International Journal of Advanced Science and Research
www.allsciencejournal.com
ISSN: 2455-4227
Received: 22-07-2025, Accepted: 21-08-2028, Published: 06-09-2025
Volume 10, Issue 2, 2025, Page No. 10-17

Blockchain-based internet identity management systems

Okumoku-Evroro O., Atonuje O. E., and Esosuakpo O. T.
Department of Computer Science, Delta State University Abraka, Delta State, Nigeria

Abstract
The way people prove who they are online is changing. Traditional internet identity systems, whether centralized or federated, place control in the hands of companies or governments, leaving users dependent on those entities for access, security, and privacy. This paper explores blockchain-based internet identity management as a response to those limitations. It examines the three main models which are centralized, federated, and self-sovereign and also explains how each uses blockchain to enhance trust, verification, and data integrity. Case studies, including Sovrin, uPort, and Civic, illustrate how these systems work in practice and the trade-offs they present. The discussion also covers regulatory and ethical considerations, such as compliance with GDPR and the protection of privacy rights, as well as technical enablers like decentralized identifiers (DIDs) and verifiable credentials. While blockchain offers transparency, immutability, and decentralization, adoption challenges remain, particularly around interoperability, user key management, and policy alignment. The paper concludes by outlining future directions, including cross-platform standards, privacy-preserving verification methods, integration with national ID programs, and user-friendly security approaches. The findings suggest that blockchain identity systems have the potential to shift control toward individuals while improving security, but their success depends on careful governance, global cooperation, and practical usability.

Keywords: Blockchain, internet identity management, self-sovereign identity, decentralized identifiers, verifiable credentials, gdpr, privacy, sovrin, uport, civic

Introduction

Obviously, the Internet is full of people that you don't know who's who. Each passing day, billions of people login, make transactions online and also exchange data across platforms. Presently, big companies or the government handle the majority of the identity systems. Each time, you sign up and give away your personal information and always trust that they'll keep it safe. But past experience had indicated a different result (Anderson, 2020; Kshetri, 2021) [2, 15]. Presently, most online identity systems are centralized. When you log into your Facebook or your bank, your details are stored in their database. If that database is hacked, your personal data can also be stolen. You also have to trust these companies not to misuse your information.

"Blockchain Identity Management provides secure and decentralized management for a digital identity ensuring the privacy, control, and safety of users by using blockchain technology to prevent fraud" (Blockchain Techs, 2025) [3].

Blockchain technology is changing the way it's been carried out. A single company won't hold the keys to your identity but it will be a blockchain letting you hold all the keys yourself. This is simple, it's a digital identity online that you own, that you can prove, and can also be used anywhere online without having to hand it over to third parties like Bank, School Portal and so on (Allen, 2016; Tobin & Reed, 2016) [1]. Blockchain could help by making identity systems decentralized, meaning no single company controls everything. This change is more than a technical upgrade; it changes how identity will work on the internet (Chiliz, 2025) [7].

Blockchain Technology will be a trusted solution that's more reliable to our known identity system we use today. It will give you control over your own identity information. And you can also store verification records on a blockchain so that they can't be secretly changed or faked. It allows you to prove things about yourself (like your age or citizenship) without revealing all your personal details.

In this paper, we'll walk through how blockchain fits into identity management, real-world examples, challenges, and what the future might look like.

Background on Internet Identity Management

Before discussing blockchain, it's important to look at what we already have. Internet identity management involves the methods and systems used to confirm who you are online and to control what you can access (OECD, 2009, as cited in UNCITRAL, 2010) [21]. The most common model is centralized. For instance, when you sign in to your bank, Facebook or a school portal. Your data is stored in their database, and you use a username and password to prove it's you. Then there's federated identity, where one login works across multiple services. If you've used "Log in with Google" or "Sign in with Facebook," you must have seen it in action. It's convenient, but it means Google or Facebook is now a gatekeeper for your identity across the web (Fett *et al*., 2017) [12].

Control and risk are the problem with this system. Centralized databases are prime hacking targets. If one company gets breached, millions of identities are exposed. Users also lose autonomy due to the fact that their data is locked into whichever system they signed up for. This creates the need for something better, a model where identity is portable, verifiable, and user-controlled (Zyskind *et al*., 2015) [38].

Understanding Blockchain Technology

Here you need to know that blockchain isn't as mysterious as it sounds. It's just a special kind of database. The difference is in how it's stored and who controls it. Instead of one server holding all the information, blockchain data is

copied across many computers in a network (Nakamoto, 2008) [20]. Every time new information is added like your transaction, your ID update, or your certificate, this new information is bundled into a "block" and linked to the previous one, forming a chain.

