THE UNIVERSITY of EDINBURGH
informatics

Lightning Talk

- Provable Security of Blockchain Target Recalculation Functions

- Transaction Order Fairness and Front-running Mitigation

Presenter: Yu SHEN

Provable Security of Target Recalculation Functions

- [GKL15, PSS17] shows that Nakamoto Consensus achieves *Consistency* and *Liveness* under static participation with appropriate network parameters.
  - Mining target is a good function in terms of the number of parties.
- Do these security properties still remain under dynamic participation?
  - [GKL17, GKL20] give an analysis of Bitcoin's target recalculation function.
  - [GS21] carries out an analysis and comparison of Bitcoin Cash's two target recalculation functions.
- We need a general framework to analyze and compare different target recalculation mechanism.

Transaction Order & Front-running Mitigation

- Nowadays, front-running constitutes a large percentage of MEV (miner extractable value) which yields 700+M USD since Jan1, 2020*.
- Nakamoto Consensus only guarantees *Consistency* and *Liveness*; however, the block producer enjoys the full power to choose the set of transactions to include.
- Existing solutions suffer from either high complexity** or external validators**.
  - High complexity hurts liveness.
  - External validators conflicts with the natural of decentralization.
- We are working on a simple but effective protocol that achieves order fairness.

*https://explore.flashbots.net/
** [KZGJ20] gives a high complexity solution and [Kursawe20] utilizes external validators.

Bibliography

1. Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. 2015. The Bitcoin Backbone Protocol: Analysis and Applications. In Advances in Cryptology – EUROCRYPT 2015, Elisabeth Oswald and Marc Fischlin (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 281–310.
2. Rafael Pass, Lior Seeman, and Abhi Shelat. 2017. Analysis of the Blockchain Protocol in Asynchronous Networks. In Advances in Cryptology – EUROCRYPT 2017, Jean-Sébastien Coron and Jesper Buus Nielsen (Eds.). Springer International Publishing, Cham, 643–673.
3. Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. 2017. The Bitcoin Backbone Protocol with Chains of Variable Difficulty. In Advances in Cryptology – CRYPTO 2017, Jonathan Katz and Hovav Shacham (Eds.). Springer International Publishing, Cham, 291–323.
4. Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. 2020. Full Analysis of Nakamoto Consensus in Bounded-Delay Networks. Cryptology ePrint Archive, Report 2020/277. (2020). https://eprint.iacr.org/2020/277.
5. Juan Garay and Yu Shen. 2021. On Bitcoin cash's target recalculation functions. In Proceedings of the 3rd ACM Conference on Advances in Financial Technologies (AFT '21). Association for Computing Machinery, New York, NY, USA, 192–204.
6. Kelkar M., Zhang F., Goldfeder S., Juels A. (2020) Order-Fairness for Byzantine Consensus. In: Micciancio D., Ristenpart T. (eds) Advances in Cryptology – CRYPTO 2020. CRYPTO 2020. Lecture Notes in Computer Science, vol 12172. Springer, Cham.
7. Klaus Kursawe. 2020. Wendy, the Good Little Fairness Widget: Achieving Order Fairness for Blockchains. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (AFT '20). Association for Computing Machinery, New York, NY, USA, 25–36.