DOI 10.37882/2223-2966.2025.05.33

ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ ОБРАБОТКИ ТРАНЗАКЦИЙ НА БЛОКЧЕЙНЕ TON

PERFOMANCE OPTIMIZATION OF TRANSACTIONS PROCESSING ON BLOCKCHAIN TON

T. Semenyuk

Summary. This article explores architectural and technical approaches to optimizing transaction processing performance in the TON blockchain ecosystem using a DEX protocol as a case study. The study addresses challenges such as high latency, gas fees, and the limitations of reactive trading under traditional interactions via external wallets. As a solution, the article proposes a transition to an intent-based interaction model, where users generate an intent to perform an operation without explicitly signing each transaction at the time of submission. This approach allows batching of requests, executing only essential steps on-chain, and significantly reducing network load. The core element of the proposed architecture is the SmartAccount, which enables non-custodial and programmable control over user funds. It operates alongside an embedded wallet and a sequencer system responsible for processing and finalizing user intents. The sequencer collects and orders intents in an off-chain execution queue, performs pre-validation, deduplication, and signature verification, and forms aggregated ExecuteBundles that are committed on-chain via a domain-specific smart contract. This results in high scalability, minimal response latency, and zero slippage. Comparative performance assessments are presented, along with recommendations for applying the intent-based processing model in high-load decentralized systems.

Keywords: blockchain, distributed ledger, transactional systems, distributed systems.

Семенюк Тимофей Андреевич
аспирант, Владимирский государственный университет им. А.Г. и Н.Г. Столетовых
rustfy@gmail.com

Аннотация. В статье исследуются архитектурные и технические подходы к оптимизации производительности обработки транзакций в экосистеме блокчейна TON на примере DEX протокола. Рассматриваются проблемы высокой задержки, стоимости газа и невозможности реализации реактивной торговли в условиях традиционного взаимодействия с внешними кошельками через внешние кошельки. В качестве решения предлагается переход к модели intent-based взаимодействия, в которой пользователь формирует интент (намерение) на выполнение операции без непосредственного подписания каждой транзакции в момент её отправки. Такой подход позволяет агрегировать запросы, выполнять onchain-подтверждение только ключевых шагов и значительно снизить нагрузку на сеть. Благодаря этому достигается высокая масштабируемость, минимальные задержки отклика и нулевое проскальзывание цен. Представлены сравнительные оценки производительности и даются рекомендации по применению модели intent-based процессинга в высоконагруженных децентрализованных системах.

Ключевые слова: блокчейн, технологии распределенных реестров, транзакционные системы, распределенные системы.

Введение

Финансовые транзакции и цифровые активы являются одними из ключевых применений блокчейн-технологий. С развитием децентрализованных бирж (DEX), протоколов кредитования, стейблкоинов и цифровых валют центральных банков (CBDC) возникает потребность в высокопроизводительных инфраструктурах, способных обрабатывать тысячи операций в секунду с минимальной задержкой. Текущие ограничения по масштабируемости, стоимости газа и времени финализации транзакций затрудняют применение классических блокчейн-платформ для реализации реактивных торговых стратегий, микроплатежей и автоматизированных систем управления активами [1].

Дополнительной критически важной характеристикой финансовых систем на блокчейне является их некастодиальность — принцип, по которому пользователи сохраняют полный контроль над своими средствами без необходимости доверять посредникам. Это обеспечивает безопасность, прозрачность и совместимость с децентрализованными протоколами.

TON (The Open Network) представляет собой высокопроизводительный блокчейн с поддержкой шардирования и быстрой финализацией блоков. Однако при построении систем высокочастотной торговли остаются ограничения по времени реакции, связанному с двухфазной ончейн-обработкой, необходимостью пользовательской подписи каждой транзакции и затратами на газ.

