Computational Finance Assignment Report

I. Question a

Bitcoins are generated by the users when they find a new block. According to the settings, the number of bitcoins discovered per block starts from 50 and decreases by 50% every 210,000 blocks. The current smallest unit of the bitcoin is satoshi, which equals to 0.00000001 bitcoin(BTC), i.e. 1BTC=10^8 satoshis. By calculation, the BTC per block will reach 0.00000001 (1 satoshi, the smallest unit of bitcoins) in the 33^{rd} reward era, which means the number of bitcoins will reach its maximum in the same era. Thus, the maximum number of bitcoins can be calculated by $\sum_{i=0}^{32} 210000 \lfloor \frac{50\times 10^8}{2^i} \rfloor / 10^8$. In this way, we can derive the maximum number of bitcoins, which is $20,999,999.9769$.

II. Question b

As discussed in the previous question, the number of bitcoins will reach the maximum by the end of the 33^{rd} reward era, when the last bitcoins will be created at the same time. The total number of blocks discovered during the 33^{rd} reward eras will be $210,000 \times 33 = 6,930,000$. As we assume that it takes 10 minutes to mine a block on average, the total time needed to discover all the blocks is $6,930,000 \times 10$ (minutes)$/60$ (minutes)$/24$ (hours) = $48,125$ days. The first block was discovered on 3rd January 2009, so the last bitcoin will be created on 8th October 2140.

The number of 97% of bitcoins is $20,369,999.977593$. We can calculate that it is larger than the number of the total bitcoins by the end of the 5^{th} reward era ($i = 4$), which is $20,343,750$ and is smaller than that of the 6^{th} reward era ($i = 5$) which equals to $20,671,875$. The BTC per block in the 6^{th} reward era is $50/2^5 = 1.5625$. Hence, the number of blocks created when 97% of bitcoins will be achieved is $(20369999.977593 - 20343750)/1.5625 = 16799.98565952 \approx 16800$. The total blocks discovered by then will be $210,000 \times 4 + 16800 = 856,800$. Thus, the date will be $856,800 \times 10/60/24 = 5,950$ days after 3rd January 2009, which is 19th April 2025.

III. Question c

A hash function provides a mapping from an input (known as 'message') to a fixed-size alphanumeric string (called 'hash value' or 'message digest'). It has three main security properties: 1. One-way (infeasible to invert). It is computationally difficult to derive the message of the function based on a given hash value, making it prevent counterfeit. 2. Collision-resistance. It is infeasible to find x and x', with $x \neq x'$ s.t. $h(x) = h(x')$, which implicates that with the same hash value, it is safe to assume the input messages are the same. In addition, birthday attack imposes a lower bound on the size of message digests[1]. To avoid the collision, the hash function used for bitcoin protocol is SHA-256, which is a member of SHA-2 (Secure Hash Algorithm 2). 3. Deterministic. The same message always results in the same hash value and any small changes to the message will completely change the digest.

Proof-of-Work is a protocol for a service provider to prove to the verifier that he/she has spent a certain level of computational power to achieve a number of security goals in a specific time interval[2].

The two applications of hash functions in designing the bitcoin Proof-of-Work protocol are Hiding problem and Puzzle-friendly problem. **Hiding problem** is described as given a hash function h and $y = h(r||x)$, where r is chosen from a high min-entropy probability distribution, find x without knowing r, s.t. $h(r||x) = y$. As the hash function is one-way and collision resistance, the only way to solve the problem is to try all possible combinations. It requires sufficient time for the miners that they have to prove their work to the verifiers by spending enough time and computing power to solve the problem. **Puzzle-friendly problem** is: given r, find x s.t. $h(r||x) = y$. The optimal way to solve this problem is the same as that of hiding problem, which is to try every possible input. In addition, as the workload of the task grows exponentially as the length of the hash being extended, the puzzle can be modified to a moderate extent by restricting the length of the hash value.

