Janani Sundaresan – 30575389 – js10n18

1 NUMBER OF BITCOINS

There will be a maximum of 21 million Bitcoins. A block is mined every 10 minutes. The initial reward for a mined coin is 50 Bitcoins. The reward is halved every four years. 6 blocks/ hour * 24 hours/day * 365 days/year * 4 years per cycle = 210,240 (approx. 210,000). So reward is halved every 210,000 blocks until the rewards will be less than the lowest unit value of a Bitcoin (Satoshi). The rate will continue halving, to 25, 12.5, 6.25, and so on. the smallest fraction is0.00000001. Sum of all the block rewards: 50BTC + 25BTC + 12.5BTC... + 0.00000001 = 100BTC. Therefore, 210,000 * 100 = 21 million total Bitcoins possible.

2 LAST BITCOIN

The last bitcoin will be mined in the year 2140. After mining 31.44 million blocks or 2,099,999,997,690,000 satoshis, 21 million bit coins would have been issued. After the last bitcoin is mined, the blocks will no longer contain new bitcoins. The miners will be rewarded only based on transaction fees. 97% of bitcoin is 20370000. Since bitcoin mining started in 2009 and it would end in 2140, there are 131 years between. So, in a year approximately 160305.343 BTC would be mined. So, 97% of bitcoins would be mined at this rate in the year 127.07th year since its inception which would be 2136. Therefore, in the year 2136 the 97% of bitcoin would be mined.

3 PROPERTIES OF HASH FUNCTION

The security properties of Hash Function make it harder for the miner to solve a puzzle.

Collision Free: It ensures the hash of a specific number is never equal to hash of another part. Impossible for two transactions to have same hash value. Given an input ‘a’, it should be difficult to find a different input ‘b’ such that hash(a) = hash(b).

Hiding: A hash function H is hiding if: when a secret value ‘r’ is chosen from a probability distribution that has high entropy, then a given H(r||x), it is infeasible to find x. || means concatenation of two strings.

Puzzle Friendly: . It is puzzle friendly and all transactions are encrypted. For all probable output value ‘b’, if ‘m’ is chosen from a very high spread of probability distribution, then it is not feasible to find the value ‘a’ such that hash of m+x=a. Impossible to say if it is a hash of 10Gb of data or one line of data.

4 TYPES OF FORKS

4.1 Stale Block

When a block is solved, all miners should stop working to find a solution to the hash puzzle of that block.Once the block is solved, the pool will not check whether another miner solved that block because it is considered to be "stale block". When we reduce the block time, there will be more stale blocks. In order to prevent the block from becoming stale, we have to wait for several confirmations which ensures your transactions are not in stale block.

4.2 Soft Fork

A softfork is a change in the bitcoin protocol and which can be reversed.e.g. is Pay-to-Script-Hash feature. The old nodes can push new blocks to blockchain network as long as they follow the new bitcoin protocol. But if they push a block that is not within the new bitcoin protocol, the new nodes will reject the blocks thereby forcing the old nodes to update their protocol policy.

4.3 Hard Fork

Bitcoin is made of two pieces: Bitcoin protocol and Blockchain. There may arise situations where a group of developers disagree the path taken by bitcoin updates or the miners disagree if the

updates to bitcoin protocol might end of causing a dip in the rewards they receive. Under these circumstances, a group of miners can chose to go on their own and fork the blockchain. These updates to bitcoin protocol are not backward compatible. They copy the bitcoin protocol code and start making updates to it in the way they desire. They come to a consensus as to when the block would go active. When that block number is reached, the miners/developers are split into two groups. Some join hands with the original bitcoin protocol and others join the new fork. Each group adds blocks to their respective groups they decide to support and the two blockchains become incompatible from that point. Hard forks are announced beforehand so that people who have invested money can gain maximum benefit. There are two types of hard fork: Planned Hard Fork and Controversial Hard Fork.In Planned Hard Fork, the miners would upgrade at their own volition to the new bitcoin protocol or continue with old bitcoin protocol. If there is a Controversial Hard Fork, the bitcoin protocol is forked into two incompatible blockchains, with their own groups and miners would continue to mine following the bitcoin protocol which is more suitable to them. Since fork is based on the original blockchain, the old transactions from old blockchain are also copied into the new fork.

