Student ID: 32672446
Username: hz5g21
Full Name: Han Zhang

1.What is the maximum number of Bitcoins? How is this calculated?
In the process of validating Bitcoin transactions, miners must mine a block. After mining, a block will be added to the blockchain. During this process, miners receive bitcoins as a reward for mining blocks. The Bitcoin protocol stipulates that the number of rewarded bitcoins found in each block starts from 50, and after every 210,000 blocks are found, the reward for finding a block will be reduced by 50%. Eventually, the reward will be reduced to zero. The smallest unit of Bitcoin currently is the satoshi, which is equal to 0.00000001 Bitcoin (BTC). It takes 33 reward era to discover that a block reward is reduced to one satoshi. So the maximum number of bitcoins is $\sum_{i=0}^{i=32} 210000 \times 50 \times (\frac{1}{2^i}) = 20{,}999{,}999.98 \approx 21,000,000$.

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?
The number of bitcoins will reach a maximum value at the end of the 33rd reward period. The total number of blocks found in the 33rd reward period will be 210,000×33 = 6,930,000. If it takes 10 minutes to mine a block, the total time spent to discover all blocks will be 6,930,000×10(minutes per block)/60(minutes per hour)/24(hours per day) = 48125 days.The last Bitcoin will be created on 8th, October 2140, since the first Bitcoin was discovered on 3rd, January 2009.

The number of 98% of bitcoins is 21,000,000×98% = 20,580,000. It is bigger than the total bitcoins by the end of the 5th reward period(2029), which is 20,343,750, and smaller than the total bitcoins by the end of the 6th reward period(2033) which is 20,671,875.the number of blocks created in the 6th reward era will be (20580000-20343750)/1.5625 = 151,200. The total blocks discovered by then will be 210,000*5+151,200= 1,201,200. Thus, the days will be 1,201,200 × 10(minutes per block)/60 (minutes per hour)/24 (hours per day) = 8341.67 days after 3rd January 2009. It is 5th November 2031.

3.Are the transactions on the Bitcoin network completely anonymous? Why?
No, it is not completely anonymous [1].An anonymous transaction is a transaction between two strangers, meaning that no personal information is required, and no transaction records are required. Although the personal information of Bitcoin transactions is encrypted, there is a transaction record. A complete transaction record and the cryptographic identity of each bitcoin user are kept on a public ledger. The researchers found that transactions involving large amounts of bitcoin could be tracked using sophisticated computer analysis, and claim that if paired with current law enforcement tools, it is possible to obtain the information of users. So Bitcoin transactions are thought to be pseudonymous, not anonymous.

4.Who governs Bitcoin? In other words, who defines the rules and writes the code? Briefly explain their roles and power.
Bitcoin is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen[2]. In theory, no one can control Bitcoin. Satoshi wrote the first version of Bitcoin's code in 2009, left the community of bitcoin in 2010. Now, Bitcoin Foundation takes on the role of maintaining and developing the code. But it cannot arbitrarily change the Bitcoin code unless the community agrees on the change. Bitcoin changes are usually through bitcoin improvement proposals. if the community achieves consensus on one particular bitcoin improvement proposal, the Bitcoin Foundation can change the code and

make this version of Bitcoin broadcast on the blockchain.

5.What is double-spending? How does the Bitcoin network achieve consensus?
Double spending is the result of a digital currency being successfully used multiple times in multiple transactions[3]. The Bitcoin network achieves consensus by Proof of Work (PoW). The PoW algorithm makes tasks of moderate difficulty, which can be solved by all miners, easily verified by other nodes. In the Bitcoin network, miners need to compete with other nodes to solve computationally difficult problems to generate new blocks. By broadcasting in the Bitcoin network, two transactions are pulled from the pool at the same time for confirmation, the transaction with the most confirmations will be included in the blockchain and the other will be discarded. The first node to discover a new block will be rewarded after the results are verified by the majority of nodes in the network.

PoW requires a lot of computing power to generate blocks, which makes it impossible to request multiple transactions without justifying the effort made to discover the block. Pow makes it extremely difficult to change any aspect of the blockchain because such a change requires the re-mining of all subsequent blocks. This also makes it difficult for users or user pools to monopolize the computing power of the network.

6.What are SegWit2x and Lightning network? Explain their similarities and differences.
One of Bitcoin's scalability issues is that since the block size of Bitcoin is 1MB, there is a limit to the number of transactions where the network can process per second, which limits network speed. Segwit2 and lightning networks are both protocols for speeding up the network born to solve this problem.

SegWit2x, an alternative to SegWit, is a proposed software upgrade designed to upgrade the block size limit and increase Bitcoin's overall transaction processing speed.SegWit2x was never implemented due to disagreement and lack of consensus. The lightning network is a second layer added to the Bitcoin blockchain that allows off-chain transactions. A Lightning Network is a "layer 2" payment protocol layered on top of a blockchain-based cryptocurrency. It enables fast transactions between two parties. By handling transactions outside of the blockchain Mainnet(layer 1), "layer 2" improves the scalability of blockchain applications.

The similarities between the two methods are to speed up the network speed, and the difference is that sigwit2x improves the overall network speed by increasing the size of the block, while The lightning network works by creating a peer-to-peer payment channel between two parties that allows them to send unlimited transactions that are almost instant and cheap.

References

[1] Edward V Murphy, M Maureen Murphy, and Michael V Seitzinger. Bitcoin: questions, answers, and analysis of legal issues. Library of Congress, Congressional Research Service, 2015.

[2] Bill Maurer, Taylor C Nelms, and Lana Swartz. "when perhaps the real problem is money itself!": the practical materiality of bitcoin. *Social semiotics*, 23(2):261–277, 2013.

[3] Ghassan O Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, and Srdjan Čapkun. Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Transactions on Information and System Security (TISSEC)*, 18(1):1–32, 2015.