Ian Loe

Decentralised Identity

Introduction

Decentralised identity, sometimes referred to as distributed identity, represents a paradigm shift in how personal and organisational credentials are managed and verified in the digital world. This approach moves away from centralised identity providers like Google, Facebook, or government institutions, instead empowering individuals to control their own identity data using blockchain and other decentralised technologies. This paper explores the history of distributed identity, the major players in the field, current applications, and the role it plays in the future of Web3.

History of Decentralised Identity

The concept of identity has evolved significantly with the advent of the internet. In the early days, identities were largely managed by centralised entities such as email providers or organisations that issued digital certificates. However, as online interactions grew more complex and concerns over privacy and security increased, the need for a more secure and user-centric identity model emerged.

In the mid-2000s, federated identity systems like OpenID and OAuth were developed, allowing users to authenticate with multiple services using a single set of credentials managed by a trusted third party. These systems introduced convenience, but they still relied on centralised control, raising concerns about data breaches and misuse of personal information.

The turning point for decentralised identity came with the rise of blockchain technology in the late 2000s. Bitcoin's decentralised ledger introduced the possibility of a "trustless" system where no single entity controlled the data. By 2015, Ethereum's introduction of smart contracts laid the foundation for decentralised applications (dApps), which allowed for the self-sovereign identity (SSI) concept to take shape. SSI empowers individuals to own and manage their digital identities, eliminating the need for centralised authorities.

Major Players in Distributed Identity

Several key organisations and platforms have emerged as leaders in the decentralised identity space, each offering unique solutions to the identity problem:

Sovrin Foundation

Sovrin is one of the early pioneers in decentralised identity, providing an open-source protocol that supports SSI. It uses Hyperledger Indy, a blockchain framework purpose-built for identity solutions, allowing individuals to create and manage their digital identities on a public ledger without intermediaries. Sovrin has been implemented in industries like healthcare and finance, where identity verification is critical. For example, organisations are using Sovrin for trusted digital identities to meet stringent data privacy regulations like GDPR.

Microsoft ION

Built on top of Bitcoin's blockchain, Microsoft's Identity Overlay Network (ION) is a decentralised identity network that aims to give individuals and organisations control over their credentials. ION enables secure and self-sovereign identities, supporting verifiable credentials that are controlled and owned by the user. Today, Microsoft is using ION to provide decentralised identity services to its Azure Active Directory users, integrating SSI into enterprise solutions. This allows users to control their own credentials when interacting with different services.

uPort

uPort is a digital identity platform built on the Ethereum blockchain. It provides users with tools to create, manage, and store their digital identities and personal data. With a focus on privacy, uPort allows users to decide what information to share with third parties while ensuring that no single entity controls the identity. uPort has been used by the Swiss city of Zug to offer citizens blockchain-based digital identities, enabling them to access government services and participate in local voting securely through the blockchain. As of now, uPort project has split into two new projects, **Serto** and **Veramo.**

Civic

Civic is another Ethereum-based identity platform that focuses on secure, low-cost, and verified identity solutions. Civic provides users with a wallet where they can store their personal information, which is then shared with third parties in a controlled manner through cryptographic proofs, rather than sharing the actual data itself. Civic is used in several industries, including financial services and cryptocurrency exchanges. It has partnered with blockchain projects to facilitate secure identity verification for token sales, ensuring compliance with KYC/AML requirements.

BrightID

BrightID offers a novel approach to decentralised identity by using a social graph to verify individuals' uniqueness. This ensures that each person has only one identity in the network, solving the problem of fake identities and bots, which is a growing issue in digital systems today. BrightID is used in blockchain applications, especially decentralised finance (DeFi) platforms, where ensuring unique user identities is critical for preventing fraud and bot-driven attacks.

SelfKey

SelfKey is a blockchain-based identity system that enables users to manage their identity data, conduct KYC (Know Your Customer) processes, and access a variety of digital services. SelfKey aims to empower individuals by giving them control over their data while offering privacy and security. SelfKey's identity wallet is used for KYC processes in crypto exchanges and financial services. SelfKey also enables users to access various services, such as setting up bank accounts and incorporating businesses, all while controlling their identity.

Evernym

Evernym is a company specialising in decentralised identity solutions, providing tools to create self-sovereign identities and verify credentials using a decentralised ledger. Evernym's technology has been implemented in global travel systems, like the IATA's OneID initiative, which enables travellers to move through airports using a single, verified digital identity, reducing the need for physical travel documents.

Kiva Protocol

Developed by the non-profit organisation Kiva, this decentralised identity system focuses on providing financial identities to the underbanked populations in developing countries. Kiva Protocol is being implemented in Sierra Leone, where it provides individuals with decentralised, verifiable identities to improve access to financial services. This allows citizens without formal credit histories to obtain loans and other banking services.

Where Decentralised Identity is Used

Decentralised identity is already being implemented in a variety of sectors, as both organisations and individuals recognise the value of decentralised, secure, and user-controlled identity systems.

