Analysis of the SUAVE Architecture, Mechanisms and Use-Cases

Master Thesis Proposal Handout

Gebele, Jonas (Matr. 03697461)

Introduction

The concept of Maximal Extractable Value (MEV) has become a focal point in the discourse around blockchain technology, particularly within the Ethereum ecosystem. Initially, MEV was a relatively obscure phenomenon, primarily exploited by savvy network participants known as MEV searchers. These individuals, leveraging complex algorithms, scoured the Ethereum network for opportunities to extract value through transaction reordering, insertion, or censorship[2]. This pursuit, while profitable for miners and searchers, introduced a range of negative externalities for the network and its users. The resultant network congestion and inflated gas prices not only degraded user experience but also emphasized the inherent inequalities in the system[2]. In the wake of these escalating concerns, Flashbots[1] emerged as a collective response. Their journey commenced with a mission to illuminate the Dark Forest[3] of MEV and to democratize its extraction, aiming to reinforce the principles of Ethereum. Their solution, the Flashbots Auction[2], marked a significant step in addressing the MEV crisis, offering a more equitable alternative that promised pre-trade privacy and mitigated the risks associated with transaction reordering[1]. However, the success story of Flashbots Auction was not without its limitations. Issues of permissioned participation, client diversity, and centralized infrastructure persisted, suggesting that the battle against centralization and trust issues in MEV extraction was far from over. Persistent issues such as permissioned participation, lack of client diversity, and reliance on centralized infrastructure indicated that the battle against centralization and trust issues in MEV extraction was ongoing[1]. As Flashbots pivoted towards their next venture, SUAVE (Single Unifying Auction for Value Expression), they aimed to reconfigure the roles of the mempool and block builder from existing blockchains. This evolution was not just a technical enhancement but also a philosophical realignment, emphasizing the need to maintain MEV decentralization and uphold the wider decentralization and neutrality of cryptocurrency[1].

[1] https://www.flashbots.net/
[2] https://github.com/flashbots/mev-geth

SUAVE promises a highly specialized and decentralized alternative, enabling not just a new way of handling MEV but also redefining the blockchain stack itself. It proposes a universal preference environment, an optimal execution market, and decentralized block building, all operating within a specialized chain. These components are designed to collaboratively address the inefficiencies and centralization tendencies inherent in traditional MEV extraction methods. By empowering users with pre-confirmation privacy, ensuring equitable distribution of MEV, and facilitating cross-domain coordination, SUAVE aims to preserve the decentralized ethos that is fundamental to cryptocurrency[1].

Problem Statement

The introduction of SUAVE heralds a new era in the landscape of MEV extraction, promising a more decentralized, fair, and efficient system. However, as with any nascent technology, it brings forth a set of challenges and questions that need to be critically examined. The effectiveness of SUAVE in real-world scenarios, its ability to truly decentralize MEV extraction, and the trustworthiness of its mechanisms remain under-explored. There is a need for an in-depth assessment of SUAVE's architectural design, its components, and the trust solutions it proposes. While SUAVE aims to neutralize the pressures from exclusive order flow and cross-domain MEV, the practicality and robustness of these solutions are yet to be proven. The decentralization of block building, a critical component in preserving network neutrality and resilience, is an ambitious goal. The platform must demonstrate its ability to withstand the centralizing forces that have historically plagued MEV extraction and block production. Moreover, the transition from a centralized to a decentralized system, especially one that involves sensitive data and complex transactions, brings about significant trust and security considerations. In light of these considerations, this thesis seeks to provide a comprehensive evaluation of SUAVE, dissecting its architecture, understanding its mechanisms, and critically assessing its potential as a trustless and decentralized solution for MEV extraction. Through this exploration, the research aims to contribute valuable insights to the discourse on MEV, decentralization, and the future of block building.

Research Questions

- **1. Assessment of SUAVE architecture and mechanisms**
  This question aims to dissect and analyze the architectural framework and operational mechanisms of SUAVE, placing them in a comparative context with traditional MEV solutions, particularly the Flashbots Auction. It seeks to identify the advancements SUAVE introduces, understand how it addresses the limitations of previous systems, and evaluate the implications of these changes for efficiency, security, and user experience.
- **2. Evaluation of Toolkit for SUAVE Applications (SUAPPs)**
  The focus here is to critically assess the toolkit provided for developing SUAVE Applications (SUAPPs). This evaluation will consider the tools' versatility, ease of use, and

their capacity to aid developers in creating effective MEV solutions. The question will delve into the capabilities and limitations of the toolkit, examining how well it equips developers to exploit the unique features of SUAVE and the overall impact on fostering innovation within the MEV space.

- **3. Analysis of Potential Real-World Use-Cases of SUAPPs**
  This question seeks to explore the practical applications and real-world utility of SUAPPs. It will investigate various scenarios and domains where SUAPPs can be effectively implemented, analyzing their potential to address existing challenges and create new opportunities within the MEV landscape and broader blockchain ecosystems.

Upon completion, this research will offer a comprehensive understanding of SUAVE's contribution to the evolving landscape of MEV solutions, providing insights that could shape the future directions of blockchain technology and decentralized finance.