Because each block is connected and verified by multiple participants, it's very hard to alter past data without everyone noticing. This structure gives blockchain three big qualities that matter for identity:

1. **Decentralization:** no single company or authority owns it (Yaga *et al*., 2018) [36]
2. **Transparency:** changes are visible to all participants
3. **Immutability:** once data is recorded, it can't be quietly changed

Blockchain has limits but these properties make it an interesting fit for identity systems, especially where trust is a problem.

How Blockchain Fits Into Identity Management

So, what does blockchain actually bring to the table for managing identity? It's controls, secure, and it's portable. In a blockchain-based identity system, your identity information can be stored in two ways, on-chain or off-chain. Most systems keep sensitive personal details off-chain for privacy, but store proofs or cryptographic links on-chain (Preukschat & Reed, 2021) [26, 27]. This way, anyone can verify that your data is legitimate without actually seeing it.

Blockchain identity systems use public and private keys instead of relying on a password database. In this case, you can hold the private key which is a kind of digital signature that proves it's you. If you lose it, you lose access, and that also removes the need for a central authority to "reset" your account (Allen, 2016) [1].

Another key concept here is Self-Sovereign Identity (SSI). Instead of companies controlling your data, you hold a digital wallet containing your credentials. You can choose to share only what's needed. For example, proving you're over 18 without revealing your exact birthday. This approach reduces data exposure and makes identity portable across all platforms and borders (Tobin & Reed, 2016; Ferdous *et al*., 2019) [11].

Models of Blockchain-Based Identity Systems

Not all blockchain identity systems are built the same way. Researchers and developers have experimented with different models, each with its own trade-offs. Let's break them down.

Centralized blockchain identity: This sounds like a contradiction, but it exists. Here, a single authority runs the blockchain nodes, and identity verification happens through them. It's more controlled but less open, and often used by governments or large organizations that want blockchain's security without giving up oversight (Bhattacharya *et al*., 2021) [4].

In a centralized blockchain identity system, the blockchain is more like a controlled database than an open network. The main authority decides who can add data, who can verify it, and in some cases, who can even see it. Users might still benefit from some blockchain features, like tamper resistance and transparency of records, but they don't get full ownership of their identity. Control is still largely in the hands of that central body (Zyskind *et al*., 2015) [38].

Take a government-issued digital ID system as an example. Imagine your country builds a blockchain-based ID platform. You register with them, they issue your ID, and it's recorded on the blockchain. But here's the catch the government manages the blockchain nodes, sets the rules for how data is used, and can revoke or suspend your identity at will. The power structure is still centralized even if the Blockchain is cryptographically secure.

This setup can be efficient. It's easier to enforce policies, integrate with existing services, and roll out large-scale programs quickly. Banks, healthcare systems, and border control agencies can verify identities instantly without relying on paper documents. But the trade-off is trust. You still have to believe that the central authority will protect your privacy, won't misuse your data, and will keep the system secure. And as history has shown, even the most secure databases can be hacked or abused (Kshetri, 2021, Okofu *et al* 2025) [15, 24].

In fact, Allen (2016) [1] warns against assuming that simply putting an identity system on a blockchain solves the deeper issues of control and autonomy. If the governance model is centralized, blockchain becomes more of a back-end tool than a true empowerment technology. The individual still doesn't have full say over how their personal information is used. There's also the regulatory angle. A centralized blockchain identity system can more easily comply with government data laws, since it's already under official control. But that also means it's vulnerable to political changes. In the wrong hands, the same system that provides convenience could be used for surveillance or to limit access to services based on political or social factors.

What this really means is that centralized blockchain identity sits somewhere between traditional identity management and self-sovereign identity. It borrows blockchain's strengths, immutability, easier verification, reduced paperwork but keeps the old power dynamics. For some use cases, especially where trust in the central authority is high, this can be acceptable. But for people seeking total control over their digital identity, it's not the final answer.

Federated blockchain identity: This model involves multiple trusted organizations running the network together. Banks, universities, or government departments might form a consortium to verify users across their systems. It's a middle ground between control and decentralization (Kuperberg, 2019) [16]. If you've ever used "Sign in with Google" or "Log in with Facebook," you've already experienced the basic idea of a federated identity system. In those setups, one account lets you access different services without creating a separate username and password for each. Instead of managing your own login everywhere, you rely on a trusted provider to vouch for you.

Now, here's where blockchain comes in. A federated blockchain identity takes that same shared-login concept but spreads the trust across a group of organizations, not just one. These organizations work together as a federation, and the blockchain acts as a common record everyone can rely on. Instead of Google or Facebook holding all the power, multiple entities participate in issuing, verifying, and managing identities.

