DeepSafe: Crypto Random AI Verification Network

DeepSafe Team

March 2025

Abstract

The year 2025 marks when the blockchain industry is striving for product-market fit while AI is booming. In this era of growing convergence between Blockchain and AI and with the concept of AI Agents gaining popularity, ensuring data trustworthiness and integrity in a decentralized environment is a key challenge. DeepSafe emerges in this context as a Crypto Random AI Verification Network. Its primary goal is to enable trustless verification of any on-chain and off-chain messages, thereby providing reliable validation for the input and output information of AI Agents. Furthermore, DeepSafe bridges the gap between the on-chain and off-chain worlds, addressing the current limitations of oracle services in reliably transmitting arbitrary messages.

1 Background and Requirements

With the continuous maturation of blockchain technology, decentralized systems have excelled in areas such as data storage, identity verification, and transaction execution. However, when it comes to processing massive amounts of data and complex information, ensuring the authenticity and integrity of data during transmission remains an urgent challenge. Meanwhile, Artificial Intelligence (AI) technology, especially AI Agent based on Large Language Model (LLM), has achieved breakthroughs in natural language processing, image recognition, and decision support. Yet, since AI models rely on vast amounts of data during training and deployment, verifying the trustworthiness of this data as well as the reliability of the model outputs has become a core challenge.

In addition, AI Agents are prone to hallucinations and may provide incorrect answers to certain questions. If an AI Agent is used to assess the outcome of a real-world event, there is still the possibility of false reports. This makes off-chain information crawling and feedback based on AI Agents not necessarily reliable. Moreover, if oracle services need to obtain arbitrary off-chain information, they have to rely on AI Agents or manual submissions, with the latter being susceptible to governance attacks, which has been exemplified by the UMA oracle governance attack case on PolyMarket.

If a blockchain smart contract intends to adopt a trustless and secure method to obtain arbitrary off-chain information, it must ensure that the results submitted by AI Agents are consistently accurate.

In this context, DeepSafe has emerged. Its design concept is to utilize cryptographic random algorithms, deep search, and distributed networks to verify arbitrary on-chain and off-chain messages in a trustless manner. This ensures that the input and output information of AI Agents is not tampered with or forged during transmission and processing, thereby providing a solid foundation of trust for various AI and cryptographic applications.

2 Core Technical Principles

2.1 Cryptographic Random Algorithms

DeepSafe employs advanced cryptographic random algorithms to generate unpredictable random number sequences, introducing randomness throughout the verification process. This approach ensures the

fairness and tamper-resistance of the verification process without relying on a central authority. The inherent randomness prevents attackers from predicting or manipulating verification steps, ensuring that each message undergoes a unique verification path, thereby enhancing security and credibility.

2.2 Deep Search

DeepSafe's deep search technology leverages efficient data structures and intelligent algorithms to enable real-time retrieval and comparison of massive on-chain and off-chain data. By constructing index structures such as Merkle trees and Trie trees, it hierarchically indexes every transaction and state change on the blockchain, allowing target data to be located in an extremely short time. At the same time, this technology integrates large language models, operates based on specific reasoning patterns, and utilizes tools to perform semantic analysis and intelligent matching on heterogeneous data from different sources, automatically detecting anomalies and risks of data tampering. Through multidimensional data fusion, deep search not only verifies oracle data and on-chain records but also conducts high-precision validation of the input and output of AI Agents, ensuring that all information remains consistent and tamper-proof during transmission and processing. This technological core provides robust data support for DeepSafe to build a trustless verification network, significantly enhancing the system's reliability and security in cross-chain and cross-platform application scenarios.

2.3 On-chain and Off-chain Message Verification

An important feature of DeepSafe is its ability to handle on-chain and off-chain message verification. For the on-chain component, all data and messages are recorded on the blockchain, leveraging its immutability and decentralized nature to ensure the authenticity and validity of the data. The off-chain component interfaces with external data sources and traditional databases, employing cryptographic verification and multi-signature mechanisms to achieve trustworthy validation of offline data. As a result, DeepSafe can not only verify transactions and smart contract executions on the blockchain but also validate off-chain business data, sensor data, and AI model outputs, establishing a trusted information transmission network across chains and systems.

