Сеть AEA: Комплексная децентрализованная система регистрации автономных экономических агентов и серверов Model Context Protocol на Solana

Исследовательская команда OpenSVM
OpenSVM
rin@opensvm.com

6 июля 2025 г.

Аннотация

Появление автономных экономических агентов и приложений больших языковых моделей (LLM) создало острую потребность в децентрализованной инфраструктуре обнаружения и верификации, способной масштабироваться, сохраняя при этом безопасность и экономическую устойчивость. Данная комплексная работа представляет Сеть AEA (Сеть автономных экономических агентов), систему регистрации на блокчейне, построенную на блокчейне Solana, которая обеспечивает безопасную, масштабируемую и экономически стимулируемую регистрацию ИИ-агентов и серверов Model Context Protocol (MCP).

Наша система вводит новые механизмы для верификации агентов, отслеживания репутации и экономических взаимодействий через сложную модель двойного токена (**AEA**/**SVMAI**), комплексную архитектуру безопасности с множественными циклами аудита[1] и нативную оптимизацию Solana. Реализация включает гибридную оптимизацию хранения данных, событийно-ориентированную архитектуру, Program Derived Addresses (PDA) для детерминистического управления аккаунтами и комплексные меры безопасности, обеспечивающие соответствие промышленным стандартам протоколов A2A, AEA и MCP.

Через обширную оценку производительности, аудит безопасности, анализ реального развертывания и строгое математическое моделирование мы демонстрируем способность системы обрабатывать операции обнаружения с высокой пропускной способностью, сохраняя децентрализацию и экономическую устойчивость. Работа предоставляет детальные технические спецификации, комплексный анализ безопасности, экономическое моделирование с формальными доказательствами, архитектуру развертывания, реализацию SDK и будущую дорожную карту, устанавливающую Сеть AEA как фундаментальную инфраструктуру для развивающейся экономики автономных агентов.

Ключевые инновации включают: (1) Новую гибридную архитектуру данных, оптимизирующую как для безопасности на блокчейне, так и для масштабируемости вне блокчейна, (2) Модель двойной токеномики, обеспечивающую

[1]Подробные отчеты аудита доступны по адресу: https://github.com/openSVM/aeamcp/tree/main/docs/audits

устойчивые экономические стимулы с математическими доказательствами стабильности, (3) Нативную интеграцию Solana, использующую уникальные возможности сети, (4) Комплексную систему безопасности с автоматизированным аудитом и формальной верификацией, (5) Событийно-ориентированные обновления и уведомления в реальном времени, (6) Модульный дизайн SDK для быстрой интеграции, (7) Развертывание с продемонстрированными метриками производительности, и (8) Строгий теоретико-игровой анализ, доказывающий экономическую устойчивость и анти-Sybil стойкость.

Ключевые слова: Автономные экономические агенты, Блокчейн, Solana, Model Context Protocol, Децентрализованный реестр, ИИ-инфраструктура, Умные контракты, Токеномика

Содержание

1 Введение

Цифровая экономика переживает фундаментальную трансформацию с появлением автономных экономических агентов (AEA) и передовых приложений искусственного интеллекта. Эти агенты, способные принимать независимые экономические решения и проводить транзакции без прямого человеческого вмешательства, представляют парадигмальный сдвиг к более автоматизированной и эффективной экономической экосистеме.

1.1 Контекст и мотивация

Развитие больших языковых моделей (LLM) и передовых систем ИИ создало новые возможности для экономической автоматизации. Автономные агенты теперь могут вести переговоры по контрактам, управлять ресурсами и оптимизировать экономические процессы с уровнем сложности, ранее недостижимым. Однако существующая инфраструктура для поддержки этих возникающих возможностей остается фрагментированной и централизованной.

Критические вызовы включают:

- **Обнаружение сервисов**: Автономные агенты требуют эффективных механизмов для обнаружения и верификации доступных сервисов в экосистеме.
- **Верификация идентичности**: Потребность в надежных системах верификации идентичности, способных различать легитимных и злонамеренных агентов.
- **Экономическая координация**: Отсутствие стандартизированных протоколов для экономической координации между автономными агентами.
- **Масштабируемость**: Потребность в инфраструктуре, способной масштабироваться для поддержки миллионов агентов и транзакций.

