanisms in place to avoid this issue.

Scalability Limitations to Proof of Work

Proof of Work has scaling issues that could prevent wider adoption even though it is a secure and decentralized algorithm. Some of the scalability limitations are discussed in this section.

The amount of transactions that can be contained in a block is limited in Proof of Work networks due to the set block size. This may result in longer processing times for transactions, increased transaction costs, and network congestion. A higher mining difficulty results in longer block delays and slower transaction processing times as more miners join the network. The number of transactions that can be executed in a given length of time is limited by Proof of Work since it takes a lot of energy to solve the puzzle.

In order to find the solution to the above problem we can suggest the following approaches that can be followed.

Increasing the block size limit is one possible means of solving the scalability issues in the Proof of Work networks. More transactions might be included in each block as a result, which would result in quicker transaction processing times and cheaper transaction costs. However, extending the block size limit also makes the blockchain bigger, which may result in storage and bandwidth issues.

Reducing the size of transactions is another solution for the scalability issues in Proof of Work networks. The use of more effective data structures, or transaction data compression can accomplish this.

Proof of Work networks' scalability issues may be resolved via layer 2 scaling techniques like sidechains and state channels. These technologies make it possible to conduct transactions off-chain, which lessens the burden on the primary blockchain and speeds up transaction processing.

Conclusion

The Proof of Work algorithm has transformed the way transactions are secured and recorded due to blockchain technology. Transparency and security of transactions on a decentralized network are ensured by the execution of the method, which includes miners competing to solve a cryptographic problem. The Proof of Work algorithm has proven to be reliable and robust in securing blockchain networks, but it also uses a lot of energy, making it an unpleasant consensus process. Although there are different algorithms yet specific needs of the network and its stakeholders ultimately determine the consensus algorithm to be used.

References

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.