

CENTRAL BANK OF EGYPT
Egyptian Banking Institute



62.432

البنك المركزي المصري
المعهد المصرفي المصري

35.715

85.204

35.254

NOVEMBER 2024

Self-Sovereign Identity (SSI)

Current Trend

12.751

www.ebi.gov.eg

NOVEMBER 2024

Current Trends

| Background

The world is becoming increasingly digitalized, and the development and convergence of advanced, ever-evolving technologies are redefining the foundations of our society. Among these disruptive innovations, Self-Sovereign Identity (SSI) stands out as transformative forces that, when integrated, offer unprecedented potential to revolutionize how we manage our identities and operate in the digital environment.

| Concept and Definition

Self-Sovereign Identity (SSI) describes an **approach in which the individual should be able to control and manage his or her digital identity, without the intervention of a third-party administrative authority.** This user-centric approach - where the individual has full power and control over the management of his or her data - is currently lacking in most user experiences on the Internet, where such data is stored, managed, and used by online service providers, sometimes without the Internet user being fully aware of the scope of use of his or her data. Self-Sovereign Identity puts the individual back at the heart of the digital experience.

Before diving into the details of Self-Sovereign Identity, it's important to know what digital identity is first. A digital identity is any data that exists online that can be traced back to an individual or organization. Identifiable data includes passwords, user names, bank accounts, and social media photos.

Self-Sovereign Identity comprises 3 pillars: blockchain, decentralized identifiers, and Verifiable Credentials.

Self-Sovereign Identity (SSI) relies on a collaborative ecosystem to establish trust and validate digital credentials. This system mirrors traditional credential issuance, such as a university issuing a degree that a student presents to a potential employer. However, SSI offers enhanced privacy and security. In SSI, this three-way interaction is known as the Trust Triangle, consisting of the issuer, holder, and verifier.

1. The Issuer

The issuer, often an organization or accredited individual, is responsible for creating and issuing verifiable credentials. Examples include universities, healthcare providers, governments, and banks. Their role is to validate and securely issue credentials to individuals.

2. The Holder

The holder is the individual who possesses and manages their verifiable credentials. They have complete control over their data, deciding when and how to share it. Holders can selectively disclose specific credential information to different verifiers, ensuring privacy control.

| Importance

3. The Verifier

Verifiers are entities or organizations that request and validate the credentials presented by the holder. They rely on this information to make informed decisions, like granting access to services or benefits. Verifiers can easily confirm the authenticity and validity of credentials by directly interacting with the issuer, eliminating manual checks and intermediaries.

SSI is built upon decentralized and distributed ledger technologies, such as blockchain, enabling the creation of verifiable, tamper-proof digital identities. In an SSI framework, individuals maintain ownership of their identity attributes, which are cryptographically secured and can be selectively shared with authorized entities. This paradigm shift not only enhances user privacy but also reduces the risk of large-scale data breaches, as there is no central repository vulnerable to cyber threats.

Self-Sovereign Identity (SSI) is an identity management model that enables organizations to create fraud-proof Verifiable Credentials and instantly verify the authenticity of those credentials. It gives individuals full ownership and control of their digital identities without relying on a central authority.

There are many advantages to Self-Sovereign, including:

- Fully owning and controlling your data
- Increased security and privacy
- Eliminating central points of failure
- Data can't be tracked and correlated (data that is used to trace back to someone's identity or track online behavior)

As per Cognitive Market Research's latest published report, the Global Self Sovereign Identity market size was \$1,147.87 Million in 2024 and it is forecasted to reach \$30,495.36 Million by 2030. Self-Sovereign Identity Industry's Compound Annual Growth Rate will be 72.19% from 2024 to 2031.

Access to open banking via digital identity using Self-Sovereign Identity (SSI) benefits the ecosystem through better onboarding, security, transparency, and choice. To date, much of the airtime in financial services, about SSI and decentralization, has been about cryptocurrencies, using algorithms such as Bitcoin, transaction auditing, or smart contracts. However, this ignores another important thread which is digital identity, and how this can help organizations and consumers secure their interactions and transactions.

| Benefits

Self-sovereign identity offers numerous benefits, enhancing privacy, security, and efficiency for individuals, organizations, and developers. Individuals gain control over their data, organizations streamline credential issuance and verification, and developers create seamless, secure user experiences.

Individuals:

- **Enhanced Privacy:** Users own their data and decide who can access it, reducing reliance on centralized servers.
- **Control & Autonomy:** Users manage their digital identities, selectively sharing information.
- **Convenient Digital Wallets:** Securely store and manage credentials on personal devices, eliminating the need for multiple passwords.
- **Revocation of Access:** Users can revoke data access at any time, effectively managing their online presence.

Organizations:

- **Streamlined Credential Issuance:** Organizations can issue credentials quickly and cost-effectively.
- **Improved Verification Efficiency:** Instant and accurate identity verification eliminates the need for manual checks.
- **Enhanced Security:** Advanced cryptography ensures credential authenticity, reducing fraud.
- **Continued Verification:** Credentials remain valid even if the issuer goes offline.

Developers:

- **Seamless User Experience:** Create password-less, user-friendly experiences through SSI-powered wallets.
- **Strong Authentication:** Provide a secure alternative to complex authentication methods.
- **Selective Disclosure:** Allow users to share only essential information, protecting sensitive data.
- **Direct Data Exchange:** Enable peer-to-peer data exchange, enhancing privacy and security by removing intermediaries.

