Производительность и масштабируемость транзакционных систем на примере шардированного блокчейна

Т.А. Семенюк

Владимирский государственный университет

Аннотация: В данной статье рассматривается вопрос повышения производительности и масштабируемости транзакционных систем на примере архитектуры шардированного блокчейна. Особое внимание уделяется применению подхода, основанного на поисковых запросах — модели, в которой транзакционные намерения пользователя обрабатываются асинхронно и агрегированно. Это позволяет значительно снизить нагрузку на сеть и достичь высокой пропускной способности без ухудшения пользовательского опыта. Предлагаемая архитектура базируется на полностью контролируемых смарт-аккаунтах, встроенных кошельках и сторонней обработке поисковых запросов пользователя через специализированный модуль. В результате достигается масштабируемость, отвечающая требованиям высокочастотной торговли и автоматизированных децентрализованных приложений. Приводятся ключевые метрики эффективности и сценарии применения вне финансового сектора.
Ключевые слова: блокчейн, технологии распределенного реестра, транзакционные системы, распределенные системы.

Введение

Масштабируемость и производительность остаются критическими задачами для современных блокчейн-платформ. С увеличением числа пользователей и частоты взаимодействий системы сталкиваются с ограничениями по скорости финализации, стоимости газа и пропускной способности. Это особенно актуально для приложений в области децентрализованных финансов (decentralized finance – DeFi), микротранзакций и IoT [1, 2]. В ответ на данные вызовы появляются архитектурные подходы, переосмысливающие модель взаимодействия между пользователем и блокчейном.

TON (The Open Network) — это высокопроизводительная платформа с поддержкой шардирования и российской национальной блокчейн-платформы Мастерчейн. Её архитектура позволяет обрабатывать десятки тысяч транзакций в секунду. Однако для реализации сценариев с высокой

интерактивностью и минимальными задержками требуется переход к более гибкой транзакционной модели. Одним из таких решений является модель, основанная на заранее подписанных пользовательским приватным ключом сообщениях (интентах).

В данной статье проводится обзор принципов построения интент-ориентированной архитектуры и предлагается схема её реализации в экосистеме TON. Также анализируются возможности масштабируемости, снижение задержек и применение модели в различных отраслях, влияние на сетевые задержки и поведенческую модель трафика транзакционной активности [3].

Архитектура и модель интентов

Смарт-аккаунты и встраиваемые кошельки

Смарт-аккаунт – это программируемый контракт, который обеспечивает управление доступом к пользовательским средствам. Он поддерживает авторизацию действий через список разрешённых устройств (DeviceID), привязанных к главному кошельку. Для генерации транзакций используется встроенный криптографический ключ устройства, что исключает необходимость вызова внешнего кошелька для каждой операции.

Такая схема обеспечивает полный контроль (некастоидальность), изоляцию доступа к средствам и повышенную безопасность. Пользователь сохраняет контроль над активами, а операции могут исполняться в автоматизированном режиме.

Пример возможной реализации интент-ориентированной архитектуры на примере шардированного блокчейна показана на рис.1.

