Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Fair Transaction Ordering Website

Bachelor's Thesis

Lucas Pfingsten Planells

lplanells@student.ethz.ch

Distributed Computing Group
Computer Engineering and Networks Laboratory
ETH Zürich

Supervisors:
Lioba Heimbach
Prof. Dr. Roger Wattenhofer

January 16, 2024

Acknowledgements

I am deeply grateful to my supervisor, Lioba Heimbach, for her support and guidance throughout my research. I extend my sincere thanks to Professor Wattenhofer for providing me with the opportunity to undertake this thesis. Their combined support has been instrumental in the completion of this thesis.

Abstract

This thesis presents the development of a Fair Transaction Ordering Website, a comprehensive online platform that categorizes and elucidates various protocols for fair transaction ordering in blockchain technology. The primary objective was to address the prevalent challenges and attacks associated with transaction ordering in blockchain networks. Through extensive research, key protocols were identified and grouped into seven categories: Optimized Trade Execution, Professional Market Makers, Third Party Ordering, Algorithmic Committee Ordering, On-Chain Commit and Reveal, Off-Chain Commit and Reveal and Randomized Ordering. Each group was thoroughly analyzed, highlighting their unique mechanisms and contributions to enhancing fairness and security in blockchain transactions. The website, developed using Webflow, serves as an educational and practical tool, offering users an accessible and detailed understanding of these protocols. The most significant outcome of this research is the successful demonstration of how complex blockchain concepts can be effectively communicated and organized in a user-friendly digital format, contributing to a deeper public understanding and application of fair transaction ordering in blockchain technology.

Contents

Chapter 1

Introduction

1.1 Background

Blockchain technology has transformed various sectors by providing a decentralized and secure framework for digital transactions. Central to blockchain's functionality is the concept of transaction ordering, a process that determines the sequence in which transactions are added to the blockchain. Although initially little emphasis was placed on transaction ordering, it is crucial, as it can affect the fairness and efficiency of the network. The decentralized nature of blockchain, while offering numerous advantages, also presents unique challenges in maintaining a fair and equitable system for transaction processing.

1.2 Problem Statement

One of the primary challenges for blockchain transactions is the susceptibility to various attacks and manipulations, such as front-running and sandwich attacks, which exploit the transparency of pending transactions. These attacks not only undermine the integrity of the blockchain but also lead to significant financial losses for users. Moreover, the increasing complexity and growth of blockchain networks have intensified the need for sophisticated methods to ensure fair transaction ordering. The lack of standardization and the diverse nature of blockchain protocols further complicate the development of universal solutions.

1.3 Objective

This thesis aims to address these challenges by developing a Fair Transaction Ordering Website. The website is designed to categorize, analyze, and present various protocols that have been proposed for fair transaction ordering in blockchain networks. By examining a range of protocols, this study seeks to provide a comprehensive overview of the current solutions and methodologies. The ultimate goal is to enhance understanding and facilitate the application of these

protocols, contributing to the improvement of fairness and security in blockchain transaction ordering.

Chapter 2

Literature Review

The literature review shows various protocol groupings each addressing specific aspects of transaction fairness and security.

2.1 Summary of Protocols

This section offers a summary of the various protocol groups. For more in depth information on each of the protocol visit the website.

2.1.1 Optimized Trade Execution

Optimized trade execution schemes are the least invasive approach to prevent front-running on the blockchain.These approaches adjust the trade parameters to make potential front-running attacks unprofitable. Thus, these schemes have negligible impact on the underlying blockchain system but are limited in scope [1],[2],[3].

2.1.2 Professional Market Makers

Instead of utilizing an automated market maker, these approaches introduce a professional market maker to handle trades and are expected to execute them at market price. Generally, these approaches involve off-chain agreements on exchange rates and on-chain transaction execution [4],[5],[6],[7],[8].

2.1.3 Trusted Third Party Ordering

Trusted third party ordering refers to schemes that entrust a trusted third party with the ordering. Transactions are sent directly to the trusted third party who then orders them. Thus, these schemes order transactions efficiently while compromising decentralization and security [9],[4],[10],[11],[12],[13].