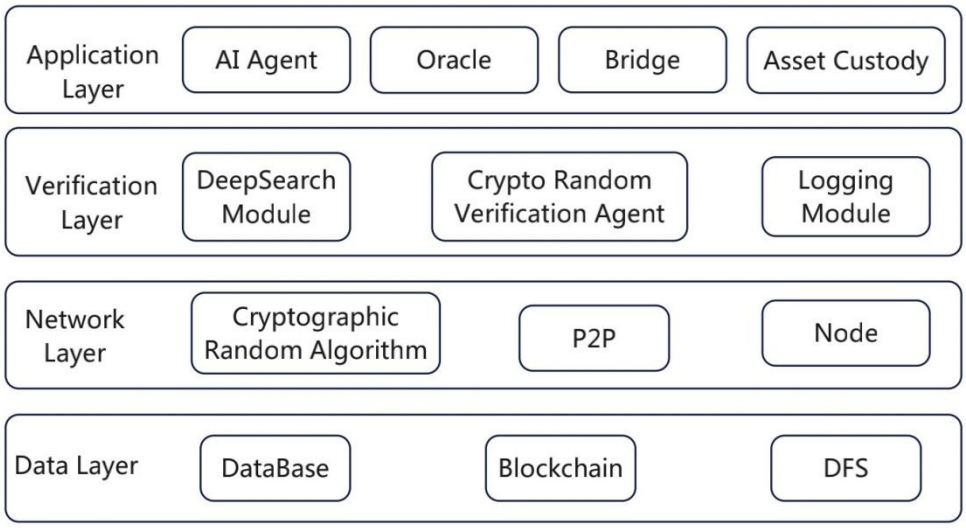
2.4 Trusted Verification of AI Agent Input and Output

When an AI Agent processes data, the authenticity of the input data and the accuracy of the model's output directly impact the accuracy of decision-making. DeepSafe ensures the reliability of every piece of input data received by the AI Agent by applying encrypted signatures and random verification to each data packet, guaranteeing that the data originates from a trustworthy source and remains untampered during transmission. Additionally, at the model output stage, DeepSafe compares the results with preset validation algorithms to ensure the output aligns with expectations. In this way, AI applications can establish a trusted data flow based on the verification results provided by DeepSafe, effectively reducing risks arising from inaccurate data.

2.5 Distributed Consensus and Trustless Mechanism

DeepSafe is based on a distributed consensus mechanism, where all participating nodes must independently compute and provide verification results during data validation. Only when a certain proportion of nodes reach a consensus does the system deem the data or message trustworthy. This trustless mechanism eliminates reliance on a single node or central server, ensuring the decentralization and security of the entire verification process. Meanwhile, nodes exchange information through encrypted communication, zero-knowledge proofs, and other technologies, making the verification process both efficient and highly resistant to tampering.

3 System Architecture



3.1 Network Layer

The network layer of DeepSafe consists of multiple verification nodes distributed globally, which collaborate to perform data validation tasks. Each node independently runs cryptographic random algorithms and broadcasts its verification results to the network. The network layer employs a P2P protocol for communication, ensuring the efficiency and robustness of data transmission.

3.2 Verification Layer

The verification layer is the core module of DeepSafe, responsible for the cryptographic verification of on-chain and off-chain messages. This layer primarily includes the following modules:

- Encryption Module: Handles data encryption, signing, and random number generation to ensure security during data transmission.
- Deep Search Module: Utilizes efficient data indexing and intelligent algorithms to enable rapid retrieval and semantic comparison of vast amounts of on-chain and off-chain data, ensuring an efficient and accurate verification process.
- Verification Module: Employs multiple verification algorithms to compare and confirm input and output data. This module uses distributed consensus algorithms to ensure consistency across the majority of nodes before presenting the final verification result.
- Logging Module: Records all data and results from the verification process, ensuring traceability and providing a basis for audits.

