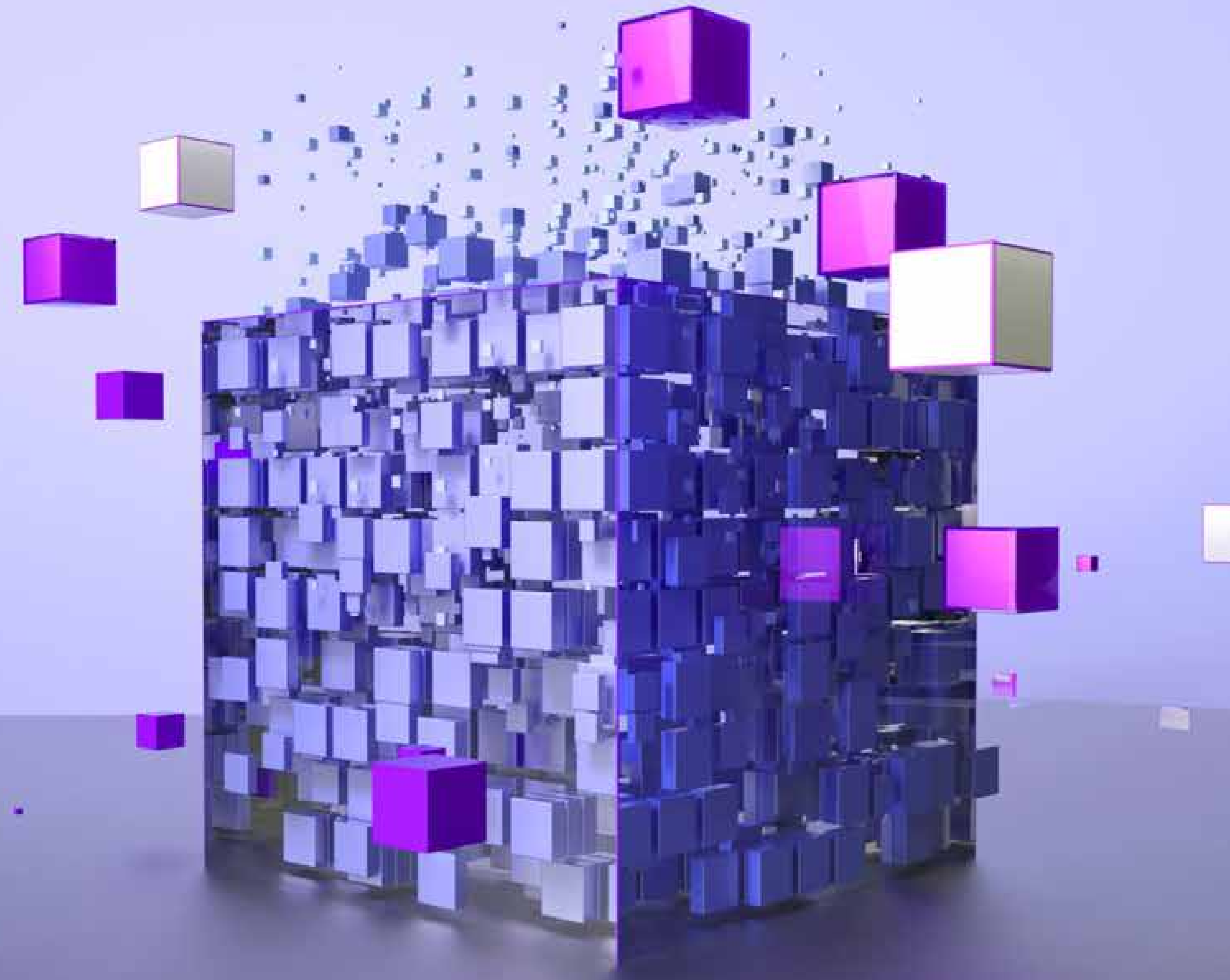
zensar

Toward a Safer New Digital Identity With Blockchain and SSI

Whitepaper



An RPG Company

Executive summary

In today's digital world, our personal information, from identification documents such as address proof/ birth certificate to sensitive data such as social security numbers and educational credentials, is being increasingly stored on the internet. While this offers quick access and convenience, it also exposes us to growing risks. Centralized authority-based identity management systems, popular at present, leave the user vulnerable to invasion of privacy, security breaches, and loss of control over personal data.

