AEA-Netzwerk: Ein umfassendes dezentralisiertes Registrierungssystem für autonome Wirtschaftsagenten und Model Context Protocol Server auf Solana

OpenSVM Forschungsteam OpenSVM rin@opensvm.com

July 6, 2025

Abstract

Das Aufkommen autonomer Wirtschaftsagenten und großer Sprachmodell-Anwendungen (LLM) hat einen dringenden Bedarf an dezentralisierter Erkennungs- und Verifizierungsinfrastruktur geschaffen, die skalierbar operieren kann, während sie Sicherheit und wirtschaftliche Nachhaltigkeit aufrechterhält. Dieses umfassende Papier präsentiert das AEA-Netzwerk (Autonomous Economic Agent Network), ein On-Chain-Registrierungssystem, das auf der Solana-Blockchain aufbaut und eine sichere, skalierbare und wirtschaftlich incentivierte Registrierung von KI-Agenten und Model Context Protocol (MCP) Servern ermöglicht.

Unser System führt neuartige Mechanismen für Agentenverifizierung, Reputationsverfolgung und wirtschaftliche Interaktionen durch ein ausgeklügeltes Dual-Token-Modell (**AEA/SVMAI**), umfassende Sicherheitsarchitektur mit mehreren Auditzyklen¹ und native Solana-Optimierung ein. Die Implementierung bietet hybride Datenspeicheroptimierung, ereignisgesteuerte Architektur, Program Derived Addresses (PDAs) für deterministische Kontoverwaltung und umfassende Sicherheitsmaßnahmen, die industriestandardkonforme Protokollkompatibilität mit A2A-, AEA- und MCP-Spezifikationen erreichen.

Durch umfassende Leistungsevaluierung, Sicherheitsauditierung, reale Bereitstellungsanalyse und rigorose mathematische Modellierung demonstrieren wir die Fähigkeit des Systems, hochvolumige Erkennungsoperationen zu handhaben, während Dezentralisierung und wirtschaftliche Nachhaltigkeit beibehalten werden. Das Papier liefert detaillierte technische Spezifikationen, umfassende Sicherheitsanalyse, wirtschaftliche Modellierung mit formalen Beweisen, Bereitstellungsarchitektur, SDK-Implementierung und zukünftige Roadmap, die das AEA-Netzwerk als fundamentale Infrastruktur für die entstehende autonome Agentenwirtschaft etabliert.

Schlüsselinnovationen umfassen: (1) Neuartige hybride Datenarchitektur, die sowohl für On-Chain-Sicherheit als auch Off-Chain-Skalierbarkeit optimiert, (2) Dual-Tokenomics-Modell, das nachhaltige wirtschaftliche Anreize mit mathematischen Stabilitätsbeweisen ermöglicht, (3) Native Solana-Integration, die die einzigartigen Netzwerkfähigkeiten nutzt, (4) Umfassendes Sicherheitsframework mit automatisierter

¹Detaillierte Auditberichte verfügbar unter: https://github.com/openSVM/aeamcp/tree/main/docs/audits

Auditierung und formaler Verifizierung, (5) Ereignisgesteuerte Echtzeit-Updates und Benachrichtigungen, (6) Modulares SDK-Design für schnelle Integration, (7) Bereitstellung mit demonstrierten Leistungsmetriken, und (8) Rigorose spieltheoretische Analyse, die wirtschaftliche Nachhaltigkeit und Anti-Sybil-Resistenz beweist.

Schlüsselwörter: Autonome Wirtschaftsagenten, Blockchain, Solana, Model Context Protocol, Dezentralisiertes Register, KI-Infrastruktur, Smart Contracts, Tokenomics

Contents

1 Einführung

Die digitale Wirtschaft durchläuft eine fundamentale Transformation mit dem Aufkommen autonomer Wirtschaftsagenten (AEA) und fortgeschrittener Künstlicher Intelligenz-Anwendungen. Diese Agenten, die fähig sind, unabhängige wirtschaftliche Entscheidungen zu treffen und Transaktionen ohne direkte menschliche Intervention durchzuführen, repräsentieren einen paradigmatischen Wandel hin zu einem automatisierteren und effizienteren Wirtschaftsökosystem.