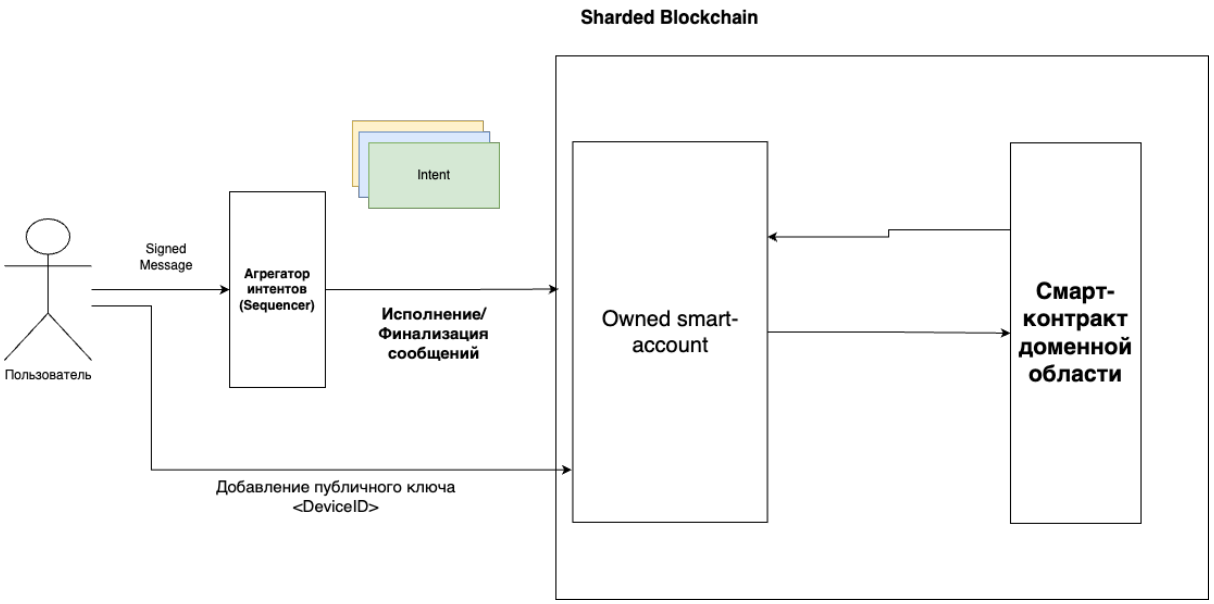

Рис. 1. Пример реализации интент-ориентированной архитектуры на примере шардированного блокчейна.

Пример работы секвенсора и собственного смарт-аккаунта

Секвенсор выполняет ключевую роль в системе. Он принимает пользовательские интенты (намерения), подписанные авторизованным устройством, и обрабатывает их вне блокчейна (off-chain):

- проверка подписи и валидности сообщения;
- фильтрация и дедупликация повторов;
- упорядочивание заявок на исполнение;
- установление расчета по сделке непосредственно в блокчейне (on-chain).

Каждый заданный интервал (например, 10–30 секунд) формируется агрегированная пачка сообщений (ExecuteBundle). Она направляется в смарт-контракт в блокчейне для единовременного (атомарного) исполнения. Это снижает сетевые издержки и устраняет проскальзывание цены. Подобный подход возможен при использовании механизма абстракции аккаунтов на

блокчейнах нового поколения, аналогичный механизм в Ethereum описан и реализован в [4].

Ниже приведён пример функции на языке FunC, реализующей верификацию подписи внешнего сообщения в рамках интент-ориентированной архитектуры. Эта функция демонстрирует ключевые шаги: извлечение подписи, проверка ключа в базе, сравнение последовательного номера и подтверждение цифровой подписи.

```
slice verify_ext_message_signature(slice in_msg_body, int storm_key_index) impure inline {
   slice signature = in_msg_body.get_last_bits(512);
   slice signed_slice = in_msg_body~load_ref().begin_parse();
   var (public_key_slice, key_found?) =
      db::public_keys.udict_get?(8, key_index);
   throw_unless(error::storm_backend_signature_not_found, key_found?);
   int spublic_key = public_keys~load_uint(256);
   int is_signature_valid = check_signature(slice_hash(signed_slice), signature, spublic_key);
   int seqno = signed_slice~load_uint(32);
   throw_unless(error::spublic_signature_invalid, is_signature_valid);
   throw_unless(error::invalid_seqno, seqno == db::seqno);
   db::seqno += 1;
   return signed_slice;
}
```

Данный фрагмент демонстрирует базовые принципы реализации безопасной интент-механики в смарт-контрактной логике TON: контроль последовательности, встроенные ключи и проверка сигнатур без необходимости вызова внешнего кошелька.

Производительность и масштабируемость

В интент-ориентированной модели достигаются следующие преимущества по сравнению с традиционной транзакционной моделью:

- Уменьшение задержки исполнения. Интенты формируются вне блокчейна и исполняются по расписанию, устраняя необходимость пользовательского взаимодействия в реальном времени [5].
- Секвенсирование пользовательских сообщений дает возможность достижения низких сетевых задержек при обеспечении безопасности пользовательских транзакций [6].
- Рост пропускной способности. За счёт агрегации операций и параллелизма на уровне смарт-аккаунта достигается высокая пропускная способность [7]. TON динамически масштабирует шарды (мелкие части блокчейна), и система способна обрабатывать десятки тысяч транзакций при условии равномерного распределения контрактов.
- Снижение затрат на газ. Групповая подача ExecuteBundle уменьшает число сообщений on-chain и сокращает совокупные издержки более чем в 2–3 раза.

Сравнительный анализ показал, что архитектура способна выдерживать конкурентную нагрузку и подходит для сценариев высокочастотной торговли, DeFi, NFT (non-fungible token, невзаимозаменяемый токен) и микроавтоматизации. В частности, это дает возможность использования блокчейна в сферах учета и бизнеса, обеспечивая достаточную устойчивость системы и безопасность [8].

Сравнительный анализ интент-ориентированных архитектур

Ниже представлена таблица сравнения различных реализаций интент-ориентированных архитектур в популярных блокчейн-платформах, включая ключевые характеристики исполнения, архитектурные особенности и метрики производительности.

Анализ показывает, что архитектура TON с интент-протоколом демонстрирует наилучший баланс между пользовательским удобством,

технической производительностью и масштабируемостью при этом сохраняя принцип no-trust доверия сторонним сервисам [9].