IV. Question d

Stale Blocks. Stale blocks are the blocks which are discovered but not included in the longest chain. Stale blocks trigger chain forks when there are inconsistent states being caused by different versions of rules[3]. In general, stale blocks could not receive mining rewards while in Ethereum, they are awarded but with a smaller rate comparing to the other blocks.

Hard Fork. Hard Fork means that the blocks considered valid by miners running new versions or agreements will be rejected by nodes running the old version. It is incompatible with the previous rules that all the nodes in the network need to upgrade the agreement[4]. Those who fail to implement the new rules will still follow the prior rules and be excluded from the blockchain running the new rules[5]. Hence, a new branch of the blockchain running the old versions of rules will be created accordingly[5]. The hard fork creates new cryptocurrencies by increasing block sizes for instance.

Soft Fork. In the contrast of the Hard Fork, Soft Fork means blocks considered valid by miners running new versions are also considered valid by nodes running the old version. The new rules are stricter but compatible with previous rules. Blocks considered valid by miners running the old version may be rejected by the nodes running the new version. The new nodes and old nodes will continue to work on the same chain without creating a new one[4].

V. Question e

Double-spending is the result of a digital currency being spent successfully for more than once in multiple transactions[6][7]. An effective double-spending attack contains four steps:

1. Broadcasting to the network that a transaction is finished by paying the attacked merchant.

2. Before the transaction in the last step is added into a block, meanwhile, mining a secret branch which builds on the last block which includes a replicated transaction paying the attacker.

3. Waiting for sufficient transaction confirmations that the merchant is confident to send the product.

4. Continually extending the secret branch until it is longer than the public branch. Broadcasting that the secret branch will become valid and the payment for the merchant will be paid to the attacker instead[8].

The bitcoin network achieves consensus by proof-of-work (PoW). The PoW algorithm enables the difficulty of the tasks to be moderate for all the miners to solve but easy for the other nodes to verify. In the bitcoin network, miners need to competing against other nodes to solve the computationally difficult problems to generate a new block[9]. By broadcasting in the bitcoin network, the first node who finds a new block will be rewarded after the result is verified by the majority of the nodes in the network. PoW requires a large amount of computational power to generate the block which makes it impossible to request multiple transactions without proving the effort made for discovering the blocks accordingly.

VI. Question f

The bitcoin depends on the miners to store and broadcast the blockchain, validate new transactions and vote on consensus. The routine tasks of a bitcoin miner include: 1. Validate all proposed transactions. 2. Validate a new proposed block to maintain the blockchain. 3. Assemble a new valid block. 4. Find the nonce to make the new block valid. 5. Make profit after everybody has accepted the new block[10].

The strategic considerations that a miner would have include: 1. Choose the transactions which the miner wants to include in a block. The transactions fee are above the minimum value. 2. Choose the block to mine on top of. By default, miners choose the longest valid chain. 3. Choose between colliding blocks. The default rule is to choose the first block heard. 4. Decide when to announce new blocks. Miners usually immediately announce the new blocks after finding them[11].

A 51% attack refers to an attack on a blockchain when a group of miners controls more than 50% of the network's mining hash rate or computing power to revise transaction history, prevent new transactions from gaining confirmations[12], and prevent other miners from mining any valid blocks[13]. The things that the attackers can not do include: reverse other node's transactions, stop transactions from being sent, change the rewards of each block, create new currencies, and use other node's coins[13].