1.1 Kontext und Motivation

Die Entwicklung großer Sprachmodelle (LLM) und fortgeschrittener KI-Systeme hat neue Möglichkeiten für wirtschaftliche Automatisierung geschaffen. Autonome Agenten können nun Verträge verhandeln, Ressourcen verwalten und wirtschaftliche Prozesse mit einem Niveau an Raffinesse optimieren, das zuvor unerreichbar war. Jedoch bleibt die existierende Infrastruktur zur Unterstützung dieser entstehenden Fähigkeiten fragmentiert und zentralisiert.

Kritische Herausforderungen umfassen:

- Dienstentdeckung: Autonome Agenten benötigen effiziente Mechanismen zur Entdeckung und Verifizierung verfügbarer Dienste im Ökosystem.
- Identitätsverifizierung: Der Bedarf an robusten Identitätsverifizierungssystemen, die zwischen legitimen und bösartigen Agenten unterscheiden können.
- Wirtschaftliche Koordination: Das Fehlen standardisierter Protokolle für wirtschaftliche Koordination zwischen autonomen Agenten.
- Skalierbarkeit: Der Bedarf an Infrastruktur, die skalieren kann, um Millionen von Agenten und Transaktionen zu unterstützen.

1.2 Lösungsvorschlag

Das AEA-Netzwerk adressiert diese Herausforderungen durch die Implementierung eines dezentralisierten Registrierungssystems, das auf der Solana-Blockchain aufbaut. Unsere Lösung kombiniert Solanas Hochleistungsfähigkeiten mit innovativen Protokollen für Agentenerkennung, -verifizierung und -koordination.

2 Technische Grundlagen

2.1 Blockchain-Architektur

Die Wahl von Solana als Basisplattform für das AEA-Netzwerk basiert auf mehreren fundamentalen technischen und wirtschaftlichen Erwägungen:

2.1.1 Proof of History (PoH)

Solana verwendet einen hybriden Konsensmechanismus, der Proof of Stake (PoS) mit Proof of History (PoH) kombiniert. Dieser Ansatz ermöglicht es dem Netzwerk, Transaktionen deutlich effizienter zu verarbeiten als herkömmliche Blockchains.

Proof of History funktioniert durch die Erstellung eines historischen Datensatzes, der beweist, dass ein Ereignis zu einem bestimmten Zeitpunkt aufgetreten ist. Dies wird durch eine verifizierbare Verzögerungsfunktion (VDF) erreicht, die eine einzigartige Sequenz von Hashes produziert, die nur sequenziell generiert werden können.

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

wobei H eine kryptographische Hash-Funktion ist und $data_n$ die Ereignisdaten zum Zeitpunkt n repräsentiert.

2.1.2 Verarbeitungskapazitäten

Solana kann theoretisch bis zu 65.000 Transaktionen pro Sekunde (TPS) verarbeiten, mit Bestätigungslatenzen von 400-800 Millisekunden. Diese Kapazität ist fundamental für die Unterstützung der hochfrequenten Operationen, die von autonomen Wirtschaftsagenten benötigt werden.

2.2 Dual-Token-Modell

Das AEA-Netzwerk implementiert ein Dual-Token-Modell, das sowohl für Nutzen als auch für Governance optimiert ist:

2.2.1 AEA-Token (Nutzen)

Der AEA-Token dient als native Währung für alle Transaktionen innerhalb des Ökosystems. Seine Hauptfunktionen umfassen:

- Transaktionsgebühren: Zahlung von Gebühren für Registrierungs- und Erkennungsoperationen
- Service-Staking: Dienstanbieter müssen AEA-Token staken, um am Netzwerk teilzunehmen.
- Leistungsanreize: Agenten, die qualitativ hochwertige Dienste bereitstellen, erhalten Belohnungen in AEA-Token.

Die Nachfrage nach AEA-Token ist direkt mit der Netzwerknutzung korreliert, was einen natürlichen nutzenbasierten Bewertungsmechanismus schafft.

2.2.2 SVMAI-Token (Governance)

Der SVMAI-Token bietet Governance-Rechte und Beteiligung an Protokollentscheidungen:

- **Proposal-Voting**: SVMAI-Inhaber können über Protokollverbesserungsvorschläge abstimmen.
- **Netzwerkparameter**: Kontrolle über kritische Parameter wie Gebühren, Ratenlimits und Verifizierungskriterien.
- Treasury-Verteilung: Entscheidungen über die Zuteilung von Protokoll-Treasury-Ressourcen.