Blockchain technology in relation to Self-Sovereign Identity (SSI) and Verifiable Credentials (VCs) promises something new, which speaks of the future of privacy, security, and having control over one's personal data.[1]

This white paper addresses the vulnerabilities of legacy identity management systems, presents benefits offered by SSI, and discusses how blockchain-based solutions might usher in a secure and trusted digital world by becoming the catalyst for a decentralized, user-centric approach to digital identity.

Introduction

The digital world has become a central hub for our personal and professional data. Consequently, protecting this information while maintaining ease of access is essential. The growing control over digital identities, particularly through single sign-on services (SSO), presents significant challenges to privacy, security, and personal autonomy. Convenient as these services are, they are filled with an array of dangers, including unauthorized use of data, identity theft, and control over personal information. With little control over how this information will be collected and stored, or even further used, users are losing faith in digital identity systems.

A blockchain-based SSI system promises to overcome such challenges. Unlike the traditional identity frameworks based on centralized authorities, SSI allows a totally decentralized digital identity with people in control of the ownership of their data. In this decentralized approach, a central authority to manage and verify credentials is not required and hence leads to greater privacy, security, and transparency.

The inherent properties of blockchain are immutability, decentralization, and cryptography, which make it an excellent technical means for creating a trusted digital identity. Blockchain-based SSI directly enables users to control and share their credentials without any intermediaries, solving the problems around identity theft, breach of privacy, and centralization risk. This technology empowers individuals to take ownership of their data and safely conduct digital transactions, paving the way for much-needed trust in digital systems.[2]

Risks in existing identity management systems

The current single sign-on gives providers immense power over personal data. A big concern is the loss of privacy, where identity providers can collect, store, and potentially share or leak sensitive user data without explicit consent. This not only erodes the individual's control over personal information but also exposes them to significant risks.

Another major concern is the increased risk of identity theft. Cybercriminals often target centralized systems that manage user identities, aiming to steal login credentials. This allows them to impersonate real users and engage in fraudulent activities. The problem is exacerbated by the increasing number of online accounts, forcing users to manage multiple usernames and passwords. This often leads to the use of weak passwords or reusing the same password across different platforms, further compromising security.

Centralization, in itself, is a major risk factor. When identity management is controlled by a single provider, users are at the mercy of these entities that can withdraw access or modify credentials without user input. Furthermore, the centralized nature of these systems makes them an attractive target for hackers. Large databases of sensitive information become high-value assets, increasing the risk of breaches where personal data can fall into the wrong hands.

All these challenges stem from a system that operates without transparency and leaves users with little control. In essence, the current approach to digital identity management is fundamentally flawed, as it lacks both the decentralization and transparency needed to empower users and protect their data. This erosion of trust calls for a reimagining of digital identity systems — one that prioritizes user control, privacy, and security. [3]

The blockchain solution

Trust is a fundamental element of any online transaction, and its absence can severely compromise the integrity and success of digital exchanges. Take the example of buying a house online: while there may be some verification of the seller's identity, the more crucial aspect is confirming the authenticity of the property. Unfortunately, in today's digital systems, this level of trust is often lacking. Existing digital identity infrastructures are centralized, meaning they rely on third-party intermediaries to verify credentials. This centralized nature leaves gaps in transparency, making it difficult to fully trust the system, especially in high-stakes transactions where absolute certainty is needed.

Traditionally, physical identification documents such as passports or driver's licenses have been used to verify identity. These are issued by trusted authorities and are difficult to forge, providing a high level of security in the physical world. However, replicating this level of trust in the digital realm introduces significant challenges. Digital systems often struggle to provide the same level of authenticity and protection, leading to critical issues such as privacy concerns and the risk of identity theft.

Blockchain and SSI solve this problem by delegating control through self-sovereign control of the digital identity by individuals themselves.