Финансовые транзакции и цифровые активы являются одними из ключевых применений блокчейн-технологий. С развитием децентрализованных бирж (DEX), протоколов кредитования, стейблкоинов и цифровых валют центральных банков (CBDC) возникает потребность в высокопроизводительных инфраструктурах, способных обрабатывать тысячи операций в секунду с минимальной задержкой. Текущие ограничения по масштабируемости, стоимости газа и времени финализации транзакций затрудняют применение классических блокчейн-платформ для реализации реактивных торговых стратегий, микроплатежей и автоматизированных систем управления активами.

TON (The Open Network) представляет собой высокопроизводительный блокчейн с поддержкой шардирования и быстрой финализацией блоков. Однако при построении систем высокочастотной торговли остаются ограничения по времени реакции, связанному с двухфазной ончейн-обработкой, необходимостью пользовательской подписи каждой транзакции и затратами на газ.

Одним из краеугольных камней в построении доверенной блокчейн-инфраструктуры является обеспечение безопасности при сохранении гибкости пользовательского опыта и обеспечения критериев высокой производительности, снижения времени отклика (latency) и увеличения количества обрабатываемых заявок во времени (throughput). В контексте intent-based execution и некастодиальных решений особое значение приобретает продуманная криптографическая модель, обеспечения достаточного уровня криптографической безопасности [2].

Intent-based Protocol реализует двухуровневую систему аутентификации, в которой пользовательские действия авторизуются не глобальным приватным ключом, а уникальным *embedded*-ключом устройства (*DeviceID*), зарегистрированным в *SmartAccount*. Эти ключи могут быть отозваны, переустановлены или ограничены по типу и частоте операций.

Для подписи ордеров используется алгоритм *Ed25519* [3], такой криптографический алгоритм ассиметричной подписи поддерживается нативно в экосистеме TON. Это обеспечивает компактность подписей, высокую скорость проверки, низкую стоимость газа и совместимость с существующей логикой смарт-контрактов. Подписи проверяются в Sequencer до агрегации и повторно валидируются on-chain в Intent-Based Execution Protocol.

Важно, что модель исключает передачу приватных ключей в сеть или необходимость взаимодействия с внешним кошельком в момент исполнения. Это достигается благодаря переносу доверия с внешнего интерфейса на авторизованное устройство пользователя, что снижает риск фишинга, вредоносных расширений и потери контроля над аккаунтом.

Проблемы пользовательского опыта и масштабируемости в блокчейне

Современные блокчейн-платформы стремятся обеспечить не только безопасность и децентрализацию, но и приемлемое качество пользовательского опыта (UX), особенно в контексте частых, мелких или автоматизированных операций. Однако анализ существующих решений на популярных блокчейнах (Ethereum, Solana, BNB Chain, Polygon) показывает, что большинство из них сталкиваются с рядом ограничений:

- необходимость подтверждения каждой транзакции пользователем вручную или через интерфейс кошелька;
- высокая стоимость газа при интенсивных вызовах (даже на L2);
- отсутствие согласованного механизма предварительных интентов и асинхронного исполнения;
- значительная зависимость задержек от сетевой конгестии и времени блоков.

Для улучшения UX в последние годы появляются модели, ориентированные на оптимизацию взаимодействия пользователя с сетью:

- batching (агрегация вызовов);
- session keys и ephemeral auth;
- account abstraction (ERC-4337) [4];
- intent-based execution (Espresso, Anoma, StarkNet).

Описание Intent-Based execution модели

Подход *intent-based execution* предлагает концептуально новую модель взаимодействия пользователя с блокчейном. Вместо немедленного подписания транзакции и её публикации в сеть, пользователь формирует «интент» — цифровое описание желаемого действия, подписанное авторизованным устройством или ключом. Этот интент может быть обработан off-chain сервисами, агрегирован, упорядочен и затем выполнен через on-chain подтверждение без необходимости участия пользователя в момент исполнения.