2.1.4 Algorithmic Committee Ordering

In algorithmic committee ordering schemes, a committee oversees the transaction ordering. Transactions are sent directly to the committee and the committee agrees upon a fair ordering through consensus. Generally, these approaches can handle less than one third of the committee members being byzantine [14],[15],[16],[17],[18],[19],[20],[21].

2.1.5 On-Chain Commit and Reveal

The on-chain commit and reveal approaches order transactions in two phases. In the first phase, users commit to their transactions by broadcasting their encrypted transaction which is included on-chain. In the second phase, after some time the transaction is either decrypted automatically once the private key becomes available or by the users themselves [22],[23],[24],[25],[26],[27],[28].

2.1.6 Off-Chain Commit and Reveal

Off-chain commit and reveal protocols order transaction in two phases. In the first phase, users send their transactions to a committee. The committee then agrees on an order through consensus. In the second phase, once the order is agreed upon, the committee decrypts the transaction with their threshold signatures [29],[30],[31],[32].

2.1.7 Randomized Ordering

In randomized ordering protocols, transactions are gathered over a set period and then executed in a random order to prevent front-running on the blockchain. This approach ensures unpredictability and fairness in transaction processing but may not be ideal for time-sensitive trades. Depending on the specific protocol, these transactions might be encrypted or not [33],[34],[35].

2.2 Comparative Analysis

This section offers a comparative analysis of the various protocol groups, assessing their strengths and weaknesses [36].

Optimized Trade Execution:

- **Pros:** Maintains decentralization, no increase in transaction cost, unchanged goodput and unchanged blockchain's transaction ordering.

- **Cons:** Limited scope to specific applications, slight transaction delay increase, and increased jostling.

Professional Market Makers:

- **Pros:** Almost no increase in transaction cost and very low jostling.
- **Cons:** Decrease in goodput, delay increases, decentralization decreases and impacted security in case of byzantine market makers.

Trusted Third Party Ordering:

- **Pros:** No delay, no increased cost, goodput remains unchanged, very low jostling, and good scope.
- **Cons:** Impacted decentralization and security concerns in the case of Byzantine third parties.

Algorithmic Committee Ordering:

- **Pros:** Goodput remains unchanged and no significant delay.
- **Cons:** Medium Scope as back-running still possible, reduced decentralization, increased costs and jostling.

On-Chain Commit and Reveal:

- **Pros:** No impact on decentralization, good scope, minimal jostling.
- **Cons:**Increased transaction fees, increased delay and decreased goodput.

Off-Chain Commit and Reveal:

- **Pros:** No decreased goodput, good scope, minimal jostling, and no increased delay.
- **Cons:** Increased cost, reduced decentralization and security issues in case of byzantine committee.

Randomized Ordering:

- **Pros:** Good scope, minimal jostling.

- **Cons:** Increased cost and delay, reduced decentralization and security issues in case of byzantine committee.

This comparative analysis highlights the diverse range of benefits and limitations associated with each protocol group. While some protocols excel in maintaining goodput and minimizing costs, others face challenges in terms of scope, security, and impact on decentralization. These findings reflect the complexity of achieving fair transaction ordering in blockchain and underscore the importance of continued research and development in this field.

Chapter 3

Methodology

This section outlines the methodology used in the development of the Fair Transaction Ordering Website and the categorization of various protocols.

3.1 Website Development

The development of the Fair Transaction Ordering Website was executed using Webflow, a web development platform that allows for the creation of responsive and interactive websites without extensive coding. The choice of Webflow was motivated by its user-friendly interface, flexibility, and the ability to rapidly prototype and deploy web designs [37].

The website development process involved several key steps:

- Design Planning: Initial design concepts were created, focusing on user experience and information architecture. The goal was to create an intuitive and informative interface that could easily convey complex blockchain concepts.
- Content Organization: Information on different blockchain protocols was systematically organized to ensure coherent presentation and ease of navigation.
- Visual Design and Interactivity: The visual aesthetic was carefully crafted to be engaging yet informative, with interactive elements integrated to enhance user engagement and learning.
- Testing and Optimization: The website underwent several rounds of testing for usability, responsiveness, and content accuracy. Feedback was incorporated to refine the website's design and functionality.