VCs represent permissions issued to users to own and control their digital credentials but only to share these with trusted parties. Data is protected with some form of cryptographic methods.

The system comprises the following entities:

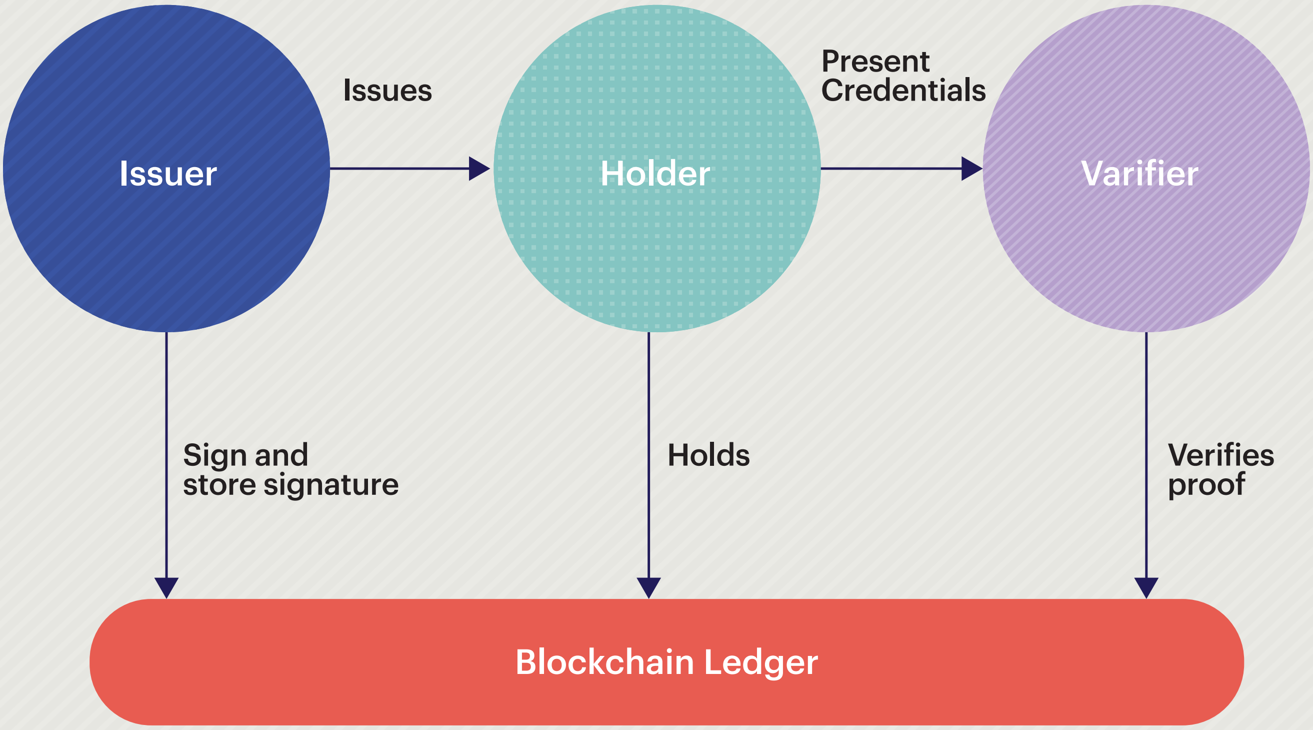
Issuer: Issues a credential to a user (the holder), and uses cryptography to store that information in a verifiable data registry such as Hyperledger Indy.

Holder: Controls the credential and decides when and where to share it.

Identifier: Information relevant to some sort of claim — age, nationality, etc.

Verifier: Organizations or entities responsible for requesting and validating the credentials provided by individuals.

This is how it works: the holder provides only the required information; the verifier verifies the credential without the issuer's need to be contacted by the verifier. This is illustrated in the diagram below.[4]



Working of SSI

Advantages of SSI

Control and privacy: Users own their credentials and, therefore, share only minimal claims to enhance privacy. Users have control over their data, determining when and how to share it.

Efficiency: Verifiers can verify claims independent of an issuer, which saves them time and money.

