Blockchain

Mohsin Khan
Department of Informatics, UiT
Username: *mkh047*
Assignment 2
mohsin.khan@uit.no

***Abstract*—Blockchain is a *Distributed Ledger Technology (DLT)*, where the records are immutable. The records are shared among nodes in a decentralized manner. The blockchain is secure and impenetrable due to the use of cryptography and consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS). This report provides an overview of blockchain technology, its types, implementation, and consensus mechanisms. The report also covers some of the disadvantages and limitations of blockchain, such as its environmental impact and scalability with potential solutions.**

***Index Terms*—Blockchain, Proof of Work (PoW), Proof of Stake (PoS), Distributed Ledger Technology (DLT)**

I. Introduction

The concept of Blockchain was introduced by Satoshi Nakamoto in 2008 [1]. A blockchain is a network of computer-based distributed digital ledger of transactions. The blocks of the blockchain are connected in a chain using encryption, especially hashing algorithms, and each block in the chain contains a record of multiple transactions. The blockchain is impenetrable and safe because once a block is added to the chain, it cannot be tampered or removed without also modifying all the succeeding blocks [2]. There are two main types of blockchain: Public Blockchain and Private Blockchain [3], [4].

A. Public Blockchain

The public blockchain is completely decentralized, and any node can become a part of it without any permission. The capacity to access the blockchain, create new blocks, and verify those blocks corresponds to every node equally. The following represents the main advantages and disadvantages of public blockchain.

Advantages:

- **Fully Decentralized Network:** Decentralization eliminates the need for a centralized authority, which offers security, resilience, trust, and resistance against tampering.
- **Transparency:** The visibility of the transactions to any node assures transparency and accountability.
- **Secure:** The use of advanced cryptographic algorithms enables secure transactions and prevents counterfeit transactions.
- **Open-source:** Any node can participate for growth and improvement of the network.

Disadvantages:

- **Laws and Regulations:** The bitcoin has been one of the contentious issues for the past few years. Due to the fact that public blockchains operates as an outlier in the established legal system, there can be disorganization and regulatory difficulties.
- **High cost:** The public blockchain is computationally intensive, thus requires greater amount of computational power to validate the transactions.
- **High electricity consumption:** The electricity consumption of a blockchain is high and increases as the nodes participate due to the computational intensive tasks.
- **Scalability:** The fully decentralized architecture of the blockchain facilitates the scalability issue, limiting the transaction speeds.

B. Private Blockchain

The private blockchain also known as permissioned blockchain is owned by a single entity and is partially decentralized. The partial decentralization means that there is a central authority that decides the inclusion of the nodes. The following represents the main advantages and disadvantages of public blockchain.

Advantages:

- **Manageability and control:** The private blockchain is easier to manage and control due to the central authority. This enables to set rules and regulations for network and each node.
- **Scalability:** The transaction throughput of private blockchain is better than the public blockchain.
- **Privacy:** Only authorized nodes are included in the network. So, the associated data with the network can be kept confidential in private blockchain.
- **Performance efficiency:** The required computational resources to validate transactions in private blockchain is limited. As a result, the network can operate effectively.

Disadvantages:

- **Centralized:** A central authority controls the network access on the private blockchain. The advantages of decentralization, such as trust and confidence, are lost as a result of this centralization.
- **Cost:** The permission of the private blockchain is limited to authorized nodes only. This means that it require a substantial initial infrastructure and upkeep cost.

II. Proof of Work (PoW)

The Proof of Work (PoW) is a consensus algorithm that verifies the transactions, creates and adds a new block in the chain [5], and the components involved are briefed as follows:

- **Miners:** The miners in blockchain are the participant nodes that performs a computational intensive task.
- **Cryptographic hash function:** The hash function produces a fixed length output called as hash, while as the input can be of any size. In blockchain, a miner uses the hash function to generate the hash of the block that is to be added to the chain.
- **Difficulty:** The difficulty establishes how challenging it is to incorporate a new block to the network. In order to ensure that blocks are created and added to the blockchain at a consistent rate, the target difficulty is frequently changed.
- **Nonce:** The nonce is a random number added to the block and changed for creating a different hash of the same block.

