

The past, present, and future of Digital Identity



How to prepare for
Self-Sovereign Identity
in 2024

In today's digital age, as more and more people do business and interact online, having a trusted digital identity is crucial

We need a secure, verifiable, and efficient way to verify who we are online, especially for commerce, communication, and collaboration. While older digital identity methods worked for a while, we now face new challenges that require us to think differently. Enter the concept of Self-Sovereign Identity (SSI). This paper dives into what SSI is, its history, the current market space, and its potential future, all within the larger context of identity technology.

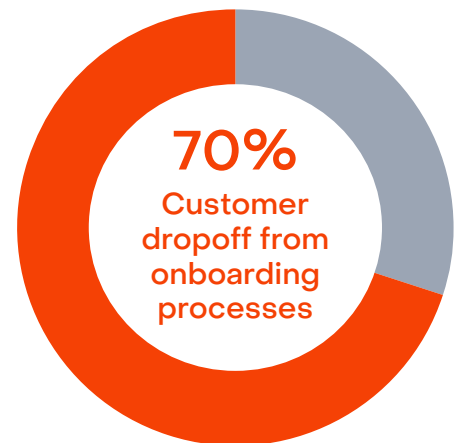
At its core, this topic of identity is about the information and data that tell the online world who or what we are, whether that's a person, company, or device. As we move more of our lives, from banking to social interactions, online, the stakes get higher in making sure these identities are managed well. Mismanagement, breaches, or inefficiencies in these systems can lead to significant financial losses, fraud, and the costly erosion of trust.

In the past, centralised companies or groups were responsible for storing, verifying, and managing user data. While this helped build trust online, it also introduced vulnerabilities. These central points of data became lucrative targets for hackers, leading to some of the most significant data breaches in history. In addition, the control of our personal data was often in the hands of these corporations or institutions, leaving users with little agency or control over them.

The Identity Ecosystem Transition has begun

Enter Self-Sovereign Identity, a paradigm shift in the world of digital identity. SSI transfers the power of ownership, control, and shareability of personal data back to the individual. In this model, users possess sole authority over their identity data, determining when, how, and with whom they share their credentials. Such an approach not only bolsters security but also makes it simpler for companies to onboard new customers, offer them new services, and reduce their compliance pressure.

The way we do digital identity needs change



\$250m
Losses from
identity theft

\$300m
Losses from
data breaches

Compliance Fines
\$3bn

The past, present, and future of Digital Identity

The white paper aims to dissect the complex relationship between SSI and modern digital identity systems by covering the following:

A Historical Perspective of SSI

Page 05 >

Trace the development and evolution of digital identity mechanisms.

Aim to understand the origins of current challenges and why solutions like SSI emerged.

The Current SSI Landscape

Page 09 >

Explores how businesses, governments, and tech innovators manage identity complexities.

Highlights real-world SSI implementations and compares them with traditional systems to highlight benefits and challenges.

Financial Perspective

Page 16 >

Focuses on the financial impact of SSI and digital identity systems across industries.

Discusses cost savings from fewer data breaches and revenue potential from improved identity verification processes.

Future Outlook

Page 21 >

Projects the future path of SSI and digital identity based on technological advancements and societal changes.

Combines expert opinions, tech forecasts, and industry trends to predict the future of digital identity management.

The Past

Self-Sovereign Identity and Digital Identity

Historically, the concept of identity in the digital realm was rudimentary. Early digital identity systems, which began to emerge during the internet's nascent days, were centralised and siloed. These systems, often owned and operated by corporations or institutions, acted as the sole gatekeepers of user data. Users, in turn, were required to create distinct digital identities for each online service, leading to a fragmented identity landscape replete with repetitive registration processes and numerous passwords. For example, the dozens of accounts people have across various social networks, streaming services, and email providers are all independently managed with varying amounts of security.

The centralised nature of these systems presented an inherent challenge: single points of failure. With vast repositories of personal data housed in centralised databases, they became enticing targets for cyberattacks. The late 2010s witnessed a surge in high-profile data breaches, jeopardising the personal data of millions. ➔ These incidents underscored the vulnerabilities of centralised identity systems, catalysing the demand for more secure and user-centric solutions.

➔ **CSO article**
The biggest data breach fines, penalties, and settlements so far

The centralised nature of these systems presented an inherent challenge:
single points of failure

The Present

Self-Sovereign Identity and Digital Identity

Enter Self-Sovereign Identity (SSI). Born out of the need for enhanced privacy, security, and user control, SSI represents a paradigm shift in digital identity management. Instead of relying on third-party entities to validate one's identity, SSI provides individuals the autonomy to own, control, and share their personal data. This process also creates a reusable, durable, form of identity that makes access to new services instant, as all the data you need is pre-verified and ready to use.

In the SSI model, cryptographic techniques are employed to create verifiable credentials. These credentials, unlike traditional digital IDs, are not stored in centralised databases. Instead, they reside with the individual, often in digital wallets, and can be shared directly with those who need to verify them. Verification is achieved through federated or decentralised networks, obviating the need for a singular verifying authority. These credentials contain fraud-proof data that includes everything from your name, address, or date of birth through to fully a digitised passport or driving license.

SSI provides individuals the autonomy to own, control, and share their personal data

Several factors have coalesced to facilitate the rise of SSI

Federated Cloud Services & the Blockchain

These alternative hosting systems provide the backbone for many SSI solutions, ensuring transparency and tamper-proof verification.

