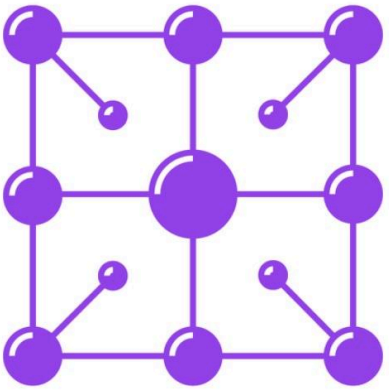

SIGNCHAIN

Blockchain signatures made simple.
Integrate off-chain data from Google Sheets or
APIs with Ethereum, Polygon, and more.

Whitepaper

Abstract

Signchain is an innovative blockchain-based platform designed to address the challenges of authenticity and trust in digital content. In today's digital era, the increasing amount of misinformation, data forgery, and unauthorized content usage has made it crucial to establish systems that can verify the authenticity of information at every stage. Signchain aims to tackle these issues by providing a decentralized and secure method for certifying and verifying the provenance of data points, enabling smart contract developers and other stakeholders to trust the data they utilize. The platform integrates seamlessly with off-chain service providers such as Google Sheets, APIs, and other dynamic data sources to ensure that every piece of off-chain data ingested into smart contracts is trustworthy and secure.

By utilizing blockchain technology, Signchain ensures the transparency, integrity, and immutability of data, thus mitigating risks associated with centralized systems. Unlike traditional systems where data validation is controlled by a central authority, Signchain leverages the power of distributed ledgers to create a decentralized infrastructure for verifying the integrity of digital content. This provides an immutable record that can be verified by anyone, enhancing trust in digital interactions. The combination of smart contracts and cryptographic signatures offers a secure mechanism for validating data without needing intermediaries, minimizing both risks and operational costs.

Signchain's approach is centered around off-chain data signing and on-chain verification, thereby avoiding the prohibitive costs of storing large volumes of data directly on the blockchain. The platform uses cryptographic methods, including elliptic curve digital signatures, to sign off-chain data, making sure that each data point comes from a verified source. Signchain introduces the Signable contract, which is designed to handle and authenticate data coming from off-chain sources. By integrating the Signable contract, developers can specify trusted signer addresses and manage key rotation securely, reducing potential vulnerabilities. Additionally, Signchain employs mechanisms to prevent replay attacks and restrict the misuse of contracts across multiple chains, thereby strengthening the security model for on-chain data verification.

This white paper outlines the technical architecture, use cases, and benefits of Signchain, focusing on its application in real-world scenarios where data integrity and trust are paramount. It also highlights the underlying technologies and protocols that make Signchain a versatile and robust solution for ensuring the trustworthiness of digital content. Signchain empowers individuals and organizations to establish reliable, tamper-proof digital content trails, enabling data-driven decision-making and reducing the risks associated with misinformation and unauthorized alterations. Whether it is used in content creation, supply chain verification, or corporate data management, Signchain

stands out as a comprehensive and efficient solution for ensuring data authenticity in an increasingly interconnected digital landscape.

1. Introduction

In an increasingly digital world, issues of trust, authenticity, and transparency are becoming critical. Fake content, misinformation, and the inability to verify the origin of off-chain data points pose significant challenges. As data becomes an essential part of decision-making processes, whether in finance, healthcare, or governance, the integrity of this data is paramount. The lack of reliable verification methods for off-chain data has led to significant inefficiencies, increased risks, and an erosion of trust among stakeholders. The rapid proliferation of misinformation has made it more difficult to determine which data can be trusted, especially when it comes to integrating off-chain data into blockchain-based systems.

Traditional centralized solutions for data verification have several inherent weaknesses. Centralized authorities can be compromised, leading to the manipulation or loss of critical data. Moreover, the lack of transparency in centralized systems often means that users must rely on third-party assurances without being able to independently verify the authenticity of the information they are provided. This has led to an increasing demand for decentralized solutions that provide transparency, immutability, and trust without relying on a single point of failure.

Signchain leverages blockchain technology to offer a reliable and efficient solution to these pressing issues, ensuring that every data point has a verifiable source and integrity that can be easily checked by anyone. By using cryptographic signatures and blockchain's inherent properties of immutability and transparency, Signchain provides a tamper-proof mechanism for certifying the authenticity of data. This allows developers, organizations, and end-users to confidently use off-chain data in their smart contracts, reducing the risks associated with incorrect or manipulated information.