The explanation of Merkle Tree is essential for better understanding of PoW consensus algorithm.

A. Merkle Tree

Merkle tree also called as hash tree is a data structure that generates a digest of all the transactions in a block [6]. It helps in consistency and verification of transactions. Hash is calculated for each set of transactions, and the hashing pairs of transactions are concatenated and hashed repeatedly until the root hash is obtained. Figure 1 illustrates the generation of merkle tree.

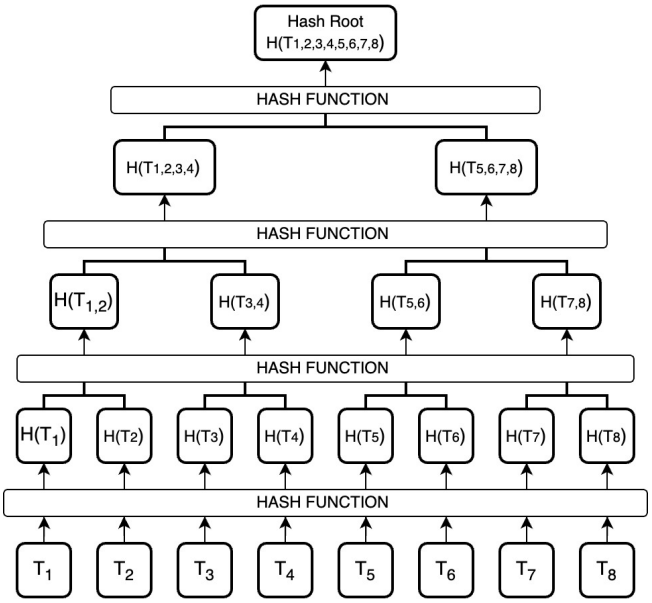

Fig. 1. Merkle Tree

In my implementation, the transactions that are retrieved by using a GET request is given as an input argument to the *MerkleTree* class. The transactions are hashed and appended in a list. Then a while loop is executed and, in each iteration, if the length of the list is greater than 1, the list is checked for the even or odd number of elements in the list. If the list have the odd number of elements, the last element is duplicated to make the list even numbered. Each consecutive pair of hash is concatenated, and the loop continues until only a single hash is obtained, which is also called as *Root hash*. Root hash is obtained by calling the method *get_root()* present in the *MerkleTree* class.

B. Functioning of PoW

As the transactions are broadcasted over the network, the minors retrieve the transactions and add it to the block [7]. The transactions are executed through merkle tree and a hash root is obtained. A block header is created which consists of previous block hash, timestamp, merkle hash root, and nonce. The components of block header are concatenated, and a hash is calculated. The calculated hash is checked for the target difficulty. i.e., number of initial zeroes in the hash. For instance, if the difficulty is set to 6, this means that the calculated hash must have six zeroes in the beginning to get the block accepted and if the difficulty is not attained then the nonce is changed until and unless the difficulty is achieved. This hash is calculated by each miner in the network, and the first minor that solves this calculation or complex mathematical problem broadcasts the block. The block is verified by the nodes in the network and added to the blockchain. If the block is verified successfully, the block is added to the blockchain and the minor is rewarded with bitcoin. Figure 2 illustrates the PoW.