5 DOUBLE - SPENDING

5.1 Double Spending

Paying more people with the exact same digital currency on more than one transaction is called double spending. It is the process of using the same set of bitcoins in more than one transaction. It has been the major road block when it comes to digital currencies. Bitcoin Network prevents bitcoins from double spending by thoroughly verifying each and every transaction within the bitcoin blockchain. Maximum of only 21 million bitcoins can be produced. Every transaction goes into transactions pool. For example, if a user with one bitcoin, makes two transactions of 1 Bitcoin, each transaction is taken from the pool and checked for validity before being added to block. The first transaction is valid since user had one bitcoin. The second transaction is invalid since he has no bitcoins left. Each transaction usually waits for 6 confirmations before it is considered to be complete. So, if both transactions are processed by two different branches at same time, the transaction that gets the first confirmation will be considered as valid transaction.

5.2 Bitcoin Network Consensus

Blockchain keeps a record of all transactions made using Bitcoin by miners. If anyone attempts to duplicate the transaction, the hash of the block changes which in turn changes the hash of the previous blocks thereby leading to a deadlock situation in arriving at consensus. This fraudulent activity would be identified and the original blocks in the chain would reject the transaction and deem it as counterfeit and block the process. This ensures only valid transactions are propagates across and unsecured or duplicate transactions are blocked at the very first node which receives them. Bitcoin achieves consensus through Proof of work. The miner should solve a computationally intensive mathematical puzzle to add a block in the network. Then he broadcasts the block to the network [d]. More than 50% of the nodes in the network should validate the block and then it will be added to the blockchain.

6 MINER TASKS

6.1 Routine Tasks of Bitcoin Miner

Miners are special nodes who hold a copy of ledger, verify and validate all transactions happening in the block.

- Collect transactions in memory pool,
- Select transactions from memory pool and mine block.

- Listen for new transactions and for new blocks mined by other nodes.
- When a new block is received, it is validated. The miner also removes the transactions which were included in the newly created block, from the memory pool. Only unconfirmed transactions are available in the memory pool.
- The miner constructs a candidate block with unconfirmed transactions.
- If miner finds the value for the nonce, solution to POW, block becomes valid.

6.2 Strategic Considerations of Miner

Block withholding - When a miner finds a block, he does not broadcast it to the network. He withholds the block and tries to find another block. If he is successful, when a new block is added, the miner broadcasts his two blocks, thus making his chain longest.

Join mining pools - To improve chances of mining, miners join their collective computational power and form pools. On winning the profit is shared with all miners. The share is proportional to computational power contributed to mining.

6.3 51% Attack

"An attacker with more than half of the total computing power in the entire P2P network can manipulate transactions maliciously. This is referred to as a 51 % attack" [a]. it is possible if hackers have access to large computing power which gives them ability to reverse the transactions in the blockchain and use same cryptocurrency twice. The attack takes place on cryptocurrency exchanges. 51% Attack on bitcoin and Ethereum is not easy due to their large size however small cryptocurrencies are easy prey to these. If a participant has resources to control 51% of the nodes to reach consensus or enough hash power to take over longest chain, the block creation can be manipulated. It can lead to selfish mining - they have computational advantage. They can keep mining on top of their blocks without letting the network know and collect all rewards. Blockchain becomes too big - they can add more blocks to their chain thus always having the longest chain.

7 BOTTLENECKS OF BITCOIN SYSTEM

Every block has a limit of 1MB. It takes 10 minutes to mine a block. So, there is a limit to the amount of transactions that can be added into the block. Though several 1000 transactions can be made in 10 minutes, only 2000 to 3000 transactions can be added in a block. So remaining transactions can be confirmed only in the next block or have to wait for blocks coming later. Another bottleneck is storage. The size of the blockchain continually grows over time. Also, addition of every block to blockchain increases the time required for a full-node to join the network. So, fixes/changes can only happen when everyone agrees.

