Advanced Distributed Systems Assignment 1; Bitcoin Mining Competition

1st Marius Møller-Hansen
Tromsø, Norway
mmo182@uit.no

2nd Håvard Livastøl
Tromsø, Norway
hli078@uit.no

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

In this assignment we were tasked with completing a Proof of work (PoW) algorithm which creates and verifies blocks as documented in the bitcoin white paper (source). This report will detail our implementation of the proof of work consensus mechanism but we will also explore the different aspects of blockchains, and other consensus mechanisms.

II. Technical Background

1) **Blockchains** are distributed ledgers, containing of blocks of transactions chained together by each block pointing to the previous block in the chain. Blockchains offer great security and immutable transactions.
2) **Public blockchains** are more decentralized as anyone can join and participate in the validation of transactions. **Private blockchains** are more centralized and are therefore less secure having single points of failure, but this private approach gives for more efficient governance and decision making. Private blockchains also provide better scalability than public blockchains since there are fewer participants private blockchains can use more efficient consensus mechanisms. Private blockchains are also more private (as the name implies), this is both a advantage and disadvantage to both as public blockchains are available for anyone to participate in and view as all transactions are public.
3) **Proof of Work** is a method for a party to cryptographicly proof for others that a certain amount of a specific computational effort has been done. The method was made popular by Bitcoin, where it is used to reach consensus among decentralized nodes. Miners compete to append blocks and mine new currency. Proof of work is used to allow a miner to prove that the work required for the creation of a new block, has been done by the miner. With this proof, the miner appends the block to the blockchain. A detailed description of the mining process is presented in II-A.
4) **Merkle Tree**, or hash tree, is a binary tree data structure where the leaf nodes are hashed data. A node has either none or two child nodes. If a node have child nodes, the node's data is the hash of the two child nodes' hashed combined. This way, a Merkle tree can be used as a cryptographic commitment scheme, where the root can the seen as a commitment and the leaves may be revealed and proven to be a part of the original commitment. [5]

A. Mining

Mining is, in the context of a proof of work blockchain network, the process where transactions are verified and added to the blockchain in form of blocks. Miners, the ones who perform the mining, use their computers to solve complex mathematical computations. When a new block is to be added, the block's data is hashed with a nonce. The complexity of this problem is to find a hash value starting with a certain amount of 0s. The amount of 0s required is defined by the blockchain's difficulty. The nonce is incremented for each failed hash value, until a valid hash is found. The first miner to find a valid hash, announces so to the network as proof of work. The miner who successfully mines a new block onto the blockchain, is awarded a reward. At the moment, this reward is 6.25 BTC, which at February 13th is worth 312 000$.

The miner then creates a block containing all the transactions waiting to be confirmed, the hash of the previous block and the newly discovered nonce. The block is then broadcasted to the network. The other nodes on the network then verify the validity of the block and its transactions. Here, each transaction is checked to see if the sender has the sufficient funds and that there is no double-spending attempts. The block's hash is checked to see if it matches the network's difficulty. The previous block hash stored in the block is also check to see if it matches the actual block stored in the blockchain.

The difficulty of the network is a measure of how hard it is to find a valid hash. In the Bitcoin blockchain, the difficulty is adjusted every 2016 blocks by the network protocol to ensure that block are added to the blockchain at a relatively constant rate. In Bitcoin, this rate is approximately every ten minutes. When blocks are added to quickly, the difficulty is increased. And of course, when blocks are added to slowly, the difficulty

is decreased to increase the rate of which blocks are added to the blockchain.

III. Design

In this section we will explore the design of our implementation of the actual mining of a block.

As blockchains work as digital ledgers, each block holds information about transactions and a pointer to the previous block in the chain. Therefore to find the block header of the next block to be minted we need to double hash the block header of the previous block + a timestamp of when we initiated the proof of work algorithm, and we need the Merkle root which sums up all the transaction hashes to included in the new block.