Think of it like a group of banks agreeing that they'll accept each other's ID checks. If you've verified your identity with

one bank, the others will trust that verification without making you go through the process all over again. In a federated blockchain setup, the blockchain stores cryptographic proofs or "anchors" of those verifications so anyone in the group can confirm they're genuine. One important thing to note is that personal data is usually kept off-chain. The blockchain is not meant to hold all your personal data in one big place. Instead, it keeps things like verification hashes, revocation lists, or credential references. That way, privacy is better protected, and the blockchain's immutability is still useful for ensuring records haven't been tampered with (Preukschat & Reed 2021; Mühle *et al*., 2018) [19, 26, 27].

The strength of this model is that no single organization controls the whole system. If one member of the federation is compromised or goes offline, the others can keep it running. It also makes fraud harder because changes have to be agreed upon and recorded across multiple parties. That shared governance builds more resilience than a single identity provider ever could.

But it's not perfect. Federated systems still require a level of trust in the organizations running them. If the majority of members collude or follow weak security practices, the system's integrity can still be at risk (Zyskind *et al*., 2015) [38]. There's also the challenge of governance deciding who can join the federation, how decisions are made, and how to resolve disputes when something goes wrong.

In practice, federated blockchain identity works well in industries or government collaborations where trust already exists among members but they want to improve transparency and verification speed. For example, healthcare networks can use it to share verified doctor credentials across hospitals. Banks can use it to share verified customer details for KYC compliance without exposing sensitive information to unnecessary risk.

What this really means is that federated blockchain identity is a middle ground. It's not as fully user-controlled as self-sovereign identity, but it avoids the weaknesses of a completely centralized system. Users benefit from fewer logins, faster verification, and stronger privacy than traditional federation, while organizations gain a tamper-evident record of identity checks.

Self-Sovereign Identity (SSI): Is the most common one. SSI puts users in charge of their identity through a digital wallet of verifiable credentials. The blockchain is not a data hub, it's performed as a verification layer. Anyone can confirm that a credential is valid without storing personal data on-chain (Tobin & Reed, 2016; Ferdous *et al*., 2019) [11].

"Self-sovereign identity (SSI) refers to a digital approach where individuals, rather than outside institutions, hold the authority to manage and control their own identity information. The principle behind SSI is that ownership of personal data rests with the individual instead of being controlled by third-party administrators" (Sovrin Foundation, 2018) [28, 29, 30, 31].

SSI was created to protect your information in a digital wallet. And also, in scenarios when someone needs proof of something about you, like your age, nationality, or qualifications, you can share just that fact, without giving away everything else. This blockchain model stores your verification record so that the other person can confirm your proof is real, without seeing the actual data. SSI increases privacy by reducing unnecessary data. It also boosts security since there's no central database for hackers to attack. SSI gives you total control over who sees your information and when.

But this model also goes with some challenges as well. If someone misplaces their private key or digital wallet, they might no longer be able to get access to their identity. And also, legal rules about deleting data don't always fit with blockchain's permanent record. Since the model is new, people will need to understand and trust the system before it can be widely used.

What's clear is that SSI is getting the most attention, especially as privacy laws like the General Data Protection Regulation (GDPR) push for more user control over personal data.

Case Studies

Theory is one thing, but blockchain identity has already moved into real projects.

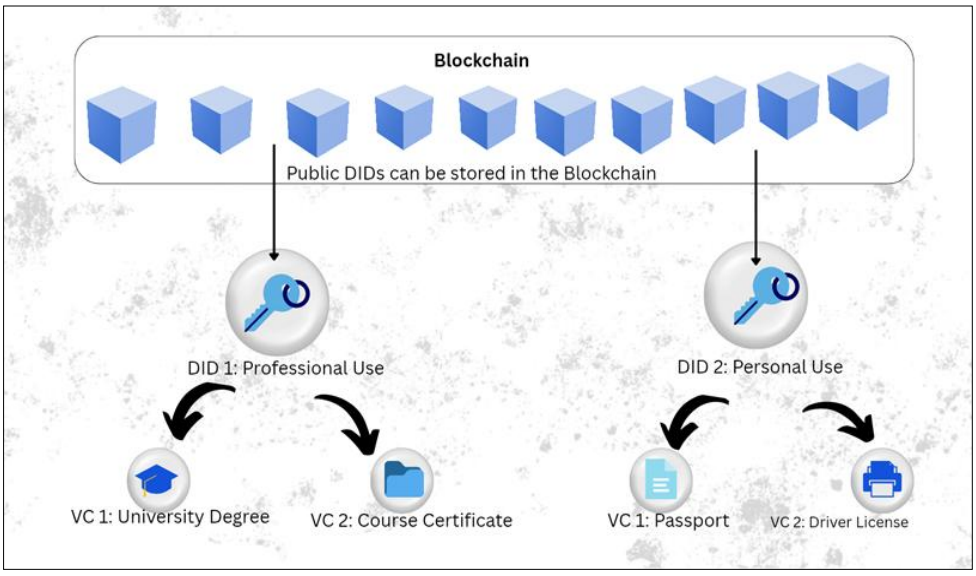

Fig 1: shows how users manage multiple identities and credentials without third-party control.

