MORGAN
STATE UNIVERSITY™
THE FINTECH CENTER

Scalability and Privacy in Blockchain Networks

How can privacy and scalability issues in Blockchain networks be overcome? By default, blockchains allow tracing the transaction history of users. They furthermore are slow and have a low throughput, i.e., the number of transactions per second is typically less than 100. Solutions for privacy include transaction mixing and cryptographic means that hide transaction information, yet none of these solutions has been widely adapted. Scalability solutions either change the consensus algorithm of the blockchain or move transactions off-chain, i.e., provide mechanisms for conducting transactions that are not recorded on the blockchain while maintaining almost the same level of security.

Can you propose innovations in scalability and privacy for blockchain based-systems, such as cross-border payment systems? Please note that the research proposal is not to address all of these questions, but just one aspect of one question.

Given below are some of the papers in this domain. These may be of interest to Computer Science, Mathematics, Electrical Engineering, Information Systems, Finance, Supply Chain Management faculty.

Kim, S., Kwon, Y., & Cho, S. (2018, October). A survey of scalability solutions on blockchain. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 1204-1207). IEEE.

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. In *13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)* (pp. 45-59).

Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2019). SoK: Off The Chain Transactions. *IACR Cryptology ePrint Archive*, *2019*, 360.

Biais, B., Bisiere, C., Bouvard, M., & Casamatta, C. (2019). The blockchain folk theorem. *The Review of Financial Studies*, *32*(5), 1662-1715.

Wu, T., & Liang, X. (2017, August). Exploration and practice of inter-bank application based on blockchain. In *2017 12th International Conference on Computer Science and Education (ICCSE)* (pp. 219-224). IEEE.

Luong, N. C., Xiong, Z., Wang, P., & Niyato, D. (2018, May). Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

Gervais, Arthur, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan 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. 2016.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S. and Danezis, G., 2019, October. SoK: Consensus in the age of blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* (pp. 183-198).

Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., and Gervais, A. . SoK: Off The Chain Transactions. In *Proceedings of Financial Cryptography and Data Security*, *2020*

Kappos, George, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. "An empirical analysis of anonymity in zcash." In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 463-477. 2018.

Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism. *IEEE Access*, *7*, 118541-118555.