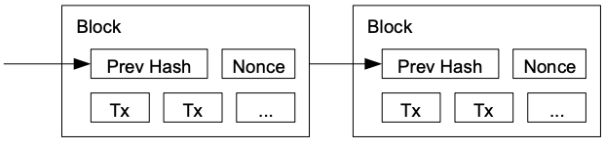

Fig. 1. Blockchain example, from the Bitcoin white-paper [1]

The overall structure of the mining implementation is split into three main parts; proof of work, Merkle tree and the blockchain server communication. The blockchain and transactions are fetched from the server. The parent block is chosen among the blocks on the blockchain, then the transaction hashes are used to form a Merkle tree. The last step of the process is the proof of work hash computation. When a valid hash is found, the block is broadcast to the blockchain.

IV. Implementation

As mentioned, to validate and create a new block we need information about the blockchain itself and the transactions that are waiting to be accepted and added to a block on the blockchain. After querying for this information we can start the proof of work algorithm. This algorithm starts by creating a Merkle tree. Merkle trees are used as a cryptographic commitment for all the transactions on the block. The transactions are hashed and placed in a leaf node of the Merkle tree. All the nodes form a tree, where a non-leaf node contains the a hash which is made up of a concatenation of its children's hashes. If the number of transaction is not an even number, extra nodes are added to make sure all nodes has either none or two child nodes.

Since Merkle trees sum up all the hashes of transactions to be included in the new block, building the Merkle tree correctly is a must. Initially the Merkle tree were built recursively but this did not work as intended as it would add more duplicates than needed/wanted. To build a Merkle tree we start by creating leave Merkle nodes where we hash the transaction hashes. We check if the number of transactions is odd or not, if it is a odd number we need to duplicate the last leave node so that we can build a parent which has the 2 hashes of its leaves to sum. Each parent then takes the hash of the sum of its children until we have a fully built tree witch the Merkle root node at the top for easy extraction of the Merkle root hash. The Merkle root confirms the transactions in the Merkle tree.

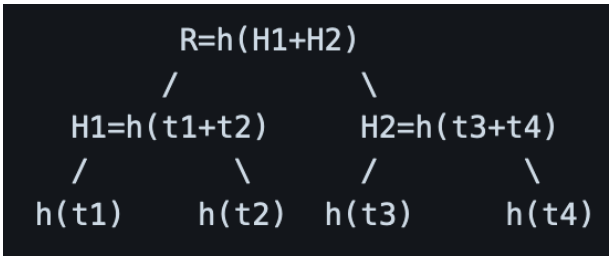

Fig. 2. Merkletree illustration from the assignment text

This is very effective since when the Merkle tree is built we can only query for the Merkle Tree root which will contain the hashed sum of all transactions we want to add to the new block. This Merkle tree root is important since (as mentioned in design) all block headers contain the previous block header + merkle root + timestamp + nonce.

After building the new block header, the block hash needs to be found using proof of work. A nonce is added to the block header and then it is double hashed to check if it passes the difficulty requirement of starting with 0 * Difficulty-level. If the double hash starts with this prefix we create a new block and propose it to the blockchain.

To build a block we need quite a bit of information. First of we need the block header of the new block. This block header is the double hash that passed the difficulty prefix requirement. We also need to include the Nonce, timestamp, the previous block in the blockchains hash and the Merkle root in the block. This is done so that other users of the blockchain can verify that our proposed block is actually valid and passes the requirements. Of course in the block we also include the transactions.

V. Proof of Work

As mentioned in earlier, proof of work is the consensus algorithm employed by bitcoin. Proof of work has some strengths and weaknesses, and in this section we will explore those and compare it with the widely adopted proof of stake consensus algorithm. So what are proof of works strengths and weaknesses? First of proof of work is extremely secure. The reason for this security lies in the underlying algorithm that is proof of work. Miners are required to compute extremely computationally heavy tasks to validate transactions and mint new blocks. This makes it extremely difficult for any malicious actor to manipulate the transactions. Secondly, proof of work is extremely decentralized in that anyone with some basic hardware can help contribute to the blockchain. The more people participate in the validations of transactions the more secure and harder these transactions are to manipulate as

malicious actors would need $> 50\%$ of the mining nodes to achieve consensus.

