COMS 6998-006 (Foundations of Blockchains) Homework Set 4 (Sol)

Matin M.Babaei M. Parsa Dini

September 9, 2023

Problem 1

A.

Problem 2

A. Ethereum (specifically Ethash) uses a memory-hard Proof-of-Work (PoW) algorithm to achieve ASIC-resistance and promote a more decentralized mining ecosystem. The key components of Ethash, including Dagger and Hashimoto, are as follows:

Dagger is a component of the Ethash algorithm that generates a large dataset called the "DAG" (Directed Acyclic Graph). The DAG is a massive, precomputed dataset that miners need to access and make computations on during the mining process. The idea behind Dagger is to create a computationally intensive task that requires a substantial amount of memory to compute efficiently. This memory-hardness is designed to deter the development of specialized ASIC mining hardware. Dagger creates the DAG dataset in a way that makes it difficult to parallelize the calculations effectively, further discouraging the development of ASICs.

Hashimoto is the name of the actual mining algorithm used in Ethash. It combines the properties of Dagger and traditional hash functions to make mining ASIC-resistant. It involves repeatedly accessing the DAG, which is memory-intensive and sequential in nature, and performing hash computations on it. The result of these calculations is used to determine the proof of work. Hashimoto also incorporates a component called "cache," which is a smaller, faster dataset that miners use to store intermediate values during the mining process. This cache requires frequent random accesses, which are challenging for ASICs to optimize.

Ethash Combination:

Ethash combines Dagger and Hashimoto to create a PoW algorithm that is memory-intensive, difficult to parallelize, and resistant to ASIC optimization. Miners in Ethereum must perform a significant number of memory-related operations, making it more challenging and costly to develop specialized ASIC hardware tailored for Ethash.

Source: Ethereum GitHub Wiki

B. ASICs are less helpful to miners in Ethereum compared to Bitcoin for several reasons:

1.Memory-Intensive Algorithm: Ethereum's Ethash is designed to be memory-hard, meaning it requires miners to perform a substantial number of memory accesses and computations. ASICs are typically optimized for raw processing power, not for memory-intensive tasks. As a result, ASICs are less effective in mining Ethereum, where memory plays a significant role in the mining process.

2.Community Support: Ethereum's community actively supports ASIC resistance to maintain a more decentralized mining network. This includes the willingness to hard fork to modify the PoW algorithm if ASICs become too dominant. This stance discourages the development of Ethereum-specific ASICs.

3.Frequent Algorithm Changes: Ethereum has a history of regular network upgrades and changes to its PoW algorithm to maintain ASIC resistance. These changes make it difficult for ASIC manufacturers to keep up, as they need to adapt their hardware to the new algorithms regularly. In contrast, Bitcoin's SHA-256 algorithm has remained stable, allowing ASICs to dominate its mining ecosystem.

Source: Ethereum's Move to Proof-of-Stake

C. Pros of using ASIC-resistant hash functions:

Decentralization: ASIC-resistant algorithms promote a more decentralized mining ecosystem. They allow a wider range of individuals and small-scale miners to participate in the network, as specialized ASIC hardware is less dominant.

Fairness: ASIC resistance can lead to a fairer distribution of rewards among miners, as it reduces the advantage of those who can afford expensive ASIC hardware. This can help prevent mining centralization.

Security: ASIC-resistant algorithms make it more difficult for a single entity or group to control a significant portion of the network's hash rate. This enhances the security and resilience of the blockchain against 51% attacks.

Cons of using ASIC-resistant hash functions:

Energy Efficiency: ASICs are often more energy-efficient than general-purpose hardware, which can lead to lower energy consumption for blockchain networks that allow ASIC mining. ASIC-resistant algorithms may result in higher energy usage per unit of computational power.

Long-Term Viability: The pursuit of ASIC resistance can lead to frequent algorithm changes and hard forks, which may disrupt the network and its stability. Miners may be hesitant to invest in hardware that could become obsolete quickly.

Innovation Challenges: ASIC-resistant algorithms can limit innovation in hardware development. Specialized ASICs can potentially offer better performance and security, but ASIC-resistant algorithms aim to level the playing field.

Therefore, the choice to use ASIC-resistant hash functions involves a trade-off between decentralization and energy efficiency. Each blockchain project must weigh these factors and make a decision based on its specific goals and community preferences.

Source: Ethereum Wiki - Mining

Problem 3

A. If miners were free to put whatever timestamps they wanted into blocks without any constraints, they could potentially manipulate Bitcoin's difficulty adjustment algorithm to boost their rewards by artificially inflating or deflating the perceived time it takes to mine a batch of 2016 blocks. Here's a concrete example of how such an attack could be carried out: this technique is named **Timestamp Manipulation Attack**.

Timestamp Inflation: Miners collude to manipulate the timestamps in the blocks they mine to make it appear as though it took much longer to mine the last 2016 blocks than it actually did in the real world.

Triggering Difficulty Decrease: Bitcoin's difficulty adjustment algorithm relies on the timestamps of the last 2016 blocks. If the manipulated timestamps make it appear that it took significantly longer to mine those blocks than it did in reality, the algorithm will lower the difficulty level for the next 2016 blocks.

Rapid Mining: With the lowered difficulty level, miners can mine the next 2016 blocks much faster than the manipulated timestamps suggest. Since the difficulty level is artificially low, they can find blocks at a much higher rate than the expected 10-minute block time.