Sovrin Network: Sovrin is one of the earliest large-scale SSI projects. Built on a public-permissioned blockchain, it uses decentralized identifiers (DIDs) and verifiable credentials so users can prove identity attributes without revealing sensitive details. The Sovrin Foundation manages governance but doesn't control user data (Preukschat & Reed, 2021) [26, 27].

Sovrin is the most common project created to make self-sovereign identity (SSI) a success everywhere. Think of it as a public utility for digital identity. You can use it, anyone can join, but not just anyone can write to it. That's because it runs on a public-permissioned blockchain. This design keeps it open enough for global adoption, while still protecting the integrity of the ledger by allowing only trusted participants called Stewards, to operate the nodes (Sovrin Foundation, 2018) [28, 29, 30, 31].

The point is, Sovrin doesn't store your private information on the blockchain. Instead, it uses something called Decentralized Identifiers (DIDs). A DID is like a unique tag that represents you in the digital space without revealing your actual name or personal details. Alongside DIDs, Sovrin works with Verifiable Credentials (VCs), which are digital proofs issued by trusted entities like a government or a university that you can show whenever you need to prove something about yourself (Preukschat & Reed, 2021) [26, 27].

What makes Sovrin special is how these pieces come together. Let's say you need to prove your age to access a service. With Sovrin, you can show only that you're "over 18" without revealing your exact birth date or other details. This selective disclosure is possible because Sovrin follows the principles of SSI: you control your identity, you decide who sees what, and no central company owns your profile. The network's governance is managed by the Sovrin Foundation, a non-profit organization that maintains the rules, standards, and legal frameworks for how the system runs. They don't own your data, they don't track you, and they don't issue your credentials. Their role is to keep the network stable and trustworthy (Sovrin Foundation, 2018) [28, 29, 30, 31]. As the Sovrin white paper puts it, "The Sovrin Network provides a global public utility for self-sovereign identity, an identity that is permanent, portable, private, and completely under the control of the identity owner" (Sovrin Foundation, 2018) [28, 29, 30, 31]. They promise portability, privacy, and personal control.

In practice, Sovrin's approach can be applied to many real-world needs. For example, banks can verify a customer's KYC credentials without storing a full copy of their documents. Universities can issue diplomas as verifiable credentials, so graduates can prove their qualifications without relying on paper certificates. Even healthcare providers can confirm a patient's insurance eligibility without pulling their full medical history. Of course, Sovrin isn't perfect. It still relies on trusted issuers to provide credentials, and those issuers could be influenced by existing political or economic systems. But the main shift here is that, instead of building more central databases, Sovrin spreads out identity control so that people have the final say over their information.

uPort: Running on the Ethereum blockchain, uPort lets users create and manage identities through a mobile app. Credentials are stored off-chain, but proofs are anchored on Ethereum so anyone can verify authenticity. It's been used in pilot programs for government services in Zug, Switzerland (Lemieux, 2017) [17, 18].

uPort was one of the first identity systems built directly on the Ethereum blockchain. The idea was simple: give people a way to create and manage their digital identity through a mobile app, while keeping control in their own hands (Dunphy & Petitcolas, 2018) [8]. Here's how it works. You download the uPort app, which becomes your personal identity wallet. With it, you can set up a Decentralized Identifier (DID) that belongs only to you. This DID is anchored to the Ethereum blockchain, but your actual personal information like your name, address, or credentials is stored off-chain, usually on your device or a secure storage service you choose. That means if the blockchain is ever hacked, your private data isn't sitting there waiting to be stolen.