3.3 Application Layer

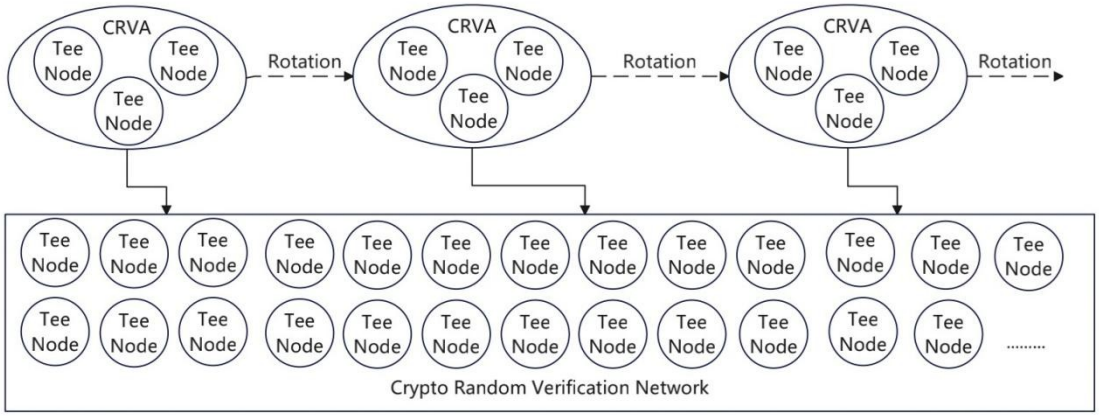
At the application layer, DeepSafe provides standardized API interfaces for use by various AI Agents, smart contracts, and off-chain applications. These interfaces include functions such as data upload, verification requests, and verification result queries. Through open APIs, developers can easily integrate DeepSafe into existing systems, enabling trustless data verification across chains and systems.

3.4 Data Storage Layer

The data storage layer employs distributed database and blockchain storage technologies to ensure the secure preservation of all verification data and log records. Through multiple backups and a redundant design, the overall system remains operational even if some nodes fail.

4 Cryptographic Random Verification Technology

The DeepSafe cryptographic random verification network integrates four core technologies—Ring VRF, Zero-Knowledge Proofs (ZK), Multi-Party Computation (MPC), and Trusted Execution Environment (TEE)—to establish a trustless, distributed data verification system. It provides verification services externally through the Cryptographic Random Verification Agent (CRVA). This system not only enables efficient data verification both on-chain and off-chain but also offers robust security guarantees for AI Agents and other application scenarios.



4.1 Core Technology Architecture

The core service of DeepSafe is implemented through the Cryptographic Random Verification Agent (CRVA). The CRVA uses Ring VRF technology to randomly select a small subset of nodes from the network's verification nodes, forming a verification committee tasked with data validation. This design ensures the randomness, unpredictability, and distributed consensus of the verification process, thereby achieving trustless verification.

4.2 Key Technology Modules

4.2.1 Ring VRF Ensures Randomness

DeepSafe utilizes Ring VRF (Verifiable Random Function) to generate unpredictable random numbers, which are used to randomly assign verification nodes. By randomly selecting the verification committee (CRVA), the system ensures that each verification follows a different path, significantly reducing the risk of attackers predicting the verification process and tampering with data.

4.2.2 Zero-Knowledge Proof Conceals Node Selection

During the verification process, to protect the information of randomly selected nodes, DeepSafe incorporates zero-knowledge proof technology. The identity and specific participation details of the verification nodes remain undisclosed to the public, thereby enhancing the privacy and security of the entire verification network and ensuring that sensitive information is not exposed.

4.2.3 MPC Enables Threshold Signatures and Dynamic Rotation

Multi-Party Computation (MPC) technology allows multiple verification nodes to collaboratively compute and jointly generate threshold signatures. Only when the preset signature threshold is reached will the verification result be confirmed, thereby ensuring the security and accuracy of data validation. At the same time, MPC supports dynamic node rotation, automatically replacing committee nodes at regular intervals, such as every hour, which reduces the risk of single-point failures and enhances the system's robustness and resistance to attacks.