Таблица №1.

Сравнение различных реализаций intent-based архитектур в популярных блокчейн-платформах

Характеристика	**TON + Intent Protocol**	**Ethereum (ERC-4337)**	**StarkNet / Cairo**	**Cosmos / Osmosis**
Тип архитектуры	L1, шардированный	L2, через абстракцию	ZK-Rollup	IBC-модули
Обработка интентов	Off-chain + ExecuteBundle	Bundler + EntryPoint	Sequencer + Prover	Relayers + Msg Intents
Подпись	Embedded Device Key (Ed25519)	EOA / WalletKey	Stark Signature	Tendermint Signatures
Механизм агрегации	ExecuteBundle (batch)	UserOps queue	Cairo Call Stack	Пакетные сообщения IBC
Финализация	Masterchain (TON)	L2 → L1 мост	SN prover → L1	Блок L1
Нагрузка на пользователя	Нулевая (Signless)	Требует WalletConnect	Через кастомный UI	Через интерфейс сети
Пропускная способность	> 20 000	~300–2 000	~1 000–5 000	~1 000
Среднее время финализации (сек)	10–30	30–90	15–60	30–60
Масштабируемость	Высокая (шарды + интенты)	Средняя (зависит от L2)	Высокая (ZK)	Ограничена IBC
Асинхронность	Полная	Частичная	Частичная	Частичная
Открытость интерфейса	Смарт-аккаунты + Device API	EntryPoint + Wallet API	Cairo runtime	SDK/IBC

Благодаря полной асинхронности, снижению затрат на газ и возможности шардирования, TON позволяет достичь более пропускную способность 20 000 при финализации в пределах 10–30 секунд. В отличие от Ethereum (ERC-4337), где нагрузка на пользователя остаётся высокой, и от StarkNet, где время финализации ограничивается криптографической доказательной системой [10], TON предлагает низкий уровень задержек и нулевую потребность в взаимодействии с внешним кошельком. Cosmos, несмотря на модульность, ограничен в масштабируемости за счёт специфики IBC и синхронной модели сообщений.

Таким образом, решение на базе TON может быть рекомендовано для сценариев, где критичны высокая пропускная способность, масштабируемость и минимальное участие пользователя в рутинных подтверждениях.

Это делает его перспективным выбором для высоконагруженных децентрализованных бирж (decentralized exchanges, DEX), DeFi-платформ, а также приложений в IoT, логистике и DAO (decentralized autonomous organization, децентрализованная автономная организация).

Применимость за пределами финансов

Модель интентов может быть успешно применена не только в децентрализованных финансах, но и в других отраслях, где критичны свойства масштабируемости, автоматизации и сниженной задержки при взаимодействии распределённых участников:

- Интенты позволяют автоматизировать управление цепочками поставок. Каждый участник может выпускать интенты, фиксирующие факт приёмки, отправки или перемещения товара. Такие события могут быть объединены в агрегированные блоки, минимизируя транзакционные издержки и повышая прозрачность происхождения продукции [11].

- Миллионы устройств могут выпускать интенты, сигнализируя о событиях (например, изменение состояния датчика, запуск исполнительного механизма). За счёт off-chain агрегации таких сигналов обеспечивается высокая масштабируемость системы, а on-chain подтверждение гарантирует неизменность записей. Это критически важно для приложений умного освещения, учёта энергоресурсов и реактивной городской автоматизации [12].
- Архитектура позволяет участникам DAO выпускать предварительные интенты на голосование или предложение инициатив. Только при достижении заранее заданных условий (например, кворума) интенты подаются в блокчейн для финализации [13]. Это снижает нагрузку на сеть и позволяет реализовывать более сложные механизмы делегирования и обратной связи.
- Цифровые идентичности и аккредитация: в системах, где требуется подтверждение атрибутов пользователя (например, квалификации, членства или статуса), интенты могут использоваться для программируемой верификации и контроля доступа без постоянной публикации данных в блокчейн.

Таким образом, интент-подход открывает широкие перспективы применения во всех сферах, где требуется автоматизированное, масштабируемое и экономически эффективное взаимодействие в распределённой среде. В каждом случае основными преимуществами являются асинхронность, высокая пропускная способность и прозрачность исполнения.

Заключение

Интент-ориентированная архитектура, построенная на базе блокчейна TON, демонстрирует значительные преимущества в аспектах

производительности, масштабируемости и удобства взаимодействия. За счёт разделения логики формирования пакетов сообщений off-chain и исполнения транзакции достигается устойчивость к сетевым задержкам и атакам на интерфейс пользователя.

Применение данной модели перспективно как в финансовом, так и в нефинансовом секторах. Она может стать основой для следующего поколения Web3-приложений, ориентированных на автоматизацию, реактивность и масштабируемость.