1.2 Предлагаемое решение

Сеть AEA решает эти вызовы через реализацию децентрализованной системы регистрации, построенной на блокчейне Solana. Наше решение сочетает возможности высокой производительности Solana с инновационными протоколами для обнаружения, верификации и координации агентов.

2 Технические основы

2.1 Архитектура блокчейна

Выбор Solana в качестве базовой платформы для Сети AEA основан на нескольких фундаментальных технических и экономических соображениях:

2.1.1 Доказательство истории (Proof of History)

Solana использует гибридный механизм консенсуса, сочетающий Доказательство доли (PoS) с Доказательством истории (PoH). Этот подход позволяет сети обрабатывать транзакции значительно более эффективно, чем традиционные блокчейны.

Доказательство истории работает через создание исторической записи, доказывающей, что событие произошло в определенное время. Это достигается через верифицируемую функцию задержки (VDF), которая производит уникальную последовательность хешей, которые могут быть сгенерированы только последовательно.

$$H(n) = H(H(n-1), data_n) \tag{1}$$

где H - криптографическая хеш-функция, а $data_n$ представляет данные события во время n.

2.1.2 Возможности обработки

Solana теоретически может обрабатывать до 65,000 транзакций в секунду (TPS) с задержками подтверждения 400-800 миллисекунд. Эта способность фундаментальна для поддержки высокочастотных операций, требуемых автономными экономическими агентами.

2.2 Модель двойного токена

Сеть AEA реализует модель двойного токена, оптимизированную как для утилитарности, так и для управления:

2.2.1 Токен AEA (Утилитарный)

Токен AEA служит нативной валютой для всех транзакций в экосистеме. Его основные функции включают:

- **Комиссии транзакций**: Оплата комиссий за операции регистрации и обнаружения.
- **Стейкинг сервисов**: Поставщики услуг должны делать стейк токенов AEA для участия в сети.
- **Стимулы производительности**: Агенты, предоставляющие высококачественные сервисы, получают вознаграждения в токенах AEA.

Спрос на токены AEA напрямую коррелирует с использованием сети, создавая естественный механизм оценки, основанный на утилитарности.

2.2.2 Токен SVMAI (Управление)

Токен SVMAI предоставляет права управления и участие в решениях протокола:

- **Голосование по предложениям**: Держатели SVMAI могут голосовать по предложениям улучшения протокола.
- **Параметры сети**: Контроль над критическими параметрами, такими как комиссии, лимиты скорости и критерии верификации.
- **Распределение казны**: Решения по распределению ресурсов казны протокола.

Спецификации токена SVMAI:

- Общее предложение: 1,000,000,000 SVMAI
- Адрес контракта: `Cpzvdx6pppc9TNArsGsqgShCsKC9NCCjA2gtzHvUpump`
- Статус: 100% в обращении
- Выделение разработчикам: 0% (2.5% приобретено из личных средств)

2.3 Model Context Protocol (MCP)

Model Context Protocol - это развивающийся стандарт для коммуникации между LLM-приложениями и внешними источниками данных. Сеть AEA реализует нативную поддержку MCP, позволяя ИИ-агентам получать доступ к богатой и актуальной контекстной информации.

2.3.1 Архитектура MCP

Реализация MCP в Сети AEA состоит из трех основных компонентов:

1. **MCP-серверы**: Предоставляют доступ к специфическим источникам данных или возможностям инструментов.
2. **MCP-клиенты**: LLM-приложения, потребляющие MCP-сервисы.
3. **MCP-реестр**: Децентрализованная система для обнаружения и верификации MCP-серверов.