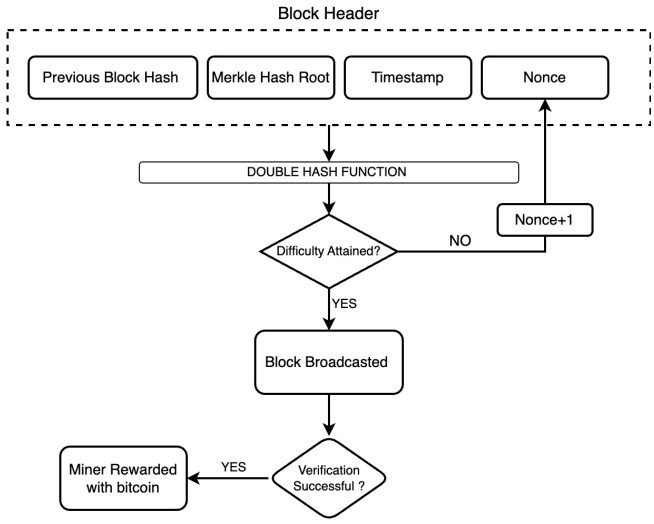

Fig. 2. Proof of Work

In my implementation, I created a class *ProofOfWork* that takes difficulty, previous block hash, timestamp, and merkle hash root as arguments. A loop is executed based on the aforementioned difficulty, i.e., until the difficulty is attained the loop continuously executes. Inside the loop, previous block hash, merkle hash root, timestamp, and nonce are concatenated

and double hashed in this specific order. The obtained hash is checked for difficulty. For instance, if the difficulty is set to 6, the first six digits are checked for zero. So, if the difficulty is not attained, the loop continues to execute by incrementing the nonce. Until the resulting hash has the mentioned difficulty, the nonce keeps incrementing in the loop. Figure 3 shows the successful mining and verification of a block.

Fig. 3. Result of mining the block

III. Comparative Analysis

Before proceeding on to the comparative analysis, a brief explanation of each consensus mechanism has been provided in the following subsections.

A. Proof of Work (PoW)

PoW is a consensus mechanism that requires a substantial amount of computational resource and energy consumption for the miners to solve complex mathematical operation to validate transactions and add blocks to the blockchain. An elaborated explanation is provided regarding the functioning of PoW in previous section. An example where PoW is used is Bitcoin (BTC) cryptocurrency.

B. Proof of Stake (PoS)

PoS is a consensus mechanism that reduces the amount of computational resources required for the validation of the blocks and transactions [8]. For a node to be a validator, it needs to stake a specific amount of coins. The validators are selected randomly for confirming transactions and validating the block information. Instead of employing a competitive rewards-based mechanism like proof-of-work, this system randomly selects who is eligible to receive fees. The cryptocurrency Ether (ETH) is a prime illustration of PoS in action.

C. Byzantine Fault Tolerance (BFT)

BFT ensures that the network is secure and functional [9]. It keeps the network secure by preventing malicious nodes that respond with incorrect information and the faulty nodes that fails to respond. Thus, by using collective decision-making to lessen the influence of the faulty and malicious nodes, a BFT mechanism seeks to protect against system failures. Some of the popular BFT based blockchains are Bitcoin, Etherium, and Quorum.

TABLE I
Comparative analysis of PoW, PoS, BFT, and PoStorage

	Strengths	Weaknesses
PoW	1. Secure 2. Reliable 3. Fully decentralized	1. High carbon footprint 2. Scalability 3. 51% attack susceptibility
PoS	1. Energy Efficiency 2. Scalability 3. No need of high-end computational resources	1. Centralization of stake 2. Nothing at stake problem 3. Convoluted distribution of rewards
BFT	1. Low Energy consumption 2. Fast Transaction 3. High security	1. Centralized 2. Limited scalability 3. Partial decentralization
PoStorage	1. Energy efficient 2. Fully decentralized 3. Secure	1. Complex implementation 2. Risk of storage failure 3. Less adopted

D. Proof of Storage (PoStorage)

PoStorage is a consensus mechanism that uses storage instead of computational power for reaching consensus [10]. This consensus mechanism is accomplished by encrypting a copy of the data and sending it to a server, where a challenge-response protocol is used to verify the integrity of the data. There are two types of participants in PoStorage: Provers and Verifiers. The Provers are the ones that store some data, while as the Verifiers are the ones that verifies that the Provers are storing the data that they are meant to. SpaceMint [16] and Filecoin [17] are the examples that employ PoStorage consensus mechanism.