Security: VCs, using cryptographic signatures, ensure that the data is tamper-proof, and therefore, one may obtain correct information from a trusted party.

No central authority: There is no need for a central authority to rule, or to remove credentials. Even if such a system were compromised, control would stay with the owner.

Removes user IDs and passwords: SSI expands the usage of verifiable credentials, empowering users to have control. Instead of relying on third-party identity providers to manage their credentials, blockchain-based SSI allows users to securely store and manage their credentials in a private, tamper-proof wallet. This gives users complete control over who can access their information.

Verification: VCs ensure secure online verification without requiring any physical document. Cryptographic signatures make VCs tamper-proof, ensuring data is accurate and issued by authorized trustworthy parties.

SSI expands the concept of verifiable credentials and takes identity back to end-user control. SSI grants users control over and management of all their credentials in a secure, private, tamper-proof wallet so they have control over who can share the credentials rather than just letting another ad hoc, third-party identity provider carry them on their behalf.[5,6,7]

Real-life applications of decentralized identity systems

Blockchain-based identity solutions are gaining popularity in various industries and government bodies due to their potential to enhance security, transparency, and efficiency in transactions. For instance, the creation of blockchain-powered verifiable credentials based on an EU-wide digital identity framework. This framework enables citizens to securely access online services across the Union. [8,9]

Financial services: SSI verifies the identity of customers during the onboarding phase, thus combating fraud while improving customer experience.

Healthcare: SSI and VCs can be used to validate medical credentials, track patient consent, and securely share health records of patients.

Benefits for people: Digital interactions become more effortless, leading to better user experience while minimizing the friction of traditional onboarding, such as by eliminating usernames, passwords, forms, or traditional identification processes. Also, online fraud and identity theft can be prevented, improving security.

Benefits for organizations: For governments and businesses, SSI offers opportunities to grow revenue by improving user experience for their customers (e.g., to reduce drop-off rates during user onboarding), strengthen their brand, or introduce new products and services. Also, SSI minimizes risk vectors related to compliance, fraud, security, and privacy. It also enables organizations to streamline and automate processes to cut costs.

Identity is a fundamental aspect of various industries, creating opportunities for countless applications. From verifying official documents for onboarding and Know Your Customer (KYC) to validating credentials for offering services or applying for jobs, identity plays a crucial role. Additionally, personal information can be used to create unique personalized experiences, enhancing user satisfaction.

Challenges and future solutions

High transaction costs
Implementing and maintaining digital identity systems incur significant costs for infrastructure, verification, and compliance, limiting access for smaller organizations and emerging markets. Layer 2 (a separate blockchain that handles transactions off the main blockchain) scaling technologies can be leveraged to optimize infrastructure and significantly lower operational costs.

Interoperability
The lack of standard protocols among identity providers creates integration issues, leading to fragmented systems and a complex user experience across platforms. As technology evolves, the development of standardized protocols will become more feasible and essential.

Trusted data exchange
Secure and reliable mechanisms for exchanging identity data are critical. However, the absence of universal standards increases the risk of breaches and undermines trust in the system. Implementing decentralized and encrypted data sharing can enhance security and trust.[10]

Conclusion

In today's digital landscape, the evolution of identity systems demands a shift toward safety, privacy, and user-centric control. Blockchain, VCs, and SSI are emerging trends shaping a future where individuals have ultimate control over their digital identities. These technologies verify the credentials of the digital world by eliminating central authorities, working toward building trust in the digital world.
By decentralizing identity management, we empower individuals, enhance privacy, and create a safer, more trusted digital ecosystem. The more we empower individuals to be their own identity, the more we build a world where trust can be decentralized, security is ensured, and abundance is well-established.

References

1. **Walt.id (2023)**. Decentralized Identity Playbook.

2. **Manning (2023)**. Self-Sovereign Identity - Livebook.

3. **Cheqd (2023)**. Know Your Customers and Finance in Self-Sovereign Identity.

4. **Hypersign.id (2023)**. Prajna Testnet - On-chain KYC.

5. **LinuxFoundation (2023)**. Linux Foundation Course - Self-Sovereign Identity.

