Scalability and Throughput of Blockchains and Decentralized Applications

Martin Perešíni, Ivan Homoliak

1 Abstract, Objectives, and Motivation

The tutorial aims to address the fundamental limitations of current blockchain technology concerning scalability and throughput. It introduces various approaches to improve scalability, including naive improvements, Bitcoin-NG, sharding methods (Elastico, OmniLedger, RapidChain), DAG-based protocols, off-chain payments, and centralized blockchains. The motivation behind this is the increasing demand for higher transaction throughput and lower latency to support real-world applications, which current blockchain technologies struggle to meet due to the inherent trade-offs between scalability, security, and decentralization (blockchain trilemma).

2 Timeline and Intended Audience

The topic explores scalability from the historical context and evolution of blockchain technology, starting with its debut in Bitcoin, the first cryptocurrency. Ethereum expands the technology's potential by introducing smart contracts and decentralized applications (dApps) to the future generation of blockchains. However, scalability remains a significant challenge for blockchains and dApps today, prompting numerous projects to explore diverse solutions for improved throughput and efficiency.

The target audience for this tutorial includes bachelor's and master's students and researchers in computer science or related fields, who will find it informative and engaging due to its delve into the technical aspects of blockchain technology, its scalability challenges, and potential solutions for improving throughput. Additionally, researchers and professionals interested in blockchain technology and its real-world applications can benefit from this comprehensive overview of current developments and future directions in blockchain scalability and performance improvements.

3 Speaker Information

Martin Perešíni received a Master of Science degree in information technology security from the Brno University of Technology (BUT FIT) in 2020, where he is currently pursuing a Ph.D. degree in computer science and engineering. He is a member of the Security research group, Faculty of Information Technology, where he focuses on analyzing blockchain security, computer and network security. His research interests include the security of systems and devices, privacy-enhancing technologies, IoT networks, cyber-physical systems, and partially machine learning in deepfake detections and LLMs.

Ivan Homoliak is an assistant professor at the Brno University of Technology and currently works on general security analysis of blockchain technologies, particularly the design and security of consensual protocols. In the past, he also focused on applying machine learning for insider threat detection. Ivan has a Ph.D. in the area of adversarial intrusion detection in network traffic from Brno University of Technology, Faculty of Information Technology (BUT FIT), Czech Re- public (2016). Ivan earned a Master of Science degree from the BUT FIT in 2012 in the areas related to intrusion detection and supervised machine learning.

4 Technical Issues Addressed

The tutorial focuses on the blockchain trilemma, highlighting the trade-off between scalability and security. It examines the limitations of current blockchain architectures in handling increasing transaction volumes. The tutorial explores various solutions, including naively increasing block

size or decreasing block creation time. It delves deeper into promising approaches like sharding, DAG-based protocols, and off-chain payments. Each method aims to enhance scalability without significantly compromising security or decentralization. Additionally, the tutorial outlines potential technical challenges and design flaws in specific protocols that could jeopardize their security and future viability.

5 Tutorial Content Outline

The tutorial will be for approximately **two hours**, structured to cover the specified topics in chronological order, each with a dedicated time slot. An overview of blockchains, their fundamental designs, and their inherent limitations will be presented. We then delve into various methods and technologies aiming to address scalability and throughput issues, categorized as follows (with a proposed schedule):

- **Introduction to Blockchain Technologies** (*15 minutes*) - An overview of blockchains, their fundamental designs, and inherent limitations.
- **Scalability Solutions** (*50 minutes*)
  - Intuitive Improvements (*5 minutes*) - Discuss simple proposals of increasing block size and/or decreasing block creation time, which offers a limited solution.
  - Advanced Solutions (*45 minutes*) - Covering Bitcoin-NG [2, 13], sharding techniques such as Elastico [6], OmniLedger [5], and RapidChain [14], DAG-Based Blockchains [12, 11, 8], and off-chain solutions [9], highlighting key innovations and proposals.
- **Permissioned blockchains and semi-centralized blockchains** (*15 minutes*) - Examining permissioned blockchains like HyperLedger [10] and semi-centralized solutions like Aquareum [4, 3], with a focus on performance efficiency and privacy preservation with leveraging of Trusted Execution Environments (TEEs) [1].
- **Interactive Demo: DAG-Based Blockchain Simulation** (*20 minutes*) - Practical demonstration showcasing experiments using DAG-Sword [7], developed as part of our ongoing research. This open-source simulation tool measures the profitability and throughput of DAG-based blockchains under various scenarios.
- **Interactive Demo: Hyperledger Fabric and Caliper Benchmarks** (*10 minutes*) - Practical demonstration showing Hyperledger Caliper to measure and benchmark distributed applications developed on Hyperledger Fabric. Hands-on experience with blockchain/DLT performance measurement tools, and deployment of permissioned blockchain.
- **Q&A and Discussion** (*10 minutes*) - Time for addressing audience questions, further clarifying complex topics, and discussing presented implications.