4.2.4 TEE Ensures Core Data Privacy

Trusted Execution Environment (TEE) provides hardware-level protection for DeepSafe's core programs and sensitive data. By running verification logic in an isolated environment, TEE prevents malicious attackers from accessing or tampering with core algorithms and data, thereby ensuring the confidentiality and integrity of the entire verification process.

4.3 Advantages and Challenges

4.3.1 Advantages

- Significantly enhanced security and transparency in data verification processes.
- Randomized path allocation prevents attackers from predicting verification workflows, thereby reducing data tampering risks.
- Distributed consensus guarantees immutability and non-repudiation of verification results.

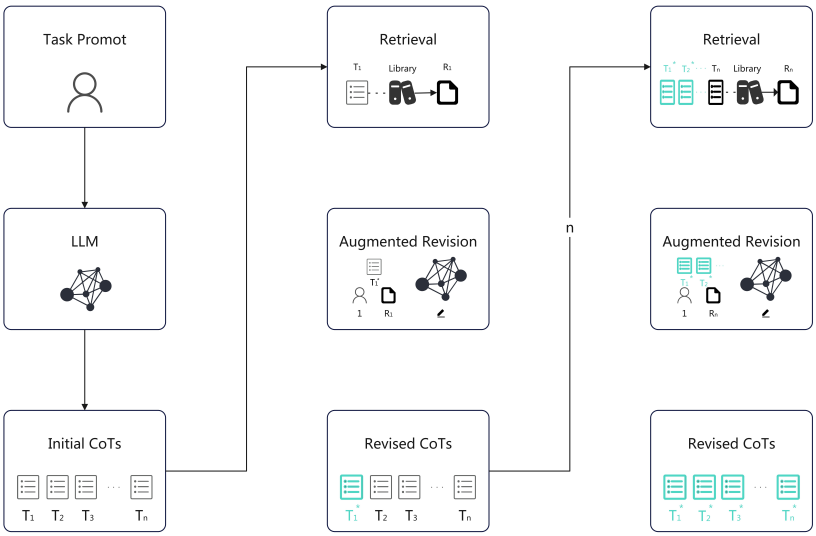
4.3.2 Challenges

- High computational demands: The efficiency of randomized algorithms requires nodes to possess strong computational capabilities.
- Algorithm optimization challenges: Path generation and result aggregation require highly optimized algorithms in high-concurrency scenarios.
- Latency issues: Distributed consensus may introduce additional delays under high network latency or with a large number of nodes.

5 Deep Search Technology

5.1 Introduction to Deep Search Technology

DeepSafe's deep search technology is fundamentally powered by large language models (LLMs) and deep learning algorithms, integrated with reasoning frameworks and external tool orchestration, to enable verification of nearly all on-chain and off-chain events. The system not only rapidly retrieves target data but also evaluates the authenticity and integrity of information through semantic matching, contextual analysis, and cross-dimensional data fusion, forming a dynamic, intelligent, and self-adaptive verification framework.



The primary objective of DeepSafe's deep search technology is to achieve efficient retrieval and intelligent analysis of massive datasets. Specifically:

- Data Indexing: Utilizes high-performance data structures, such as Merkle Trees and Trie Trees, to build hierarchical indexing for on-chain data, enabling rapid data localization and retrieval.
- Intelligent Matching: Integrates large language models (LLMs) and deep learning techniques to perform semantic analysis and pattern recognition on verification data, automatically identifying correlations and anomalies across datasets.
- Cross-Source Data Convergence: Supports not only blockchain data but also integrates off-chain data sources, such as enterprise databases, IoT device streams, through a unified indexing system for deep search and cross-referencing.

5.2 Core Implementation Principles

5.2.1 LLM-Based Semantic Parsing

DeepSafe leverages advanced Large Language Models (LLMs) to perform deep semantic parsing of target verification data. Unlike traditional verification methods relying on static rule matching, LLMs comprehend complex natural language descriptions and contextual relationships, converting event data into vector representations with semantic labels. This enables the system to not only identify numerical and state-based data but also detect latent contradictions or anomalies in descriptive or textual information.