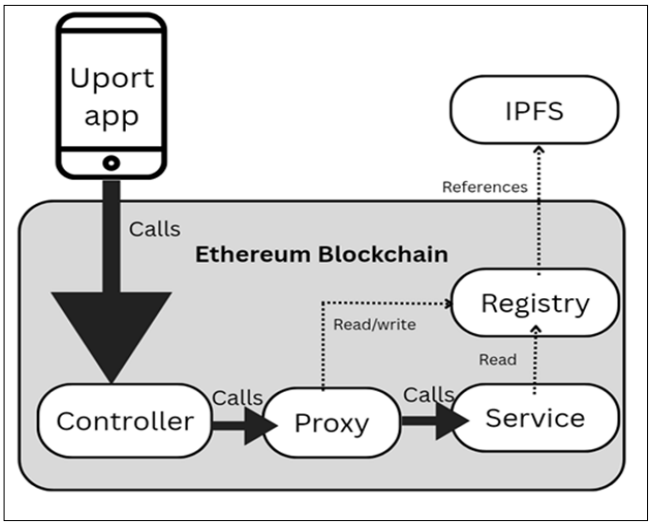

Fig 2: A breakdown of Uport's key components

One of uPort's strong points is that it lets you collect credentials from trusted issuers and then decide when and where to share them. For example, the city of Zug in Switzerland used uPort for a pilot project where residents could register their digital identity with the city and then use it to access local government services without creating new accounts each time (Lemieux, 2017) [17, 18]. When you use uPort to prove something like your membership in a professional organization, the proof is verified through the Ethereum network. Because the verification process happens on a public blockchain, it's easy for others to confirm its authenticity, but without exposing your private details. The architecture is straightforward: your phone is the gateway, Ethereum acts as the notary, and your credentials stay wherever you decide they should stay. You're not logging into a central database, and you're not relying on a single company to keep your identity safe. In summary, uPort turns your smartphone into a portable, blockchain-backed ID card you can use anywhere online or in real life.

Civic: Civic offers a reusable digital identity that can be used for logins, age verification, and secure transactions. Their model focuses heavily on user consent, requiring explicit approval before any data is shared (Mühle *et al.*, 2018) [19]. Civic takes a slightly different approach. It

focuses heavily on user consent and reusability. The core product is a reusable digital ID that works for logins, age verification, and secure transactions (Mühle *et al*., 2018) [19]. With Civic, you create your identity once and verify it through their process, which usually involves document checks and biometric confirmation. Once you can store and verify your identity on your machine not on Civic's servers, the only thing kept on the blockchain is only the cryptographic proof that your identity has been verified.

It means that when you need to prove something, for example, you're over 21 for a bar entry, you can do it without handing over your ID card or revealing your exact birth date. The relying party gets the answer they need (yes, you're of legal age), but they don't get your address, your ID number, or any other sensitive information. Civic also builds in a strong consent layer. Nothing gets shared unless you approve it in real time through the Civic app. That makes it harder for companies to collect or sell your information without you knowing.

The system's flexibility means it can be used in many situations: logging into websites without passwords, passing airport security checks faster, or verifying your identity before making a cryptocurrency transaction. By putting users in direct control, Civic reduces both the risk of large-scale data breaches and the amount of personal data floating around the internet, (Ikem, &Akazue 2025; Yoro *et al* 2025) [14, 35]

Each of these projects takes a slightly different approach, but they share the same backbone: decentralized verification, reduced reliance on central authorities, and giving users more control.

Benefits of Blockchain Identity

When you strip away the hype, the biggest win with blockchain identity is control. Users no longer have to hand over their personal details to every website or service they interact with. Instead, they share only what's needed, when it's needed, and keep the rest private (Allen, 2016) [1].

1. **Privacy by design:** With SSI, you can prove facts about yourself without disclosing the raw data. Want to prove you are of legal drinking age? You can do that without revealing your full date of birth (Tobin & Reed, 2016).

2. **Security against breaches:** Since personal information isn't sitting in a massive central database, hackers can't just hit one target and walk away with millions of records (Zyskind *et al*., 2015) [38].

3. **Portability:** With a blockchain identity, you don't need to re-register everywhere. The same identity can move with you across apps, countries, and services. This could make onboarding processes faster and less repetitive (Ferdous *et al*., 2019) [11].

4. **Transparency and trust:** Public blockchain records make it easy for others to verify credentials, reducing the risk of forged documents or false claims (Yaga *et al*., 2018) [36].

5. **Compliance with modern laws:** Projects can be designed to meet privacy regulations like GDPR while still allowing verifiable digital interactions (Kuperberg, 2019) [16].

Challenges and Risks

It's not all smooth sailing. Blockchain identity comes with its own set of issues, and ignoring them would be a mistake.

1. **Key management:** In SSI, the private key is everything. Lose it, and you lose access to your identity. "*Recovering a lost blockchain key is not as simple as resetting a password, and in many cases, it can be very hard to do"* (Preukschat & Reed, 2021, Okofu *et al* 2024) [23, 26, 27].