The rise of smart contracts has further highlighted the need for secure and trustworthy off-chain data. Smart contracts are self-executing programs that run on blockchain networks, and they often require external data to function correctly. This data may include anything from price feeds for financial contracts to user-generated content for decentralized applications. Without a reliable method for verifying the authenticity of this data, the entire smart contract ecosystem is at risk. Signchain aims to bridge this gap by providing a secure and decentralized method for signing and verifying off-chain data before it is ingested by smart contracts.

Signchain also addresses the challenges associated with integrating data from various sources. Modern applications rely on diverse data points, including data from APIs, off-chain databases, and even spreadsheets. By providing a standardized mechanism for certifying and signing this data, Signchain simplifies the integration process for developers. Developers can be confident that the data they are using in their smart contracts is authentic, up-to-date, and has not been tampered with, thereby enhancing the reliability of their decentralized applications.

In addition, Signchain's focus on user empowerment and decentralized control ensures that data ownership and accountability are distributed across multiple participants rather than being concentrated in a central authority. This democratized approach aligns with the core values of blockchain technology and helps build a more resilient and trustworthy digital ecosystem. By enabling users to self-host the Signchain Vault or use a centrally managed service, Signchain caters to a wide range of use cases, from individual developers to large enterprises, each with their own unique security and control requirements.

Ultimately, Signchain is designed to foster a more transparent and accountable digital world. By providing a comprehensive solution for certifying and verifying the authenticity of off-chain data, Signchain enables individuals and organizations to establish reliable and tamper-proof digital content trails. This, in turn, helps mitigate the risks associated with misinformation, data forgery, and unauthorized use of digital content, paving the way for a future where digital trust is the default rather than the exception.

2. Problem Statement

The digital age has made it easier than ever to share information. However, it has also given rise to a new set of problems, including misinformation, data forgery, and a lack of accountability. As digital systems become more interconnected, the need for secure and transparent mechanisms to bring off-chain data on-chain has become increasingly important. The integration of off-chain data into blockchain environments poses significant security challenges, particularly when it comes to ensuring that the data is accurate, trustworthy, and has not been tampered with.

One of the most pressing issues in the current landscape is the lack of standardized and secure methods for managing signer keys and bringing off-chain data onto the blockchain. Many projects, in an attempt to bridge the gap between off-chain data sources and on-chain environments, end up implementing their own solutions for securing signing wallets. These custom implementations are often simplified and lack the robustness required to effectively secure the private keys used for signing off-chain data. This results in vulnerabilities that can be exploited by malicious actors, leading to data breaches, unauthorized transactions, and loss of trust.

Security is a complex and challenging aspect of blockchain development. Ensuring that signing wallets are adequately secured requires not only strong encryption mechanisms but also effective key rotation, access control, and secure key storage. Without these elements, the risk of compromised signing keys becomes a serious concern. Projects that attempt to implement their own key management systems often do so without fully understanding the complexities involved, which can lead to weak security practices and significant vulnerabilities.

Signchain addresses these challenges by offering a comprehensive, full-service solution for managing signer keys and integrating off-chain data stores. By providing a secure and decentralized platform, Signchain ensures that developers do not need to create their own solutions for managing signing keys. Instead, they can leverage Signchain's infrastructure to securely sign off-chain data and bring it on-chain with confidence. This eliminates the need for developers to worry about the complexities of key management, allowing them to focus on building their applications.

Signchain also integrates live Data Stores from across Web2, providing a seamless way to bring data from sources like Google Sheets, DynamoDB, and REST APIs onto the blockchain. This integration follows a user-pays-gas-fees model, meaning that the costs of bringing data on-chain are distributed among users, rather than being borne entirely by the developer or the platform. This model not only reduces costs for developers but also ensures that data is brought on-chain in a way that is efficient and scalable.

The transparency offered by Signchain is another key differentiator. Current systems for certifying authenticity are often centralized, which makes them prone to manipulation and limits their accessibility. In contrast, Signchain's decentralized architecture ensures

that no single entity has control over the certification process. This makes the system more resilient to attacks and provides greater transparency for users, who can independently verify the authenticity of the data being brought on-chain.

By providing a robust and secure mechanism for managing signer keys and integrating off-chain data, Signchain solves the key challenges of security, transparency, and scalability in blockchain development. The platform's full-service solution not only enhances the security of the signing process but also simplifies the integration of off-chain data, making it easier for developers to create trusted and reliable smart contracts. With Signchain, organizations can bring off-chain data on-chain with confidence, knowing that their data is secure, authentic, and transparent.

3. Vision and Objectives

Signchain envisions a future where digital content is inherently trustworthy, and where the authenticity of any data point or media can be verified instantly. Our core objectives are:

- To create a secure and decentralized on-chain signing solution for off-chain data.