Ключевые особенности подхода:

- Асинхронность: интенты могут быть созданы заранее и обработаны без немедленного участия пользователя;
- Гибкость: обработка интентов может зависеть от внешних условий (например, рыночной цены);
- Экономичность: группировка интентов в пачки снижает стоимость газа на единицу операции;
- Улучшенный пользовательский опыт: отсутствие модальных окон подтверждения, реактивность и предсказуемость исполнения.

В контексте архитектуры *Intent-Based Execution*, интенты реализуются через структуру сообщения, подписанного встроенным приватным ключом. Пользовательские сообщения обрабатываются в *offchain* в сервисе (*sequencer*), который проверяет подписи, проверяет валидность пользовательского сообщения, дедуплицирует дублирующие запросы и формирует агрегированные *ExecuteBundle* для *on-chain* исполнения на блокчейне.

Тем не менее, ни одно из решений не стало универсальным стандартом, а применение подобных подходов в TON до сих пор ограничено. Современные блокчейн-платформы стремятся обеспечить не только безопасность и децентрализацию, но и приемлемое качество пользовательского опыта (UX), особенно в контексте частых, мелких или автоматизированных операций. Однако анализ существующих решений на популярных блокчейнах (Ethereum, Solana, BNB Chain, Polygon) показывает, что большинство из них сталкиваются с рядом ограничений:

- необходимость подтверждения каждой транзакции пользователем вручную или через интерфейс кошелька;
- высокая стоимость газа при интенсивных вызовах (даже на L2)
- отсутствие согласованного механизма предварительных интентов и асинхронного исполнения;
- значительная зависимость задержек от сетевой конгестии и времени блоков.

Тем не менее, ни одно из решений не стало универсальным стандартом, а применение подобных подходов в TON до сих пор ограничено. Анализ пользовательского опыта на примере DEX на TON показывает, что при взаимодействии с кошельками через ton-connect возникают задержки:

- высокая стоимость газа при частом исполнении;
- необходимость подтверждения каждой операции в внешнем кошельке;
- задержки, связанные с распространением и подтверждением транзакций в TON (до 1 минуты).

Это делает невозможным, например, эффективную реализацию 1-кликовой торговли и реактивных стратегий на быстро меняющемся рынке.

Архитектура Intent-Based Execution Protocol

Пользователь создает персональный SmartAccount, связанный с мастер-адресом через ончейн-сообщение от главного кошелька. Он может привязать одно или несколько устройств (DeviceID), каждое из которых может подписывать сообщения без участия внешнего кошелька с помощью встраиваемого кошелька (embedded wallet).

Свойства SmartAccount контракта:

- некастодиальный: доступ к средствам сохраняется за пользователем;
- изолирован от внешнего вывода средств вне протокола;
- управляется через смарт-контракт, проверяющий подписи устройств.

Вместо немедленной ончейн-обработки каждый ордер пользователя отправляется в модуль Sequencer, где:

- превалидируется пользовательское сообщение, устанавливаются необходимые дополнительные параметры (например, время приема сообщения);
- упорядоченные сообщения формируют список исполняемых заявок;
- формируется ExecuteBundle каждые N секунд и передается в смарт-контракт исполнения заявок

Экспериментальным путем вылявлено что ExecuteBundle может содержать до 100 ордеров и агрегированно передаётся в смарт-контракт в блокчейн TON, что снижает издержки газа до ~2.5 раз.

Оптимизация задержек и масштабируемости

End-to-End Latency: для пользователя задержка остается фиксированной фиксированная и зависима только от пользовательского интерфейса и скорости обработки offchain. Задержка между созданием и обработкой (финализацией) заявки на блокчейне достигает 40с и ограничивается исключительно пропускной способность блокчейна.

При оптимизации процесса генерации блоков, например, генерация блоков со средним временем в 1 секунду, задержка финализации на блокчейне уменьшается до 10 секунд, и ограничивается только реализацие протокола доменной области блокчейн.

