Understanding the Mathematics behind Cryptocurrencies

Double Master Maths & Info MAFI 2023

1 Introduction, Motivation and Related Works

In "Mathematics of Bitcoin" [4], Grunspan and Pérez-Marco provide a deep analysis of the mathematical foundations of the Bitcoin protocol [7], including its cryptography, distributed ledger [8], and consensus mechanism [3]. The principles discussed in the paper are based on well-established mathematical concepts (analysis, probability, cryptographic hash functions and Merkle trees [4, Section 2], combinatorics with Dyck words [4, Section 7], etc.) and can be applied to other blockchain systems, as well.

In [4], the authors present several Theorems, Lemmas, and their rigorous proofs, such as the following (informal):

Theorem 1: The probability of an attacker successfully generating a block and catching up to the longest chain is exponentially small in the computational resources they possess.

Lemma 1: The probability of an honest node finding the next block is proportional to its computational power.

Theorem 2: The total work done by all miners is proportional to the probability that a node will validate a new block and add it to the blockchain.

Theorem 3: If a dishonest miner controls less than 50% of the total computational power, their probability of successfully carrying out a double-spending attack decreases exponentially with the number of confirmations received by the transaction they are trying to double-spend.

Interested readers are invited to explore the paper [4] and its references in more depth.

2 Task of the group

Here are a few possible suggestions of future works:

1. Generalize to other consensus mechanisms: Theorem 1 applies specifically to the Bitcoin protocol and its proof-of-work consensus mechanism. The group could try to generalize the result to other consensus mechanisms, such as proof-of-stake [5] or delegated proof-of-stake [6]. This would require understanding the key features and security properties of those consensus mechanisms, and then using mathematical analysis to derive similar bounds on the probability of a successful attack.

2. Do not limit your work on "bounds on probabilities", for example Eyal and Sirer work [2] presents a formal model of a 51% attack on Bitcoin[1] and derives an expression for the expected time to success of such an attack.

3. Carlsten *et al* [1] presents a model and analysis of the security of Bitcoin mining in the absence of block rewards. Again, how such an approach can be generalized to other cryptos and other consensus mechanisms.

[1] Also, check other cryptocurrencies! Do not limit your work on the pair (Bitcoin, Proof-Of-Work).

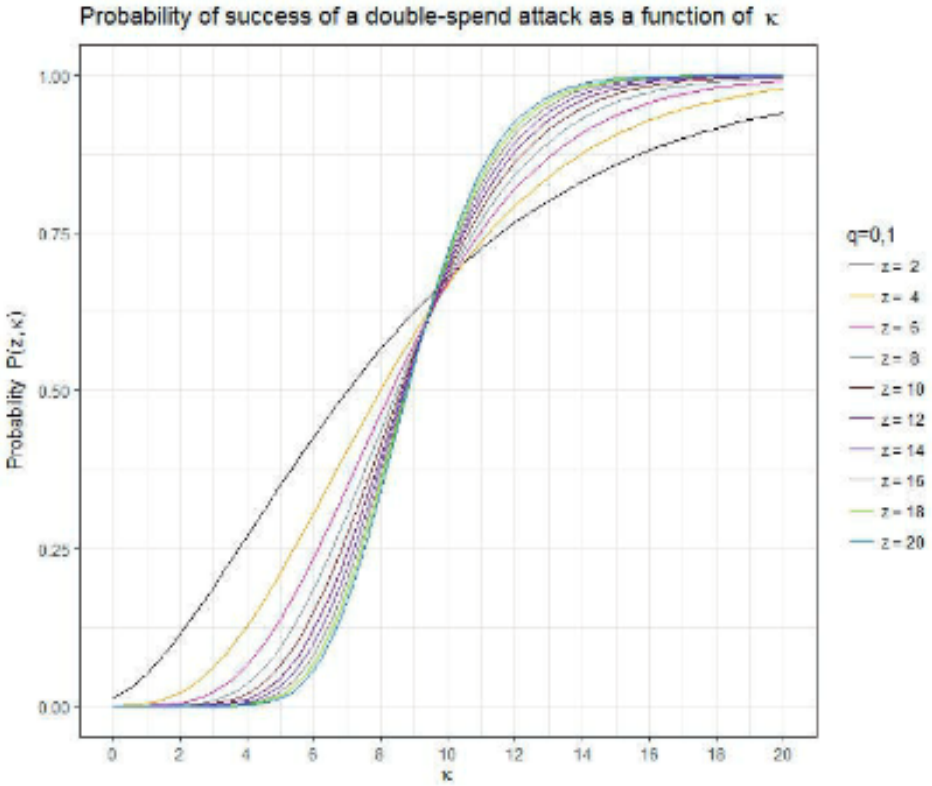

Figure 1: Probability of success of a double-spend attack (image from [4]). It seems that there should be a phase transition (clearly we have a "step function" here.

4. Generalize to attacks other than block generation: Theorem 1 focuses specifically on the probability of an attacker successfully generating a block and catching up to the longest chain. Students could try to generalize the result to other types of attacks, such as double-spending attacks or 51% attacks. This would require understanding the specific attack vectors and security properties of the system, and then using mathematical analysis to derive bounds on the probability of a successful attack (or other quantification than probability).

Works with the same flavour can be done with the other Theorems in [4].

3 Conclusion

In addition to conducting novel and innovative research, it is also important to present your results in a clear and concise manner, and to provide rigorous experimental evaluation and validation of your methods. This will increase the likelihood that your research will be accepted by the scientific communities.

Firstly, blockchain and cryptocurrencies are still relatively new fields, and there is a lot of ongoing research and development in these areas. As such, being involved in research can provide opportunities to contribute to cutting-edge developments and potentially make significant contributions to the field.

Secondly, blockchain and cryptocurrencies are becoming increasingly important in various industries, such as finance, supply chain management, and healthcare. Having expertise in these areas can make someone an attractive candidate for jobs or consulting opportunities in these industries.

Lastly, blockchain and cryptocurrencies are inherently interdisciplinary fields, drawing from computer science, economics, mathematics, and law, among others. Thus, research in these areas can provide opportunities to develop a broad range of skills and knowledge that could be valuable in a variety of contexts.

Overall, research in blockchain/cryptocurrencies can be a valuable asset for someone interested in

pursuing a career in these areas, or for someone just looking to develop a broad range of skills and knowledge.

References

[1] Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. On the instability of Bitcoin without the block reward. In *2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 154–167. ACM, 2016.

[2] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *2014 IEEE Symposium on Security and Privacy*, pages 463–479. IEEE, 2014.

[3] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. *Proceedings of the 26th Symposium on Operating Systems Principles*, 2017.

[4] Cyril Grunspan and Ricardo Pérez-Marco. The Mathematics of Bitcoin. *Notices of the American Mathematical Society*, 65(06):706–719, 2018.

[5] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017.

[6] Daniel Larimer. Delegated proof of stake. In *Proceedings of the Second Workshop on Bitcoin Research*, 2014.

[7] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *bitcoin.org*, 2008.

[8] Melanie Swan. Blockchain: blueprint for a new economy. *O'Reilly Media, Inc.*, 2015.