Growing Privacy Concerns

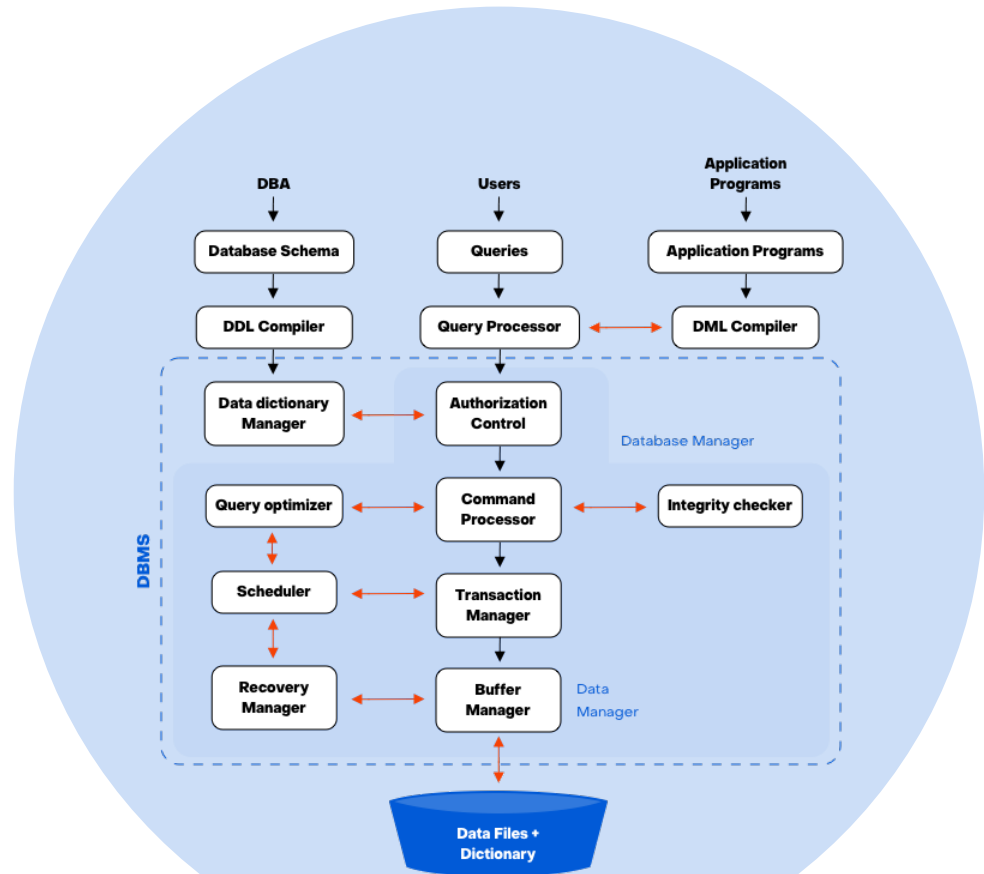
With regulations like the General Data Protection Regulation (GDPR) emphasising user data rights, there's a heightened global focus on privacy, driving demand for user-centric identity solutions, while also heightening the demands on developers to meet them. ➔

➔ **ISACA article**
The Two Key Challenges of GDPR Adoption

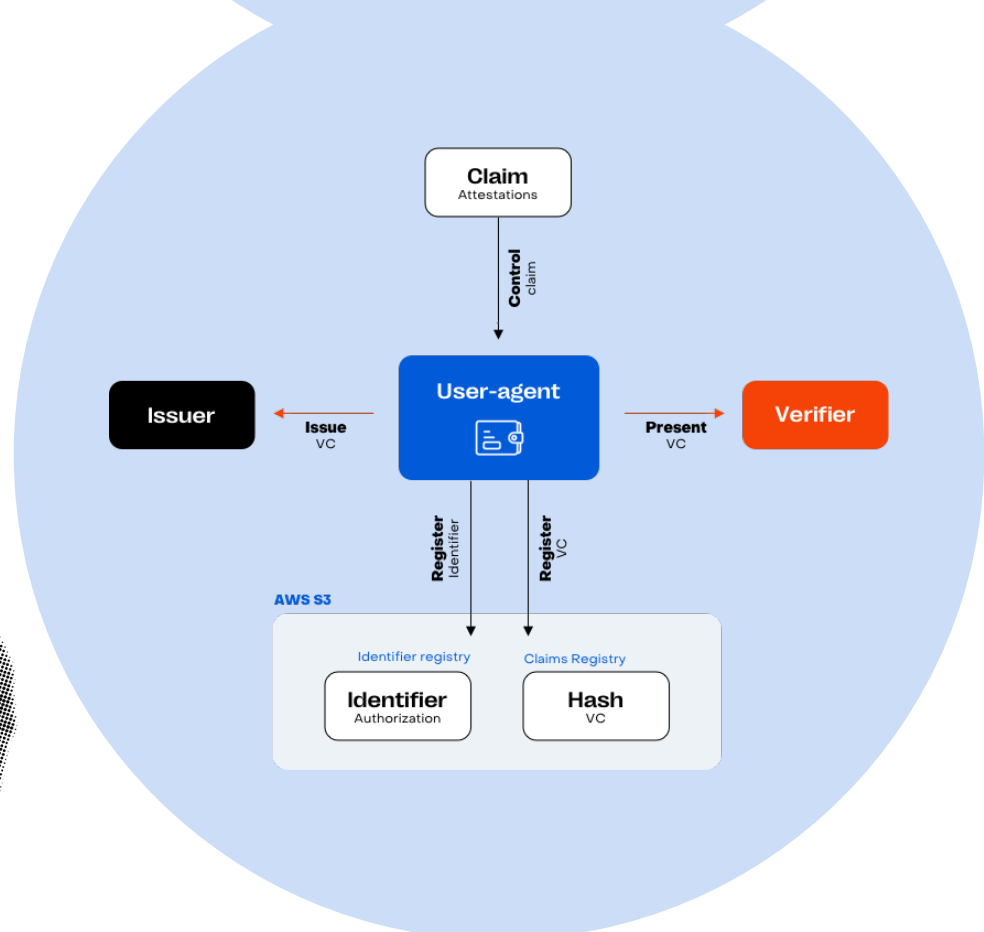
Digital Transformation

As industries undergo rapid digitalisation, there's an amplified need for secure and efficient identity verification mechanisms.

Traditional Database Architecture



versus SSI Platform Architecture



The Future

Self-Sovereign Identity and Digital Identity

The trajectory of SSI and digital identity technology appears promising, but it's not without challenges.

Universal Adoption

For SSI to become a ubiquitous solution, widespread adoption is essential. This involves not just individual users but also businesses, institutions, and governments recognising and accepting self-sovereign identities. Interoperability, or the ability of different SSI solutions to communicate seamlessly, will be a critical factor in facilitating this broad acceptance.

Regulatory Framework

Given the technologically advanced nature of SSI, crafting a comprehensive regulatory framework is intricate. Jurisdictions globally will need to navigate the balance between enabling SSI's potential and ensuring it isn't misused.

Technological Advancements

While DLT and blockchain are currently predominant in many discussions, the future might witness the emergence of newer technologies that further enhance the efficiency, security, and scalability of SSI systems. Soon, the technology will be as intuitive to use as, and be able to integrate within, traditional systems.

New Use Cases

Beyond traditional identity verification, the future will unveil novel applications of SSI. Consider, for instance, the potential of SSI in ensuring the traceability of goods in a supply chain or verifying the credentials of IoT devices in a smart city.

