Student ID: 29466423
Username: rsb1g17
Full Name: Rohan Bungre

COMP6212 Computational Finance 2020/21

Solutions to the Bitcoin Protocol Assignment (25%)

1 What is the maximum number of Bitcoins? How is this calculated?

The maximum number of Bitcoins hardwired into the Bitcoin protocol is 21 million. Assuming that an average block is mined every 10 minutes and the initial 50BTC reward is halved every 4 years; the total number of Bitcoins can be calculated as the sum of a geometric series.

$$\sum_{n=0}^{\infty} \frac{blocks\_per\_4\_years \times initial\_reward}{2^n} = \sum_{n=0}^{\infty} \frac{210000 \times 50}{2^n} = \frac{210000 \times 50}{1 - \frac{1}{2}} = 21000000 \tag{1}$$

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?

Assuming it takes 10 minutes to mine a Bitcoin and the reward halves every 4 years starting at 50BTC, the last Bitcoin will be created in the year 2140, approximately 3rd January 2140. 98% of Bitcoin will be mined by the year 2032, approximately in 2030. These dates can be calculated using an exponential halving formula.

$$\frac{start\_value}{2^n} = end\_value \rightarrow n = \log_2 \frac{start\_value}{end\_value} \tag{2}$$

The last Bitcoin will be created in the year when the block reward falls below 1 Satoshi (1×10^{-8} BTC). This is because 1 Satoshi is the smallest currency in the Bitcoin Protocol. This will happen after $32.2 \approx 33$ halves, 132 years after the first block was mined in 2009, which is 2140.

$$n = \log_2 \frac{50}{1 \times 10^{-8}} = 32.2 \approx 33 \tag{3}$$

98% of Bitcoin will have been mined when the block reward falls to 2% of its original value. This will happen after $5.64 \approx 6$ halves, 24 years after the first block was mined in 2009, which is 2032.

$$n = \log_2 \frac{50}{50 \times 0.02} = 5.64 \approx 6 \tag{4}$$

3 Are the transactions on the Bitcoin network completely anonymous? Why?

Transactions on the Bitcoin network are not completely anonymous, they are in fact pseudo-anonymous meaning that transactions are not linked to real-world entities but rather bitcoin addresses. Owners of bitcoin addresses are not explicitly identified, but all transactions on the blockchain are public. Although the user's wallet address is generated randomly and can be changed per transaction, some retailers and wallet vendors will require personal information. This means that there may be at least one user address with a personal link. This personal link could also be in the form of an IP address. It is possible to cluster these different addresses used by a single user, meaning if just one address in the cluster is compromised anonymity is lost. Although transaction data is fed through a random set of network nodes, if several nodes within the network can be analysed, the combined data collected from these different nodes might be enough to determine where a transaction originated from. There have been attempts to anonymise the network using VPNs and Mixers, however the public ledger and network structures often prevent true anonymous behaviour.

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

Bitcoin is a decentralised system meaning there is no central authority controlling it. With no central servers and no central storage, the Bitcoin ledger is publicly distributed and maintained by a network of equally privileged miners. The Bitcoin source code and initial protocol was created as an open source project by Satoshi Nakamoto. Due to its open source nature anyone can create their own Bitcoin implementation that interacts with the network. There is a core team that maintain the most popular implementation 'Bitcoin Core' which runs on 96% of the network's nodes. This core team updates the software and removes bugs found within the code. These developers can improve the software but they can not force a change in the rules of the Bitcoin protocol. This is because if the team implement rules and features that are unpopular, users will move to another Bitcoin implementation. In order to stay compatible with each other, all users need to use software complying with the same rules. Bitcoin can only work well if there is a complete agreement on the software standard between all users. Therefore, all users and developers are encouraged to use and protect this standard. These maintainers don't actually have the power to make decisions that run against the consensus of the users. If there is a governing power over Bitcoin, it would be the Bitcoin users themselves.

5 What is double-spending? How does the Bitcoin network achieve consensus?

Double spending is a flaw within digital currencies where a digital token has the potential to be used in multiple transactions, meaning the same token could be spent multiple times by a single owner. This problem is prevented in cryptocurrencies such as Bitcoin that use a blockchain, using a consensus technique known as proof of work. This is done with a decentralised network of miners who validate the integrity of transactions on the blockchain, which in turn detects and prevent double spending. For a transaction to be valid and accepted onto the blockchain, a miner must collect it into a block, and calculate the corresponding nonce value. This is proof of work as it requires compute power to guess the nonce, verified by other users in the network. If a user attempts to double spend, it will be stopped as the original transaction will be on the public blockchain. To ensure the transaction is valid, it is advised to wait for 6 new blocks to be added to the blockchain so the transaction isn't lost. There are other vulnerabilities which could allow double spend attacks to take place. If an attacker is able to control at least 51% of the network, they can commit double spending as they could reverse transactions and create a separate blockchain which includes the double spend transaction.

6 What are SegWit2x and Lightning network? Explain their similarities and differences.

Both SegWit2x and Lightning network are attempts to fix the scalability issues of the Bitcoin protocol. SegWit2x was an unsuccessful hard fork, aimed to upgrade the bitcoin protocol in two ways. The first was to implement an increase to the volume of transactions that fit into each block without increasing the block size. The second involves updating the Bitcoin protocol rules to allow for 2MB blocks. Lightning network is a payment protocol that operates on top of existing blockchain protocols like Bitcoin. It successfully aims to increase the transaction speed on the Bitcoin blockchain by introducing off-ledger transactions. Because of this not every transaction on the channel has to be stored on the blockchain, only the start and ending payments. The similarities between SegWit2x and Lightning are that both methods aim to improve the transaction speed of the Bitcoin network; both aim to reduce the transaction fee; both are not created by the Bitcoin Core team; and both aim to fix the scalability issues of Bitcoin. The differences between SegWit2x and Lightning are that SegWit2x is a protocol rule change that involves a hard fork of the network whilst Lightning is a layer 2 protocol that works with Bitcoin Core; SegWit2x was a failed implementation whilst Lightning is operational and successful; and SegWit2x writes all transactions to the blockchain whilst Lightning only stores the initial and final transactions.