Profitable Mining: Miners can accumulate more rewards in a shorter time frame due to the artificially low difficulty level. They can then either hold these rewards or sell them on the market, potentially profiting substantially.
Reverting Timestamps: After mining the 2016 blocks at a rapid pace, miners could reset the timestamps to reflect the real-world time more accurately to avoid raising suspicions. This may involve correcting the timestamps in a coordinated manner to make the manipulation less obvious.

Finally we can say that this attack essentially allows miners to trick the difficulty adjustment algorithm into lowering the difficulty level, making it easier and more profitable to mine blocks in the short term. However, it's important to note that this attack would likely be detected and countered by the broader Bitcoin community. Timestamp manipulation would be visible on the blockchain, and the Bitcoin community, including full nodes and miners not participating in the attack, would likely reject blocks with suspicious timestamps.

Bitcoin's security relies on the collective vigilance of its users and miners to maintain the integrity of the blockchain, and any attempts at manipulation are typically met with resistance from the network. Additionally, any long-term manipulation attempts would likely lead to a loss of trust in the currency, negatively impacting its value and viability.

B. (a) **Monotonic Increase:** According to the Bitcoin protocol, block timestamps must be monotonically increasing. This means that the timestamp of each new block should be greater than the timestamp of the previous block. This rule helps maintain the chronological order of blocks in the blockchain.

(b) **Median Time Past (MTP):** To prevent miners from manipulating timestamps and skewing the difficulty adjustment process, Bitcoin uses a concept called "Median Time Past" (MTP). The MTP of a block is calculated as the median of the timestamps of the 11 previous blocks. Miners must ensure that the timestamp in their block is greater than the MTP of the previous block but not too far in the future. This rule is defined in the Bitcoin Improvement Proposal (BIP) 66[1].

(c) **Network Adjusted Time (NAT):** In addition to the MTP rule, Bitcoin clients also use a network-adjusted time (NAT) to further limit the acceptable timestamp range for a block. NAT helps prevent miners from setting timestamps too far in the future by comparing the miner's timestamp to the network's synchronized time. NAT is explained in BIP .

(d) **Median Time Rule for Locktime:** Block timestamps also play a role in determining the validity of transactions with a locktime set. Transactions with a locktime cannot be included in a block until the block's timestamp is greater than or equal to the locktime. This ensures that certain transactions are not spendable until a specific time in the future.

Problem 4

A. Bitcoin Cash (BCH) and Bitcoin (BTC) have different difficulty adjustment algorithms.

In Bitcoin Cash (BCH), the difficulty adjustment algorithm is similar to Bitcoin's original algorithm, but with a key difference: it adjusts the difficulty every 6 blocks (approximately every 12 hours) by looking at the median time of the last 11 blocks. This approach aims to provide a smoother adjustment compared to Bitcoin's 2016 block difficulty adjustment period.

In Bitcoin (BTC), the difficulty adjustment algorithm changes every 2016 blocks (approximately every two weeks). Bitcoin uses a retargeting mechanism where it calculates the time it took to mine the last 2016 blocks and adjusts the difficulty level such that it should take approximately 10 minutes to mine each block on average. This periodic adjustment helps Bitcoin maintain a consistent block time.

Source: Bitcoin Cash Difficulty Adjustment Algorithm

Source: Bitcoin Difficulty Adjustment Algorithm

[1] See more here

B. Selfish mining attacks could be more effective in Bitcoin Cash (BCH) compared to Bitcoin (BTC) under certain circumstances. Selfish mining involves a mining pool attempting to keep a portion of its blocks secret to gain a competitive advantage.

In Bitcoin Cash, the shorter time between difficulty adjustments (every 6 blocks) means that a selfish mining pool could potentially gain a temporary advantage more quickly by withholding blocks, leading to a larger percentage of the total network hashrate. This could result in more frequent chain reorganizations.

Example: Suppose a selfish mining pool controls 40% of the BCH network's hashrate. If they manage to keep their blocks secret for two difficulty adjustment periods (12 hours each), they could launch an attack where they release their hidden blocks, causing significant chain reorganizations.

In Bitcoin, with a longer difficulty adjustment period (every 2016 blocks or approximately two weeks), selfish mining attacks would require a sustained effort over a longer period, making them less effective.

C. Additional pros and cons between the Bitcoin Cash and Bitcoin difficulty adjustment algorithms include:

Pros of Bitcoin Cash:

1.Faster adjustment: BCH adapts to changes in network hashrate more quickly, providing stability in block times during periods of rapid hashrate fluctuations.

2.Reduced risk of large miner migration: Miners are less likely to switch between BCH and BTC in response to profitability fluctuations due to shorter adjustment periods.

Cons of Bitcoin Cash:

1.Potential for more frequent chain reorganizations: The shorter adjustment period can lead to more frequent fluctuations in block difficulty, increasing the likelihood of temporary forks and reorganizations.

2.Possible higher volatility in block times: The BCH algorithm may result in more significant fluctuations in block times, impacting user experience.

Pros of Bitcoin:

1.Longer-term stability: Bitcoin's difficulty adjustment algorithm ensures a more consistent block time over extended periods, making it suitable for long-term storage of value.

2.Reduced risk of frequent forks: The longer adjustment period minimizes the chances of frequent chain reorganizations, enhancing network security.

Cons of Bitcoin:

1.Slower response to hashrate changes: The BTC algorithm may lead to longer periods of suboptimal block times if there are rapid shifts in network hashrate.

2.Potential miner migration: Miners might switch between BTC and BCH in response to profitability changes during the two-week adjustment period, leading to fluctuations in network security.

These are some of the key differences and trade-offs between the difficulty adjustment algorithms of Bitcoin Cash and Bitcoin.