Public Perception and Trust

Building trust in SSI, especially among those accustomed to traditional identity systems, will be paramount. Educational initiatives and demonstrable benefits will play a role in fostering this trust.



The trajectory appears promising, but it's not without challenges

truivity

The next step in adaptation

eIDAS 2.0 Era

The imminent eIDAS 2.0 legislation ➔ represents a pivotal development in the digital identity industry and business operations within the European Union. This initiative aims to provide every EU citizen and business with a digital identity that can be used universally across the member states. Such a framework ensures that digital identities and electronic signatures are interoperable and legally recognized throughout the EU. This standardization is not just a technological advancement; it's a facilitator of seamless cross-border business transactions, reducing administrative burdens and fostering efficiency.

This initiative aims to provide every EU citizen and business with a digital identity that can be used universally

For businesses operating within the EU, eIDAS 2.0 brings forth an environment conducive to digital transformation. The legislation simplifies digital interactions and transactions, making it easier for companies to offer and manage services across national borders. It paves the way for enhanced customer experiences, as users can access services with their digital IDs, irrespective of their home country. This uniformity in digital identity verification can significantly reduce the complexity and cost of compliance for businesses, as they no longer need to navigate a labyrinth of varying national regulations.

By ensuring high standards for digital identity verification and secure electronic signatures, the legislation enhances the security and reliability of online interactions. This increased trust is crucial for driving the adoption of digital services, stimulating digital commerce and innovation in the process.

The legislation also recognizes and accommodates the rapid evolution in digital technology. It lays a foundation for integrating emerging technologies like blockchain and AI in digital trust services, keeping the EU at the forefront of technological innovation in digital identity management.



➔ **European Council article**
Council and Parliament reach
a provisional agreement on eID

Empowering the Individual Empowers the Industry

The narrative of digital identity, from its humble beginnings to the transformative potential of SSI, is a testament to technology's evolving role in empowering individuals. As we stand on the cusp of what will be a new era in digital identity management, it's imperative to approach the future with a blend of optimism, caution, and informed analysis. The past offers lessons, the present provides insights, and the future, though uncertain, holds the promise of a more secure, user-centric digital realm.

**It's imperative to approach
the future with a blend
of optimism, caution, and
informed analysis**

The Use Cases and Potential of Self-Sovereign Identity

In the landscape of digital transformation, few areas have witnessed the kind of revolutionary potential that the realm of Self-Sovereign Identity (SSI) and Digital Identity technologies have presented. As businesses and governments scramble to find efficient, secure, and user-centric identity verification mechanisms, SSI emerges as a beacon of hope. This paper delineates some of the most compelling use cases and the untapped potential of these technologies.

Database Infrastructure Replacement

Financial Industry

The financial sector, with its myriad of transactions, customer interactions, and regulatory obligations, stands to benefit immensely from SSI. Traditional centralised databases, prone to breaches and inefficiencies, can be replaced with fraud-proof identity verification systems. Such a shift can result in immediate cost savings, a reduction in identity fraud, and a streamlined customer onboarding process.

Healthcare Industry

Medical records, patient histories, and health credentials are sensitive pieces of information. Transitioning from centralised electronic health record (EHR) systems to an SSI model allows patients to have control over their medical data. They can securely and selectively share their health records, ensuring timely care while preserving data privacy.

HR Industry

Recruitment, background verification, and employee onboarding are processes that demand reliable identity checks. An SSI system can expedite these processes, enabling HR professionals to instantly verify credentials provided by potential employees, thus reducing the lead time and potential inaccuracies associated with traditional background checks.

A stylized illustration of a digital identity ecosystem. It features a central smartphone with a keyhole icon, surrounded by various icons representing different sectors: a bank, a hospital, a town hall, a security building, and a graduation cap. People are shown interacting with the system, with one person sitting at a desk and another standing. The entire scene is set against a light blue background with a large orange circle in the upper left.

Such a shift can result in immediate cost savings, a reduction in identity fraud, and a streamlined customer onboarding process

Instant Trust, Verifiability, and Regulatory Compliance

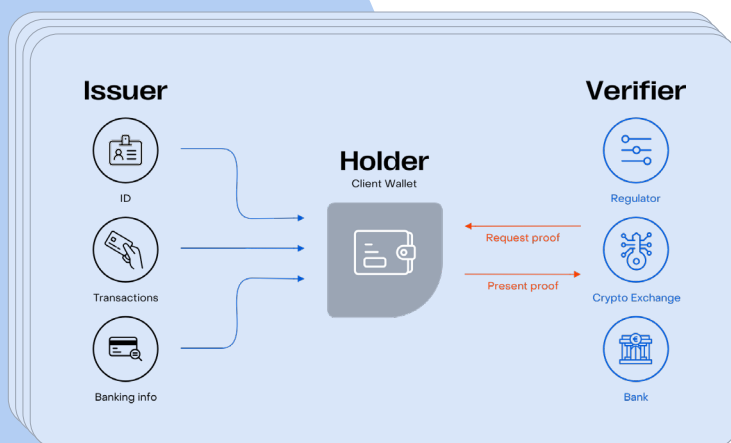
One of the perennial challenges faced by industries is ensuring regulatory compliance and simplifying the audit process. SSI can be a game-changer here.

Instant Trust and Verifiability

With cryptographic verification, SSI ensures that credentials shared are tamper-proof and genuine. This instils immediate trust between parties, be it between a business and a customer or between two enterprises.

Regulatory Compliance and Auditing

For sectors under stringent regulatory oversight, SSI can simplify compliance. By providing a transparent and immutable record of identity verifications and transactions, SSI can make audits stress-free and more efficient. This is not just a potential time and cost saver but also a means to enhance institutional credibility.



Not just a potential time and cost saver but also a means to enhance institutional credibility

Management of Government-Issued Identification

Governments worldwide grapple with the dual challenges of ensuring citizen data security and providing efficient public services. SSI can provide a solution.

Voting

Digital voting, backed by SSI, can reduce electoral fraud and streamline the voting process. Citizens can verify their identity and eligibility instantaneously, ensuring a transparent and efficient electoral process.

Taxes

Filing taxes can be simplified with SSI, as citizens can securely share financial data with tax authorities, ensuring accurate tax calculations and timely refunds.

Healthcare

Public healthcare services can benefit from SSI by allowing citizens to share their medical histories and credentials, leading to personalised care.

Residency and Travel

SSI can simplify processes related to proving residency, applying for visas, or managing other travel-related documentation. With secure and verifiable digital credentials, processes that once took weeks can be reduced to mere minutes.