Количество операций в секунду ограничено только числом активных SmartAccount, что обеспечивает теоретически неограниченную масштабируемость из-за динамического шардирования архитектуры блокчейна

Таблица 1.
Сравнение с классической моделью TON

Метрика	Классическая модель	Intent-based Protocol
Подписание	Через внешний кошелёк	Signless embedded wallet
Газ	Высокий (1 txn = 1 msg)	Агрегация, -2.5x затрат
Финализация	По 1 ордеру	Агрегированные интенты
Масштабируемость	Ограничена seqno контракта кошелька	Параллельно (SmartAccount * N)

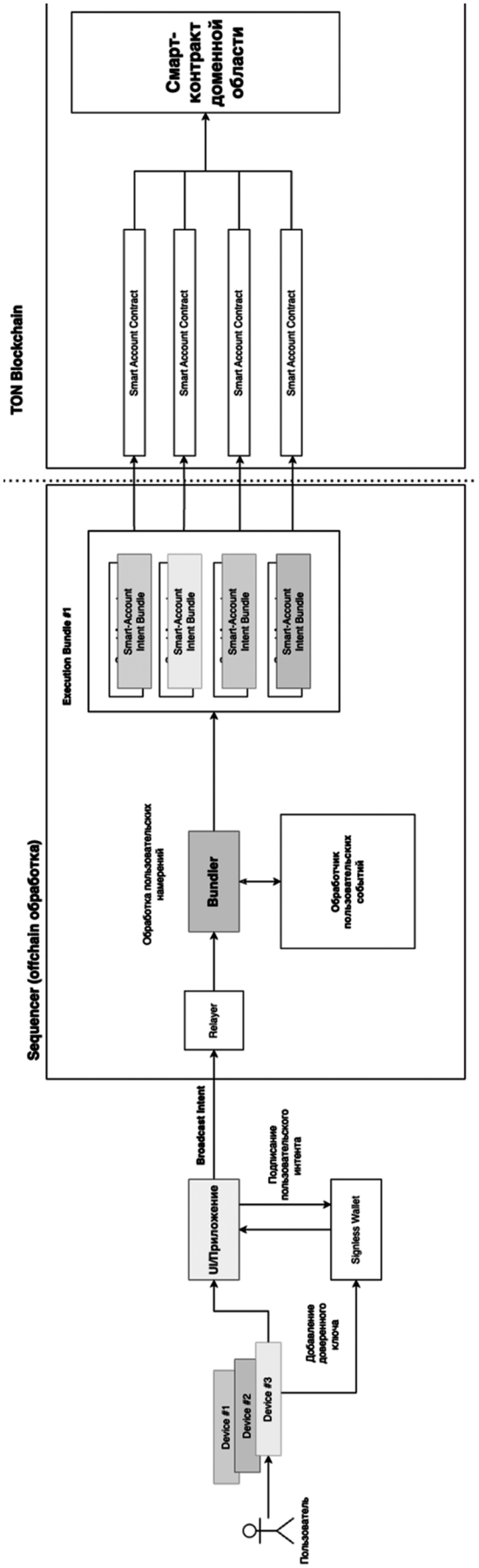

Рис. 1. Архитектура предполагаемого решения

TON, данное основание валидно в случае, если смарт-контракты распределенны равномерно по шардам блокчейна.

На рис. 2 приведены результаты имитационного моделирования, при котором сравнивались решения классической обработки транзакций на блокчейне и intent-based архитектуры.

Применимость модели за пределами финансового сектора

Архитектура intent-based execution, реализованная в Intent-based Protocol, применима не только к финансовым операциям, но и к широкому спектру нефинансовых сценариев взаимодействия в децентрализованных системах.