VII. Question g

The bottlenecks of the bitcoin system consist of four main aspects: **Energy consumption**. Mining bitcoins and verifying transactions consume a large number of energy resources. This carbon-intensive machinery is a potential threat to the global environment. The estimated energy consumption per transaction is 200 kWh, which is inefficient compared to that of visa with only 0.1 kWh[14]. **Scalability Problem**. This problem refers to the limitation of the number of transactions that the network can process. The average generating time of each block is 10 minutes to reach consensus and the size of each block is 1 megabyte, which was limited by Satoshi Nakamoto[15]. Blocks can hold a few thousand transactions with the processing speed: 3.3 to 7 transactions per second[16]. **Politics (Government Regulation)**. Bitcoin is a decentralized payment system aiming to eliminate the need for central banks and governmental institutions to avoid corruption[17]. To prevent bitcoins from competing with the current centralized financial system, regulatory actions limiting the bitcoin-related business have been taken in certain countries. **Centralization mining**. Mining pools enable miners to share proportional rewards of discovering blocks by contributing hash power. The centralized mining pools make the rewards predictable while it is against the decentralized nature of the blockchain. A pool called GHash.IO held 54% (the attack threshold is 51%[13]) of the hash rate for one day in 2014. Mining pools increase the risks of double spending and blocked transactions.

VIII. Question h

There was no initial limitation of the **block size** until it was explicitly limited to 1 MB as a maximum by Satoshi Nakamoto in 2010 [15]. Increasing the block size is an effective way of improving the transaction rate, but it requires more storage to maintain a full node. Another concern is the increasing **number of forks** caused by the time needed to communicate with other nodes through the network[18]. As the average **block propagation time** was 2 seconds plus 0.008 seconds per kilobyte in the block, the time consumed for broadcasting would increase significantly when the block size becomes bigger[18][19].

In addition, the longer block propagation time increases the probability to create new blocks. The blockchain forks when there are more than valid blocks being verified, one of the chains become the main chain after verification. The blocks which are not added to the main chain become stale blocks. As the block size becomes larger, both the **number of stale blocks** and the **length of forks** increase accordingly[3], which makes the network become vulnerable[20]. Furthermore, another approach known as shortening **block generation interval** is proposed as a solution to the bitcoin scaling problem. The original block generation interval is set to be 10 minutes [20]. If we short the block generation interval, the process of PoW would be sped up as well. The chances of producing stale blocks would increase proportionally to the time needed for learning new blocks and the block generation interval. Hence, the results caused by shortening block generation interval are as the same as increasing block size[18].

IX. Question i

The **advantages** of mining pools are: The rewards are predictable and the incomes are stable for miners. Comparing to solo mining, mining pools provide lower variance and they are easy for miners to join. For the ecosystem, mining pools assemble prospective blocks intensively and facilitate network update. The **disadvantages** include: Mining pools are centralized as they rely on concentrated mining power, which is against the decentralized property of the bitcoin. They raise the possibility of being attacked when the nodes of a pool take more than 50% hash rate of the network. The miners no longer run full nodes although one mining pool does, which reduces the number of full nodes in the network.

There are three common ways that a mining pool distributes the block reward to individual miners. **Pay per share:** A mechanism allows every share submitted by the miners to receive a determined reward. It has zero variance and is easy to verify the expected rewards, which is ideal for beginners. Meanwhile, the pool operator needs to take the variance and charge a higher fee than the miners correspondingly. The risk is that when the pool operator fails to manage the risks, the mining pool may go bankrupt[21]. **Proportional ("Share-based"):** Payments are calculated based on the number of shares submitted by the miners. It works when the pool has a fixed miner base. When a miner tries to direct his hash rate to

another pool (known as *pool-hopping*), he will receive more rewards and the other miners who continually work in the original pool end up with receiving fewer rewards[21]. **Score-based:** A method built on the proportional method aims to combat pool-hopping. It gives scores to each share based on the amount of time elapsed since the round started. It encourages miners to start mining at the beginning of the round while it can not completely avoid pool-hopping and the scores are difficult to calculate[21].