3.2 Categorization Method

The categorization of blockchain protocols was a critical aspect of this project, intended to provide a structured and comprehensible framework for users to understand various approaches to fair transaction ordering.

- Literature Review and Analysis: An extensive literature review was conducted to gather information on different blockchain protocols. This was followed by an analysis to understand their mechanisms, applications, and implications.
- Criteria for Categorization: Protocols were categorized based on specific criteria such as their operational mechanism, targeted blockchain issues, and their impact on decentralization, security, and transaction efficiency.
- Group Formation: Based on the criteria, protocols were grouped into categories like Optimized Trade Execution, Professional Market Makers, and others. This grouping was aimed at providing clarity and facilitating easier comprehension of the protocols' purposes and functionalities.
- Continuous Updating: The categorization process is dynamic, allowing for the addition of new protocols and the reevaluation of existing categories as the field evolves.

The methodology employed in this thesis combines website development with a systematic approach to categorizing blockchain protocols, ensuring that the final product is both educational and practical for users interested in fair transaction ordering in blockchain technology.

Chapter 4

Website Overview

The Fair Transaction Ordering Website is meticulously designed to offer an engaging, intuitive, and informative experience for users interested in blockchain transaction protocols. The site combines aesthetic appeal with functional design to facilitate easy navigation and comprehension of complex concepts. Here a link to the website.

4.1 Design and Structure

4.1.1 Homepage Layout

The homepage showcases a responsive 3x3 grid of cards, each representing a different group of transaction protocols. This grid adapts to various screen sizes, changing to a 2x4 or 1x6 layout on smaller displays, ensuring a seamless user experience across devices.

4.1.2 Interactive Cards

Each card on the homepage provides interactive visual feedback when hovered over. This feature not only enhances user engagement but also makes the website dynamic and modern. The cards contain brief summaries of the protocol groups, offering users a snapshot of what each category entails.

4.1.3 Navigation Bar

A consistent navigation bar is present on all pages. It includes a home button for easy return to the main page, a contact option for user inquiries or protocol submissions, and a dropdown menu for direct access to all protocol groups. This design choice underscores the website's focus on user-friendly navigation.

Figure 4.1: Homepage

4.2 Content Presentation

4.2.1 Detailed Group Pages

Clicking on a card leads users to a dedicated page for that protocol group. Each group page starts with an expanded summary, providing more context and details about the group's focus and methodologies.

4.2.2 Pros and Cons Tables

Accompanying the summary is a table listing the advantages and disadvantages of the protocols within the group. This feature allows users to quickly grasp the strengths and limitations of each approach.

4.2.3 Individual Protocol Exploration

Each group page also features a grid of clickable cards for individual protocols. These cards, similar to those on the homepage, reveal detailed information about each protocol upon interaction. This layered approach to information presentation helps in gradually guiding the user from a general overview to specific details.

4.2.4 Interactive Elements

The interactive elements of the cards are designed to reveal concise yet comprehensive descriptions of each protocol, accompanied by links to relevant papers and websites for further reading. This interactive design engages users and encourages exploration.

4.2.5 Educational Focus

The website maintains a strong educational focus, with content crafted to be accessible and understandable to a broad audience. Explanations are concise and avoid excessive jargon to cater to both beginners and advanced users.

4.2.6 Abbreviations and Terminology

A dedicated section on the website explains all abbreviations and technical terms used. This glossary-like feature is designed to support users new to blockchain technology and enhance the overall learning experience.