Supply Chain (цепочки поставок)

- **Отложенное исполнение заказов:** поставщик может выпустить интент на отгрузку после получения цифрового подтверждения платежа или сертификации;
- **Автоматизация логистики:** интенты могут триггерить перемещение товаров, обновление статуса доставки или начисление страховки без необходимости подтверждения вручную;
- **Верификация происхождения:** участники цепочки могут подписывать последовательные интенты, фиксирующие происхождение продукции.

IoT и Smart City

- Датчики и устройства могут выпускать интенты на запись событий (например, превышение порога температуры) или запросы к инфраструктуре (например, активация освещения);
- Автоматические контракты реагируют на события, поступающие от авторизованных устройств, без участия пользователя;
- Групповое исполнение: пачки интентов от разных устройств могут агрегироваться и обрабатываться атомарно.

DAO и управление

- Голосование через интенты: участники выпускают интенты, отражающие голос или инициативу, которые агрегируются и финализируются в блокчейне;
- Программируемое участие: интенты могут содержать условия, при которых голос должен вступить в силу (например, при достижении кворума).

Таким образом, intent-based архитектура представляет собой универсальный механизм асинхронного и мас-

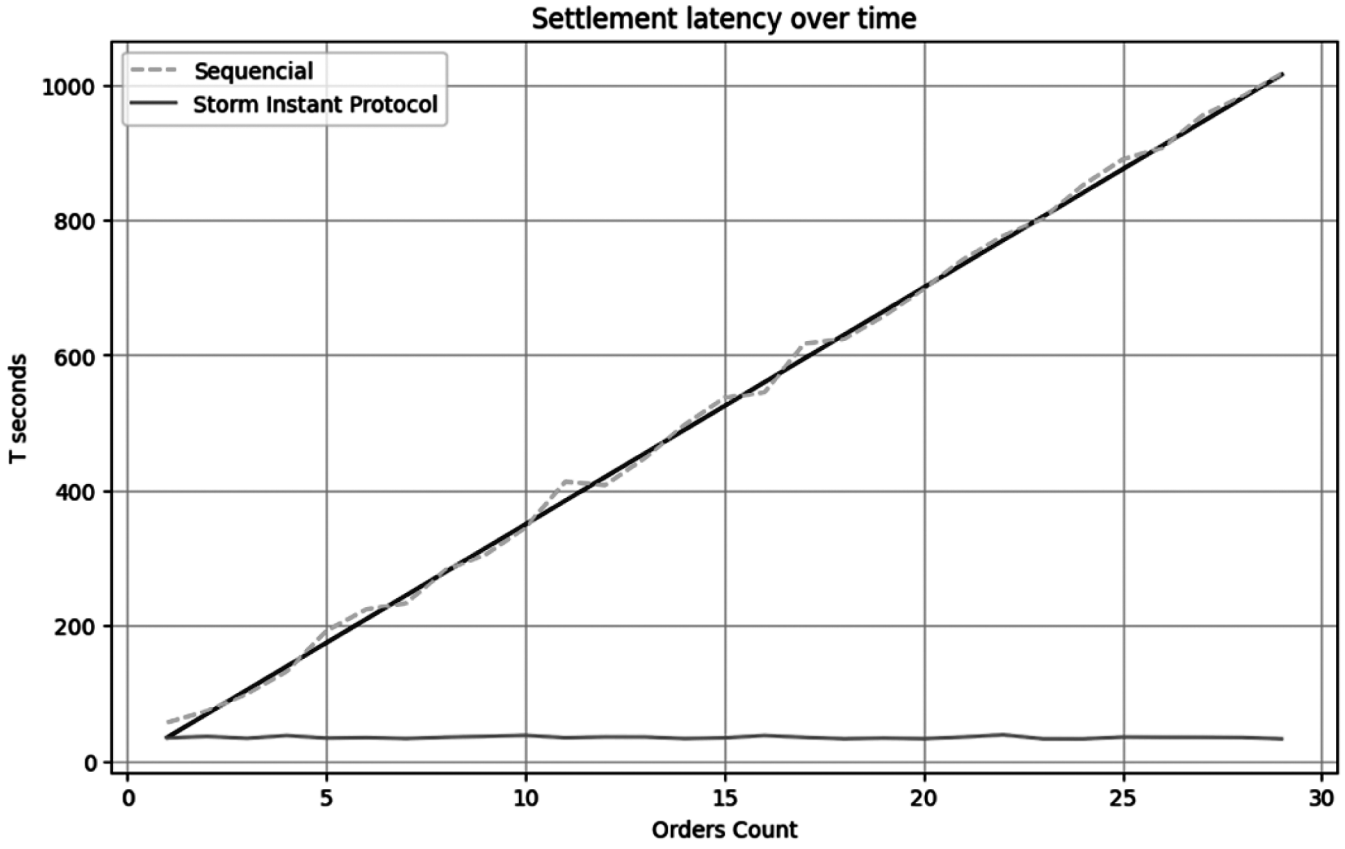

Рис. 2. Результаты моделирования обработки пользовательских сообщений

штабируемого взаимодействия между пользователями и смарт-контрактами, выходящий далеко за рамки торговли или DeFi.

Заключение

Архитектура intent-based на базе блокчейна TON демонстрирует принципиально иной подход к построению высокопроизводительной DEX-платформы. Использование смарт-аккаунтов, встроенных кошельков и промежуточной агрегации позволяет достичь уровня производительности, ранее недоступного в классических блокчейн-сценариях.

Такая модель может быть расширена на другие сферы, включая DeFi, игровые приложения и автоматизированные торговые системы, где важна мгновенная реакция, низкие комиссии и высокая масштабируемость.