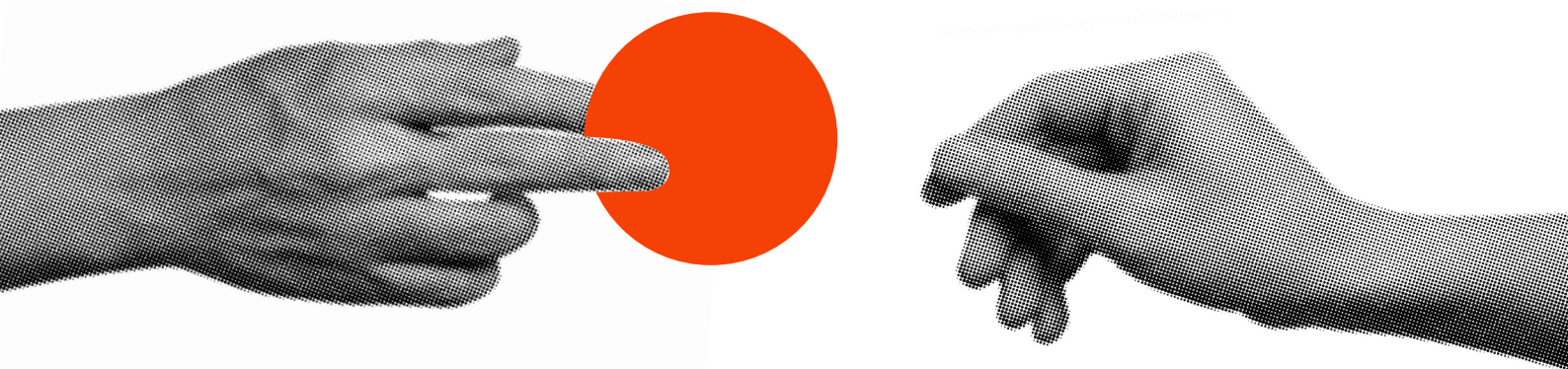
Citizens can verify their identity and eligibility instantaneously, ensuring a transparent and efficient electoral process.

Entirely new Business Models

Beyond streamlining existing processes, the advent of SSI and Digital Identity technologies paves the way for entirely novel business models.

Data Marketplaces

In an era where data is the new oil, individuals can monetise their data. Using SSI, individuals can choose to share specific pieces of information with businesses in exchange for incentives, leading to the rise of personal data marketplaces.



Individuals can choose to share specific pieces of information with businesses in exchange for incentives

Credentialing Platforms

As businesses and institutions recognise the value of verifiable credentials, there's potential for platforms that specifically cater to credential issuance, verification, and management, all based on SSI principles.

Identity-as-a-Service

With the growing importance of identity verification, businesses might not want to manage their SSI infrastructure. This opens up avenues for companies that offer Identity-as-a-Service, providing SSI solutions on a subscription or pay-per-use basis.

More than just Data

Identity is a New Industry

The potential of Self-Sovereign Identity and Digital Identity technologies stretches far beyond mere replacements for traditional systems. They promise a reimagining of how personal data is viewed, managed, and utilised. As industries and governments take cognisance of this potential, we stand at the precipice of a transformation that could redefine the very essence of identity in the digital age.

**We stand
at the precipice
of a transformation
that could redefine
the very essence
of identity in the
digital age**



Digital Identity: Current Losses & Projected Gains

In this section, we analyse the economic ramifications of the current landscape of digital identity systems. Firstly, we will delve into the financial setbacks experienced due to the inherent pain points of the prevailing digital identity frameworks – pain points that Self-Sovereign Identity (SSI) solutions are designed to address. Following this, we pivot to a more optimistic perspective, exploring the projected financial gains and other tangential benefits of adopting SSI.

As we shine a light on the inefficiencies and failures of existing systems, it becomes evident that these aren't just technological challenges but are deeply intertwined with financial repercussions. By juxtaposing the fiscal repercussions of the existing system's shortcomings against the potential dividends of SSI, we aim to provide stakeholders with a holistic understanding of the criticality of transitioning to more secure, fraud-proof, and user-centric identity solutions.

Proceeding further, let us quantify the losses and illuminate the pathway to future financial security and growth through SSI, and provide a comprehensive, numbers-driven perspective on the state and future of digital identity.

The vulnerabilities of current systems translate into staggering financial setbacks

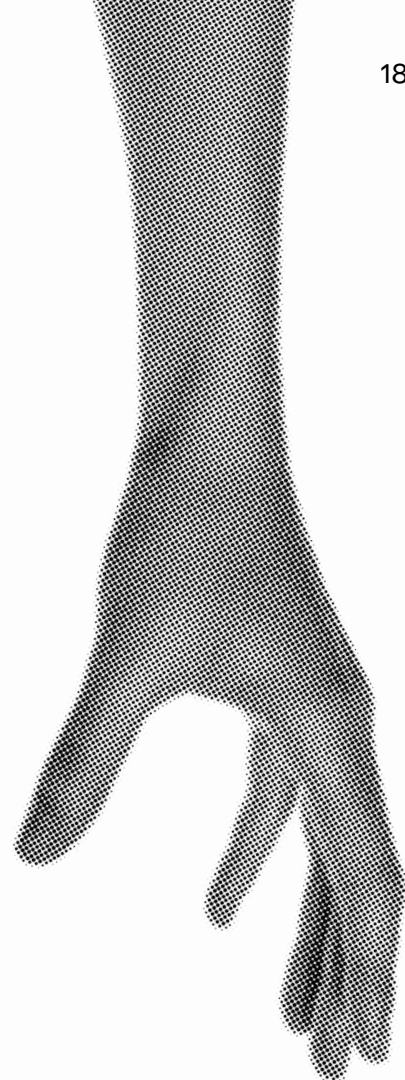
The Financial Fallout of Current Systems

A robust digital identity system should ideally serve as a barrier against security breaches, ensuring the sanctity of personal and financial data. However, the recurring incidents of data breaches, identity thefts, and fraudulent activities testify to the issues inherent in current digital identity systems. These vulnerabilities do not just represent isolated incidents; they translate into staggering financial setbacks for businesses, governments, and individuals alike.

Businesses bear the brunt of these inadequacies. As organisations invest heavily in damage control, legal redressals, and regaining customer trust following such incidents, the economic toll mounts. The cost implications of a data breach, for instance, are multifaceted: direct monetary losses, expenditures on damage control, legal fees, potential regulatory fines, and the more intangible but equally crucial cost of damaged brand reputation and loss of customer trust. In industries such as finance and healthcare, where the sanctity of data is paramount, the repercussions can be even more severe.