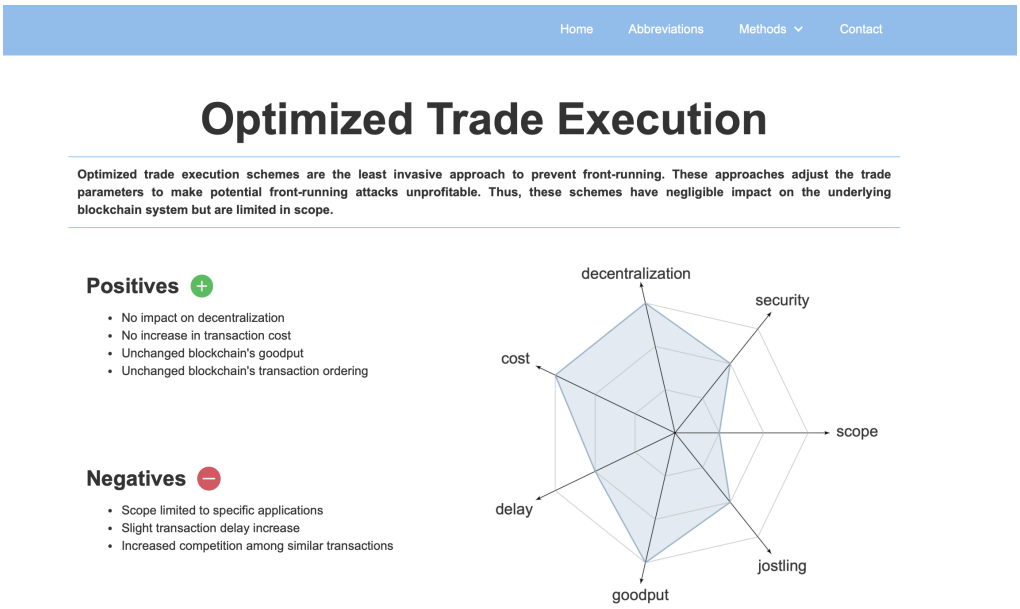

Figure 4.2: Optimized Trade Execution

The website's design, with its focus on interactivity, ease of navigation, and structured content presentation, aims to demystify the complexities of blockchain protocols. It serves as an educational tool, guiding users from a basic understanding of transaction protocols to a more detailed and comprehensive knowledge.

Chapter 5

Conclusion

The Fair Transaction Ordering Website, developed as part of this thesis, serves as an educational tool that simplifies complex blockchain transaction ordering concepts for a diverse audience. Its development faced several challenges and provides opportunities for future enhancements.

5.1 Challenges Encountered

- The categorization of protocols required balancing technical accuracy with accessibility for non-experts, a task that was both challenging and crucial for the website's success.
- Keeping the website's content current in the rapidly evolving field of blockchain technology necessitates ongoing updates.

5.2 Future Enhancements

- Plans for enhancing the website could include adding interactive elements like simulations, incorporating a community forum for user interaction, and continuously updating the content to include new developments in block chain protocols.

This project highlights the importance of making complex technological concepts accessible to a wider audience and sets a foundation for future educational tools in the blockchain space.

Bibliography

[1] L. Zhou, K. Qin, and A. Gervais, "A2mm: Mitigating frontrunning, transaction reordering and consensus instability in decentralized exchanges," *arXiv preprint arXiv:2106.07371*, 2021.

[2] P. Züst, T. Nadahalli, and Y. W. R. Wattenhofer, "Analyzing and preventing sandwich attacks in ethereum," *ETH Zürich*, 2021.

[3] L. Heimbach and R. Wattenhofer, "Eliminating sandwich attacks with the help of game theory," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022, pp. 153–167.

[4] "Flashbots," 2023, accessed: 2023. [Online]. Available: https://www.flashbots.net

[5] M. Ciampi, M. Ishaq, M. Magdon-Ismail, R. Ostrovsky, and V. Zikas, "Fairmm: A fast and frontrunning-resistant crypto market-maker," in *International Symposium on Cyber Security, Cryptology, and Machine Learning*. Springer, 2022, pp. 428–446.

[6] "Hashflow," 2023, accessed: 2023. [Online]. Available: https://www.hashflow.com

[7] "Rook," 2023, accessed: 2023. [Online]. Available: https://www.rook.fi

[8] A. Canidio and R. Fritsch, "Batching trades on automated market makers," in *5th Conference on Advances in Financial Technologies (AFT 2023)*. Schloss-Dagstuhl-Leibniz Zentrum für Informatik, 2023.

[9] "Eden," 2023, accessed: 2023. [Online]. Available: https://www.edennetwork.io

[10] "bloxroute," 2023, accessed: 2023. [Online]. Available: https://bloxroute.com

[11] "openmev," 2023, accessed: 2023. [Online]. Available: https://openmev.xyz

[12] "Cowswap," 2023, accessed: 2023. [Online]. Available: https://swap.cow.fi

[13] "Gnosis," 2023, accessed: 2023. [Online]. Available: https://www.gnosis.io

[14] C. Cachin, J. Mićić, N. Steinhauer, and L. Zanolini, "Quick order fairness," 2022.