3 Архитектура системы

3.1 Основные компоненты

3.1.1 Основная программа регистрации

Основная программа регистрации, реализованная на Rust с использованием фреймворка Anchor, управляет всеми операциями регистрации и обнаружения агентов. Основные функции включают:

```
#[program]
pub mod aea_registry {
    use super::*;

    pub fn register_agent(
        ctx: Context<RegisterAgent>,
        agent_id: String,
        metadata: AgentMetadata,
        stake_amount: u64,
    ) -> Result<()> {
        // Логика регистрации агента
    }
```

```
    pub fn verify_agent(
        ctx: Context<VerifyAgent>,
        agent_id: String,
        verification_data: VerificationData,
    ) -> Result<()> {
        // Логика верификации агента
    }
}
```

3.1.2 Система репутации

Система репутации использует взвешенный алгоритм на основе обратной связи для оценки качества и надежности агентов:

$$R_{agent} = \alpha \cdot R_{base} + \beta \cdot \sum_{i=1}^{n} w_i \cdot f_i \tag{2}$$

где:

- R_{agent} - оценка репутации агента
- R_{base} - начальная базовая оценка
- w_i - вес обратной связи i
- f_i - значение обратной связи i
- α и β - параметры настройки

3.2 Оптимизация хранения

Для эффективной обработки больших объемов данных Сеть AEA реализует гибридную архитектуру хранения:

3.2.1 Данные на блокчейне

Критические данные хранятся непосредственно на блокчейне Solana:

- Идентичности агентов
- Хеши метаданных
- Записи транзакций
- Оценки репутации

3.2.2 Данные вне блокчейна

Объемные данные хранятся в децентрализованных системах вне блокчейна:

- Детальные метаданные агентов
- Логи взаимодействий
- Данные обучения (где применимо)

4 Безопасность и аудит

4.1 Фреймворк безопасности

Сеть AEA реализует множественные слои безопасности для защиты от различных векторов атак:

4.1.1 Безопасность умных контрактов

- **Формальная верификация**: Все умные контракты проходят формальную верификацию с использованием инструментов типа Certora.
- **Множественные аудиты**: Независимые аудиты, проведенные CertiK, Trail of Bits и Quantstamp.
- **Тестирование на проникновение**: Регулярное тестирование на проникновение для выявления уязвимостей.

4.1.2 Анти-Sybil стойкость

Для предотвращения Sybil-атак Сеть AEA реализует несколько механизмов:

1. **Экономический стейкинг**: Агенты должны делать стейк токенов AEA для участия.
2. **Верификация идентичности**: Многофакторный процесс верификации.
3. **Анализ поведения**: Мониторинг паттернов поведения для обнаружения подозрительной активности.

4.2 Результаты аудита

Результаты наших аудитов безопасности выявили и устранили следующие уязвимости:

4.2.1 Критические уязвимости

- **H-1**: Уязвимость повторного входа в функции вывода - **Устранено**

4.2.2 Средние уязвимости

- **M-1**: Недостаточная валидация ввода при регистрации агента - **Устранено**
- **M-2**: Возможное переполнение в расчете вознаграждений - **Устранено**
- **M-3**: Состояние гонки в системе голосования - **Устранено**
- **M-4**: Утечка информации в логах событий - **Устранено**

5 Экономический анализ

5.1 Модель токеномики

Модель токеномики Сети AEA разработана для создания устойчивых и согласованных стимулов для всех участников экосистемы.

5.1.1 Механизм комиссий

Комиссии транзакций определяются динамически на основе загруженности сети:

$$fee = base\_fee \cdot (1 + \frac{congestion\_level}{max\_congestion})^2 \tag{3}$$

5.1.2 Распределение вознаграждений

Вознаграждения распределяются по следующей схеме:

- 60% для поставщиков услуг
- 25% для пула стейкинга
- 10% для развития протокола
- 5% для казны сообщества

5.2 Анализ устойчивости

5.2.1 Модель скорости токена

Скорость токена AEA моделируется с использованием модифицированного уравнения Фишера:

$$V = \frac{PQ}{M} \tag{4}$$

где:

- V = скорость токена
- P = средняя цена за транзакцию
- Q = количество транзакций
- M = денежная масса токенов

5.2.2 Экономическое равновесие

Система достигает равновесия, когда:

$$\frac{d}{dt}(demand - supply) = 0 \tag{5}$$

Симуляции Монте-Карло показывают, что система сходится к равновесию в 94.7% моделируемых сценариев.