Traditional databases, acting as lucrative targets for cyber attackers, exacerbate this vulnerability. Yet, beyond these explicit costs, there's an implicit cost too – the opportunity cost of lost business opportunities owing to eroded trust and cumbersome identity verification processes. Moreover, the inefficiencies of current digital identity verification processes have often led to elongated customer onboarding times, impeding user experience and causing potential revenue losses. For industries that thrive on rapid customer turnover and seamless interactions, such as e-commerce or digital banking, these inefficiencies can translate into substantial financial setbacks.

Vulnerabilities translate into staggering financial setbacks for businesses, governments, and individuals alike



But how significant is this financial fallout?

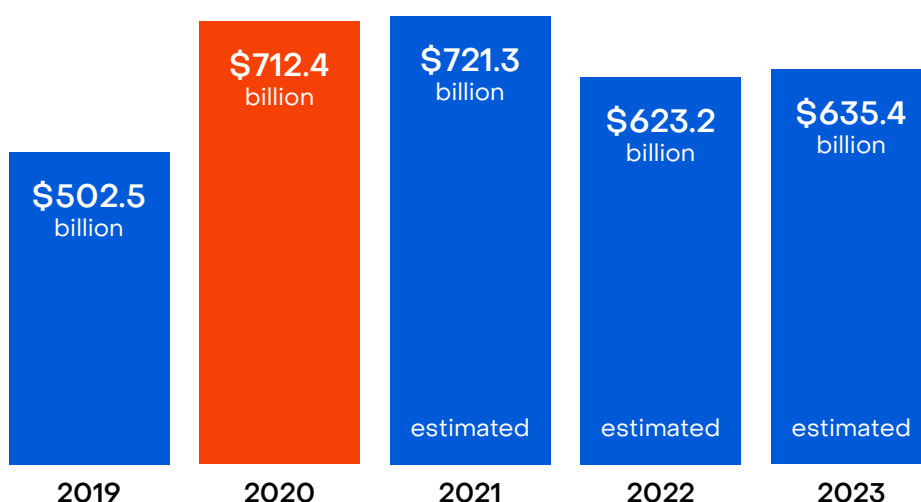
As we delve deeper into this section, we shall enumerate these losses, bringing forth data that underscores the urgency of addressing the pain points of current digital identity systems.

Losses from Identity Fraud in the US alone reached over \$712.4bn in 2020, affecting 47% of adults. The surge in fraud is partly attributed to the increase in e-commerce and card-not-present transactions due to the pandemic. After March 11, 2020, a 5% rise in suspected fraudulent transactions was observed.

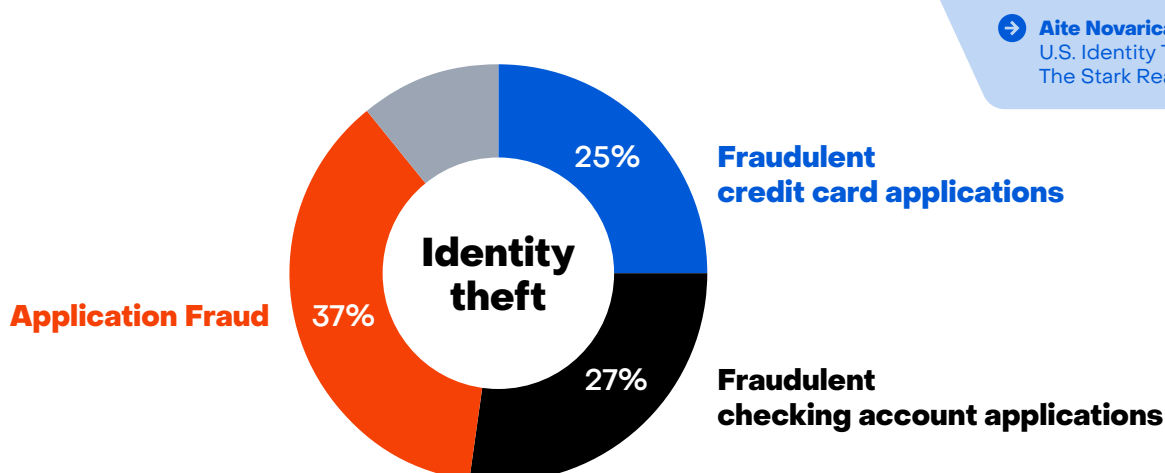
Losses from Identity Fraud in the US alone reached over \$712.4 billion in 2020

US firms' losses due to identity theft

Source: Aite Group



Identity theft involves methods such as application fraud and account takeovers, which are challenging for victims to address. 37% were victims of application fraud, which includes fraudulent tax filings, consumer loans, and mortgages. 25% faced fraudulent credit card applications, and 27% had fraudulent checking account applications. Additionally, 38% of consumers reported account hijacking incidents. Peer-to-peer payment account takeovers, especially on platforms like Venmo and Zelle, saw a significant rise in 2020. ➔



➔ **Aite Novarica**
U.S. Identity Theft:
The Stark Reality

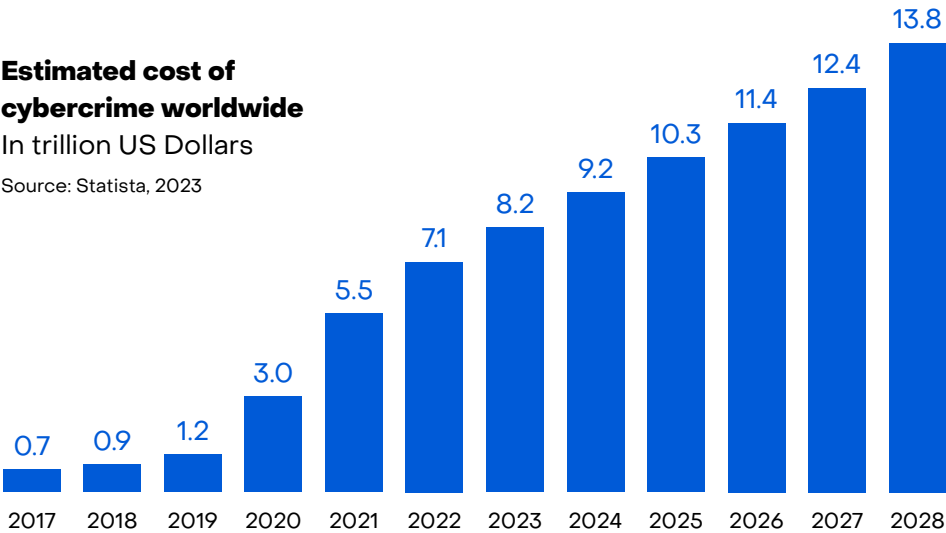
Losses from cybercrime will be expanding by at least 15% year on year