- To empower creators and organizations to maintain ownership over their intellectual property.

- To provide transparency in on-chain transaction signing, reducing the risk of misinformation and forgery.

4. Technical Overview

Signchain leverages blockchain's inherent properties of immutability and transparency to create a decentralized certification platform. The technical components of Signchain include:

Blockchain Backbone

Signchain is built on a robust blockchain infrastructure that ensures data immutability and transparency. Each transaction registered on Signchain is assigned a unique cryptographic hash, stored on the blockchain. The blockchain layer is implemented using Ethereum-compatible blockchains to leverage the extensive tooling and security features available in the ecosystem.

Smart Contracts

Smart contracts are used to automate the certification and verification processes, reducing manual intervention and ensuring that rules are consistently enforced. Signchain smart contracts are written in Solidity and utilize standardized libraries such as OpenZeppelin for security and upgradeability. The smart contract developer integrates by inheriting from the Signable contract and implementing their own method to set the signer address, allowing for the rotation of keys and supporting secure key management.

Signable Contract

The Signable contract is at the core of the Signchain solution. It secures blockchain transactions by verifying that the data injected into the smart contract method has been signed by an off-chain backend signer address. The contract ensures that only data coming from the Signchain service, authenticated through an ECDSA signature, is accepted by the smart contract. The Signable contract employs industry best practice security measures, including the prevention of replay attacks for signatures submitted on-chain. This is achieved by using unique nonces that are tracked and validated, ensuring that each signature can only be used once. Additionally, the Signable contract prevents attacks such as deploying the contract on multiple chains, ensuring that signatures are only valid on the intended chain.

EVM Signature Details

In an Ethereum Virtual Machine (EVM) context, signatures are used to ensure the authenticity of transactions and data inputs. The signature process involves the following steps:

Message Hashing

Data or messages are hashed using the Keccak-256 algorithm, providing a fixed-length output regardless of the input size, ensuring consistency and security.

Signing

The hashed message is signed with the signer's private key using the Elliptic Curve Digital Signature Algorithm (ECDSA). This produces a 65-byte signature consisting of r, s, and v values.

Verification

On-chain, the smart contract uses the ecrecover function to verify the signature against the signer's public key, ensuring the integrity of the data.

Off-Chain Data Integration

Signchain supports integration with off-chain data sources such as APIs and Google Sheets. Data integration is facilitated by the Signchain Vault, which acts as an off-chain data signing service. The Vault can be self-hosted by developers or organizations, allowing them to maintain control over the signing keys. Off-chain data is signed by the Vault and then submitted to the blockchain through transactions, ensuring data integrity and authenticity without requiring data to be directly stored on-chain.

Signchain Vault

The Signchain Vault is a critical component for secure key management and signing operations. The Vault uses multiple layers of encryption, including data encrypting keys (DEKs) and key encrypting keys (KEKs). The DEKs are used to encrypt the private keys of signer addresses, and the KEKs are used to encrypt the DEKs, providing a hierarchical security structure.

Data Stores Functionality

By leveraging the Data Stores functionality of Signchain, developers can easily integrate user-supplied data such as the amount they want to purchase, with Google Sheets data, live DynamoDB table data, JSON REST APIs, GraphQL APIs, as well as data from services such as The Graph. All signed by Signchain with verifiable signatures from a secure hosted or self-hosted Signchain Vault. By leveraging Signchain Data Stores functionality, developers can have a completely serverless model to integrate Signchain data, as well as integrating simpler backend API endpoints to execute additional custom functionality on top of the Data Store's data, enabling non-technical users of the organization to manage the data seamlessly, giving developers freedom to focus on

other areas of the business without the need to constantly redeploy data into their data stores.

5. Use Cases

Content Creators

Artists, authors, and musicians can use Signchain to certify their work, proving ownership and protecting their intellectual property. By leveraging the immutability of blockchain, creators can establish an unchangeable record of their work, ensuring verifiability.

Corporate Data Management

Businesses can utilize Signchain to certify sensitive data, ensuring that shareholders and stakeholders can verify its authenticity. Data points from corporate databases can be signed off-chain and verified on-chain, providing an auditable trail of information.

Educational Certifications

Institutions can issue diplomas and certifications through Signchain, preventing forgery and ensuring that employers can verify credentials. Certification data is signed off-chain by the educational institution and stored immutably on-chain for easy verification.

GameFi and NFT Minting

Signchain provides seamless integration for NFT minting, with live views of off-chain data, and GameFi applications that allow users to convert points into on-chain assets. By using Signchain's signing mechanism, in-game achievements and NFT whitelists can be maintained off-chain while preserving their integrity during blockchain interactions.

