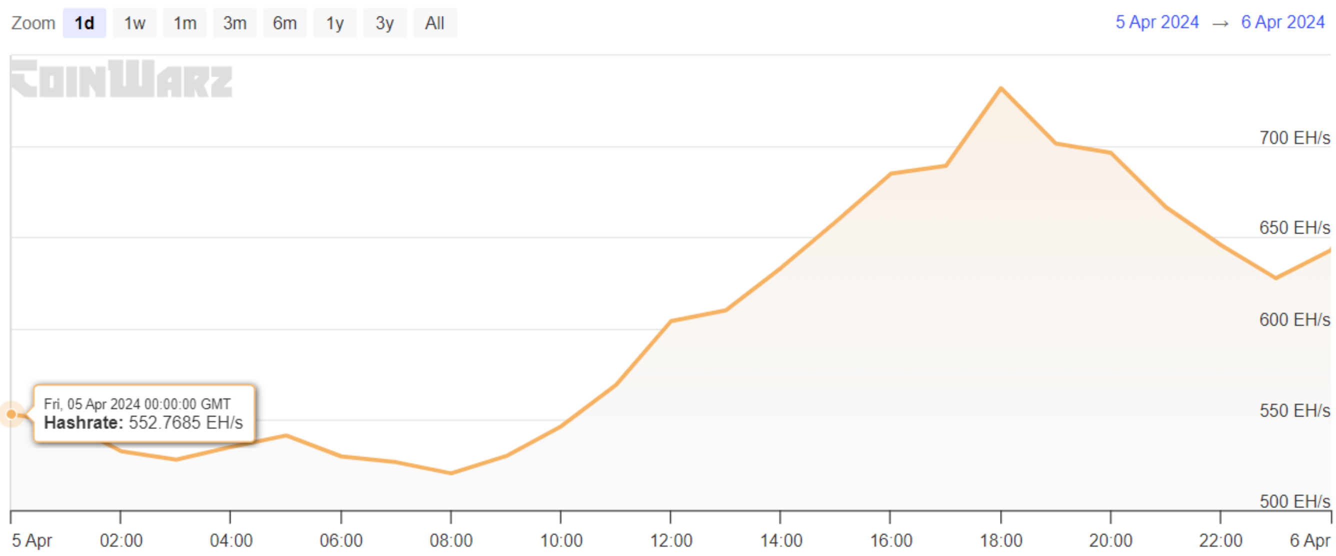
HW2

Mohammadreza Mohammadhashemi

810100206

Q1

Determine the total computational power of the Bitcoin network on the first block mined on April 5, 2024.

