УДК 004.057.4

РАЗРАБОТКА ДЕЦЕНТРАЛИЗОВАННОЙ БИРЖИ С КОНФИДЕНЦИАЛЬНЫМ ИСПОЛНЕНИЕМ ТОРГОВЫХ ЗАЯВОК

Смекалов А. А. (Санкт-Петербургский политехнический университет Петра Великого)
Научный руководитель – доцент Шошмина И. В.
(Санкт-Петербургский политехнический университет Петра Великого)
fy.fa2018@yandex.ru

Введение.

Блокчейн Solana является одной из наиболее популярных и производительных платформ для децентрализованных финансовых приложений, обрабатывающий тысячи транзакций в секунду. Несмотря на отсутствие публичного мемпула (списка обрабатываемых транзакций) в архитектура Solana, валидаторы имеют контроль над порядком обработки транзакций, что создает возможности для MEV-атак (maximal extractable value), в частности к sandwich-атакам [1]. Sandwich-атака представляет собой манипуляцию, при которой злоумышленник размещает свои транзакции до и после транзакции жертвы, извлекая прибыль за счёт искусственного изменения цены [1]. Существующие DEX (decentralized exchange) на Solana не обеспечивают должной защиты от подобных угроз, поскольку все параметры сделки видны в открытом виде до момента исполнения транзакции. Специфика архитектуры Solana требует разработки специализированных решений, учитывающих особенности её консенсуса и модели параллельного выполнения транзакций.

Основная часть.

Предлагаемое решение представляет собой децентрализованную биржу на базе Solana с интеграцией протокола Arcium MPC (secure multi-party computation) [2, 3]. Ключевая идея заключается в том, что критически важные параметры торговой операции (объём свопа, текущие параметры ликвидности пула) шифруются на стороне клиента и обрабатываются в распределённой сети MPC-узлов без возможности восстановления исходных данных ни одним из участников, включая валидаторов [2]. При размещении заявки пользователь формирует зашифрованное представление параметров сделки, которое передаётся в сеть Arcium MPC [3]. Узлы выполняют необходимые расчёты и возвращают результат в виде готовой транзакции, которая публикуется в блокчейне Solana. Критически важно, что в момент нахождения транзакции в очереди на обработку валидатором все её параметры остаются зашифрованными, а расшифровка происходит только на этапе непосредственного исполнения в смарт-контракте [4]. Это делает невозможным построение атакующих транзакций вокруг сделки пользователя [5]. В рамках планируемой экспериментальной оценки предполагается измерить следующие метрики: задержка с момента отправки торговой заявки до финального подтверждения транзакции, потребление вычислительных ресурсов смарт-контракта (compute units, CU) на транзакцию в сравнении с другими децентрализованными биржами, время MPC-вычисления в зависимости от числа узлов, а также эффективность защиты от sandwich-атак посредством моделирования атаки в тестовой сети.

Выводы.

Разработанное решение представляет собой практическую реализацию DEX на Solana с защитой от MEV-атак на основе конфиденциальных вычислений [2, 5]. Система позволит существенно снизить финансовые потери пользователей от sandwich-атак и повысить доверие к децентрализованным финансовым сервисам на блокчейне Solana. Перспективы исследования включают расширение функциональности биржи и масштабирование решения для работы с высокими объёмами торговых операций.

Литература:

1. Gramlich V., Jelito D., Sedlmeir J. Maximal extractable value: Current understanding, categorization, and open research questions // Electronic Markets. — 2024.
2. Lindell Y. Secure Multiparty Computation // Computations of the ACM. — 2021
3. Arcium Protocol Documentation. Confidential Computing Infrastructure [Электронный ресурс]. – 2024. – URL: https://docs.arcium.com/ (Дата обращения: 10.01.2026).
4. 4. Yakovenko A. Solana: A new architecture for a high performance blockchain [Электронный ресурс]. – 2018. – URL: https://solana.com/solana-whitepaper.pdf (Дата обращения: 08.01.2026).
5. Heimbach L., Wattenhofer R. Eliminating Sandwich Attacks with the Help of Game Theory // Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security. — New York, 2022. — P. 153–167.