IV. Environmental impact of Proof of Work (PoW) blockchain networks

The energy consumption of bitcoin that uses PoW as the consensus mechanism has been one of the main issues due to the high computational power required to solve the complex mathematical problem and secure the network. The necessity for specialized hardware, such as Application-Specific Integrated Circuits (ASICs), and the ongoing operation of these components are the main cause of PoW's high energy consumption. The energy consumption has a direct impact on the environment, such as production of greenhouse gasses. According to the study performed by Mora et al. in 2018, if the use of bitcoin increases at the same rate as the use of other widely adopted technologies, the global temperature might rise above 2 °C in less than three decades [11]. The PoW consensus in bitcoin promotes hash rate competition among miners for the chance of a block reward, which prompts additional miners to participate and increase the energy consumption of the entire bitcoin network [12].

The transparency in bitcoin is attained by all the participant nodes in the network by keeping a replica of the transactions. Due to the fact that everyone on the network is storing, the process uses a tremendous amount of energy and duplicates

the data being recorded [13]. The high energy consumption of PoW-based apps is more than the energy consumption of several nations, including Finland and Belgium [14]. Furthermore, the equipments such as GPUs or ASIC miners needs to be kept at optimum temperature to work seamlessly. The additional cooling equipments further increases the energy consumption. Another option is to install the equipments at a large scale in a cold place to diminish the cooling costs, but the immense amount of heat generated from those miners directly leads to global warming. In Iceland, a crypto mining farm established by Genesis mining was set up in 2014. Icelandic energy expert reported in 2018 that the country will use more electricity to mine bitcoin than it does to power every home in the upcoming years [15].

Potential solution

There are a few potential solutions for reducing the environmental impact of blockchain networks, which are enlisted as follows:

- Using an alternative to PoW such as PoS, where transaction validation and secure network needs not to be attained by solving complex cryptographic puzzles. Validators are instead selected according to the quantity of cryptocurrency they hold in the network. As a result, the network uses less energy and minimizes carbon footprint.
- Using solar or wind power plants or other renewable energy sources to power the computational intensive PoW blockchain network can help minimize the carbon footprint.
- There are some recent researches in consensus mechanisms such as Proof of Space (e.g., SpaceMint) [16] where hard-disk space is used to secure the network instead of computing power. This can help the environment in minimizing the energy consumption and associated carbon footprint.

V. Potential security threats to Proof of Work (PoW) blockchain networks

The following are some of the main security vulnerabilities encountered by PoW blockchain networks [19]:

- **51% Attack:** This attack means that theoretically, if a group takes over more than 50 percent of the computational mining power in a blockchain network, it can validate the fraudulent transactions [18].
- **Sybil attack:** In this attack, the attacker creates fake replica nodes on the blockchain network, which they can use to acquire a 51 percent majority and execute invasive transactions.
- **Routing Attack:** A routing attack can be executed by an attacker by manipulating the network traffic and redirecting it to the unintentional node/nodes. As a result, the attacker may be able to isolate certain nodes from the rest of the network. The creation of parallel blockchains by the attacker causes the transactions invalid.
- **Double Spending:** Double spending refers to the act of using the same digital currency more than once to produce counterfeit digital currency. The routing attack can be further exploited by delaying the delivery of the mined block which can lead to double spending.
- **Mining Pools:** To maximize the odds of mining a block and earning the related reward, miners form mining pools to pool their resources. Thus, if a mining pool comprises more than 50 percent of computational mining power, 51 percent attack can be carried out.