Faster onboarding

In-branch, the process of opening a new bank account can take anywhere up to an hour or more, and that is assuming that all paperwork is in order. If any detail is questionable, incomplete, or altogether missing, the likelihood is that the process will extend by hours or days until whatever certificate or proof becomes available to the customer.

Digital credentials can turn this cumbersome process into a straightforward one. Because SSI centers around the individual's control over their own personal information (which is immutable and immediately verifiable on the blockchain), opening a new bank account would take minutes.

| Challenges

Built-in SSI in regulatory compliance

Finance is one of the most tightly regulated industries out there. A wide array of rules and regulations define how banking institutions are supposed to act. Customer charters, KYC, AML, and so on provide the regulatory basis that controls how financial institutions operate.

However, all these guidelines are not fully integrated yet. Some gaps and cracks might lead to fraudulent activity. By building on SSI principles, and by digitizing the identity process, these gaps disappear.

Mortgage applications

- Applying for a mortgage is a slow, time-consuming, and paperwork-heavy process. Yet, it is too easy to apply and obtain different mortgages under different identities. Cases of applicants using fake identities to apply for home loans are not uncommon. Again, the use of digital credentials, which are verifiably unique on the blockchain, would remove this risk.
- **Global Acceptance:** Individuals, governments & entities need to embrace the Self-Sovereign Identity models collectively for its successful implementation. This may take years to switch over SSI from federated and centralized ID systems.
- **Misuse of Identity:** Another challenge in SSI is the misuse of identities as the user fully controls personal information sharing. The user can misuse this control to engage in different illicit and fraudulent activities.
- **Technological Limitations:** Certain groups may be left behind due to limited access to resources and technologies used to implement SSI. This may create disparities or worsen them for existing outdated systems. This requires full system upgradation and may cost more than the organization's budget.
- **Interoperability:** Due to a trust-minimized decentralized blockchain interoperability is a critical challenge in Self-Sovereign Identity (SSI) systems. SSI allows individuals to have control over their digital identities, but it also means that there are multiple, often independent identity providers. Achieving interoperability among these various SSI systems is essential to ensure that digital identities can be universally recognized and accepted. Without interoperability standards and protocols, individuals might face difficulties using their SSI credentials across different services, organizations, or platforms.

Practices in the banking sector

- **Lack of Regulatory Framework:** Federated Identity Management Systems and other traditional IDV systems are regulated by established regulatory bodies. Unlike these IDVs SSIs are still awaiting regulations which can cause legal recourse in case of fraud or non-compliance. Also, non-regulated SSI can easily be compromised and legal actions against them are difficult.
- **Privacy & Consent:** Self-sovereign identity raises an underlying concern about data privacy & consent as the data is shared among different parties over the decentralized network. To establish trust and Verification, information-sharing can cause unintentional sharing of sensitive information over the internet.
- **Discrimination & Exclusion:** Not everyone has equal access to the data stored. SSI is intended to empower users with their personally identifiable information and privacy. However, limited to no access to technologies necessary for SSI can be a limitation—also, SSI stores data provided by individuals which may create an issue of bias and discrimination. This may result in discriminatory onboarding, hiring, and lending decisions that can occur based on SSI credentials.
- Japan's three leading financial institutions – MUFG, SMBC, and Mizuho – are embarking on a joint digital identity initiative towards enhancing online banking authentication. The cohort of banks will implement an initiative building upon past proof-of-concept trials of digital ID that enable secure transactions for their customers.
- Other jurisdictions such as the UAE and Pakistan have launched shared KYC, which isn't the same, but has a similar objective.
- Korea has been one of the jurisdictions to actively explore digital identity. In 2021 it went live with a digital identity initiative for banks in conjunction with the regulator.
- Canada Bank : A network of major Canadian banks and other service providers are federating identity across a permissioned Hyperledger Fabric blockchain. The network streamlines logins, data sharing, and account setup so users can conduct traditionally face-to-face business online.
- Streamline the recruitment process: Organizations that want to recruit high-quality candidates efficiently can verify educational and professional credentials like a university degree and professional certificates instantly with SSI. This will save days to weeks compared to traditional manual verification processes.

What would it be like to pay on Amazon... without using your credit card information?

If a customer were to pay for a good on a merchant site, taking an SSI approach, this is what the new customer journey would look like after purchasing a product on Amazon:

- The customer submits a proof of payment request to their bank to validate the purchase. The bank then issues a Verifiable which contains all the information for the payment (Amazon wants to verify the customer's identity and creditworthiness). Thanks to selective disclosure and the Zero Knowledge proof, Amazon does not need any other information
- The customer receives the proof of payment in his digital wallet. The wallet thus becomes a means of payment like any other.
- The customer demonstrates his or her ability to pay by presenting proof of payment to Amazon. - Amazon will ensure that the proof is genuine and certified by the customer's bank by querying the customer's wallet, which is connected to the distributed ledger.

Current Trends

HOTLINE
15200
One number to better serve you!

Headquarters – Nasr City
22 A, Dr. Anwar El Mofty St., Tiba 2000
P.O.Box: 8164 Nasr City, Cairo, Egypt

www.ebi.gov.eg



Like us on
facebook.com/EgyptianBankingInstitute



Follow us on
twitter.com/EBItweets



Join us on
linkedin.com/company/egyptian-banking-institute



Watch us on
YouTube Channel: Egyptian Banking Institute (EBI)