2. **Scalability:** Public blockchains, especially those like Ethereum, can get congested and expensive to use. This slows down adoption for high-volume identity systems (Mühle *et al*., 2018) [19].

3. **Regulatory uncertainty:** Governments are still figuring out how to treat decentralized identities. "*There are still open issues around how these identities will be legally recognized, who takes responsibility when problems arise, and how they work across borders*" (Bhattacharya *et al*., 2021) [4].

4. **Adoption barriers:** For users, blockchain identity is still new. Learning to manage keys and digital wallets can be intimidating, and without user-friendly designs, mass adoption will be slow (Fett *et al*., 2017) [12].

5. **Data permanence:** While the immutability of blockchain is a feature, it can also be a legal problem. For example, GDPR's "right to be forgotten" conflicts with the permanent nature of on-chain records (Kuperberg, 2019) [16].

Regulatory and Ethical Considerations

When we start talking about identity, we're not just discussing technology. We're talking about something deeply tied to human rights, privacy, and trust. Blockchain identity management might sound purely technical, but the reality is that it intersects with laws, ethics, and individual freedoms in ways we can't ignore.

1. The Regulatory Side: GDPR and Privacy Laws,

Let's start with one of the big names in global privacy regulation: the General Data Protection Regulation (GDPR). Enforced across the European Union since 2018, GDPR sets strict rules on how personal data can be collected, processed, and stored. It's built around principles like data minimization, user consent, and the right to be forgotten (European Parliament and Council, 2016) [9]. Here's the challenge, blockchain is designed to be immutable. Once information is written to the ledger, it's not supposed to be erased or altered. GDPR gives individuals the power to ask for their personal data to be erased whenever they want. This creates a tension between the two worlds. Some blockchain identity systems avoid storing personal data directly on-chain, keeping it off-chain and using the blockchain only for proofs or hashes. This approach makes compliance easier while preserving blockchain's integrity (Okumoku-Evroro 2016; Finck, 2019) [13, 25].

It's not just GDPR. Different countries have their own privacy frameworks like the California Consumer Privacy Act (CCPA) in the U.S., Personal Data Protection Bill in India, or Nigeria's NDPR (Nigeria Data Protection Regulation). For global blockchain identity projects, this

means navigating a maze of laws that can sometimes conflict with one another.

2. Ethical Considerations: Power, Consent, and Inclusion

On the ethical side, one of the core debates is who gets to control identity systems. Centralized systems have often been criticized for creating data monopolies where big companies or governments hold massive power over individuals. Blockchain promises to fix that by making identities self-sovereign. But the issue is, technology alone can't guarantee fairness. If the rules, governance, and access to these systems aren't designed inclusively, blockchain identity could end up reinforcing existing inequalities instead of breaking them down (Zwitter & Gstrein, 2020) [37].

Consent is another key ethical pillar. In traditional systems, consent often means clicking "I agree" on a long document nobody reads. Self-sovereign identity changes this by letting users approve or deny each data request in real time. Still, ethical design has to ensure that users truly understand what they're agreeing to, especially in communities with lower digital literacy.

There's also the matter of digital exclusion. If blockchain identity systems require internet access, smartphones, and technical know-how, millions of people especially in rural or low-income areas might be left out. An ethical rollout needs to address this gap through accessible tools, local language support, and non-digital alternatives.

3. Balancing Transparency with Privacy

Blockchain's transparency is one of its strengths, but in identity management, too much transparency can be harmful. Nobody wants their personal identifiers visible to everyone on the network. Privacy-preserving technologies like Zero-Knowledge Proofs (ZKPs), selective disclosure, and encryption are becoming essential for meeting both legal and ethical expectations (Mühle *et al*., 2018) [19]. The Sovrin Foundation, for example, explicitly designed its system so that personal information is never stored on-chain, only cryptographic proofs. This is a way of meeting privacy regulations while keeping the benefits of a public ledger (Sovrin Foundation, 2018) [28, 29, 30, 31].

4. The Bigger Picture: A Shared Responsibility

In the end, regulatory compliance and ethical responsibility are two sides of the same coin. It's not enough to build a technically sound blockchain identity system; it has to respect human dignity, work within legal frameworks, and adapt to local cultural contexts. As Allen (2016) [1] put it, "The promise of self-sovereign identity will only be realized when technology and governance work together in service of the individual."

Identity is not just a tech problem; it's also a legal and ethical one. Blockchain-based identity systems bump into existing laws, especially around privacy and data protection. In the European Union, the General Data Protection Regulation (GDPR) sets strict rules for collecting, storing, and processing personal data (Voigt & Von dem Bussche, 2017) [34]. While SSI models are designed to keep personal data off-chain, there's still debate about whether certain blockchain records could be considered personal data if they can be linked back to someone (Finck, 2019) [13].