X. Question j

As block rewards halve every 210,000 blocks, transaction fees will dominate the block reward eventually. The transaction fees regime is time-varying, which encourages miners to hop to the pool whenever it maximizes their rewards instead of staying in one pool from the beginning. There are three main changes comparing to the block reward. 1. It raises the chance of new mining behaviors such as Petty Compliant. The miners are more likely to mine on the block that has the fewest transaction fees, instead of mining on the end of the longest chain. Miners can gain profit even without a high hash power share or a strong connection within the network. 2. It increases the variance of the block reward to a high level due to the block arrival time is distributed exponentially, which will affect the bitcoins stability seriously. 3. When mining the same fraction of blocks, the selfish miner's blocks are larger and can get more reward.

The potential risks to the bitcoin ecosystem include: Firstly, constant forks caused by undercutting will magnify the effective hash power of the attackers to make 51% attack possible with less than 51% of the hash power. Secondly, miners who use the same mining strategy will make an equilibrium, inducing increasing the transactions backlog. Furthermore, it will break down the consensus of the network due to blocks withholding or increasingly aggressive undercutting[22], which makes the network unstable and insecure.

References

[1] D. Stinson, *Cryptography: Theory and Practice,Second Edition*. CRC/C&H, 2nd ed., 2002.

[2] M. Jakobsson and A. Juels, *Proofs of Work and Bread Pudding Protocols(Extended Abstract)*. Boston, MA: Springer US, 1999.

[3] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 3–16, ACM, 2016.

[4] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges.," *IJ Network Security*, vol. 19, no. 5.

[5] J. Atik and G. Gerro, "Hard forks on the bitcoin blockchain: Reversible exit, continuing voice," *Stan. J. Blockchain L. & Pol'y*, vol. 1, p. 24, 2018.

[6] "Irreversible transactions." https://en.bitcoin.it/wiki/Irreversible$_{T}ransactions. Accessed : 2019 - 04 - 12$.

[7] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 1, p. 2, 2015.

[8] M. Rosenfeld, "Analysis of hashrate-based double spending," *arXiv preprint arXiv:1402.2009*, 2014.

[9] Z. Dong, Y. C. Lee, and A. Y. Zomaya, "Proofware: Proof of useful work blockchain consensus protocol for decentralized applications," *arXiv preprint arXiv:1903.09276*, 2019.

[10] "The task of bitcoin miners, from the course by princeton university: Bitcoin and cryptocurrency technologies." https://www.coursera.org/lecture/cryptocurrency/the-task-of-bitcoin-miners-0htpQ. Accessed: 2019-04-13.

[11] "Mining incentives and strategies, from the course by princeton university: Bitcoin and cryptocurrency technologies." https://www.coursera.org/lecture/cryptocurrency/mining-incentives-and-strategies-hvRiW. Accessed: 2019-04-13.

[12] "51% attack, majority hash rate attack." https://bitcoin.org/en/glossary/51-percent-attack. Accessed: 2019-04-13.

[13] M. Bastiaan, "Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin," in *Availab le at http://referaat. cs. utwente. nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin. pdf*, 2015.

[14] J. Truby, "Decarbonizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies," *Energy research & social science*, 2018.

[15] "Block size limit controversy." https://en.bitcoin.it/wiki/Block$_{s}ize_{l}imit_{c}ontroversy. Accessed : 2019 - 04 - 13$.

[16] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, *et al.*, "On scaling decentralized blockchains," in *International Conference on Financial Cryptography and Data Security*.

[17] P. De Filippi and B. Loveluck, "The invisible politics of bitcoin: governance crisis of a decentralized infrastructure," *Internet Policy Review*, vol. 5, no. 4, 2016.

[18] "Blockchain scaling." https://medium.com/coinmonks/blockchain-scaling-30c9e1b7db1b. Accessed: 2019-04-13.

[19] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*.

[20] "Bitcoin: Too big to scale?." https://medium.com/blockchainspace/3-1-bitcoin-in-detail-part-2-scalability-393f1d445b5e. Accessed: 2019-04-13.

[21] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," *arXiv preprint arXiv:1112.4980*, 2011.

[22] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the instability of bitcoin without the block reward," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 154–167, ACM, 2016.