5.2.2 Deep Search & Dynamic Tool Orchestration

DeepSafe embeds domain-specific reasoning frameworks to simulate "logical inference" capabilities. For instance, when verifying a transaction or event, the system autonomously constructs an event causality graph to analyze:

- Entity correlations (e.g., counterparty relationships in DeFi transactions).
- Temporal consistency (e.g., sequence of cross-chain operations).
- Logical plausibility (e.g., compliance with smart contract constraints).

By combining LLM-driven semantic understanding with deep search results, DeepSafe executes multi-layered cross-validation (semantic, temporal, and logical dimensions) to generate comprehensive, adaptive verification conclusions.

5.3 Comparison with Traditional Verification Methods

5.3.1 Static Rules vs. Dynamic Semantic Comprehension

Traditional verification systems rely on predefined rules and simplistic pattern matching, which are prone to missing anomalies in complex scenarios. In contrast, DeepSafe achieves holistic semantic and contextual understanding through LLMs and deep search technology, enabling the detection of subtle inconsistencies and anomalies. This approach significantly enhances verification accuracy and flexibility, such as identifying disguised wash trading in DeFi or fabricated timestamps in supply chain logs.

5.3.2 Fixed Indexing vs. Real-Time Dynamic Retrieval

Conventional systems often depend on rigid indexing architectures, such as SQL databases, which may suffer from degraded performance as data scales or updates dynamically. DeepSafe's intelligent indexing—powered by adaptive Merkle-Patricia Trie hybrids and on-demand external data ingestion—ensures verification outcomes are always grounded in the most recent on/off-chain states, achieving sub-second responsiveness even in high-throughput environments like NFT marketplaces.

5.3.3 Centralized Verification vs. Decentralized Intelligent Verification

Traditional verification methods often rely on centralized institutions or databases, which inherently present single points of failure and trust risks. In contrast, DeepSafe leverages a trustless distributed verification network and multi-node collaboration, combined with cryptographic random verification technology, to ensure that the verification process is distributed, transparent, and tamper-proof. This approach provides enhanced security guarantees for cross-chain and cross-platform applications.

5.4 The Role of Deep Search in Data Verification

In the DeepSafe system, deep search technology plays a crucial role in several aspects:

- Rapid Retrieval of On-Chain Data: Every transaction and state change on the blockchain is recorded in detail. By leveraging deep search technology, verification nodes can quickly locate target data and compare it with the data to be verified, thereby assessing its authenticity. This not only accelerates the verification process but also improves the accuracy of data retrieval.
- Integration and Verification of Off-Chain Data: For off-chain data, such as data transmitted from IoT devices, internal enterprise records, and AI Agent output results, DeepSafe builds a unified distributed indexing system to integrate this data with on-chain data. The deep search algorithm then compares and verifies these heterogeneous datasets, ensuring data consistency and trustworthiness during cross-platform and cross-system transmission.
- Anomaly Detection: Deep search technology, when combined with machine learning algorithms, is capable of automatically detecting and flagging data anomalies. The system can analyze data flows in real time to identify abnormal patterns-such as duplicate submissions, signs of tampering, or abnormal delays-and swiftly trigger alert mechanisms to safeguard the overall security and stability of the verification process.
- Multidimensional Data Fusion: In practical applications, data formats vary across different scenarios. Deep search technology supports the retrieval of text and numerical data while also enabling semantic matching and feature extraction for multimedia data (such as images and videos). This capability facilitates trustless verification across different data types, which is particularly important for verifying the input and output data of AI Agents and ensuring accuracy throughout the transmission process.

5.5 Advantages

- Efficiency: Utilizing advanced data structures and indexing algorithms, deep search technology can quickly pinpoint target information within massive datasets, enabling real-time verification.
- Intelligence: By integrating machine learning and NLP algorithms, deep search technology performs semantic analysis and intelligent matching on the data, allowing it to automatically detect anomalies and potential risks.
- Cross-Platform Compatibility: It is capable of integrating both on-chain and off-chain, as well as structured and unstructured data, providing consistent verification standards for various scenarios such as cross-chain bridges and asset custody.