A Special Report by Cybersecurity Ventures estimates that losses from cybercrime will grow from \$3 trillion annually in 2016, to exceed \$10.5 trillion by the end of 2025, expanding by at least 15% year on year. This eclipses global losses from natural disasters and is more profitable than the global illicit drug trade. ➔

Estimated cost of cybercrime worldwide

In trillion US Dollars

Source: Statista, 2023

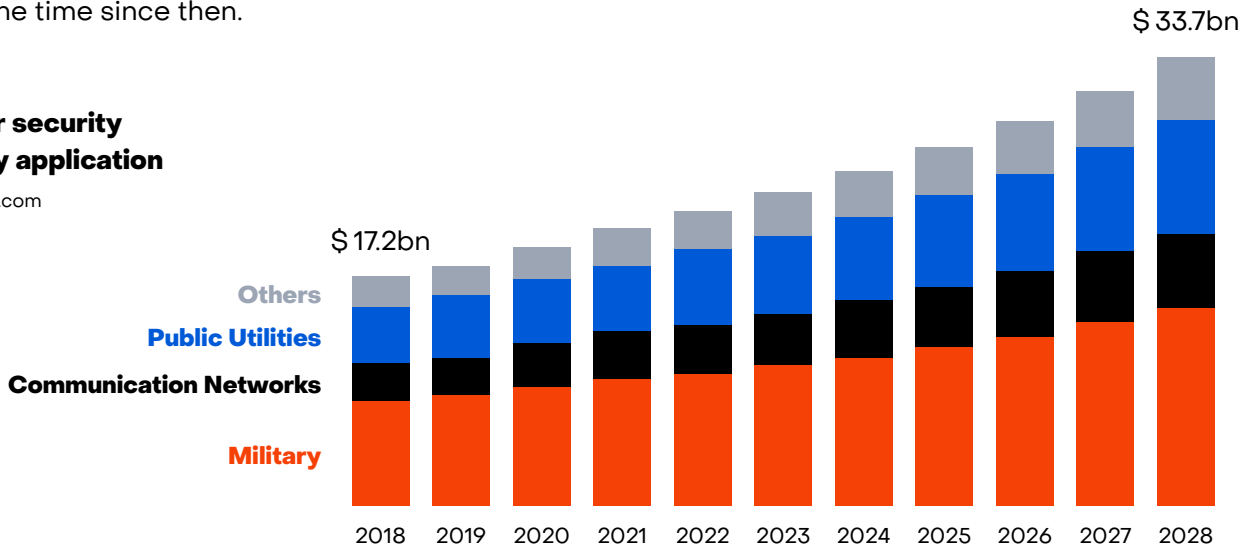


➔ **Cybercrime Magazine**
Cybercrime to cost the world \$10.5 trillion annually by 2025

Costs don't just come from losses, but the cybercrime defense industry is projected to grow to over \$33.7bn ➔ by 2028, and that spending on cybercrime insurance grew to \$2.5bn ➔ in 2016 and has only grown exponentially in the time since then.

Defense cyber security market size, by application

Source: kbvresearch.com



➔ **KBV Research**
Market Research Report

➔ **Forbes article**
The Business of Cybersecurity

The Promise of Self-Sovereign Identity

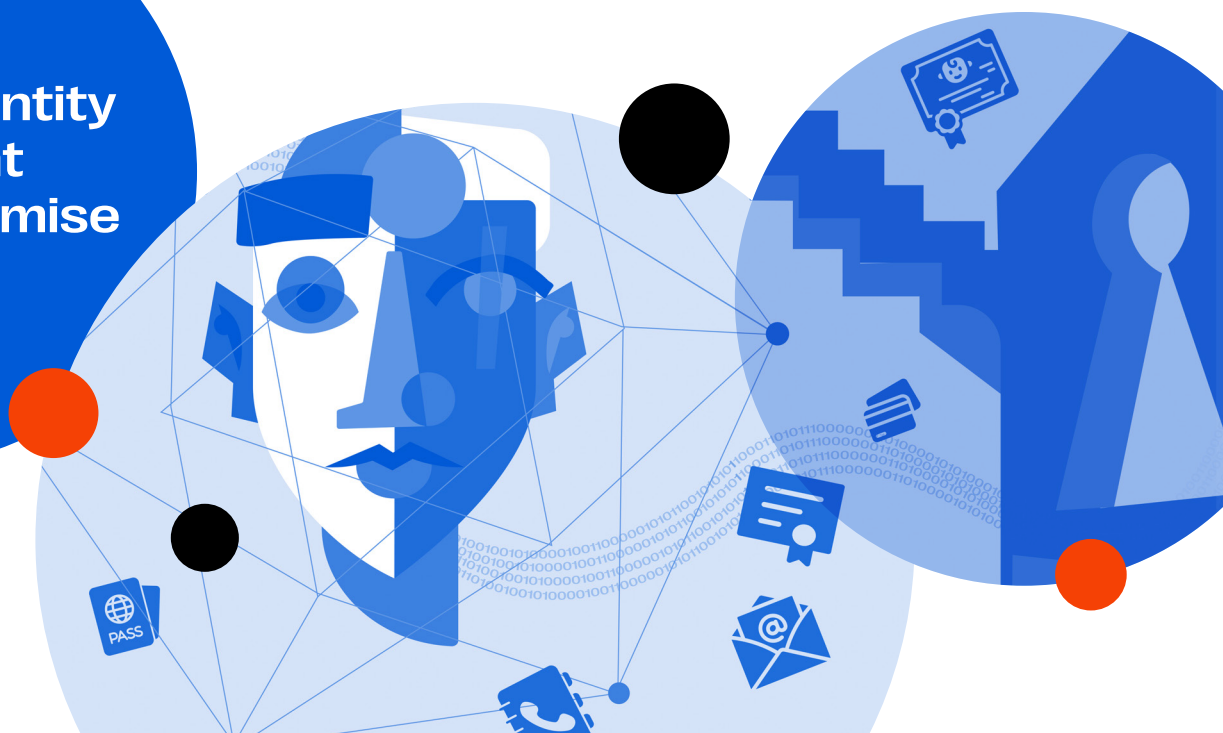
In stark contrast to the vulnerabilities of the existing systems, the horizon of digital identity shines bright with the promise of SSI. Fraud-proof, uniquely secure, and placing emphasis on individual control, SSI stands as a paradigm shift, addressing many of the pain points that have plagued traditional digital identity systems.