Also the proof of work consensus algorithm is fair in its distribution of rewards. Miners are awarded based on their contribution to the blockchain and therefore one cannot generate a reward that is asymmetric to the computational contribution. But then what are some weaknesses? Well the most discussed weakness of proof of work is that it is extremely computationally heavy. Miners need to use hardware and energy to secure the network and receive a reward. With the rising market price of Bitcoin more and more people invest in hardware to secure the network and receive a reward. Because of this bitcoin mining uses extremes amount of energy and has led to Graphical processing units being hard to buy with the increased demand. Based on numbers from digiconimist we can see that bitcoin mining around the world uses the equivalent of the power usage of Ukraine [2]. This source also states that a single transaction on the bitcoin network uses the same amount of power as an average U.S household over close to 27 full days. Further on this, the increased demand of GPUs to mine bitcoin has driven the price of GPUs up, making them more unavailable making it harder for new actors to participate in the network [3]. While the hardware aspect of Proof of work can be challenging on new contributors to the system it can also help out tremendously when it comes to big actors or so called ”whales”. Buying, installing and configuring hardware is much more demanding than just allocating funds (as we will see with proof of stake) when it comes to overtaking the system. This means that even if someone were incredibly wealthy buying, installing, configuring and maintaining all this hardware is much more demanding than buying one GPU and mining or allocating stake.

Briefly mentioned in the last section, proof of stake is another consensus algorithm that has recently gained a lot of ground in the blockchain/crypto community. Projects like Ethereum, the second biggest blockchain by market capitalization migrated from using proof of work to using proof of stake in recent years. We will therefore now explore proof of stake and compare its features with proof of work.

Proof of stake separates itself from proof of work by that it does not require the extensive computations being done by each miner, but instead relies on validators staking in the system. Based on staked amount of tokens, validators are selected to validate the system and are rewarded with more tokens for this. Proof of work is considered as more secure since miners have to use significant computational power to validate transactions/blocks. On the other hand in a proof of stake validators offer up tokens that they are willing to stake on their own credability as validators. If they proved to be unreliable validators their stake would be slashed yielding in a loss compared to validating non-maliciously and therefore receiving a reward. Like in the proof of work consensus algorithm the participants often group into pools to share their resources, being either hardware or tokens. This Makes it so participants with less hardware/stake can still get a reward for every new block minted even though they don't have enough hardware/tokens to be selected to validate. Both these systems offer their form of decentralization even if its based on either hardware or stake. Proof of stake can be said to be more scalable as it does not rely on the underlying heavy computing that proof of work does, saving lots of energy. As we can see from this, both proof of work and proof of stake have their advantages and disadvantages, but it seems like blockchain creators and companies favor Proof of stake as indicated by Ethereums switch from Proof of Work to Proof of Stake [4].

A. Environmental Concerns

Proof of work requires a lot of power. As mentioned, the process of mining new blocks in Bitcoin is yearly assumed to use approximately the same amount of electricity as the whole country of Ukraine [2]. Due to the increased amount of competition in mining and a growing computational difficulty, the power usage is steadily increasing, making the matter worse.

The competition between miners leads to the miners pushing each other to invest in more powerful and energy consuming gear to increase their chances of successfully mining blocks and earning the rewards. This race for the rewards further increases the power usage problem of Bitcoin.

The increase in miners also affect the difficulty of the blockchain, because the increased amount of miners will increase the mining rate on the network. As we have discussed earlier, an increase in mining rate will cause the network to adjust its difficulty, as the network has a target mining rate. The higher the difficulty, the more computational power is required to successfully mine a block. The more popular Bitcoin becomes, the more computational power and electricity is required to maintain the security of the blockchain. This is one of the big environmental problems with the proof of work method.