5.6 Challenges

- Data Volume and Complexity: With the rapid growth in data volume, the deep search system requires continuous optimization of its indexing and query algorithms to avoid performance bottlenecks.
- Heterogeneous Data Fusion: The fusion and standardization of different data sources and data types is a complex issue that necessitates the design of unified protocols and interfaces to ensure data comparability and verification accuracy.
- Security and Privacy: During the integration of data from multiple sources, protecting the privacy of sensitive data while still achieving efficient verification is a critical technical challenge that must be overcome.

6 Application Scenarios

6.1 AI Agent Data Verification

DeepSafe can provide trustworthy verification services for various AI Agents. Whether it is an intelligent trading bot in the financial sector, a medical imaging analysis system, or a content-generating AI on social media, DeepSafe can verify their input data and output results to ensure the authenticity of the data and the reliability of the model's outcomes.

6.2 DeFi Scenario: Anti-Manipulation Oracles

Traditional oracles are unable to verify complex off-chain events, such as whether Tesla's Q2 net profit exceeded expectations. DeepSafe could solve by aggregating data from multiple sources, utilizing NLP models to extract key indicators, conducting cross-validation, and updating on-chain state when over 70% of the nodes are in agreement.

6.3 Cross-Chain Data Interoperability

In a cross-chain ecosystem, data on different blockchains often exist in isolated silos. DeepSafe acts as a bridge by performing a trustless verification of data across different chains, enabling reliable data sharing across blockchains. This is highly significant for DeFi, cross-chain trading, and multi-chain applications.

6.4 Supply Chain and Internet of Things (IoT)

For supply chain management and IoT, the authenticity and real-time nature of data are crucial. DeepSafe can verify sensor data and logistics information both on-chain and off-chain in real time, ensuring that data at every link remains tamper-proof and thereby improving overall system transparency and efficiency.

6.5 Privacy Protection and Compliance

In certain scenarios, data verification must also protect user privacy. DeepSafe employs cryptographic techniques and zero-knowledge proofs to complete the verification process without disclosing specific data contents, meeting compliance requirements while safeguarding user privacy.

7 Future Outlook and Challenges

7.1 Scalability and Performance Enhancement

As data volume and verification requests increase, DeepSafe must continuously optimize its consensus algorithms and verification processes to improve system scalability. In the future, the platform will explore more parallel verification and sharding techniques to ensure it can maintain high TPS and low latency even in large-scale application scenarios.

7.2 Cross-Chain and Multi-System Integration

DeepSafe will further refine its cross-chain data verification capabilities to enable seamless interoperability among various public blockchains, private blockchains, and off-chain systems. By integrating with existing blockchain platforms, enterprise databases, and IoT devices, DeepSafe aims to build a comprehensive data verification ecosystem that bridges the on-chain and off-chain worlds.

7.3 Security and Auditing

Given that DeepSafe handles a substantial amount of sensitive data and fund flows, security remains paramount. In the future, the platform will introduce additional security measures—such as regular third-party audits, multi-signature mechanisms, and automated security monitoring—to ensure that the system remains robust and reliable against various attacks.

7.4 Community and Ecosystem Development

A successful trustless verification network relies heavily on strong community support. DeepSafe will attract more developers and enterprises through open-source initiatives, incentive programs, and strategic partnerships, thereby collaboratively building a decentralized verification ecosystem. With ongoing ecosystem enhancements, DeepSafe is well-positioned to become the standard platform for cross-chain and cross-system data verification.

8 Summary

DeepSafe, as a cryptographic random AI verification network, enables trustless verification of on-chain and off-chain messages, providing reliable validation for AI Agent inputs and outputs. Its core technologies include cryptographic random algorithms, deep search technology, on-chain and off-chain verification, distributed consensus, and vault-based incentive mechanisms. These technologies not only effectively prevent data tampering but also provide efficient, low-latency data verification services across various application scenarios. With continuous improvements in scalability, security, and cross-chain integration, DeepSafe is poised to play an increasingly critical role in the convergence of blockchain and AI, driving sustained innovation and development in the decentralized data verification field.