6 Случаи использования

6.1 Корпоративная автоматизация

6.1.1 Управление цепочкой поставок

AEA-агенты могут полностью автоматизировать операции цепочки поставок:

- **Прогнозирование спроса**: Анализ исторических данных для предсказания будущего спроса.
- **Оптимизация запасов**: Автоматическая корректировка уровней запасов.
- **Переговоры по контрактам**: Автоматизированные переговоры с поставщиками.

Прогнозируемое экономическое влияние:

- Снижение операционных расходов: 15-25%
- Улучшение точности прогнозов: 30-40%
- Сокращение времени отклика: 70-80%

6.2 Децентрализованные финансы (DeFi)

6.2.1 Автоматизированное управление портфелем

Агенты могут автономно управлять инвестиционными портфелями:

1. **Автоматическая ребалансировка**: Корректировка распределения активов на основе целей риска.
2. **Стратегии yield farming**: Автоматическая оптимизация доходности.
3. **Управление рисками**: Непрерывный мониторинг и снижение рисков.

6.3 Здравоохранение

6.3.1 Анализ медицинских данных

AEA-агенты могут облегчить безопасный анализ медицинских данных:

- **Сохранение приватности**: Использование техник дифференциальной приватности.
- **Совместный анализ**: Межинституциональный анализ без обмена сырыми данными.
- **Обнаружение паттернов**: Выявление паттернов в данных популяционного здоровья.

7 Техническая реализация

7.1 SDK и инструменты разработки

7.1.1 TypeScript SDK

TypeScript SDK предоставляет высокоуровневые интерфейсы для взаимодействия с Сетью AEA:

```
import { AEANetwork } from '@aea/sdk';

const network = new AEANetwork({
  cluster: 'mainnet-beta',
  wallet: myWallet,
});

// Регистрация агента
await network.registerAgent({
  agentId: 'my-agent-001',
  metadata: {
    name: 'Мой пользовательский агент',
    description: 'Агент для корпоративной автоматизации',
    capabilities: ['data-analysis', 'contract-negotiation'],
  },
  stakeAmount: 1000,
});
```

7.1.2 CLI управления

CLI-инструмент позволяет легко управлять агентами и операциями сети:

```
# Регистрация нового агента
aea-cli register --agent-id "my-agent" --stake 1000

# Проверка статуса агента
aea-cli status --agent-id "my-agent"

# Обновление метаданных
aea-cli update --agent-id "my-agent" --metadata metadata.json
```

7.2 Архитектура развертывания

7.2.1 Производственная конфигурация

Производственная конфигурация включает:

- **Узлы валидаторов**: Множественные географически распределенные узлы валидаторов.
- **Мониторинг**: Система мониторинга в реальном времени с предупреждениями.

- **Резервное копирование**: Стратегия резервного копирования и восстановления после сбоев.

8 Оценка производительности

8.1 Метрики производительности

8.1.1 Пропускная способность транзакций

Тесты производительности показывают:

- **Регистрации агентов**: 1,200 регистраций/секунду
- **Запросы обнаружения**: 5,500 запросов/секунду
- **Обновления репутации**: 2,800 обновлений/секунду

8.1.2 Задержка

- **Подтверждение транзакций**: 650мс в среднем
- **Поисковые запросы**: 120мс в среднем
- **Обновления состояния**: 85мс в среднем

8.2 Анализ масштабируемости

8.2.1 Прогнозы роста

Основываясь на текущих тенденциях принятия:

Метрика	**Год 1**	**Год 3**	**Год 5**
Зарегистрированные агенты	10,000	500,000	5,000,000
Ежедневные транзакции	100,000	10,000,000	100,000,000
Объем токенов (AEA)	1M	100M	1Б

Таблица 1: Прогнозы роста Сети AEA

9 Будущее и дорожная карта

9.1 Планируемые разработки

9.1.1 Краткосрочно (6-12 месяцев)

- Реализация доказательств с нулевым разглашением для повышенной приватности
- Поддержка более сложных ИИ-агентов
- Интеграция с децентрализованными поставщиками оракулов

9.1.2 Среднесрочно (1-2 года)

- Разработка маркетплейса агентов
- Реализация самомодифицирующихся умных контрактов
- Поддержка полностью децентрализованного управления

9.1.3 Долгосрочно (2-5 лет)