Financial Services

Decentralised identity is gaining traction in the financial sector, particularly in areas such as Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance. Traditional KYC processes are often time-consuming and expensive, but with decentralised identity, users can present verified credentials that are reusable across institutions, reducing costs and improving customer experience.

Healthcare

Healthcare organisations are using decentralised identity to provide patients with control over their medical records. Patients can grant access to healthcare providers or insurance companies without the need for intermediaries, ensuring their data is secure, private, and easily accessible when needed.

Supply Chain Management

In supply chains, decentralised identity can be used to verify the authenticity of products, ensuring that goods have not been tampered with or counterfeited. Blockchain's immutable ledger provides transparency and traceability across the entire supply chain, and decentralised identities help authenticate parties involved.

Voting Systems

Several projects are exploring decentralised identity for secure voting systems, ensuring that only eligible voters can participate while maintaining privacy and preventing fraud. Digital credentials, stored securely on a blockchain, allow for transparent and auditable elections.

Travel and Border Control

The travel industry is beginning to experiment with digital identities for passengers. Airlines and border agencies are working on decentralised identity systems where passengers can present verifiable credentials for travel, reducing reliance on physical documents and improving security at borders.

The Future of Decentralised Identity

The future of decentralised identity is intertwined with the evolution of Web3 and other emerging technologies like blockchain, cryptography, and artificial intelligence. As we move toward a more decentralised digital landscape, decentralised identity systems will play a crucial role in empowering individuals and organisations to manage their data securely, with greater privacy, autonomy, and trust. Here's an exploration of the major trends and potential advancements in the future of decentralised identity.

Widespread Adoption and Interoperability

For decentralised identity to reach its full potential, **widespread adoption** across industries and platforms is essential. Currently, many organisations are experimenting with decentralised identity solutions, but in the future, it will become a standard for identity verification across multiple sectors, including finance, healthcare, education, government, and entertainment.

- **Interoperability** will be a key driver in making decentralised identity scalable. Identity solutions that work seamlessly across different blockchains and platforms will allow users to move freely between decentralised applications (dApps), financial services, and social networks using a single digital identity.

- **Standardisation** of protocols and systems will be vital to achieving this interoperability. Organisations such as the World Wide Web Consortium (W3C) are already working on standards for decentralised identifiers (DIDs) and verifiable credentials. As these standards mature, the DiFi ecosystem will become more cohesive and user-friendly.

Increased Privacy and Data Ownership

One of the primary motivations behind DiFi is the desire for **greater privacy** and user **data ownership**. Traditional identity systems rely on centralised authorities that control vast amounts of personal data, often leading to privacy breaches, identity theft, and misuse of information. Decentralised identity, on the other hand, empowers individuals to control and decide who has access to their personal data.

- **Zero-Knowledge Proofs (ZKPs)** and other advanced cryptographic techniques will further enhance privacy in decentralised identity systems. ZKPs allow users to prove the authenticity of their identity or credentials without revealing any additional information. For example, a user could prove they are over 18 without disclosing their date of birth. This level of privacy will become increasingly important in regulatory environments where personal data protection is a priority, such as the General Data Protection Regulation (GDPR) in Europe.
- **Selective Disclosure** will allow users to share only the necessary aspects of their identity, keeping sensitive information private. Instead of handing over entire sets of personal information, users will be able to provide verifiable credentials for specific purposes.

Decentralised Finance (DeFi) Integration

Decentralised finance (DeFi) is one of the most promising applications for decentralised identity. As the DeFi ecosystem continues to grow, decentralised identity will play an essential role in enabling **secure, permissionless financial transactions**. In the future, DiFi systems will serve as the backbone for DeFi platforms, providing users with verifiable credentials to access financial services.

- **Unbanked and Underbanked Populations** will particularly benefit from decentralised identity. In many parts of the world, individuals lack access to traditional financial institutions due to the absence of formal identity documentation. DiFi solutions will enable these individuals to create self-sovereign identities, allowing them to participate in the global economy, secure loans, and access financial services that were previously unavailable to them.

- **KYC and AML Compliance** will also become more efficient through DiFi. Currently, many DeFi platforms face challenges in complying with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. With decentralised identity, users can present verified credentials without needing to repeatedly undergo KYC processes for each platform, enhancing user experience and reducing costs for DeFi providers.

Tokenisation of Identity

In the future, the tokenisation of identity may become a reality, where digital identities can be **tokenised** and traded within the blockchain ecosystem. Tokenised identities will allow individuals and organisations to monetise their credentials and reputation while maintaining control over their data.

- **Reputation Systems**: In Web3, identity will not only be about verifying credentials but also about building and trading reputation. For example, a user's contribution to decentralised networks (such as open-source projects or DeFi communities) could be reflected in their digital reputation, which could then be tokenised and used for access to exclusive opportunities or benefits.
- **Identity as a Service**: As identities become tokenised, a marketplace for identity services could emerge, where users can sell access to specific verifiable credentials or rent out their reputation to participate in decentralised networks or governance systems. For instance, an individual with a strong reputation in online communities may offer verification services for projects, ensuring that new participants are credible.