In some countries, digital identity is already tied to national security and governance, which means decentralizing it could meet resistance (Bhattacharya *et al*., 2021) [4]. There's also the ethical question of inclusivity. If blockchain identity relies on smartphones and internet access, people without those tools risk being left out (Allen, 2016) [1]. Then there's the right to be forgotten. Blockchain's immutability clashes with the legal requirement to delete personal data when a user asks. Some solutions use off-chain storage with on-chain proofs to navigate this, but the legal clarity is still evolving (Kuperberg, 2019) [16].

5. Future Directions

What this really means is that blockchain identity is heading toward a model where people own their data, credentials can move freely between systems, and trust isn't tied to one company or government. The challenge will be balancing ease of use with security and privacy, but the potential payoff is a safer, more open internet identity layer which is worth aiming for, (Aghware *et al* 2025).

We can expect to see more hybrid models that combine blockchain with privacy-preserving cryptography like zero-knowledge proofs. This could allow even more selective disclosure of information without weakening security (Mühle *et al*., 2018) [19]. Governments may begin to issue verifiable credentials directly to citizens, as seen in pilots in Estonia and Zug, Switzerland (Lemieux, 2017; Oboro, & Akazue (2025) [17, 18, 22].

Interoperability is another big area. For blockchain identity to work across borders and industries, different systems will need to talk to each other using common standards like W3C's Decentralized Identifiers (DIDs) and Verifiable Credentials (Sporny *et al*., 2019) [32, 33]. Education will also be key. Until managing a digital wallet is as simple as unlocking a phone, blockchain identity will stay a niche. But as more user-friendly designs emerge, the shift from centralized identity systems to decentralized ones could be as big as the move from physical mail to email.

Conclusion

Blockchain-based internet identity management systems aren't just another tech trend, they represent a fundamental rethinking of how identity works online. The shift from centralized and federated systems toward self-sovereign identity puts control back into the hands of users. Instead of trusting large corporations or government agencies to guard our data, blockchain offers a way to prove who we are without handing over everything about us.

Still, the road ahead is far from simple. Key management, regulatory clarity, and user adoption remain big hurdles. And while the technology's transparency and immutability are strengths, they can also be liabilities when laws like GDPR demand the ability to erase data.

What's encouraging is that progress is happening on multiple fronts. Standards bodies like W3C are defining interoperability protocols, projects like Sovrin and uPort are proving real-world use cases, and researchers are exploring ways to balance privacy with trust. If these efforts succeed, the internet of the future might be one where digital identity is as personal and portable as the keys in your pocket but far harder to lose or steal.

