Student id: 31990401 - **Username:** gg1e20 - **Full Name:** George Giamouridis

---

COMP6212 Computational Finance 2020/21

Solutions to the Bitcoin Protocol Assignment (25%)

Question 1

One block is mined approximately every 10 minutes, so 144 blocks are mined every day. The number of Bitcoins generated per block is decreased with a 50% reduction every 210,000 blocks, a process which is called halving. Since 144 blocks are mined every day, we need 4 years to mine 210,000 blocks. The Bitcoin reward started at 50 BTC in 2009. After the last halving the block reward will be 0 BTC. If we add all these numbers, the maximum number of Bitcoins is:

$$\sum_{n=0}^{\infty} \frac{210{,}000*50}{2^n} = 210{,}000 * 50 * \frac{1}{1-\frac{1}{2}} = 21{,}000{,}000 \text{ BTC}$$

Question 2

Block reward in 2009 was $r(2009) = 50 * 10^8$, so $r(2013) = \frac{1}{2} * r(2009)$ and so on. That means that $r(x+1) = \frac{1}{2} * r(x)$. The last block will reward 0 BTC. So $r(n) = r(0) * (\frac{1}{2})^n = 0$ and the next to last block will be $r(n-1) = 50 * 10^8 * (\frac{1}{2})^n - 1 = 1 \rightarrow \ln(50 * 10^8) + (n-1) * \ln(0.5) = 0 \rightarrow n \approx 33$. That means that there are 33 halvings in total. As a result, the last year will be $2009 + 33 * 4 \approx 2140$. Thus, the last Bitcoin will be created approximately in 2140.

Total Bitcoin circulation is 210m BTC so the 98% is 205.8m BTC. Until the first halving, 144 * 50 * 365 * 4 = 10.512m BTC left to be mined. Next, 144 * 25 * 365 * 4 = 5.256m BTC left to be mined. Next, 144 * 12.5 * 365 * 4 = 2.628m BTC left to be mined. Next, 144 * 6.25 * 365 * 4 = 1,314m BTC left to be mined. Next, 144 * 3.125 * 365 * 4 = 657000 BTC left to be mined. Next, 144 * 1.5625 * 365 * 4 = 328500 BTC left to be mined. Now if we subtract the number of Bitcoins left to be mined in the fifth halving from the total Bitcoin circulation, we get 21,000,000 – 328500 ≈ 205.8m. Thus, the 98% of Bitcoin will be mined at the end of the 5th halving (2032).

Question 3

Bitcoin transactions add a degree of anonymity, but in reality, Bitcoin transactions are pseudonymous and not anonymous. Since Bitcoin's ledger is public, all transactions that stored in it are accessible from anyone. That means that everyone can see each other's address, balance and history of transactions. Bitcoin protocol uses TCP in order for the nodes to be able to broadcast their transactions, and therefore transactions can be tracked and analyzed through the IP addresses. If a Bitcoin address could be linked to a person then all related transactions can be identified. Thus, Bitcoin transactions are pseudo-anonymous and therefore they cannot hide the user's identity and activity.

Question 4

When Satoshi Nakamoto left the Bitcoin project, this was passed to a new development community. Bitcoin protocol is public, and everyone can review and modify it. Although this community is responsible for the protocol maintenance, Bitcoin is not governed either by this community or by anyone else. When a new update is

proposed it is announced publicly and requires approval for the whole community (developers, users, miners) in order to be integrated. No one can force updates and changes to the protocol without the approval of the rest community. At this point it should be noted that a user or a miner can be at the same time a developer, and vice versa. Developers are those who have direct access to the code, so in theory they also have the ability to drop the whole network.

Question 5

Double spending is an issue which allows spending an amount of cryptocurrency more than once. The attacker broadcasts a transaction to the network and starts secretly mining a branch that is built upon the block before the transaction (a transaction which actually pays him). Once the initial transaction is confirmed by the mining pool the merchant sends the product. The attacker continuous the secret mining, and when his chain is longer the attacker publish it. The network identifies the secret branch as the longest chain and the payment to the merchant is replaced by the payment to the attacker. To achieve such an attack the attacker should have at least 51% of the network power.

Bitcoin network achieves consensus through the mining process. Miners provide processing power on the network in exchange for the opportunity to be rewarded in Bitcoin. In order to receive their reward, they must compete to solve a difficult mathematical cryptographic problem. The solution to this problem, called proof-of-work (PoW). Mining is the main process of decentralized settlement of transactions, through which transactions are approved and cleared. Mining secures the Bitcoin system and allows emerging network consensus. Rewarding is an incentive for miners, in order to contribute to the network's security.

Question 6

SegWit2x was a failed Bitcoin hard fork which was proposed in 2007 in order to increase block size from 1mb to 2mb, with the ultimate goal of mitigating the increase of mining fees and improving the transaction time.

Lightning network is an overlay network which operates on top of Bitcoin and uses its features in order to secure its transactions process. It can also operate in other blockchains like Litecoin. The key idea is that transactions don't have to be stored in the blockchain a technique which is called off-chain approach.

Similarities:
Both aim to solve scalability issues (faster transactions). Also, both aim to keep users in the same blockchain. Finally, SegWit2x and Lightning are predicated on SegWit code change.

Differences:
SegWit2x uses block size increase while Lightning uses payment channels and multi-signature addresses to mitigate scalability issues. Lightning is not a fork (as SegWit2x), but an additional network layer. Lightning allows trading from cross platforms (Bitcoin to Litecoin), while SegWit2x does not.

References

- Bitcoin Reward Schedule - https://bit.ly/3uwvZeJ (accessed 02/27/2021)