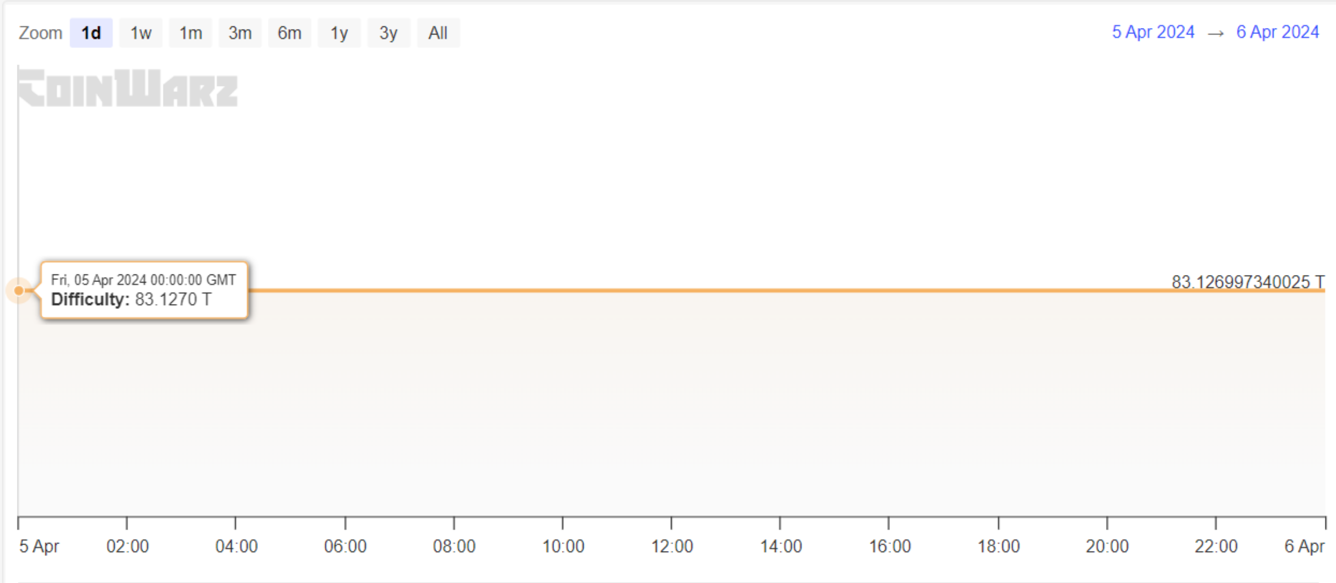


According to the photo provided, the processing power of the entire network is equal to :

$$552.76\frac{EH}{s}$$

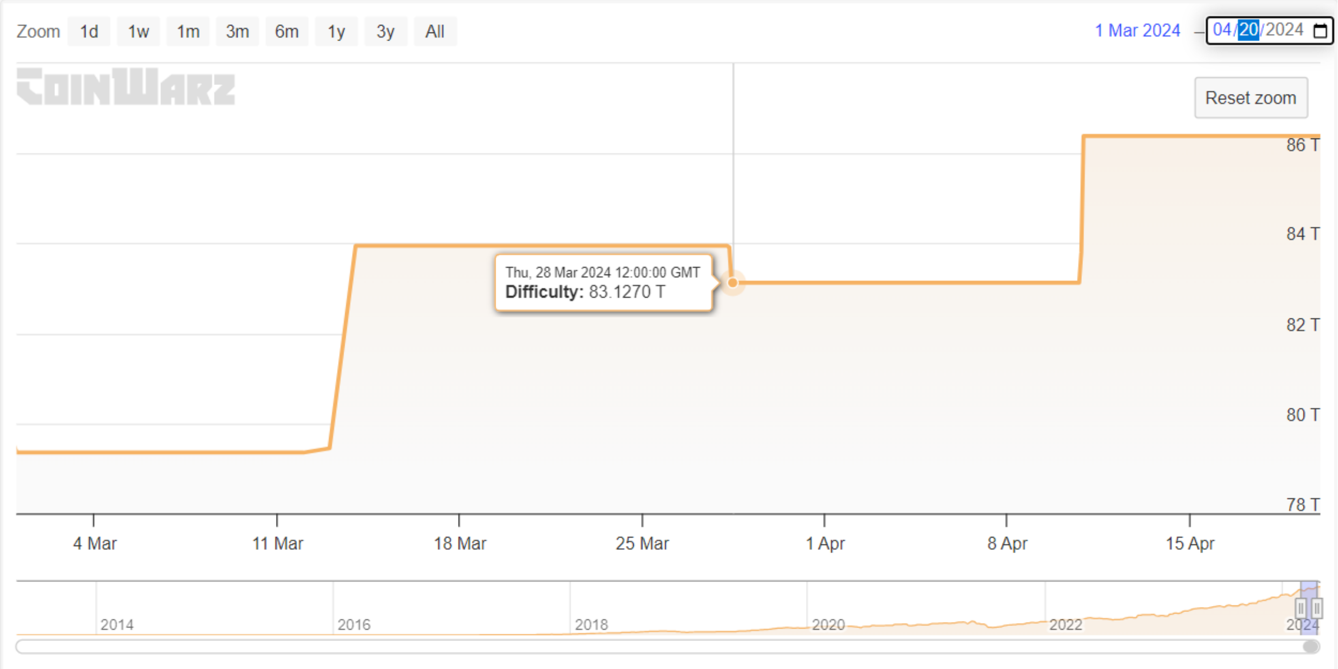
A) Estimate the hash rate threshold on that day using the total computational power from part 1, and compare it to the actual threshold. Explain why there might be a difference between the estimated and actual thresholds.

$$\text{Difficulty} = \frac{\text{hashrate} * 600}{2^{32}} = \frac{552.76 * 600 * 10^{18}}{2^{32}} \approx 77.22T$$



According to the presented image, the difficulty was equal to 83.127 that day which is different from our calculated number.

The difficulty of the network is updated every 14 days to create an average block in 10 minutes. According to the photo below, the last hard update was on March 28, so this difference was created during this period due to the difference in the hash rate of the network.



B) Assume that on this date, all the processes were done by Antminer S21 miner devices with a processing power of 200 terahertz per second and a power consumption of 3550 watts. What is the electricity consumption of the entire bitcoin network on this day? Compare this amount of consumption with the amount of daily electricity consumption in different countries and see how much electricity Bitcoin has consumed in which country?

$$\text{power consumed} = \frac{552.76 * 10^{18}}{200 * 10^{12}} * 3550 \approx 9,811,312,500$$

$$\frac{9,811,312,500 * 24 * 365}{10^{9}} \approx 85,947 GWh/yr$$

It is almost equal to Finland .

Q2

As we know, mining pools are a virtual place where a community of miners combine the computational power of their devices to increase their chances of profitability in mining. Generally, in mining pools, miners receive rewards in two ways: finding a new valid block and finding a block close to the valid block. The definitions of these rewards are as follows:

- Reward for finding a valid block: Each miner who finds the next valid block and submits it to the mining pool's central node receives their reward.
- Reward for finding a block close to the valid block: Miners can also receive a reward by submitting a block with a specified lower difficulty level compared to the actual valid block. (For example, if the valid block has a minimum of 77 leading zeros, nearby blocks could have a minimum of 70 leading zeros). The computational power contributed by miners participating in the pool is measured using this mechanism, and they are rewarded accordingly.

A) Can miners, after finding the next block, withhold it from the central node and instead announce it themselves to claim the entire block reward? Explain. (5 points)

When a miner cooperates with a mining pool, it is not possible to take the transaction fee for himself because in the creation of the hash of each puzzle hash solved for a mining pool, there is the merkel root of all transactions inside the block whose coinbase transaction is specified by the mining pool. which includes the address of the pool wallet and if any changes are made to the address of this transaction, the obtained hash will change and most likely become invalid.

B) One action miners could take is to only report blocks close to the valid block to the central node. Discuss the impact of this and propose a solution to address this issue. (10 points)

Yes .

Miners can report only the blocks close to the valid block and record their processing share in the system.

The problem that this issue causes is the reduction of the overall reward of the pool, which causes the reward of individual miners to decrease.

In order to solve this problem, pools can put verification methods for their miners. Also, in a considerable period of time, with the help of statistical methods, a miner who does not report the valid blocks found can be identified with a good probability and banned from the pool.

C) Can miners share the valid blocks they find with each other and receive multiple rewards from the central node for finding the same block? If not, explain why they cannot. If yes, propose a solution to address this issue.

NO .

Miners cannot directly share valid blocks with each other and receive multiple rewards from the central node for the same block. Here’s why:

- Central Node Verification: The central node independently verifies each submitted block. If multiple miners claim the same valid block, the central node will recognize only one submission.

- Unique Block Identification: Each valid block has a unique cryptographic hash. Duplicate submissions are easily detected. Reward Distribution: The central node ensures fair distribution by awarding rewards based on the miner’s contribution (shares submitted) to finding the block.

Q3

As we learned, we can model block mining in Bitcoin using the Poisson process.

A) For what types of problems is the Poisson process used for modeling, and why is it suitable for modeling block mining? (5 points)

The Poisson process is used to model the occurrence of events in time or space, where the events occur independently of one another and at a constant average rate. It is suitable for modeling block mining in Bitcoin because:

- The mining of new blocks can be considered as a series of independent events.
- The rate of block mining is roughly constant on average, determined by the total computational power of the network.

B) Prove that the time intervals between mining two blocks are independent random variables with an identical exponential distribution with the rate λT in a Bitcoin network with total computational power λ. (10 points)

We know that in order to be iid, the following equations must hold:

$$F_X(x) = F_Y(x) \quad \forall x \in I$$

$$F_{X,Y}(x, y) = F_X(x) \cdot F_Y(y) \quad \forall x, y \in I$$

We also know that the mining of blocks in the blockchain follows the Poisson process, which will have a Poisson distribution, and as a result, the time interval between two events in the Poisson distribution follows an exponential distribution, so if Fx is the time interval between the mining event of two blocks and Consider Fy as the time interval between the mining of two other blocks, both follow the exponential distribution, and as a result, the following relationship:

$$F_X(x) = F_Y(x) \quad \forall x \in I$$

According to the memoryless property of the Poisson process, the probability of event B is independent of the time elapsed before event A. Therefore, P(B) is independent of the value of x, and we can write:

$$P(X = x, Y = y) = P(A) \times P(B) = P(X = x) \times P(Y = y)$$

C) In a Bitcoin network with total computational power λT, let miners A and B have computational powers λA and λB, respectively. They both start mining for the next block simultaneously. What is the probability that miner B finds the next block before miner A? (10 points)

$$P(A<B) = \int_0^\infty \int_0^b p(A<a) * P(B>b) da * db = \int_0^\infty \lambda_B e^{-\lambda_B b} \int_0^b \lambda_A e^{-\lambda_A a} da * dx =$$

$$\int_0^\infty \lambda_B e^{-\lambda_B b}(1-e^{-\lambda_A b})db =$$

$$\int_0^\infty \lambda_B e^{-\lambda_B b} db - \int_0^\infty \lambda_B e^{-(\lambda_B+\lambda_A)b} db = 1 - \frac{\lambda_B}{\lambda_A+\lambda_B} = \frac{\lambda_A}{\lambda_A+\lambda_B}$$

Q4

Let X be a random variable that follows a geometric distribution with probability p of success. The geometric distribution is defined as follows.

$$P(X=k) = (1-p)^{k-1} * p \qquad \text{for k = 1, 2, 3, ...}$$

$$\text{Mathematical hope and variance of random variable of geometric distribution are resp}$$

$$= \frac{1}{p} \text{and } Var(X) = \frac{1-p}{p^2}$$

$$\text{Given the constant c} > \text{1, use the Markov, Chebyshev, and Chernov inequalities to provide an up}$$

$$p(X > cE(X))$$

$$\text{Markov's inequity} = p(X \geq a) \leq \frac{E(X)}{a}:$$

$$p(X \geq cE(X)) \leq \frac{E(X)}{cE(X)} = \frac{1}{c}$$

$$\text{Chebyshev's inequity} = p(|X-E(x)| \geq a) \leq \frac{Var(X)}{a^2}:$$

$$p(|X-E(x)| \geq (c-1)E(X)) \leq \frac{Var(X)}{((c-1)E(X))^2}$$

$$p(X \geq cE(X)) = p(X-E(X) \geq cE(X)-E(x)) =$$

$$p(X-E(X) \geq (c-1)E(X)) \leq p(X-E(X) \geq (c-1)E(X))$$

$$+ p(E(X)-X \geq (c-1)E(X)) = p(|X-E(x)| \geq (c-1)E(X))$$

$$\implies P(X) \leq \frac{\frac{1-p}{p^2}}{((c-1)\frac{1}{p})^2} = \frac{1-p}{c^2-2c+1}$$

$$\text{Chernoff's inequity} = p(X \geq a) = p(e^{sX} \geq e^{sa}) \leq min_s \frac{E(e^{sX})}{e^{sa}}$$

$$E[e^{sX}] = \sum_{k=1}^{\infty} e^{sk} * p(1-p)^{i-1} = \frac{p}{1-p} \sum_{k=1}^{\infty} e^{sk} * (1-p)^k = \frac{p}{1-p} \sum_{k=1}^{\infty} (e^s * (1-p))^k$$

$$\text{regaurding}: \sum_{k=1}^{\infty} a^k = \frac{a}{1-a} \implies E[e^{sX}] = \frac{p}{1-p} * \frac{e^s(1-p)}{1-e^s(1-p)} = \frac{p * e^s}{1-e^s(1-p)}$$

$$\implies p(X \geq cE(X)) \leq min_s \frac{\frac{pe^s}{1-e^s(1-p)}}{e^{\frac{sc}{p}}}$$

Q5

Consider a blockchain that uses a balanced binary Merkle tree to manage transactions in each block. The blockchain is designed to dynamically adjust the block sizes based on the network's needs, allowing for an efficient and scalable transaction verification process. Suppose the number of transactions in a block follows a Poisson distribution with a mean of λ = 20 transactions per block.
A) Statistical Distribution of Merkle Tree Depth: Given that the blockchain adjusts its block sizes based on the number of transactions, and assuming that each block is represented as a balanced binary Merkle tree, calculate the expected depth (D) of the Merkle tree. Assume that the depth of a Merkle tree with one transaction (a single node) is zero. Provide a formula for the calculation (no need to simplify the final formula).

$$\sum_{n=1}^{\infty} e^{-20} * \frac{20^n}{n!} * \log_2 n \approx 4.27858$$

B) Probability of Verifying a Transaction with a Given Depth: Consider a transaction in a block. Calculate the probability that verifying this transaction requires interaction with a Merkle tree of exactly depth D = 4. Assume that the verification process for a transaction involves receiving all sibling nodes along the path from the transaction leaf to the root of the Merkle tree (all transactions are at the leaves).