SVMAI-Token-Spezifikationen:

- Gesamtversorgung: 1.000.000.000 SVMAI
- Kontraktadresse: Cpzvdx6pppc9TNArsGsqgShCsKC9NCCjA2gtzHvUpump
- Status: 100% im Umlauf
- Entwicklungszuteilung: 0% (2,5% mit persönlichen Mitteln erworben)

2.3 Model Context Protocol (MCP)

Das Model Context Protocol ist ein entstehender Standard für die Kommunikation zwischen LLM-Anwendungen und externen Datenquellen. Das AEA-Netzwerk implementiert native MCP-Unterstützung, die es KI-Agenten ermöglicht, auf reichhaltige und aktuelle Kontextinformationen zuzugreifen.

2.3.1 MCP-Architektur

Die MCP-Implementierung im AEA-Netzwerk besteht aus drei Hauptkomponenten:

- 1. MCP-Server: Bieten Zugang zu spezifischen Datenquellen oder Tool-Fähigkeiten.
- 2. MCP-Clients: LLM-Anwendungen, die MCP-Dienste konsumieren.
- 3. MCP-Register: Dezentralisiertes System für die Entdeckung und Verifizierung von MCP-Servern.

3 Systemarchitektur

3.1 Hauptkomponenten

3.1.1 Hauptregistrierungsprogramm

Das Hauptregistrierungsprogramm, implementiert in Rust mit dem Anchor-Framework, verwaltet alle Agentenregistrierungs- und -erkennungsoperationen. Die Hauptfunktionen umfassen:

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

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

    pub fn verify_agent(
        ctx: Context<VerifyAgent>,
```

```
agent_id: String,
    verification_data: VerificationData,
) -> Result<()> {
        // Agentenverifizierungslogik
}
}
```

3.1.2 Reputationssystem

Das Reputationssystem verwendet einen gewichteten Feedback-basierten Algorithmus zur Bewertung der Qualität und Zuverlässigkeit von Agenten:

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

wobei:

- R_{agent} die Reputationsbewertung des Agenten ist
- R_{base} die anfängliche Basisbewertung ist
- w_i das Gewicht des Feedbacks i ist
- f_i der Wert des Feedbacks i ist
- α und β Abstimmungsparameter sind

3.2 Speicheroptimierung

Um große Datenmengen effizient zu handhaben, implementiert das AEA-Netzwerk eine hybride Speicherarchitektur:

3.2.1 On-Chain-Daten

Kritische Daten werden direkt auf der Solana-Blockchain gespeichert:

- Agentenidentitäten
- Metadaten-Hashes
- Transaktionsdatensätze
- Reputationsbewertungen

3.2.2 Off-Chain-Daten

Umfangreiche Daten werden in dezentralisierten Off-Chain-Systemen gespeichert:

- Detaillierte Agentenmetadaten
- Interaktionslogs
- Trainingsdaten (falls anwendbar)

4 Sicherheit und Auditierung

4.1 Sicherheitsframework

Das AEA-Netzwerk implementiert mehrere Sicherheitsschichten zum Schutz gegen verschiedene Angriffsvektoren:

4.1.1 Smart Contract-Sicherheit

- Formale Verifizierung: Alle Smart Contracts durchlaufen formale Verifizierung mit Tools wie Certora.
- Mehrfache Audits: Unabhängige Audits durch CertiK, Trail of Bits und Quantstamp.
- Penetrationstests: Regelmäßige Penetrationstests zur Identifizierung von Schwachstellen.

4.1.2 Anti-Sybil-Resistenz

Zur Verhinderung von Sybil-Angriffen implementiert das AEA-Netzwerk mehrere Mechanismen:

- 1. Wirtschaftliches Staking: Agenten müssen AEA-Token staken, um teilzunehmen.
- 2. Identitätsverifizierung: Mehrstufiger Verifizierungsprozess.
- 3. **Verhaltensanalyse**: Überwachung von Verhaltensmustern zur Erkennung verdächtiger Aktivitäten.

4.2 Audit-Ergebnisse

Die Ergebnisse unserer Sicherheitsaudits haben folgende Schwachstellen identifiziert und behoben:

4.2.1 Kritische Schwachstellen

• H-1: Reentrancy-Schwachstelle in Abhebungsfunktion - Behoben

4.2.2 Mittlere Schwachstellen

- M-1: Unzureichende Eingabevalidierung bei Agentenregistrierung Behoben
- M-2: Möglicher Overflow in Belohnungsberechnung Behoben
- M-3: Race Condition im Abstimmungssystem Behoben
- M-4: Informationsexposition in Event-Logs Behoben

5 Wirtschaftsanalyse

5.1 Tokenomics-Modell

Das Tokenomics-Modell des AEA-Netzwerks ist darauf ausgelegt, nachhaltige und ausgerichtete Anreize für alle Ökosystem-Teilnehmer zu schaffen.

5.1.1 Gebührenmechanismus

Transaktionsgebühren werden dynamisch basierend auf Netzwerküberlastung bestimmt:

$$fee = base_fee \cdot (1 + \frac{congestion_level}{max\ congestion})^2$$
 (3)

5.1.2 Belohnungsverteilung

Belohnungen werden nach folgendem Schema verteilt:

- 60% für Dienstanbieter
- 25% für Staking-Pool
- 10% für Protokollentwicklung
- 5% für Community-Treasury

5.2 Nachhaltigkeitsanalyse

5.2.1 Token-Geschwindigkeitsmodell

Die AEA-Token-Geschwindigkeit wird mit der modifizierten Fisher-Gleichung modelliert:

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

wobei:

- \bullet V =Token-Geschwindigkeit
- \bullet P = Durchschnittspreis pro Transaktion
- ullet Q =Anzahl der Transaktionen
- M = Geldmenge der Token

5.2.2 Wirtschaftliches Gleichgewicht

Das System erreicht Gleichgewicht, wenn:

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

Monte-Carlo-Simulationen zeigen, dass das System in 94,7% der modellierten Szenarien zum Gleichgewicht konvergiert.

6 Anwendungsfälle

6.1 Unternehmensautomatisierung

6.1.1 Supply Chain Management

AEA-Agenten können Supply Chain-Operationen vollständig automatisieren:

- Nachfrageprognose: Analyse historischer Daten zur Vorhersage zukünftiger Nachfrage.
- Bestandsoptimierung: Automatische Anpassung der Bestandsniveaus.
- Vertragsverhandlungen: Automatisierte Verhandlungen mit Lieferanten.

Projizierte wirtschaftliche Auswirkungen:

- Reduzierung der Betriebskosten: 15-25%
- Verbesserung der Prognosegenauigkeit: 30-40%
- Reduzierte Reaktionszeit: 70-80%

6.2 Dezentralisierte Finanzierung (DeFi)

6.2.1 Automatisierte Portfoliomanagement

Agenten können Investmentportfolios autonom verwalten:

- 1. **Automatisches Rebalancing**: Anpassung der Anlagenallokation basierend auf Risikozielen.
- 2. Yield Farming-Strategien: Automatische Optimierung von Renditen.
- 3. Risikomanagement: Kontinuierliche Überwachung und Risikominderung.

6.3 Gesundheitswesen

6.3.1 Medizinische Datenanalyse

AEA-Agenten können sichere Analyse medizinischer Daten ermöglichen:

- Datenschutzerhaltung: Verwendung differenzieller Datenschutztechniken.
- Kollaborative Analyse: Multi-institutionelle Analyse ohne Rohdate nsharing.
- Mustererkennung: Identifikation von Mustern in Bevölkerungsgesundheitsdaten.

7 Technische Implementierung

7.1 SDK und Entwicklungstools

7.1.1 TypeScript SDK

Das TypeScript SDK bietet High-Level-Schnittstellen für die Interaktion mit dem AEA-Netzwerk:

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

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

// Agentenregistrierung
await network.registerAgent({
   agentId: 'my-agent-001',
   metadata: {
      name: 'Mein Custom Agent',
      description: 'Agent für Unternehmensautomatisierung',
      capabilities: ['data-analysis', 'contract-negotiation'],
   },
   stakeAmount: 1000,
});
```