Supply Chain Verification

Signchain can be used to track the origin and journey of goods within supply chains. Off-chain data, such as supplier information, transport logs, and quality checks, can be signed by trusted entities and verified on-chain. This allows consumers to verify the authenticity and quality of products, reducing fraud and enhancing transparency across supply chains.

Healthcare Data

In the healthcare sector, Signchain can be used to verify patient data, clinical trial information, and drug authenticity. Sensitive healthcare data can be signed off-chain by healthcare providers and stored immutably on-chain. This ensures the integrity of data, prevents tampering, and allows authorized entities to verify the accuracy of information.

6. Benefits

Trust and Transparency

Signchain provides a transparent way to certify and verify digital content, allowing users to trust the information they interact with. By using cryptographic signatures, the integrity of data can be easily verified by anyone with access to the blockchain.

Decentralization

By leveraging blockchain, Signchain ensures that no single entity has control over the certification process, making it secure and resilient. The use of decentralized signer nodes (Signchain Vault) further strengthens the system against single points of failure.

Ownership and Protection

Creators can register their content, ensuring that their intellectual property is protected from unauthorized use or forgery. The ownership information is securely linked to cryptographic identities, making unauthorized claims of ownership virtually impossible.

Efficient Data Integration

Signchain alleviates the high costs and inefficiencies of directly storing large off-chain datasets on-chain, providing a streamlined approach that minimizes gas fees for users. By signing data off-chain and verifying it on-chain, users benefit from cost efficiency without sacrificing data integrity.

Scalability

Signchain's architecture allows for the integration of large volumes of off-chain data without compromising performance. By keeping the bulk of data off-chain and only storing signatures and cryptographic proofs on-chain, the platform can scale to meet the needs of various industries, including supply chain, healthcare, and finance.

Security and Prevention of Replay Attacks

The Signable contract employs mechanisms to prevent replay attacks. Every signed message contains a unique nonce, and the contract tracks previously used nonces to ensure that signatures cannot be reused maliciously. This feature is crucial in preventing double-spending or other forms of transaction fraud.

Deployment-Specific Signature Validation

Each instance of the Signable contract has a unique hash generated from the timestamp of deployment and the contract address. This means that multiple deployments of the same contract code use a cryptographically different set of signatures, whether on the same chain or on different chains. This prevents attackers from deploying the contract on a different chain or redeploying it on the same chain and attempting to reuse signatures, thereby ensuring that signatures are specific to the unique deployment of the contract.

7. Summary

Signchain is a decentralized platform designed to address the growing challenges of trust and authenticity in digital content. By leveraging blockchain technology, Signchain offers a robust solution for certifying and verifying off-chain data in a transparent and immutable manner. This platform addresses the increasing risks associated with misinformation, data forgery, and unauthorized use of digital content, which are particularly problematic in today's interconnected digital landscape.

The core innovation of Signchain lies in its ability to sign off-chain data using cryptographic methods, such as elliptic curve digital signatures, and verify this data on-chain through smart contracts. The platform's **Signable contract** allows developers to securely integrate off-chain data into their smart contracts without worrying about vulnerabilities like replay attacks or improper key management. By employing **key rotation**, secure signer addresses, and a **nonce-based security system**, Signchain ensures that only trusted, authenticated data is allowed on-chain, enhancing the overall security and reliability of blockchain-based applications.

Signchain tackles key challenges in blockchain development, including the **secure management of signer keys** and the **integration of off-chain data** from various sources like APIs and Google Sheets. Its infrastructure provides developers with a full-service solution that reduces operational risks, eliminates the need for building custom security solutions, and offers efficient, cost-effective methods to bring data on-chain without storing large volumes directly on the blockchain.

Real-world applications for Signchain span a wide range of industries. These include **content creators** looking to protect their intellectual property, **corporate data management** for secure and auditable information trails, **supply chain verification**, **healthcare data integrity**, **educational certification issuance**, and **NFT/GameFi development**. The platform’s scalability and decentralized control empower both individual users and large enterprises to maintain ownership, accountability, and trust in their digital content.

In summary, Signchain’s blockchain-based infrastructure provides a secure, transparent, and scalable solution for certifying off-chain data. Its decentralized model ensures trust without relying on a central authority, making it a resilient and efficient system for ensuring digital content authenticity across various sectors. The platform’s technical architecture, focused on security, cost-efficiency, and prevention of misuse, positions it as a key player in the future of trusted digital interactions.