Bitcoin: A Peer-to-Peer Electronic Cash System
Review by Abhishek Dalvi (50320110)

The primary motivation for Bitcoin is to have a system where the financial transaction doesn't involve a 3rd party that charges a transaction fee. Satoshi Nakamoto proposes Bitcoin, a peer-to-peer electronic cash system, which is an ingenious integration of existing protocols and algorithms.

The paper shows how transactions can be made using an electronic coin, a chain of digital signatures. The sender hashes the previous hash and the recipient's public key and adds this to the end of the coin. In such a setting, it is not possible to detect double-spending, i.e, spending the money more than once. The traditional way of solving this is by having a mint-based system, a 3rd party that oversees all the transactions; which Nakamoto wants to avoid. To solve this problem, Nakamoto proposes a method where all the transactions are publicly announced so that all nodes can agree to only one history of the transaction order using a time-stamped server. A timestamp server takes the hash of the block contents and the previous block's hash. This hash is then published publicly, and this process repeats. Therefore, due to this chain-like hashing, the transaction history is reinforced with every timestamp.

Bitcoin uses a proof of work consensus. In bitcoin, the proof of work task is to find the correct nonce in a block such that when the block is hashed, the hash begins with a certain number of zeros. The proof of work puzzle should be challenging for the algorithm to work correctly(increasing the number of zeros increases the difficulty). Unlike Paxos, there isn't any majority quorum; all the nodes try to find the valid nonce, and when a node finds the correct nonce, the hash of the block is broadcasted. The commit in Nakamoto consensus is just broadcasting the puzzle solution, other nodes might or might not acknowledge this. Therefore, the Nakamoto consensus is not deterministic but is a probabilistic commit. Hence, FLP impossibility results and coordinated attack impossibility results do not apply in the Nakamoto consensus (This was mentioned in class).

The assumption of an honest node is problematic, and to circumvent this problem, the concept of incentive has been introduced to bitcoin. There are two incentive mechanisms in bitcoin.

1) Coin generation incentive:-
   When a node creates a block, it also gets a special coin creation transaction, and usually, the transaction recipient is the block creator's address. However, a dishonest node can create a block with invalid transactions, but the new block must be on the consensus chain for the coin generation process—this one way to reinforce against double-spending. The incentive for Bitcoin started with 50 coins and is reduced by 50%, approximately after every four years. As of now, the incentive is currently 6.25 coins.

2) Transaction Fees:-
   The transaction creator can make the output value of the transaction less than the input value. The difference between these values is the transaction fee, which goes to the block creator. This is a voluntary fee that the transaction creator can make.

The coin generation incentive will end because there is a limit on the number of bitcoins that can be mined i.e, 21 million. When the coin generation limit of 21 million is reached, transaction fees might become mandatory to ensure a good quality of service for a transaction. One cannot give the exact prediction of the outcome when the coin generation incentive ends due to the scale of the system. However, one can view the users as players and can use Game Theory to predict the final outcome. There are certain speculations that using such an approach might predict the final outcome, but this is still a very open research question. I think that the system is currently in a Nash Equilibrium, which means that every player plays their best strategy knowing every other player's strategy. When the coin generation incentive ends the Nash Equilibrium may not destabilize at all, but the outcome of the system could be dependent on making the Transaction Fee mandatory:-

1) Transaction Fee becoming mandatory right now(in 2020):- Miners will keep on mining because they will have at least one incentive irrespective of the number of coins mined.

2) Transaction Fee becoming mandatory when coin limit is reached(in the year 2140):- Miners will adopt a better strategy, i.e a probabilistic strategy. Miners will turn off their system with a higher probability($P\{X:1\}=0.8$) or miners will mine(use computational resources) with a lower probability($P\{X:2\}=0.2$). As we approach the coin limit, P1 will increase and P2 will decrease as there is less incentive.

The paper demonstrates really simple but clever ways to circumvent problems in a peer-to-peer distributed system. It is an innovative integration of existing methods which results in a near-full proof system. One thing which I like about the paper is the simplistic approaches to circumvent problems that are used to save space and to verify transactions. To save space, one simply has to prune off the spent transactions in the Merkel Tree. This is a very simple, yet effective way to save disk space without breaking the hash chain. Another simple approach used in the algorithm is used to verify that a transaction is a part of the block. To verify, one would need the transaction details and hash values of higher-level(parent) non-branches in the Merkel Tree. There is no need to go through the whole Merkel Tree to verify transactions.

In the calculations section, Satoshi Nakamoto hasn't clearly explained why he/she/they have used a Poisson Process, which considers continuous random variables. The derivation shows that double spending is very unlikely in a blockchain because it is difficult for the attacker to catch up

with the other part of the fork. It turns out that the derivation is an approximation but is an excellent approximation. If one closely looks at the problem, this is a classic example of a sequence of independent Bernoulli trials. The attacker has to find the correct nonce for the block; ergo, each attempt to find the correct nonce is an independent Bernoulli trial with binary events: the valid nonce(1) and the invalid nonce(0). The attacker keeps on trying to get the valid nonce after every unsuccessful attempt. Hence we observe this sequence of unsuccessful attempts, i.e., 'r' unsuccessful trials, followed by a successful attempt. In such cases, the Negative Binomial Model is used. Since solving the puzzle or getting the correct nonce is a really hard problem, Nakamoto approximates the number of attempts to a huge number, hence, $r \to \infty$. When $r \to \infty$, the Negative Binomial Model converges to a Poisson distribution.

$$\text{Poisson}(\lambda) = \lim_{r\to\infty} \text{NB}\left(r, \frac{\lambda}{r+\lambda}\right).$$

https://en.wikipedia.org/wiki/Negative_binomial_distribution#Poisson_distribution

Blockchain is majorly only used and suitable for cryptocurrency, and new applications should be explored. As of now, the only potential applications are smart contracts. One industry where smart contracts are promising is in the music industry, where this algorithm is perfectly suited for music royalty deals. When it comes to bitcoin's future, it is challenging to have a long-term prediction about it. As mentioned before, Game Theory predictions could be a possible way to predict long term behavior. Perhaps, concepts like these could also predict bitcoin prices as they related to the players' behavior.