As a consequence of the high power consumption of proof of chain blockchains, EU's financial regulator's vice chair, Erik Thedéen, suggested to ban proof of work network in the EU back in January 2022. He said that ”Bitcoin is now a national issue for Sweden because of the amount of renewable energy devoted to mining” [7].

Later in 2022, the governor of New York banned all Bitcoin mining which did not use 100% renewable energy. The reasoning for this was that the state was looking to decrease their carbon footprint, and therefore wanted to get rid of all miners who used electricity from fossil fueled power plants. [10]

These two cases show that authorities are beginning to look at the proof of work model Bitcoin uses as an environmental problem. It shows that Bitcoin and other proof of work networks are a concern for all of the world, as we do not have unlimited power, neither electrical nor computational. Therefore, it can be thought that improvements are needed

for Bitcoin to continue grow as an alternative to centralized currencies. But what can be done?

One of the most logical and easiest measures to introduce is what was done in New York, require that all Bitcoin mining, and other proof of work computation, must be done with 100% renewable energy. We, as citizens of the world, need to lower our carbon footprint, and to start using renewable energy is a great place to start. By forcing all proof of work computation to use renewable energy, you also encourage development and improvement of renewable energy sources.

Mobile off-grid mining units powered by renewable energy sources would remove the pressure Bitcoin mining applies to the power grids it is connected to. Forcing all mining to be isolated energy ecosystems could be a good solution to the environmental problem Bitcoin and other proof of network blockchains bring to the table. These off grid mining units can for example be large mining facilities built with either a solar, water or even a nuclear power plant which will provide the needed energy for the proof of work computation.

As discussed in V, authorities have asked and encouraged Bitcoin to move from proof of work to proof of stake, due to the enormous power consumption of Bitcoin. But with a proof of stake model, you most likely loose some of the decentralization which is the point of Bitcoin and other digital currency; to move the power away from states and large banks. Therefore, banning proof of work blockchains and forcing all to use other protocols is a bad idea. These regulatory measures will most likely be a double no from the Bitcoin miners, as they are all for the decentralization of Bitcoin. It is one of the properties that makes Bitcoin so popular. Being forced to move to a more centralized structure from a centralized power like either EU government or a local state government would most likely not be popular at all.

Another improvement to the Bitcoin mining power consumption could be to encourage the community to turn off mining equipment in periods of low profitability or excess energy demand. This would at least lower the overall usage a bit. Then you can ask how realistic it is to get the community to agree on such terms. It could work to some extent, but as long as there are people with large investments at risk, some will profit on being unfair to the community by not following the orders of turning of equipment.

A field who has benefited a lot on the energy expensive Bitcoin mining is the hardware industry. During the COVID period, it was almost impossible to get your hands on a new GPU for a reasonable price, caused by cryptocurrency miners willing to pay a lot for GPUs to use them to mine [11]. It went so far that NVIDIA implemented a mining limiter on their 3000 range of GPUs to limit the hash rates of the cards to make them less attractive to miners. Even though it was a great iniative, it did not take long before some broke the hash limiter [12]. The demand of hardware capable of performing the heavy computations of proof of work, shows that the hardware industry need to take such use into consideration when developing new generations of hardware. It pushes them to research and develop efforts on designing more energy-efficient hardware which fits the requirements of mining. This can help decrease the power consumption per hash performed, thus decreasing the total energy consumption of the whole blockchain.

Proof of work network, for example Bitcoin, has a clear environmental problem caused by the energy consumption. As mentioned and discussed, there are multiple different measures which can be taken to reduce the energy consumption of proof of work blockchains. The best would be to motivate all miners to use 100% renewable energy, and ideally also being off grid to fully isolate the mining from the rest of the power grid. This would require all miners to invest in their own renewable energy power plant, which is a bit too much to ask. Therefore, we should be happy if all mining will be using renewable energy in the future.