8 BLOCK INFORMATION

Increase in block size will enable more transactions to be added in the block. It leads to increase in block propagation time since it takes more time for the block to be broadcasted across the network. Hence the nodes near the center of the newly created block starts mining well before the nodes in the edge of the network. New blocks might be created by edge nodes before they learn about the latest block added to blockchain. This leads to increase in the number of forks. Blockchain takes time to converge into one main chain because it depends on the computational power. In the meantime, the length of the forks increase. When one fork is merged into the blockchain, the blocks in other forks becomes orphan blocks or stale blocks. The increase in stale rate leads to double spending thereby weakening the security of the chain. Decrease in network difficulty decreases block generation interval. This increases the size of the blockchain.

9 POOLED MINING

The pooled mining is a concept where hundred to thousands of miners based on specific pool-mining rules. Advantages include - The difficulty target is very easy compared to the difficulty target in case of solo mining. There is no risk of running out of juice. Disadvantages include - Hashing Power increases every year and the growth has been humongous since it's inception and still increasing mainly due to heavy competition between the miners. Difficulty level increases as a function of hash power.

9.2 Distribution of Block Reward

A difficulty target is set for getting a share in a pooled mining. Whenever any miner solves a block, the reward is shared among all the miners in the pool proportional to the computing power and resources they contributed towards successfully solving the block. Reward is paid to the pool bitcoin address directly and not to miners. Pooled mining distributed the reward to in's miners in three ways.

9.1 Pay Per Share

The miners get rewarded for each share they contributed irrespective of the rounds. This mechanism solves the problem of delay in submission of shares by the miners. The miner can estimate their rewards. But if the pool is unsuccessful in mining a block for a period of time, the miners should still get paid. Hence the pool operator should estimate mining failure. He should have sufficient funds to pay for the miners. A fixed price is associated with each block/share that is solved. The payout is from the pool's current balance. Miner can withdraw the cash instantly and need not wait for the block to be confirmed. Advantage lies with miners since they have least variance and the risk is all transferred to pool. The pool compensates this risk by setting a payout to miner which is less than the reward expected for solving a block.

9.2 Pay Per Last N Shares

This is the most common reward sharing mechanism. The miner gets more payouts then in PPS mechanism. But it is difficult to estimate the income. Payouts are based only on the blocks found and the miner's reward is proportional to the number of shares he contributed towards the full solution. Miners join pool with more hash power to get more payouts. This method has the highest payout and advantageous especially for miners who want to make fast cash. There will be a lot of fluctuations in a window of 24 hours.

9.3 Proportional mechanism

The time between two successfully mined blocks is called round. The miners get their reward according to the computational power contributed by them in each round. The number of shares submitted by a miner in a round can be counted. So, the reward for each share depends on the length of round. It causes delay in submission of shares by the miner increases the reward. If more miners withhold shares, it leads to increase in consumption power. Also, more shares are submitted if the round takes longer time thereby reducing the profitability of miners.

10 TRANSACTION FEES

The dominance of transaction fees over rewards would happen gradually till the year 2140 when the last bitcoin would be mined. Since smallest fraction of bitcoin is 0.00000001, trading can be done. Otherwise fees will be very high to meet the computational power demands leading to decrease in use of Bitcoin. This will discourage miners who might then move on to mine alternate coins leaving the bitcoin ecosystem. This will further decline the value of bitcoin and its usage.

In future, Transaction fee can be reasonable if,

1. Digital currency is used predominantly
2. Mining technology improves
3. Mining can be done in energy efficient way

There is no risk in the transaction except if you forget your wallet passkey and mnemonic key then it won't be recoverable.

REFERENCES

[a] J. Bae and H. Lim, "Random Mining Group Selection to Prevent 51% Attacks on Bitcoin," 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Luxembourg City, 2018, pp. 81-82.

[b]Rosenfeld, Meni. (2014). Analysis of Hashrate-Based Double Spending.

[c]Mastering Bitcoin, by Andreas M. Antonopoulos

[d] Torun, Abdulvahit. (2018). Geodata Enabled Hierarchical Blockchain Architecture for Resolving Boundary Conflicts in Cadastre Surveys and Land Registration.