ЛИТЕРАТУРА

1. Володкевич С.И. Современные условия и источники формирования цифровых навыков субъектов малого и среднего предпринимательства // Креативная экономика. 2020. Т. 14. №4. С. 485–496.
2. Демидов Н.В. Трудовое право: учеб. пособие для вузов / ред.-сост. Н.В. Демидов. М.: Издательство Юрайт, 2023. 203 с.
3. Крымский А.И. Правовое регулирование трудовых отношений в субъектах малого предпринимательства: дис. . . . канд. юрид. наук. Томск, 2004. 229 с.
4. Кузнецова Н.В., Золотарева Л.Г. Особенности документационного обеспечения работы с персоналом у субъектов малого и среднего предпринимательства // Активизация интеллектуального и ресурсного потенциала регионов: Материалы IV Всероссийской научно-практической конференции. 2018. С. 284–289.
5. Куренной А., Костян И., Хныкин Г. Цифровая экономика России. Электронное делопроизводство трудовых отношений // ЭЖ-Юрист. 2017. № 37. С. 10.
6. Парфенова Д.С., Перцева П.В. Зарубежный опыт цифровизации в социально-трудовых отношениях // Исследование инновационного потенциала общества и формирование направлений его стратегического развития: сборник научных статей 9-й Всероссийской научно-практической конференции с международным участием. 2019. С. 14–20.
7. Пряженников М.О. Дифференциация локального правового регулирования в зависимости от масштаба предприятия // Трудовое право в России и за рубежом. 2016. № 4. С. 20–23.
8. Щербак С.С. Расширение дифференциации в трудовом законодательстве Российской Федерации в зависимости от объема предпринимательской деятельности работодателя // Право и экономика. 2017. № 10. С. 63–69.
9. Иванова Ж.Б. Интерактивный игровой процесс в преподавании юридических дисциплин // Научно-методический электронный журнал «Концепт». — 2017. — Т. 9. — С. 40–43. [Электронный ресурс]. Режим доступа://e-koncept.ru/2017/870007.htm: (дата обращения: 01.02.2024).
10. Колесова Д.В., Харитонова А.А. «Игра слов: во что и как играть на уроках русского языка». С-П.: Златоуст, 2011 — с. 152.

Журнал «Современная наука: актуальные проблемы теории и практики»