B. Security concerns

While proof of work is considered secure and decentralized there are still some security concerns associated with Proof of work.

The usual main security concern of proof of work is that anyone controlling $> 50\%$ of the miners in the network will effectively control 100% of the network as they make up the majority and can therefore dictate the consensus. This concern is present but one can also say unrealistic based on the scale of the bitcoin network and number of miners/participants. Since the network is so large in scale, controlling over 50% of the nodes would take extremes amount of power and resources beyond a realistic scope.

While outside the scope of the actual bitcoin networks safety, users of the network can be more vulnerable to attacks as transactions can not be reverted. This means that if one looses their funds in a scam, they are likely gone forever. This happens when users of the network have their private keys discovered meaning malicious can sign transactions with their key and therefore transfer their funds.

These two security threats are very general, and while one of them concerns users private key safety there are some ways to mitigate both of these risks. When it comes to protecting private keys some users have turned to hardware wallets. These hardware wallets are more secure as they are not connected to the internet and therefore more secure from attacks. This is a solution to the user security problem but it comes at a price as users of the system have to buy these hardware wallets from private companies which might not always have their customers best interest in mind. [9]

While the 51% attack threat is a bit unrealistic thanks to the scope of the network. One way to mitigate this threat is increasing the required consensus to more than half the network. While this would mitigate the the risk as malicious actors would have to own even more nodes in the system, it would also have the cost of having transactions be verified by

even more miners before being minted. This is obliviously a big trade off as this is not a big security threat but each block would take more resources to be minted.

C. Scalability

As explored in the comprehensive review of the proof of work consensus mechanism, it is not the best at scaling. The reason for this is based on the 51% acceptance rate and the fact that the block header needs a prefix of significant amount of 0's to be accepted. Further on the proof of work scalability issues Bitcoins lightning network has a transaction throughput of 7 transactions a second or 420/minute. This number is far from impressive considering MasterCard processes around 5 000 transactions a second [8]. This also poses some problems as developers want to develop smart contracts on the lightning network.

An improvement which would have increased the transaction throughput of proof of work blockchain network is to increase the block size. As mentioned previously, Bitcoin, for example, aims to mine a block every ten minutes. If the block size is increased, meaning each block can hold more transactions, the transaction rate will obviously increase. However, increasing the block size is controversial within the community, as some "worry that larger blocks would lead to centralization and make running a full node more difficult." [13] As mentioned in V-A, the decentralization of Bitcoin is one of the most important features, if not the most, of Bitcoin for the community to defend, so this being a threat to the decentralization is not good. So for now, the block size will be standing at one megabyte.

Another problem with the scalability ability of proof of work blockchain networks is the block propagation time. When the size of the network increases, the time ti takes for blocks to be propagated across the network increases. This can lead to longer confirmation times and potential centralization risks as larger miners have an advantage in propagating blocks faster. This is because miners who can propagate blocks faster have a higher likelihood of having their blocks added to the blockchain first. The transactions included in these blocks are confirmed more quickly, leading to shorter confirmation time for users. Conversely, smaller miners may take longer to find valid blocks and propagate them, resulting in longer confirmation times for their blocks and transactions. To solve this issue, block propagation protocols and network infrastructure could have been optimized to help reduce the time it takes for blocks to propagate.

The environmental aspect of proof of work blockchain networks is a part of the scalability problem to. The larger the blockchain, the more energy is required to mine new blocks. Mining will most likely centralize around regions with cheap electricity and access to specialized hardware, leading to mining centralization tendencies. This is a problem because of the 51% attack. Another reason for this being a problem, is that centralized mining facilities can enable miners to censor transactions they disagree with or manipulate the order of transactions in blocks. This ability to control which transactions that are included into blocks in the blockchain undermines the trustworthiness and neutrality of the blockchain, in worst case leading to unfair treatment of users.

Centralization of mining can cause a lot of unwanted consequences for the blockchain network. If a significant amount of the network's hash rate is controlled by a small amount of miners, disruptions like hardware failures, power outages and malicious attacks on these miners could lead to network instability, slowdowns or even temporary halts in transaction processing.