Government and Institutional Adoption

Although decentralised identity is gaining traction in the private sector, the **adoption by governments** and public institutions will play a pivotal role in its mainstream success. Governments may begin to implement decentralised identity systems for issuing **digital passports**, **voter IDs**, **driver's licenses**, and other forms of identification.

- **Border Control and Travel**: The travel industry is exploring how decentralised identity can simplify border control and airport security. Digital passports stored in decentralised identity wallets could allow travellers to present verifiable credentials at border checkpoints, reducing reliance on physical documents and enhancing security.

- **Voting Systems**: Governments could implement decentralised voting systems using decentralised identities, ensuring that only eligible voters participate while maintaining privacy and transparency. This could lead to more secure and transparent elections, eliminating voter fraud and enhancing democratic processes.

Cross-Border Identity Systems

Currently, verifying identities across borders is a challenge due to differences in legal frameworks, trust mechanisms, and data privacy laws. The future of DiFi envisions a **global decentralised identity system** that transcends borders, allowing individuals to move freely between countries while using the same verifiable credentials for everything from banking to healthcare.

- **Global Identity Networks**: In the long run, decentralised identity systems will form a **global identity network** that allows for trusted, interoperable identities worldwide. Projects like the Sovrin Network and initiatives by international organisations are already laying the groundwork for such a system. Global DiFi systems will also make it easier for businesses to operate across borders, enabling secure international trade and collaboration.

Enhanced Security and Fraud Prevention

DiFi systems will greatly improve **security** and **fraud prevention** by leveraging blockchain's immutability and the distributed nature of identity storage. Centralised identity systems are vulnerable to hacking and data breaches, whereas decentralised systems distribute risk across the network.

- **Self-Sovereign Identities (SSI)**: The concept of SSIs, where individuals have full control over their identity without relying on a centralised entity, will become the standard. With SSIs, users can easily revoke access to their credentials, protecting themselves from identity theft and ensuring that their data remains under their control.
- **Biometric Integration**: DiFi systems will likely integrate with advanced **biometric systems** such as fingerprinting, retina scans, or facial recognition to further enhance security. These systems will add an additional layer of verification, ensuring that only the rightful owner of the identity can use it.

Artificial Intelligence and Machine Learning

As AI and machine learning advance, they will integrate into decentralised identity systems, enabling **more intelligent and adaptive identity solutions**. AI could assist in detecting fraudulent identities, analysing user behaviour to prevent identity theft, and automating the verification process for both individuals and organisations.

- **AI-Driven Identity Verification**: AI systems could streamline the process of verifying identity credentials across decentralised networks, providing a faster and more accurate method of confirming identities.
- **Machine Learning for Fraud Detection**: Machine learning algorithms could be employed to detect patterns of identity fraud in real-time, learning from previous attacks and continuously improving security in decentralised identity networks.

Challenges to Overcome

While the future of DiFi is promising, several challenges need to be addressed:

- **Scalability**: Current blockchain technologies face scalability issues that could hinder the wide adoption of decentralised identity systems. Improvements in blockchain throughput and efficiency will be necessary for large-scale implementation.
- **Regulatory Uncertainty**: Governments worldwide are still grappling with how to regulate decentralised technologies, and there is uncertainty around how DiFi will fit into existing legal frameworks. Developing robust legal structures that protect users' rights while encouraging innovation will be crucial.
- **User Experience**: For mainstream adoption, decentralised identity solutions need to offer a seamless and intuitive user experience. As the technology evolves, UX improvements will be critical to ensure that decentralised identity systems are accessible to everyone, not just tech-savvy individuals.

Key Trends Shaping the Future of Distributed Identity

Interoperability

For Web3 to thrive, interoperability between identity systems will be crucial. Different platforms and blockchains will need to support shared standards for identity credentials so users can seamlessly move between different services.

Privacy Enhancements

Privacy is one of the most significant advantages of distributed identity. With advances in zero-knowledge proofs and other cryptographic techniques, users will be able to prove their identity and credentials without revealing unnecessary personal information.

Regulation and Legal Frameworks

As decentralised identity grows, regulators are likely to take a closer look at the technology. Ensuring that distributed identities comply with local laws and regulations will be necessary to drive adoption, especially in sectors like finance and healthcare.

Tokenisation and DeFi

Distributed identity will be a cornerstone of decentralised finance (DeFi) applications. Users will need verifiable credentials to participate in tokenised ecosystems, where digital assets, NFTs (Non-Fungible Tokens), and other tokenised items require secure identification.

Conclusion

Distributed identity marks a significant departure from traditional centralised identity systems, providing individuals with control over their digital identities in a secure and decentralised manner. As the Web3 ecosystem continues to grow, distributed identity will become an essential component, enabling users to interact across decentralised platforms while maintaining privacy and security. The future of the internet will rely heavily on these technologies to provide “trustless”, user-centric systems that protect personal data while allowing for seamless interaction across the digital landscape.

DN: email=ian@ianloe.net
Date: 2024.09.30 08:05:21 +08'00'