Methodology

The research will employ a comprehensive, multi-faceted approach:

- **Technical Analysis:** An in-depth examination of SUAVE's technical documents, whitepapers, and official documentation will be conducted to understand its architecture and mechanisms. This will involve reviewing and analyzing the foundational technology and theoretical framework that underpins SUAVE.
- **Comparative Study:** This involves comparing SUAVE's approach with traditional and existing MEV solutions like Flashbots Auction. Key metrics for comparison will include efficiency, security, and decentralization. The aim is to highlight the advancements SUAVE introduces and assess whether these innovations address the limitations and challenges prevalent in existing systems.
- **Practical Engagement:** Gaining firsthand experience with SUAVE by setting up a node, interacting with the SUAVE testnet, and potentially developing a simple SUAPP. This practical engagement aims to provide insights into the system's workings, usability, challenges, and potential from a developer's perspective.
- **Community and Developer Insights:** Engaging with the SUAVE community and developers through forums, discussions, and possibly interviews to gather varied perspectives and insights. This will help collect a diverse range of opinions and experiences, offering a well-rounded understanding of SUAVE's benefits and areas for improvement as seen by its users and contributors.
- **Case Study Analysis:** Identifying and analyzing potential real-world use cases for SUAPPs. This step involves exploring how SUAPPs are being used or can be used in

various scenarios, focusing on their practicality, scalability, and impact. The aim is to provide concrete examples of SUAPPs in action and to understand their implications for the future of MEV and blockchain technology.

Starting Literature

The following resources will provide a foundational understanding and context for the research:

- **SUAVE's Official Documentation**[3]**:** Comprehensive documents that detail the foundational concepts, technical specifications, and operational mechanisms of SUAVE. This will serve as the primary resource to understand the intricacies of the SUAVE platform.
- **GitHub Repositories**[4]**:** Analysis of the codebase and developmental progress of SUAVE and related tools will be conducted. Reviewing the repositories will provide insights into the practical implementation of the SUAVE protocols and the community's contributions to its development.
- **Setting Up Own Node:** Gaining practical experience with SUAVE by setting up and operating a node. This hands-on experience will provide a deeper understanding of how SUAVE operates in a real-world setting and its interactions with users and other network participants.
- **SUAVE Forum Discussions**[5]**:** Engaging with ongoing discussions and insights from the SUAVE community and developers. Forums are a valuable source of community sentiment, troubleshooting, innovative ideas, and the challenges faced by users and developers.
- **Related Academic and Industry Papers:** Exploring existing literature on MEV, blockchain auction mechanisms, and decentralized solutions. Academic and industry papers will provide a broader context and understanding of the MEV landscape, the evolution of auction mechanisms, and how SUAVE fits within this broader ecosystem.

Timeline

This Master Thesis will be conducted over a six-month period, starting on 15th January 2024 and culminating in the submission of the thesis on 15th July 2024. The timeline is structured as follows:

- **January - March 2024: Literature Review** The initial phase will be dedicated to an extensive review of SUAVE's official documentation, related academic and industry papers, and engagement with community forums to establish a robust theoretical foundation.

[3] https://suave.flashbots.net/
[4] https://github.com/flashbots
[5] https://collective.flashbots.net/

- **March 2024: Setting Up Own Infrastructure** During this time, setting up a personal node and engaging with the SUAVE test network will provide practical experience and a deeper understanding of the operational aspects of SUAVE.
- **April - June 2024: Evaluation of Architecture, Infrastructure, and Toolkit** This period will focus on a detailed analysis of SUAVE's architecture and infrastructure, comparing it with existing MEV solutions to identify advancements and areas for improvement. Concurrently, experimenting with the toolkit provided for SUAVE applications and assessing various real-world use cases will be conducted to understand the practical implications and potential of SUAVE in the MEV landscape.
- **June - July 2024: Writing Thesis** The final phase will involve compiling all research findings, analyses, and evaluations into a comprehensive thesis. This period will ensure that all aspects of the research are well-documented, analyzed, and presented in a cohesive manner.

This adjusted timeline provides a structured and systematic approach to exploring SUAVE, from theoretical understanding to practical application, culminating in a well-researched and detailed Master Thesis.

Summary

This Master Thesis Proposal is dedicated to a rigorous and comprehensive examination of the SUAVE platform, focusing on its architectural and operational innovations in the context of Maximal Extractable Value (MEV) within the Ethereum ecosystem. It aims to critically analyze SUAVE's potential to decentralize MEV extraction, enhance fairness, and bolster security in blockchain transactions. By investigating SUAVE's technological advancements, trust mechanisms, and real-world application potentials, this thesis aspires to contribute substantive insights and evaluations to the ongoing scholarly and practical debates in the fields of blockchain technology and MEV. The findings are expected to not only enrich academic understanding but also inform future developments and strategies in MEV solutions.

Literatur

[1] Flashbots. "The Future of MEV is SUAVE". In: *Flashbots Blog* (2022).

[2] Philip Daian;Steven Goldfeder;Tyler Kell;Yunqi Li;Xueyuan Zhao;Iddo Bentov;Lorenz Breidenbach;Ari Juels. "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges". In: *Cryptography and Security* (2019).

[3] Dan Robinson; Georgios Konstantopoulos. "Ethereum is a Dark Forest". In: *Pardigm Blog* (Aug 28, 2020).