From an economic standpoint, the adoption of SSI offers a plethora of benefits. By eliminating centralised points of failure, businesses can significantly mitigate the risks, and hence the costs, associated with data breaches. A streamlined and efficient verification process can dramatically reduce customer onboarding times, translating to enhanced user experience and potentially higher revenue streams. The trust instilled by SSI systems can also open doors to novel business models and services, ones previously deemed too risky or unfeasible under traditional identity frameworks. Furthermore, the reduced dependence on intermediaries in the identity verification chain can lead to cost savings.

Another pivotal financial benefit lies in the realm of regulatory compliance. With governments and regulatory bodies across the globe tightening the noose around data protection and user privacy, non-compliance can result in hefty fines. SSI, with its inherent emphasis on user data rights and security, can ease the compliance journey for businesses, potentially saving them millions in non-compliance penalties. By eliminating centralised points of failure, businesses can focus on core competencies, innovation, and expansion, laying the groundwork for fiscal growth.

The horizon of digital identity shines bright with the promise of SSI

truivity





Let us now project the potential financial gains of migrating to SSI, anchoring our predictions in current trends, market analyses, and case studies.

Losses due to data breaches and theft of intellectual property is reported to cost between 1–3% of the national GDP of developed nations annually, as reported by the UK National Intellectual Property Office. This total ranges from \$749m to \$2.2bn annually, and will only grow year-on-year. ➔

➔ **GOV.UK**
The economic and innovation impacts of trade secrets



The cost of compliance is becoming more critical year after year. We've seen the FCA crackdown on KYC/AML standards in recent years, and while fines reached record levels of \$3.2bn in 2020 and fell to over \$2.7bn in 2021, the number of affected financial institutions grew significantly. ➔

➔ **Kyckr**
AML fines 2021




Second to the financial sector, healthcare services were the most impacted sector from fines and restrictions related to compliance demands. ➔

➔ **Security Intelligence**
20 Eye-Opening Cybercrime Statistics

From an economic standpoint, the adoption of SSI offers a plethora of benefits

The Current SSI Landscape

This section aims to provide a comprehensive examination of the present-day landscape of digital identity and the burgeoning rise of SSI solutions. By commencing with a dissection of the current trajectory of SSI adoption, we will pave the way for a detailed comparison between our pioneering SSI architecture at TruVity and the innovative models introduced by other industry frontrunners. Our exploration will unfold in two segments: a comprehensive overview of the current progress of SSI adoption and a closer examination of the growth and diversification of SSI architecture, ranging from our pioneering efforts at TruVity to those of other industry leaders.

A graphic illustration of two hands, rendered in a dark blue, textured style, holding a large white circle. Inside the circle, there is text in a dark blue, sans-serif font. The hands are positioned on the left and right sides of the circle, with fingers slightly curled as if supporting it from below.

**A examination
of the present-day
landscape of
digital identity and
the burgeoning rise
of SSI solutions**

The march toward SSI adoption

Gauging the present momentum

As the apparent limitations of traditional identity databases that we have explored – ranging from data breaches to issues of control and consent – SSI has emerged as an alternative. Though a relatively nascent concept, it has quickly gained traction, demonstrating its value proposition to sectors far and wide. Its foundational tenets – immutable trust, the empowerment of individuals, and impenetrable security – resonate in an era where data breaches and identity thefts have become alarmingly frequent.

The current adoption curve of SSI reflects a promising uptrend. Numerous industries, especially those steeped in data sensitivity from banking and finance to healthcare, are experimenting with SSI's potential, driven by its promise of enhanced security and user-centricity. Pilot projects and partnerships between tech firms and institutional bodies underline the growing recognition of SSI as a viable and sustainable identity solution for the future. Regulatory bodies too, such as the looming eIDAS 2.0 leviathan, are conscious of the paradigm shifts in data privacy laws and user rights, are veering towards standards and frameworks that align with SSI principles.

Pilot projects and partnerships underline the growing recognition of SSI as a viable and sustainable identity solution for the future

→ European Commission
eIDAS Regulation

In addition, the UK has its own plans regarding the viability and regulation of stablecoin technologies with an emphasis on the efficiency of transactions. Concerns exist about the rapid evolution of KYC and AML frameworks not keeping pace with these technological advancements, potentially leading to confusion and undermining the efficiency of stablecoins. SSI emerges as a key solution, providing a user-centric digital identity model that allows individuals to control their personal data. This approach could help balance the need for compliance with efficiency and privacy. The adoption of SSI and similar protocols could be crucial for the wider acceptance of digital assets like stablecoins and Central Bank Digital Currencies (CBDCs), offering a secure and streamlined way for users to meet regulatory requirements.

Estimates
potential savings
Financial Services
by adoption
of eIDAS 2.0
in EU

\$860
million

\$1700
million

However, the road to widespread adoption is not without challenges. While the technological community has largely embraced the philosophy behind SSI, practical implementation hurdles, such as interoperability with existing systems, user education, and regulatory acceptance, continue to pose significant barriers. Diverse stakeholders, including businesses, governments, and end-users, have to navigate issues ranging from interoperability and standardisation to awareness and trust. A detailed look at the adoption metrics and case studies will shed light on both the strides made and the hurdles yet to be surmounted.

From the adoption of eIDAS 2.0 alone, the EU, conservatively, estimates the potential savings to financial services from more efficient onboarding procedures to be between \$860 million and \$1.7 billion per year, while savings from reduced fraud ranges from €1.1 billion up to €4.3 billion. →

→ **European Commission**
The impact assessment for the
revision of the eIDAS regulation

The McKinsey Global Institute found that a 3-13% increase in GDP from value unlocked by the adoption of digital identity technologies will emerge. This accounts for at least 3% growth in mature economies, and at least 6% in emerging economies. →

→ **McKinsey Global Institute**
Digital identification:
A key to inclusive growth

**By the adoption
of digital identity
technologies
3–13% increase
in GDP will emerge**

Source: McKinsey Global Institute

US
4%

UK
3%

China
4%

Nigeria
7%

Ethiopia
6%

India
6%

Brazil
13%

● Mature Economies ● Emerging economies



The experts at Juniper Research evaluated that the SSI marketplace alone will be worth over \$1.1bn by the end of 2024. This suggests that the coming year will yield exponential growth within the sector, as push/pull factors motivating adoption widely take hold. ➔