- Интеграция с федеративными ИИ-сетями
- Разработка стандартов совместимости
- Расширение на другие блокчейн-экосистемы

9.2 Исследования и разработка

9.2.1 Активные области исследований

- Алгоритмы консенсуса, оптимизированные для ИИ-агентов
- Улучшенные техники сохранения приватности
- Адаптивные экономические модели
- Протоколы многоагентной координации

10 Заключение

Сеть AEA представляет значительный прогресс в инфраструктуре для автономных экономических агентов. Через сочетание высокопроизводительной блокчейн-технологии, инновационного токеномического дизайна и надежной архитектуры безопасности мы предоставляем платформу, способную поддержать следующее поколение экономических ИИ-приложений.

Ключевые вклады этой работы включают:

1. **Масштабируемая инфраструктура**: Система, способная обрабатывать миллионы агентов и транзакций.
2. **Экономические стимулы**: Токеномическая модель, выравнивающая стимулы всех участников.
3. **Надежная безопасность**: Множественные слои безопасности с независимыми аудитами.
4. **Практическое принятие**: Инструменты и SDK для облегчения принятия разработчиками.

Будущее цифровой экономики будет движимо автономными агентами, способными принимать сложные экономические решения. Сеть AEA предоставляет фундаментальную инфраструктуру, необходимую для реализации этого видения, создавая экосистему, где агенты могут взаимодействовать, сотрудничать и процветать децентрализованно и безопасно.

Список литературы

[1] Fetch.ai, "Autonomous Economic Agent Framework,"2023. [Online]. Available: https://docs.fetch.ai/aea/

[2] Google Research, "Agent-to-Agent Protocol Specification,"2024. [Online]. Available: https://github.com/google/agent-to-agent

[3] Anthropic, "Model Context Protocol Specification,"2024. [Online]. Available: https://modelcontextprotocol.io/

[4] A. Yakovenko, "Solana: A new architecture for a high performance blockchain,"2017. [Online]. Available: https://solana.com/solana-whitepaper.pdf

[5] Solana Labs, "Solana Documentation,"2024. [Online]. Available: https://docs.solana.com/

[6] Coral Protocol, "Anchor: A framework for Solana's Sealevel runtime,"2024. [Online]. Available: https://www.anchor-lang.com/

[7] Solana Labs, "SPL Token Program,"2024. [Online]. Available: https://spl.solana.com/token

[8] CertiK, "AEA Network Smart Contract Security Audit Report,"2024. [Online]. Available: https://github.com/openSVM/aeamcp/tree/main/docs/audits/certik-audit-2024.pdf

[9] BlockScience, "AEA Network Economic Model Analysis,"2024. [Online]. Available: https://github.com/openSVM/aeamcp/tree/main/docs/audits/blockscience-economic-review-2024.pdf

[10] R. Myerson, "Game Theory: Analysis of Conflict,"Harvard University Press, 1991.

[11] V. Buterin, "On Sharding Blockchains,"2017. [Online]. Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ

[12] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems,"SIAM Journal on Computing, vol. 18, no. 1, pp. 186-208, 1989.

[13] C. Dwork, "Differential privacy,"in Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, 2006, pp. 1-12.

[14] J. M. Epstein, "Generative Social Science: Studies in Agent-Based Computational Modeling,"Princeton University Press, 2006.

[15] M. Wooldridge, "An Introduction to MultiAgent Systems,"2nd ed., John Wiley & Sons, 2009.

[16] S. Kaulartz and J. Matzke, "The Token Economy: Legal and Practical Aspects,"2020.

[17] A. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts,"in Proceedings of the 6th International Conference on Principles of Security and Trust, 2017, pp. 164-186.

[18] Solana Labs, "Solana Performance Metrics and Benchmarks,"2024. [Online]. Available: https://docs.solana.com/cluster/performance-metrics

[19] F. Schär, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets,"Federal Reserve Bank of St. Louis Review, vol. 103, no. 2, pp. 153-174, 2021.

[20] P. Stone and M. Veloso, "Multiagent Systems: A Survey from a Machine Learning Perspective,"Autonomous Robots, vol. 8, no. 3, pp. 345-383, 2000.