VI. Scalability limitations of Proof of Work (PoW) blockchain networks

The constant growth of the nodes in blockchain has caused scalability issues. The following are some of the main scalability issues faced by PoW blockchain networks [20]:

- **Traffic Congestion:** Congestion in the network is caused by the constant addition of numerous nodes. Every transaction on the blockchain is broadcast to all nodes in the network. When a block is mined, it is then once more broadcast to all nodes. As a result, the procedure can use a lot of network resources while also prolonging the propagation delay. Apparently, the transaction fee increases and confirmation times are delayed as a result of the congestion in the network.
- **Difficulty:** The average difficulty of Bitcoin is 47.89, currently [21]. As a result, earning the reward becomes more challenging as more computational resources are needed to mine a block.
- **Size of Blockchain:** Performance degrades as a result of the growing blockchain's length and the rising computational cost of maintaining every node's copy of the blockchain.
- **Transaction Throughput:** Due to the time required to validate transactions and build new blocks, the PoW consensus mechanism can only handle a certain amount of transactions.

Potential solutions

The scaling solution is provided within layer 1 and layer 2 networks. Layer 1 refers to the primary blockchain, whereas Layer 2 refers to the network that lies on top of the primary blockchain [22]. For instance, bitcoin comprises layer 1 network and the layer 2 comprises lightning network [23]. Some potential solutions to address the key factors that affect scalability are enlisted as follows:

- **Sharding:** This technique is a layer-1 scaling solution. In this technique, the transactions are divided into smaller datasets, which are called as *shards*. The subsequent parallel processing of the shards boosts transaction throughput [24].
- **Segregated Witness (SegWit):** SegWit separated the signature data from the transaction data to increase transaction throughput, which led to an increase in the block size limit and reduction of transaction fees [25].
- **Improved consensus mechanism:** PoS is a consensus mechanism with a higher transaction throughput and lower computational resource requirements than PoW.

- **Nested Blockchains:** This technique is a layer-2 scaling solution. In nested blockchain, the main blockchain determines the parameters for the overall network, ensuring the process of carrying out transactions over a secondary chain network.
- **State Channel:** It is a two-way communication channel that lies in layer 2 scalability solution. The participants can directly interact with each other without involving miners and only the participants are able to see those transactions. The main blockchain only keeps track of a transaction's initial and final states [26].
- **Side Chains:** As the name implies, side chains arises from the main blockchain called as parent blockchain and lies in layer-2 scaling solution. Those secondary blockchains have its own consensus mechanism and are connected to the parent chain using a 2-way peg [27]. This aids in the scaling process by reducing a certain amount the load on the primary blockchain.

VII. Conclusion

Blockchain is the future not only for cryptocurrency but for a wide range of applications such as Supply Chain Management (SCM), healthcare, etc. The implementation of blockchain in python as an assignment helped me to understand the intricate working of the technology. However, PoW based blockchain networks have adverse environmental impact and scalability issues. But, the researchers have provided a few potential solutions to curb those issues and as time passes, more advanced technologies and solutions will become available. Thus, as the technology develops and becomes more sophisticated, we may anticipate seeing an increasing amount of utilization of blockchain and its advantages in different fields in the years to come.

References

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized business review, 21260.

[2] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.

[3] Guegan, D. (2017). Public blockchain versus private blockhain.

[4] Comparing public and private blockchain features, Pros & Cons. BSV Blockchain. (n.d.). Retrieved April 12, 2023, from https://www.bsvblockchain.org/news/comparing-public-and-private-blockchain-features-pros-cons

[5] Napoletano, E. (2023, February 16). Proof of work explained. Forbes. Retrieved April 12, 2023, from https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-work/

[6] Frankenfield, J. (2023, January 5). Merkle tree in Blockchain: What it is and how it works. Investopedia. Retrieved April 12, 2023, from https://www.investopedia.com/terms/m/merkle-tree.asp

[7] Frankenfield, J. (2023, February 9). What is proof of work (POW) in Blockchain? Investopedia. Retrieved April 12, 2023, from https://www.investopedia.com/terms/p/proof-work.asp