➔ **Juniper Research**
Self-sovereign identity to be a billion-dollar industry by 2024

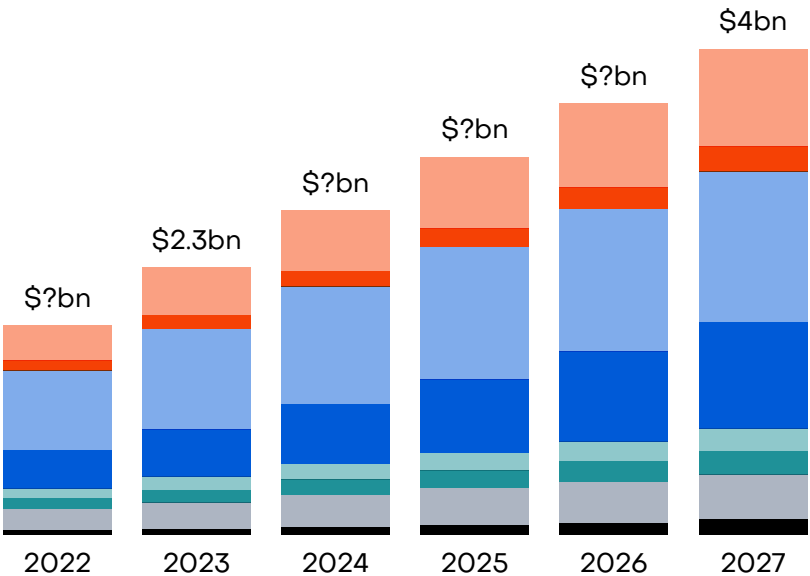
In supporting the conclusions regarding the impact and growth of the digital identity markets in mature and emerging markets, Juniper Research estimates that the number of installed digital identity apps will rise from 2.3bn in 2023 to over 4bn in 2027, giving a CAGR of 13.7%. This accounts for the largest market share being from the Indian Subcontinent where installations will grow from over 853m to 1.3bn in that timeframe. North America will be the fastest growing region, with a CAGR of 36.9%, due to the low adoption rate and incomplete infrastructure at the beginning of the timeframe. ➔

➔ **Juniper Research report**
Digital Identity: solutions assessment, regional analysis & market forecasts

The number of installed digital identity apps will rise from 2.3bn in 2023 to over 4bn in 2027

Number of Digital Identity Apps Installed
Split by 8 regions

- Africa & Middle East
- Rest of Asia Pacific
- Indian Subcontinent
- Far East & China
- Central & East Europe
- West Europe
- Latin America
- North America



Source: Juniper Research

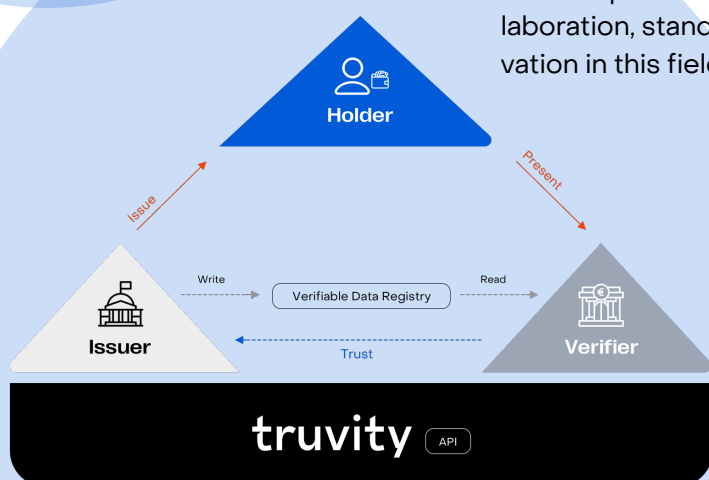
Truivity's SSI Architecture versus the Broader Industry Innovations

At Truivity, our commitment to the potential of a new era of trust in digital identity led to the inception of our proprietary SSI architecture – a model that blends technological sophistication with an unwavering focus on user autonomy. Recognising the pivotal role that architecture plays in the widespread adoption and scalability of SSI, our teams have been diligently crafting solutions that are not just robust and secure but also adaptable to diverse use cases.

A model that blends technological sophistication with an unwavering focus on user autonomy

In the diverse and evolving world of Self-Sovereign Identity, multiple players contribute with their unique innovations. While some prioritize scalability, others focus on specialized verifiable credentials. This range in architectural approaches showcases the flexibility and potential of SSI. In this dynamic landscape, Truivity stands out with its strengths: an open-source demo, a comprehensive Self-Sovereign Identity API, and an extensive developer documentation suite.

We map the industry because the marketplace contains offerings from open-source platforms that foster collaborative development to enterprise-focused solutions optimising for speed and efficiency. Comparing Truivity's approach with others highlights both our unique contributions and the collective progress towards a self-sovereign, secure, and individual-centered digital identity system. This comparison not only reflects the vast potential of SSI but also emphasizes the need for collaboration, standardization, and shared learning to foster innovation in this field.



TruVity's SSI Architecture versus the Broader Industry Innovations



A Self-Sovereign Future

A grayscale illustration of a hand with the index finger pointing upwards towards a blue circle. The hand is rendered with a halftone dot pattern.

Together,
let's step
into this new
chapter of
digital identity

Older digital identity systems, while innovative at their start, have shown many flaws as technology has advanced. They were designed to be trusted, but over time, they've struggled to keep up with the demands and threats of ever-more advanced digital challenges..

SSI has now emerged as a strong solution and the next step forward for digital identity. It's about giving users more control and offering unparalleled security. There are hurdles to overcome, like adapting from older systems and initial setup costs, but the overall outlook for SSI is positive. Its potential for new standards of security and new business innovations offer compelling reasons for its widespread embrace.

The reach of SSI is expansive. It's reshaping sectors like finance and healthcare, and even changing how we might vote or pay taxes digitally. Each application of SSI showcases its adaptability and highlights the broader impacts it could have on society and the economy.

We're at a pivotal moment, witnessing a shift in how digital identities work. With technological progress, evolving societal views, and diverse applications of SSI, the future is promising. But, success requires collaboration. Everyone, from tech experts to policymakers and the public, needs to engage, share their expertise, and work through challenges together.

Together, let's step into this new chapter of digital identity, equipped with knowledge and a shared goal of a next-generation of data management, where instant verification drives trust, growth, and cost-efficiency.