In order to need a tree with a depth of 4, we need to have 2^4 to 2^5-1 transactions

$$\sum_{n=16}^{31} e^{-20} * \frac{20^n}{n!} \approx 0.835$$

Q6

In a scenario where the Bitcoin blockchain sees a rapid increase in the number of transactions and participating miners, challenges for consensus can arise. Check any of the following:

- Scalability: How does increasing the rate of block creation affect the stability and security of the PoW consensus?

  By increasing the transaction rate of the network, the transaction fee increases to be placed in the next block faster and the stability of the network decreases. On the other hand, You have to wait longer to be in the block and confirm it. The communication problems in the Internet and the decentralized nature of the Bitcoin network make it more difficult for this network to reach consensus. This becoming more difficult and increasing the number of miners in the network causes several miners to find the next block almost at the same time and create a fork in the network. This same phenomenon can lead to double spending attack and waste of network resources on another branch. This can cause the creation of orphan blocks in the network.

- Chain splits: What potential problems might occur if rapid growth leads to frequent chain breaks and reorganization?

  This issue can cause double spending because the transactions that were considered valid at the beginning may be forked and no longer remain in the blockchain.

On the other hand, the process of recognizing the longest chain becomes more difficult for network nodes and increases the delay in the network and also reduces the effectiveness of honest nodes.

- Concentration of Miners: How can the arrival of a new stream of miners with significant resources lead to concerns of concentration and how does this affect consensus?

  With the increase in the number of centralized miners in the network, network decisions may fall into the hands of miners with stronger resources. And in fact, the practical chance of miners who have low processing power is close to zero, and this issue of decentralization practically disappears. which can ultimately increase the risk of 51%attack.

Q7

One of the basic theorems in distributed systems is CAP Theorem. According to the above theorem, in a distributed system that has the task of maintaining data, among the features of Consistency, Availability and Partition Tolerance, only 2 features can be established simultaneously in the system in question.

A) Explain each of the 3 features of Consistency, Availability and Partition Tolerance.

- Consistancy: It means that all clients, regardless of which node they are connected to, can see the same data at the same time. To do this, the data placed on one node must be sent quickly to all other nodes in the network.

- Availablity: It means that even if one or more nodes fail, it is still possible to respond to the client by other network nodes. That means all nodes will return the same response for a request.

- It means that the system can continue to work regardless of the number of communication interruptions or communication failures between two nodes.

B) Explain why the third feature cannot be selected by choosing both of the three features established.

According to the CAP theorem, in the presence of network partitions (partition tolerance), a distributed system can only achieve either consistency or availability, but not both simultaneously. The reason for this trade-off is as follows:
If you choose consistency and partition tolerance:
You cannot have availability because during a network partition, some nodes will be unavailable to ensure consistent data across all remaining nodes. In other words, to maintain consistency, the system must stop serving requests from the partitioned nodes to prevent divergent data states.
If you choose availability and partition tolerance:
You cannot have consistency because during a network partition, different nodes may return different values to maintain availability, leading to inconsistency. The system must prioritize serving requests from all nodes, even if it means returning stale or inconsistent data, to maintain availability.

C) Explain the relationship of CAP Theorem with the Bitcoin network. In your opinion, which of the mentioned features are present in the Bitcoin network?

In the context of the Bitcoin network, the CAP theorem's properties can be analyzed as follows:
Consistency:
The Bitcoin network prioritizes consistency by following the longest valid chain rule. All nodes eventually converge to the same state (blockchain) once network partitions or reorganizations are resolved. Transactions on the shorter chain become invalid, ensuring consistent data across the network.
Availability:
The availability property may be compromised during network partitions or reorganizations in the Bitcoin network. Specifically:

- During a temporary network partition, some nodes may be unavailable to maintain consistency across the remaining nodes.
- After a reorganization (chain split), transactions on the shorter chain become invalid, leading to temporary unavailability until the longer chain is accepted.

Partition Tolerance:
The Bitcoin network is designed to operate even if there are network partitions or nodes fail. This property is a fundamental requirement for a decentralized system like Bitcoin.
Given the trade-offs dictated by the CAP theorem, the Bitcoin network prioritizes partition tolerance and consistency over availability.