[8] Frankenfield, J. (2023, January 10). What does proof-of-stake (pos) mean in crypto? Investopedia. Retrieved April 12, 2023, from https://www.investopedia.com/terms/p/proof-stake-pos.asp

[9] Binance Academy. (2022, December 12). Byzantine fault tolerance explained. Binance Academy. Retrieved April 12, 2023, from https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained

[10] Kamara, S. (n.d.). Proof-of-storage (POS) - wiki. Golden. Retrieved April 12, 2023, from https://golden.com/wiki/Proof-of-storage_(PoS)-MN4DJY3

[11] Mora, C., Rollins, R. L., Taladay, K., Kantar, M. B., Chock, M. K., Shimada, M., Franklin, E. C. (2018). Bitcoin emissions alone could push global warming above 2 C. Nature Climate Change, 8(11), 931-933.

[12] Jiang, S., Li, Y., Lu, Q., Hong, Y., Guan, D., Xiong, Y., Wang, S. (2021). Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China. Nature communications, 12(1), 1-10.

[13] Sedlmeir, J., Buhl, H. U., Fridgen, G., Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. Business and Information Systems Engineering, 62(6), 599-608.

[14] Sapra, N., Shaikh, I., Dash, A. (2023). Impact of Proof of Work (PoW)-Based Blockchain Applications on the Environment: A Systematic Review and Research Agenda. Journal of Risk and Financial Management, 16(4), 218.

[15] Iceland will use more energy mining bitcoin than powering the country. World Economic Forum. (n.d.). Retrieved April 12, 2023, from https://www.weforum.org/agenda/2018/02/iceland-may-use-more-electricity-to-mine-bitcoins-than-it-does-to-power-all-of-its-houses-this-year

[16] Park, S., Kwon, A., Fuchsbauer, G., Gaži, P., Alwen, J., Pietrzak, K. (2018). Spacemint: A cryptocurrency based on proofs of space. Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, 2018.

[17] Kothari, R., Jakheliya, B., Sawant, V. (2019). A distributed peer-to-peer storage network. 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT),

[18] Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., Wightman, P. (2021). The 51% attack on blockchains: A mining behavior study. IEEE Access, 9, 140549-140564.

[19] Khawaja, M. F. (2022, December 25). 4 security threats to blockchain networks you need to know about. MUO. Retrieved April 12, 2023, from https://www.makeuseof.com/security-threats-blockchain-networks/

[20] Geroni, D. (2022, August 15). Blockchain scalability problem - why is it difficult to scale blockchain. 101 Blockchains. Retrieved April 12, 2023, from https://101blockchains.com/blockchain-scalability-challenges/

[21] Bitcoin average difficulty (I:bad). Bitcoin Average Difficulty. (n.d.). Retrieved April 12, 2023, from https://ycharts.com/indicators/bitcoin_average_difficulty

[22] Binance Academy. (2022, September 29). Blockchain layer 1 vs. Layer 2 scaling solutions. Binance Academy. Retrieved April 12, 2023, from https://academy.binance.com/en/articles/blockchain-layer-1-vs-layer-2-scaling-solution

[23] Poon, J., Dryja, T. (2015). The bitcoin lightning network. Scalable o-chain instant payments.

[24] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., Saxena, P. (2016). A secure sharding protocol for open blockchains. Proceedings of the 2016 ACM SIGSAC conference on computer and communications security

[25] Frankenfield, J. (2022, December 13). Segregated witness (segwit): Definition, purpose, how it works. Investopedia. Retrieved April 12, 2023, from https://www.investopedia.com/terms/s/segwit-segregated-witness.asp

[26] Dziembowski, S., Faust, S., Hostáková, K. (2018). General state channel networks. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security,

[27] Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P. (2014). Enabling blockchain innovations with pegged sidechains. URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, 72, 201-224.