The tutorial is designed to provide a balanced mix of theoretical and practical insights, ensuring that participants understand blockchain scalability challenges and potential solutions.

6 Previous Tutorial Experience

This tutorial is based on material, lectures, and topics covered in the "Blockchain and Decentralized Applications" course at Brno University of Technology, Faculty of Information Technology. This established course is now in its third year, ensuring consistent updates and alignment with current trends and themes. Martin Perešíni experience is that he is a lecturer and delivers specific lectures within the mentioned course. Ivan Homoliak is the course guarantor and main lecturer; he has also presented on various blockchain-related topics in invited talks held at different international locations, including Qingdao City, Shandong Province, China, Canadian University in Dubai Singapore University of Technology and Design (SUTD). His presentations cover blockchains, authentication methods of cryptocurrency wallets, electronic voting in blockchains, blockchain scalability, secure logging, and data provenance, and Central Bank Digital Currency (CBDC) usage.

7 Similar Tutorials and Differentiators

While there are several tutorials and workshops on blockchain technology and its applications, this tutorial distinguishes itself through its focus on scalability and throughput, which are critical challenges in the blockchain that are on par with security attributes. Unlike generic introductions to blockchain technology, our tutorial delves into specific scalability solutions, offering a nuanced discussion on advanced topics like sharding, DAG-based protocols, and permissioned blockchains.

References

[1] Costan, V., and Devadas, S. Intel sgx explained. *Cryptology ePrint Archive* (2016).

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

[3] Homoliak, I., Perešíni, M., Holop, P., Handzuš, J., and Casino, F. Cbdc-aquasphere: Interoperable central bank digital currency built on trusted computing and blockchain. *arXiv preprint arXiv:2305.16893* (2023).

[4] Homoliak, I., and Szalachowski, P. Aquareum: A centralized ledger enhanced with blockchain and trusted computing. *arXiv preprint arXiv:2005.13339* (2020).

[5] Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., and Ford, B. Omniledger: A secure, scale-out, decentralized ledger via sharding. In *2018 IEEE Symposium on Security and Privacy (SP)* (2018), pp. 583–598.

[6] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., and Saxena, P. A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, 2016), CCS '16, Association for Computing Machinery, p. 17–30.

[7] Perešíni, M., Hladký, T., Malinka, K., and Homoliak, I. DAG-Sword: A Simulator of Large-Scale Network Topologies for DAG-Oriented Proof-of-Work Blockchains. In *57th Hawaii International Conference on System Sciences, HICSS 2024, Hilton Hawaiian Village Waikiki Beach Resort, Hawaii, USA, January 3-6, 2024* (2024), T. X. Bui, Ed., ScholarSpace, pp. 5960–5969.

[8] Perešíni, M., Benčić, F. M., Hrubý, M., Malinka, K., and Homoliak, I. Incentive attacks on dag-based blockchains with random transaction selection. In *2023 IEEE International Conference on Blockchain (Blockchain)* (2023), pp. 1–8.

[9] Poon, J., and Dryja, T. The bitcoin lightning network. *Scalable o-chain instant payments* (2015), 20–46.

[10] project team Hyperledger Fabric. Hyperledger fabric docs, 2023.

[11] Silvano, W. F., and Marcelino, R. Iota tangle: A cryptocurrency to communicate internet-of-things data. *Future Generation Computer Systems 112* (2020), 307–319.

[12] Sompolinsky, Y., Wyborski, S., and Zohar, A. Phantom ghostdag: a scalable generalization of nakamoto consensus: September 2, 2021. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies* (New York, NY, USA, 2021), AFT '21, Association for Computing Machinery, p. 57–70.

[13] Szalachowski, P., Reijsbergen, D., Homoliak, I., and Sun, S. {StrongChain}: Transparent and collaborative {Proof-of-Work} consensus. In *28th USENIX Security Symposium (USENIX Security 19)* (2019), pp. 819–836.

[14] Zamani, M., Movahedi, M., and Raykova, M. Rapidchain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, 2018), CCS '18, Association for Computing Machinery, p. 931–948.