6. **LinuxFoundation (2023)**. Linux Foundation Course - Verifiable Credentials.

7. **LinuxFoundationX (2023)**. Self-Sovereign Identity - Course Block.

8. **European Commission (2023)**. European Digital Identity.

9. **SAP (2023)**. How SSI Improves Online Trust.

10. **TruID (2023)**. Decentralized Identity: One Step Closer to Self-Sovereign Digital Identity.

11. **Nagware, K. (2023)**. Digital identity and decentralized identifiers: W3C and their impact.

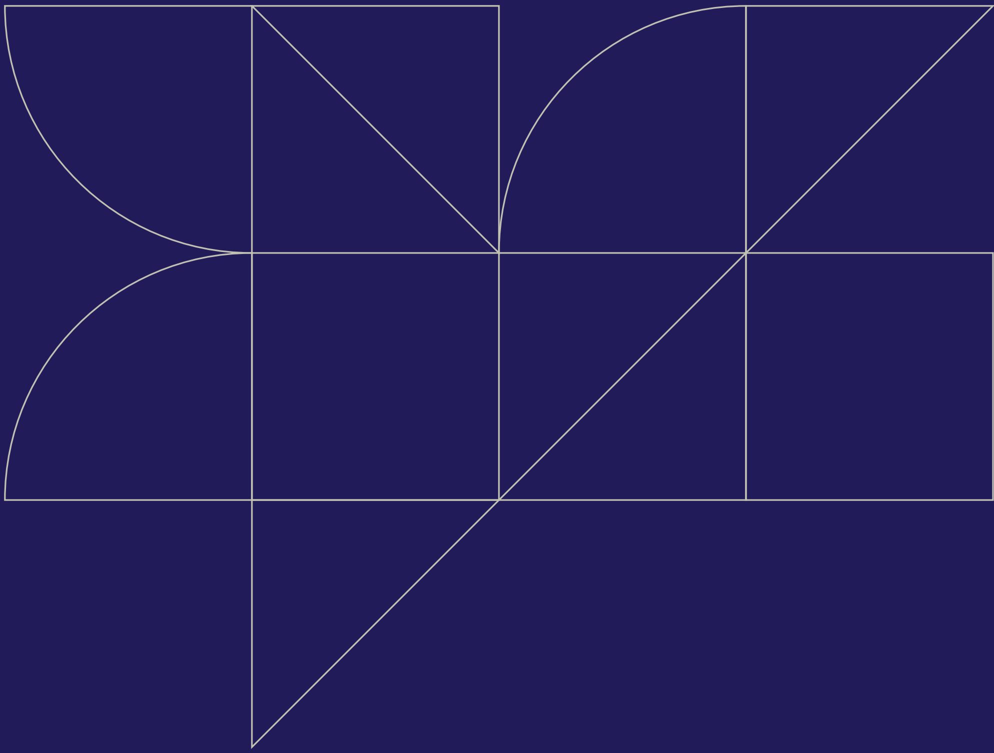
12. **Scouten, E. (2024)**. IIW38 - Internet Identity Workshop 2024.

13. **Ibero-American World (2020)**. The Decentralized Digital Identity Ecosystem.

14. **SSIMeetup (2023)**. SSI Blog - Page 7.

15. **Hypersign.id (2023)**. Prajna Testnet - On-chain KYC.

Author: **Mayank Agrawal**, Technical Consultant,
Data Engineering and Analytics (Blockchain, AI/ML)
Contact: ZenLabsAIML@zensar.com



zensar
An RPG Company

At Zensar, we're 'experience-led everything.' We are committed to conceptualizing, designing, engineering, marketing, and managing digital solutions and experiences for over 145 leading enterprises. Using our 3Es of experience, engineering, and engagement, we harness the power of technology, creativity, and insight to deliver impact.

Part of the $4.8 billion RPG Group, we are headquartered in Pune, India. Our 10,000+ employees work across 30+ locations worldwide, including Milpitas, Seattle, Princeton, Cape Town, London, Zurich, Singapore, and Mexico City.

For more information, please contact: info@zensar.com | www.zensar.com