References

1. Allen C. The path to self-sovereign identity. Life with Alacrity, 2016. Available from: https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html
2. Anderson R. Security engineering: A guide to building dependable distributed systems. 3rd ed. Wiley, 2020.
3. Blockchain Techs. Blockchain for identity management, 2025. Available from: blockchaintechs.io
4. Bhattacharya P, Tanwar S, Tyagi S, Kumar N. Blockchain-based decentralized applications: Technology review and future trends. J Netw Comput Appl,2021:165:102730. https://doi.org/10.1016/j.jnca.2020.102730
5. Bünz B, Bootle J, Boneh D, Poelstra A, Wuille P, Maxwell G. Bulletproofs: Short proofs for confidential transactions and more. J Cryptol,2020:33(4):1802–1878. https://doi.org/10.1007/s00145-019-09391-0
6. Cameron K. The laws of identity. Microsoft Corporation, 2005. Available from: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
7. Chiliz. What Is Decentralized Identity and Why It Matters in Web3. Chiliz, 2025. Available from: https://www.chiliz.com/what-is-decentralized-identity-and-why-it-matters-in-web3
8. Dunphy P, Petitcolas FAP. A first look at identity management schemes on the blockchain. IEEE Secur Privacy,2018:16(4):20–29. https://doi.org/10.1109/MSP.2018.3111247
9. European Parliament and Council. Regulation (EU) 2016/679 of the European Parliament and of the Council. Off J Eur Union, 2016. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj
10. European Commission. Proposal for a framework for a European Digital Identity, 2021. Available from: https://ec.europa.eu/digital-strategy/our-policies/european-digital-identity_en
11. Ferdous MS, Chowdhury F, Alassafi MO. In search of self-sovereign identity leveraging blockchain technology. IEEE Access,2019:7:103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173
12. Fett D, Küsters R, Schmitz G. The web SSO standard OpenID Connect: In-depth formal security analysis and security guidelines. IEEE Eur Symp Secur Priv, 2017, 1–16. https://doi.org/10.1109/EuroSP.2017.27
13. Finck M. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? Eur Parliam Res Serv, 2019. Available from: https://www.europarl.europa.eu/thinktank
14. Ikem OC, Akazue MI. Data misuse and theft protection model in internet of things devices. Scientia Africana,2025:24(2):277–282
15. Kshetri N. Blockchain and the economics of crypto-tokens and tokenized assets. J Strateg Innov Sustain,2021:16(2):36–49.
16. Kuperberg M. Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. IEEE Trans Eng Manage, 2019:67(4):1123–1139. https://doi.org/10.1109/TEM.2019.2932263
17. Lemieux VL. Trusting records: Is blockchain technology the answer? Rec Manag J,2017:27(3):234–252. https://doi.org/10.1108/RMJ-12-2016-0042
18. Lemieux VL. Trusting records: Is blockchain technology the answer? Rec Manag J,2017:27(3):234–250. https://doi.org/10.1108/RMJ-12-2016-0042
19. Mühle A, Grüner A, Gayvoronskaya T, Meinel C. A survey on essential components of a self-sovereign identity. Comput Sci Rev,2018:30:80–86. https://doi.org/10.1016/j.cosrev.2018.10.002
20. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, 2008. Available from: https://bitcoin.org/bitcoin.pdf
21. OECD Working Party on Information Security and Privacy. The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers (DSTI/ICCP/REG(2008)10/FINAL), 2009.
22. Oboro E, Akazue M. A Pilot Study of Automated Predictive Models for Retinal Diseases. Int J Innov Sci Res Technol,2025:10(8):423–430. https://doi.org/10.38124/ijisrt/25aug280
23. Okofu SN, Bisina J, Okumoku-Evroro O, Akazue MI. Cash on delivery risk mitigation CMRR model. J Manage Sci,2024:61(9):142–155.
24. Okofu C, Asuai O, Okumoku-Evroro MI, Akazue MI. Development of an Enhanced Point of Sales System for Retail Business in Developing Countries. J Behav Inf Digit Humanit Dev Res,2025:11(5):1–24. Available from: https://www.isteams.net/behavioralinformaticsjournal dx.doi.org/10.22624/AIMS/BHI/V11N1P1
25. Okumoku-Evroro O. Development of an online repository and search engine for Delsu alumni. Asian J Comput Inf Syst,2016:4(3). Available from: http://www.ajouronline.com/index.php?journal=AJCIS&page=article&op=view&path /1882
26. Preukschat A, Reed D. Self-sovereign identity: Decentralized digital identity and verifiable credentials. Manning, 2021.
27. Preukschat A, Reed D. Self-sovereign identity: Decentralized digital identity and verifiable credentials. Manning Publications, 2021.
28. Sovrin. What is self-sovereign identity? Sovrin, 2018 Dec 6.
29. Sovrin Foundation. The Sovrin Self-Sovereign Identity System, 2018 Mar. Available from: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-SSI-Architecture.pdf
30. Sovrin Foundation. The Sovrin Self-Sovereign Identity System, 2018. Available from: https://sovrin.org
31. Sovrin Foundation. The self-sovereign identity framework, 2018. Available from: https://github.com/animo/awesome-self-sovereign-identity
32. Sporny M, Longley D, Chadwick D. Verifiable credentials data model 1.0. World Wide Web Consortium (W3C), 2019. Available from: https://www.w3.org/TR/vc-data-model/
33. Sporny M, Longley D, Chadwick D. Decentralized identifiers (DIDs) v1.0. W3C Recommendation, 2019. Available from: https://www.w3.org/TR/did-core/
34. Voigt P, Von dem Bussche A. The EU General Data Protection Regulation (GDPR): A practical guide. Springer, 2017.

35. Yoro RE, Okpor MD, Akazue MI, Okpako EA, Eboka AO, Ejeh PO. Adaptive DDoS detection mode in software defined SIP-VoIP using transfer learning with boosted meta-learner. PLoS One,2025:20(6):0326571. https://doi.org/10.1371/journal.pone.0326571
36. Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview. Natl Inst Stand Technol (NIST), 2018. https://doi.org/10.6028/NIST.IR.8202
37. Zwitter A, Gstrein OJ. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. J Int Humanit Action,2020:5(1). https://doi.org/10.1186/s41018-020-00072-6
38. Zyskind G, Nathan O, Pentland A. Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security and Privacy Workshops*, 2015, 180–184. https://doi.org/10.1109/SPW.2015.27