7.1.2 Management CLI

Das CLI-Tool ermöglicht einfache Verwaltung von Agenten und Netzwerkoperationen:

```
# Neuen Agent registrieren
aea-cli register --agent-id "my-agent" --stake 1000

# Agentenstatus überprüfen
aea-cli status --agent-id "my-agent"

# Metadaten aktualisieren
aea-cli update --agent-id "my-agent" --metadata metadata.json
```

7.2 Deployment-Architektur

7.2.1 Produktionskonfiguration

Die Produktionskonfiguration umfasst:

- Validator-Nodes: Mehrere geographisch verteilte Validator-Nodes.
- Monitoring: Echtzeit-Überwachungssystem mit Alerts.
- Backup: Backup- und Disaster-Recovery-Strategie.

8 Leistungsevaluierung

8.1 Performance-Metriken

8.1.1 Transaktionsdurchsatz

Performance-Tests zeigen:

• Agentenregistrierungen: 1.200 Registrierungen/Sekunde

• Discovery-Anfragen: 5.500 Anfragen/Sekunde

• Reputationsupdates: 2.800 Updates/Sekunde

8.1.2 Latenz

• Transaktionsbestätigung: 650ms durchschnittlich

• Suchanfragen: 120ms durchschnittlich

• Statusupdates: 85ms durchschnittlich

8.2 Skalierbarkeitsanalyse

8.2.1 Wachstumsprojektionen

Basierend auf aktuellen Adoptionstrends:

Metrik	Jahr 1	Jahr 3	Jahr 5
Registrierte Agenten	10.000	500.000	5.000.000
Tägl. Transaktionen	100.000	10.000.000	100.000.000
Token-Volumen (AEA)	1M	100M	1B

Table 1: AEA-Netzwerk Wachstumsprojektionen

9 Zukunft und Roadmap

9.1 Geplante Entwicklungen

9.1.1 Kurzfristig (6-12 Monate)

- Implementierung von Zero-Knowledge-Beweisen für erhöhte Privatsphäre
- Unterstützung für sophistiziertere KI-Agenten
- Integration mit dezentralisierten Oracle-Anbietern

9.1.2 Mittelfristig (1-2 Jahre)

- Entwicklung eines Agenten-Marktplatzes
- Implementierung selbstmodifizierender Smart Contracts
- Unterstützung für vollständige dezentralisierte Governance

9.1.3 Langfristig (2-5 Jahre)

- Integration mit föderierten KI-Netzwerken
- Entwicklung von Interoperabilitätsstandards
- Expansion auf andere Blockchain-Ökosysteme

9.2 Forschung und Entwicklung

9.2.1 Aktive Forschungsgebiete

- Für KI-Agenten optimierte Konsensalgorithmen
- Verbesserte Techniken zur Privatsphäreerhaltung
- Adaptive Wirtschaftsmodelle
- Multi-Agent-Koordinationsprotokolle

10 Fazit

Das AEA-Netzwerk stellt einen signifikanten Fortschritt in der Infrastruktur für autonome Wirtschaftsagenten dar. Durch die Kombination von Hochleistungs-Blockchain-Technologie, innovativem Tokenomics-Design und robuster Sicherheitsarchitektur bieten wir eine Plattform, die die nächste Generation wirtschaftlicher KI-Anwendungen unterstützen kann.

Die Schlüsselbeiträge dieser Arbeit umfassen:

- 1. **Skalierbare Infrastruktur**: Ein System, das Millionen von Agenten und Transaktionen handhaben kann.
- 2. Wirtschaftliche Anreize: Ein Tokenomics-Modell, das die Anreize aller Teilnehmer ausrichtet.
- 3. Robuste Sicherheit: Mehrere Sicherheitsschichten mit unabhängigen Audits.
- 4. Praktische Adoption: Tools und SDKs zur Erleichterung der Entwickleradoption.

Die Zukunft der digitalen Wirtschaft wird von autonomen Agenten angetrieben werden, die fähig sind, komplexe wirtschaftliche Entscheidungen zu treffen. Das AEA-Netzwerk bietet die fundamentale Infrastruktur, die notwendig ist, um diese Vision zu verwirklichen und ein Ökosystem zu schaffen, in dem Agenten dezentralisiert und sicher interagieren, zusammenarbeiten und prosperieren können.

References

- [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.