Литература

1.Goldstein A.B., Sokolov N.A., Elagin V.S., Onufrienko A.V., Belozertsev I.A. Network Characteristics of Blockchain Technology of on Board Communication // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, March 20-21, 2019, pp. 1-5.

2. Mougayar W. The business blockchain. New Jersey: John Wiley & Sons Inc., Hoboken, 2016. 208 p.

3. Elagin V, Spirkina A., Levakov A., Belozertsev I. Blockchain Behavioral Traffic Model as a Tool to Influence Service IT Security // Future Internet 2020, V. 12(4). URL: doi.org/10.3390/fi12040068.

4. ERC-4337: Account Abstraction Using Alt Mempool. URL: eips.ethereum.org/EIPS/ eip-4337#abstract.

5. Wetzel B. Intent-based architectures and projects experimenting with them, 2023 URL: bwetzel.medium.com/intent-based-architectures-and-projects-experimenting-with-them-c3ee63ae24c.

5. Li X., Jiang P., Chen T., Luo X., Wen Q. A survey on the security of blockchain systems // Future Generation Computer Systems. 2020. V. 107. pp. 841-853.

6. Елагин В.С., Спиркина А.В., Владыко А.Г., Иванов Е.И., Помогалова А.В., Аптриева Е.А. Основные сетевые характеристики blockchain трафика и

подходы к моделированию // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 4. С. 39-45.

7. Carlozo L. What is blockchain? // Journal of Accountancy. 2017. V. 224. №. 1. URL: journalofaccountancy.com/issues/2017/jul/what-is-blockchain/.

8. Yaga D., Mell P., Roby N., Scarfone K. Blockchain technology overview URL: arxiv.org/abs/1906.11078.

9. Ahram T., Sargolzaei A., Sargolzaei S., Daniels J., Amaba B. Blockchain technology innovations // 2017 IEEE technology & engineering management conference (TEMSCON). IEEE, 2017. pp. 137-141.

10. Risius M., Spohrer K. A blockchain research framework // Business & Information Systems Engineering. 2017. V. 59. №. 6. pp. 385-409.

11. Pieroni A., Scarpato N., Felli L. Blockchain and IoT Convergence-A Systematic Survey on Technologies, Protocols and Security // Appl. Sci. 2020. V.10(19). URL: doi.org/10.3390/app10196749.

12. Нараян П. Блокчейн. Разработка приложений. СПб: БХВ-Петербург, 2018. 256 с.

References

1. Mougayar W. The business blockchain. New Jersey: John Wiley & Sons Inc., Hoboken, 2016. 208 p.

2. Goldstein A.B., Sokolov N.A., Elagin V.S., Onufrienko A.V., Belozertsev I.A. Network Characteristics of Blockchain Technology of on Board Communication // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, March 20-21, 2019, pp. 1-5.

3. Elagin V, Spirkina A., Levakov A., Belozertsev I. Future Internet 2020, V. 12(4). URL: doi.org/10.3390/fi12040068.

4. ERC-4337: Account Abstraction Using Alt Mempool. URL: eips.ethereum.org/EIPS/ eip-4337#abstract.

5. Wetzel B. Intent-based architectures and projects experimenting with them, 2023 URL: bwetzel.medium.com/intent-based-architectures-and-projects-experimenting-with-them-c3ee63ae24c

5. Li X., Jiang P., Chen T., Luo X., Wen Q. Future Generation Computer Systems. 2020. V. 107. pp. 841-853.

6. Elagin V.S., Spirkina A.V., Vladyko A.G., Ivanov E.I., Pomogalova A.V., Aptrieva E.A. T-Comm: Telekommunikatsii i transport. 2020. V. 14. № 4. pp. 39-45.

7. Carlozo L. Journal of Accountancy. 2017. V. 224. №. 1. URL: journalofaccountancy.com/issues/2017/jul/what-is-blockchain/.

8. Yaga D., Mell P., Roby N., Scarfone K. Blockchain technology overview URL: arxiv.org/abs/1906.11078.

9. Ahram T., Sargolzaei A., Sargolzaei S., Daniels J., Amaba B. Blockchain technology innovations // 2017 IEEE technology & engineering management conference (TEMSCON). IEEE, 2017. pp. 137-141.

10. Risius M., Spohrer K. Business & Information Systems Engineering. 2017. V. 59. №. 6. pp. 385-409.

11. Pieroni A., Scarpato N., Felli L. Applied Science. 2020. V.10(19). URL: doi.org/10.3390/app10196749.

12. Narayan P. Blokcheyn. Razrabotka prilozheniy [Blockchain. Application development]. SPb: BKhV-Peterburg, 2018. 256 p.

Дата поступления: 4.03.2025

Дата публикации: 25.04.2025