[15] L. Baird, "The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance," *Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep*, vol. 34, pp. 9–11, 2016.

[16] Y. Zhang, S. Setty, Q. Chen, L. Zhou, and L. Alvisi, "Byzantine ordered consensus without byzantine oligarchy," in *14th USENIX Symposium on Operating Systems Design and Implementation (OSDI 20)*, 2020, pp. 633–649.

[17] K. Kursawe, "Wendy, the good little fairness widget," *arXiv preprint arXiv:2007.08303*, 2020.

[18] M. Kelkar, F. Zhang, S. Goldfeder, and A. Juels, "Order-fairness for byzantine consensus," Cryptology ePrint Archive, Paper 2020/269, 2020, https://eprint.iacr.org/2020/269. [Online]. Available: https://eprint.iacr.org/2020/269

[19] M. Kelkar, S. Deb, S. Long, A. Juels, and S. Kannan, "Themis: Fast, strong order-fairness in byzantine consensus," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 475–489.

[20] M. Kelkar, S. Deb, and S. Kannan, "Order-fair consensus in the permissionless setting," in *Proceedings of the 9th ACM on ASIA Public-Key Cryptography Workshop*, 2022, pp. 3–14.

[21] A. Constantinescu, D. Ghinea, L. Heimbach, Z. Wang, and R. Wattenhofer, "A fair and resilient decentralized clock network for transaction ordering," *arXiv preprint arXiv:2305.05206*, 2023.

[22] A. Tatabitovska, "Mitigation of transaction manipulation attacks in uniswap," 2021.

[23] L. Breidenbach, P. Daian, F. Tramèr, and A. Juels, "Enter the hydra: Towards principled bug bounties and {Exploit-Resistant} smart contracts," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1335–1352.

[24] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," 1996.

[25] Y. Doweck and I. Eyal, "Multi-party timed commitments," *arXiv preprint arXiv:2005.04883*, 2020.

[26] H. Zhang, L.-H. Merino, Z. Qu, M. Bastankhah, V. Estrada-Galiñanes, and B. Ford, "F3b: a low-overhead blockchain architecture with per-transaction front-running protection," in *5th Conference on Advances in Financial Technologies (AFT 2023)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2023.

[27] D. Malkhi and P. Szalachowski, "Maximal extractable value (mev) protection on a dag," 2022.

[28] J. H.-y. Chiang, B. David, I. Eyal, and T. Gong, "Fairpos: Input fairness in permissionless consensus," *Cryptology ePrint Archive*, 2022.

[29] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The honey badger of bft protocols," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 31–42.

[30] A. Asayag, G. Cohen, I. Grayevsky, M. Leshkowitz, O. Rottenstreich, R. Tamari, and D. Yakira, "A fair consensus protocol for transaction ordering," in *2018 IEEE 26th International Conference on Network Protocols (ICNP)*. IEEE, 2018, pp. 55–65.

[31] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[32] M. K. Reiter and K. P. Birman, "How to securely replicate services," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 16, no. 3, pp. 986–1009, 1994.

[33] "Blockswap," 2023, accessed: 2023. [Online]. Available: https://www.blockswap.network

[34] O. Alpos, I. Amores-Sesar, C. Cachin, and M. Yeo, "Eating sandwiches: Modular and lightweight elimination of transaction reordering attacks," *arXiv preprint arXiv:2307.02954*, 2023.

[35] A. Kavousi, D. V. Le, P. Jovanovic, and G. Danezis, "Blindperm: Efficient mev mitigation with an encrypted mempool and permutation," *Cryptology ePrint Archive*, 2023.

[36] L. Heimbach and R. Wattenhofer, "Sok: Preventing transaction reordering manipulations in decentralized finance. arxiv," *arXiv preprint arXiv:2203.11520*, 2022.

[37] "Webflow," 2023, accessed: 2023. [Online]. Available: https://webflow.com