When most of the hash rate is centralized on a few miners, the economy of the blockchain network is centralized. The rewards for mining new blocks are concentrated in the hands of a few dominant miners on the network. This can again create inequalities within the network and undermine its long-term sustainability and fairness. With economic power comes general power, as with such centralized power among few miners decreases the trust level within the network. It can deter new users from joining the network, ultimately limiting the growth and adoption of the network.

As a conclusion, addressing the scalability limitations of proof of work blockchain networks requires a combination of technical innovations and community collaborations. By implementing such solutions that increase transaction throughput and optimize block propagation, while keeping the network decentralized, proof of work blockchains like Bitcoin will be able to scale better. The thing is, as discussed, this is easier said than done. The security and decentralization of such networks are valued way higher than the scalability. So nothing will be done here as long as there are no solutions securing the decentralization and security of the network.

VI. Conclusion

All in all while proof of work has its downsides it provides a extremely reliable, secure and decentralized system which is widely adopted. Other blockchain projects have aimed to build on bitcoins success but address its shortcomings like Ethereum with proof of stake.

References

[1] Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto. 2008 https://bitcoin.org/bitcoin.pdf

[2] DigiEconomist. (n.d.). Bitcoin Energy Consumption. Digiconomist. https://digiconomist.net/bitcoin-energy-consumption

[3] Warren, T. (2021, March 10). GPU Shortages Worsen As Cryptocurrency Coin Miners Turn To Ethereum. Tom's Hardware. https://www.tomshardware.com/news/gpu-shortages-worsen-cryptocurrency-coin-miners-ethereum

[4] Technology Review. (2022, March 4). Ethereum 2.0 is speeding toward a new way to run the internet. Retrieved from https://www.technologyreview.com/2022/03/04/1046636/ethereum-blockchain-proof-of-stake/

[5] Merkle Tree; https://en.wikipedia.org/wiki/Merkle_tree. Accessed February 8th 2024

[6] Proof of Work; https://en.wikipedia.org/wiki/Proof_of_work. Accessed February 8th 2024

[7] EU regulator calls for a ban on proof of work Bitcoin mining to save renewable energy https://www.euronews.com/next/2022/01/19/eu-regulator-calls-for-a-ban-on-proof-of-work-bitcoin-mining-to-save-renewable-energ Accessed February 8th 2024

[8] Cointelegraph. (2022, August 24). Bitcoin Lightning Network vs. Visa and Mastercard: How Do They Stack Up? Cointelegraph.https://cointelegraph.com/news/bitcoin-lightning-network-vs-visa-and-mastercard-how-do-they-stack-up Accessed February 11th 2024.

[9] Decrypt. (2023, May 16). Is There a Backdoor in Ledger Hardware Wallets? Decrypt.https://decrypt.co/140364/is-there-a-backdoor-in-ledger-hardware-wallets. Accessed February 11th 2024.

[10] New York governor signs first-of-its-kind law cracking down on bitcoin mining — here's everything that's in it; https://www.cnbc.com/2022/11/23/new-york-governor-signs-law-cracking-down-on-bitcoin-mining.html. Accessed February 8th 2024

[11] Inside the GPU Shortage: Why You Still Can't Buy a Graphics Card; https://uk.pcmag.com/graphics-cards/133865/inside-the-gpu-shortage-why-you-still-cant-buy-a-graphics-card. Accessed February 12th 2024

[12] Nvidia Confirms 'LHR' Mining Limiter for GPUs Has Been Eliminated; https://uk.pcmag.com/graphics-cards/133865/inside-the-gpu-shortage-why-you-still-cant-buy-a-graphics-card. Accessed February 12th 2024

[13] Bitcoin Network Scaling: Challenges and Evolving Solutions; https://www.doubloin.com/learn/bitcoin-network-scaling. Accessed February 13th 2024