Student ID: **32864477** Full Name: **Supritha Konaje** Username: **ssk1n21**

COMP6212 Computational Finance 2021/22

Solutions to the Bitcoin Protocol Assignment (25%)

1. **What is the maximum number of Bitcoins? How is this calculated? [2 marks]**
   - The maximum number of Bitcoins that can be created is 21 million.
   - The reward for mining a bitcoin will be halved every 4 years and it can be calculated in the given way:
     - In 10 minutes – 1 block (It is said that every 10 minutes, 1 block is mined)
     - In an hour – 6 blocks will be mined; In a day – 24 * 6 = 144 blocked per day
     - In a year – 365 * 144 = 52560; In 4 years – 4 * 52560 = 210240 ~= 210,000
     - 210,000 blocks same reward and after that the reward is halved. Sum of the block events: 50 + 25 + 12.5 + 6.25 + …… + 0.000000001 = 100
     - Hence, when we multiply, 100 to the blocks mined in 4 years is approximately equal to 21,000,000 (21 million).
     - 1 Satoshi = 0.000000001 BTC which is the monetary unit of Bitcoin.

2. **If, on average, it takes 10 minutes to mine a block, when will the last Bitcoin be created? When will 98% of Bitcoin be mined? How is this calculated? [2 marks]**

   The predicted year to mine the last bitcoin is 2140. The number of coins that will be mined after the 5th halving event that will take place in the year 2028 is 20, 343,700 and after the 6th halving event that would be in the year, 2032 will be 20,671,825. The difference in the coins between the 5th and 6th halving period = 236,300 BTC.

   Dividing 236,300 BTC into rewards per block based on the reward rate of 5th halving is 1.5625. Number of blocks present = 151,232. So, 151,233 is the block after the 6th halving period.

   Since 151,232 is less than the size of the block 210,000. Hence, 98% of bitcoin will be mined by 2030 and the number of coins mined will be 20,580,000 which lies between the period between the 5th and 6th halving reward event.

3. **Are the transactions on the Bitcoin network completely anonymous? Why? [3 marks]**

   It has been assured that transaction via bitcoin is secure and anonymous. The transactions are public, but they are linked with a user's bitcoin using an electronic address. So, if we tend to buy anything using bitcoin it will not directly trace out our identity.

   But there is a possibility to trace back the identity using the electronic address which can be termed as a pseudonym. This is used to receive or send Bitcoins. Every transaction that took place so far using Bitcoin is stored in a blockchain. If by chance, our address is linked to our identity then there might be a possibility that our identity will be revealed. If a user makes any purchase using Bitcoin, the time and amount are recorded and if we trace back to a blockchain using that time and amount (after converting it to the exchange rate at the mentioned time), we might get the address of that particular transaction and that will lead to the blockchain in which the transaction details are stored. If an individual knows the user's email id or name, they can easily track down all the transactions and the user's identity. Hence it is said that transactions on the Bitcoin network are not completely anonymous.

   The best practice to secure one's identity is by using different transaction IDs for every transaction. This way, even if one of the transactions is identified other transactions will not be identified.

4. **Who governs Bitcoin? In other words, who defines the rules and writes the code? Briefly explain their roles and power. [6 marks]**

   No one governs Bitcoin. Those who agree to the rules and regulations of the network can participate. The founder widely known as Satoshi Nakamoto introduced the idea of Bitcoin in the year 2018 and launched the Bitcoin network in 2019. It was uploaded in their official bitcoin.org in .rar file. Soon it was moved to GitHub and now it is an open-source project. People are free to modify the official Bitcoin client and there have been many independent implementations according to one's own needs. But the initial rules that were created by Satoshi Nakamoto cannot be changed. It has been improved to a great extent, but everyone must use a

particular software so that it complies with the same rules. It can work only if it works with a complete consensus among all the users.

We have a wallet for bitcoin in which user sends and receives bitcoins. There is a public ledger that contains every transaction ever processed to verify the authenticity and validity of every transaction called the "Blockchain".

Then we can maintain the transactions of two bitcoin wallet that is logged into a blockchain. Bitcoin wallet keeps a secret piece of data called a private key which is used to sign transactions. These transactions are broadcasted to a network, and they usually begin to confirm within 10-20 minutes through a process called mining. It is a distributed consensus system that authorises pending transactions by including them in a blockchain [1]. Transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all the subsequent blocks. No one can control what is written in that block to roll back their expenditure.

5. What is double-spending? How does the Bitcoin network achieve consensus? [5 marks]

Double-Spending is a risk in cryptocurrency in which a user uses the same currency twice. When a transaction takes place, a block is created and each block has a hash number that consists of a timestamp, previous block hash and transaction data. This is encrypted using a security protocol SHA-256 algorithm. Once, this is verified by the miners the next is a completely new block that follows the same procedure as before. When a hash is verified, a bitcoin is awarded to a miner.

There can be intruders in this procedure, where they try to forge a block with special functions and replace this with the original block which out-spaces the creation of the blockchain. To double-spend, they need to introduce it to the network and the network would identify it as a new block. The intruder can award themselves with cryptocurrency and then it can be used again.

To maintain an honest environment in the nodes of the network, a consensus agreement is used. It is a fault tolerance mechanism among distributed processes or multi-agent systems. The bitcoin blockchain is maintained by Proof of Work (PoW) which uses a high-powered computation power to solve a difficult mathematical/arbitrary puzzle.

Public blockchains are decentralized and self-regulating on a global scale without any single authority. Contributions are made from many participants who work on authorizing and checking the authenticity of transactions that take place in a blockchain. In this dynamic environment, shared ledgers need an efficient, fair, real-time, reliable, and secure mechanism to ensure all transactions occurring on the network are genuine and all participants agree on the consensus mechanisms which is made a set of rules made by various nodes and transactors of the blockchain [2].

6. What are SegWit2x and Lightning network? Explain their similarities and differences. [7 marks]

As it is known that transaction takes a lot of computational power and because of this it takes a lot of processing speed. SegWit2x is the software upgrade of SegWit which changes the block size limit of the Bitcoin blockchain. It falls under the category of hard-fork which means the previous code will be invalid. There will not be any backward compatibility when a new chain is created by splitting the block. This involves way too much transaction cost.

Lightning Network is a fix for both transaction cost and speeds. It is an additional layer. It does an off-chain transaction in which the affected block is moved away from its original network and then it works on resolving it independently in its layer. They are updated in the main network only when the two parties agree on the channel. Within this period, they can transact as much as possible, and it will not affect the main network.

Similarities: They both speed up the transaction in the main network. It can be used to perform low-cost transactions. Both are predicated on SegWit's code change.

Differences: SegWit2x tends to split in the same network, which will increase the transaction and block size. Lightning Network operates on a different layer and does not affect the main network's transaction size. SegWit2x increases only the capacity of the block size but, the Lightning network not only increases the capacity it also scales the block size. SegWit2x is more secure as compared to the Lightning network.

References

[1] Bitcoin Project, "Bitcoin," [Online]. Available: https://bitcoin.org/en/how-it-works.

[2] J. FRANKENFIELD, "Consensus Mechanism (Cryptocurrency)," Investopedia, 30 November 2021. [Online]. Available: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp.