ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Social Impact of Blockchain-Based Digital Identity Systems

Simran Sethi

USA

ABSTRACT

The advent of blockchain technology has fundamentally changed digital identity management through secure and self-sovereign identity (SSI) systems. This paper aims to examine the social consequences of these identity systems, especially concerning the more marginalized groups such as those living as homeless or refugee populations. This works relies on literature review and personal experience gained through the VerifiD project at the UBC Blockathon for Social Good by analysing governance and implementation of systems, privacy, and regulatory issues. The paper also discusses North American cases to demonstrate the possibilities of using the system in practice and the attendant obstacles to its implementation and the ethical issues that arise.

***Corresponding author**

Simran Sethi, USA.

Received: April 11, 2024; **Accepted:** April 18, 2024, **Published:** April 25, 2024

Keywords: Blockchain Based Identity, Self Sovereign Identity (SSI), Homeless Populations, Refugee Identity, Privacy and Data Control, VerifiD Project, Decentralized Governance, Regulatory Compliance, Digital Divide, Token Incentives, User Adoption, Ethical Data Usage, Hybrid Governance Models, Stakeholder Collaboration

Introduction

It is necessary to have a digital identity to access social services, financial services, and even healthcare. Nevertheless, vast portions of the global populace remain unduly identified, thus being disenfranchised from vital services and making socio-economic movement exceedingly cumbersome [1]. Over the past ten years, countless efforts have been trying to use a host of technologies to close this identity gap. Particular attention has been paid to blockchain-based digital systems because they promise to be secure, decentralized, and user centered in short, they seem to promise a Self Sovereign Identity (SSI) [2].

Traditional centralized systems are far more rigid as they depend on a single trusted authority for identity verification. Unlike those approaches, this new system employs cryptographic methods, distributed ledgers, and tokenization to achieve identity verification. The blockchain-based identity system aims to solve and grant concerns of privacy, control over one's data, and credentials disclosure, data integrity, and user empowerment. However, there are still concerns about regulatory issues, equitable access, and the overarching impact on vulnerable social groups.

The issue of social impacts revolving around blockchain-based digital revolves around the most vulnerable populations such as homeless and refugees. The paper analyzes literature, directly or indirectly related to the topic and includes lessons learned from VerifiD project from UBC Blockathon for Social Good in governance, implementation challenges, ethical considerations, and usability. It accentuates the need to exercise caution in the real deployment of the technologies based on these guiding principles, while illustrating the transformative potential accompanying those technologies.

Background on Blockchain-Based Identity Systems

Key Concepts

Block chains primary function is to store transactions between users on a distributed ledger blockchain networks without any possibility for tampering. This translates to identity management as the ability to design identity tokens that are both authenticable and indelible. Conventional identity management is usually cloud-based, relying on an authoritative registrar like government registries and private companies to manage identity information. In comparison, systems based on blockchain grant the users the ability to sign and share parts of their identities with authorized users, placing control at the hands of the users themselves.

Self-Sovereign Identity (SSI)

A salient feature of blockchain enabled identity systems is Self Sovereign Identity (SSI) which allows users to own their digital identities and delete them when they choose to without requiring a service provider to validate their passport, credit car or any digital identity and asset they possess [2, 4]. SSI allows the ability to restrict the range of information that can be presented, hence the risk of unnecessary data being revealed is lessened. This is very useful for at-risk groups who tend to have intricate security and confidentiality issues.

Security and Privacy Mechanisms

The public key infrastructure (PKI) is a form of cryptography used by blockchain to protect the authenticity of users and information [3]. Although blockchain ledgers can contain proof of identity records like credential hashes, sensitive information is usually kept off-chain to ensure privacy. Using these techniques, blockchain solutions can reduce data breaches and unwanted access by employing on-chain verification methods and storing additional data off-chain.

Broader Social Implications

These systems can create a societal impact in addition to the most straightforward operational efficiency. Identity based on blockchain technology has the potential to remove social discrimination by assisting the unbanked to gain access to basic banking, refugees to retain educational or medical credentials, and the homeless to confirm eligibility for aid [1, 5]. Whatever the future benefits that are possible, however, can only materialize if issues of inclusiveness, regulatory compliance, and development of appropriate governance frameworks are addressed, which is a major challenge.

Table 1: Comparison of Traditional ID, Centralized Digital ID, and Blockchain-Based ID

Aspect	Traditional ID	Centralized Digital ID	Blockchain-Based ID
Issuing Authority	Government or institution	Single trusted institution or consortium	Decentralized network of stakeholders
Data Storage	Paper-based or centralized DB	Centralized servers (institution-controlled)	Distributed ledger with cryptographic references
User Control Over Data	Minimal	Limited (subject to provider policies)	High (self-sovereign credentials, selective disclosure)
Security & Tamper Resistance	Physical security, forgery risk	Relies on institutional cybersecurity	Cryptographic immutability, peer-validated transactions
Accessibility	Often requires in-person renewal	Dependent on internet/device but might be widely adopted if mandated	Requires reliable internet/device, but portable once established
Scalability	Large-scale (but slow to update)	Potentially high if well funded; limited by central authority	Potentially global, but subject to network constraints and standardization
Trust Model	Trust in issuing body	Trust in the central authority/ consortium	Trust distributed across the network (consensus-driven)
Example	Government ID, Passport	Bank-based digital ID, Single-sign-on systems (e.g., social media login)	SSI platforms (e.g., Hyperledger Indy, Ethereum-based ID solutions)

Literature Review

Governance and Societal Impact of SSI

Self-Sovereign Identity Systems introduce novel frameworks of governance that regulate the relations between end-users, issuers, and verifiers in a decentralized manner. Gans et al. [6] explain that, SSI may indeed promote privacy, but it also creates a need for hybrid governance models which accommodate community standards alongside regulatory frameworks. Effective governance structures should enable freedom to self-manage identities while constraining identity fraud, exclusion, and the inappropriate handling of sensitive information. Concerns are particularly heightened for vulnerable populations who could be further victimized through data breaches and abuse of their data [3].

Blockchain for Homeless Populations

As part of research done in Austin, Texas, Khurshid and Gadnis recommended the use of blockchain to form digital identities that can be carried around conveniently by homeless individuals [7]. The authors argue that this strategy diminishes fragmentation and misdiagnosis by integrating identity and health records from various providers into one system. After that trial study, Khurshid et al. reported that while the blockchain solution facilitated service access, privacy and usability remained as critical issues [8]. The majority of homeless people do not own a smartphone nor have the required skills to use modern technology, which makes deployment of these blockchain-based measures more impactful and challenging.

Digital Identity in Canada

Canada has emerged as a frontrunner when it comes to experimenting with block chain-based identity solutions. Boysen discusses how an identity solution has been built using a Verified. Me platform that was developed by the collaboration of multiple technology firms and financial institutions to offer secure, user friendly digital identities [9]. Canada as a whole has moderately effective regulations and is more focused on consumer-centric policies which are good, but inter-institutional cooperation and actual usage by people are barriers. Apart from that, some groups, like Indigenous peoples living in the hinterlands, continue to have severe infrastructure gaps which excludes them from joining the digital identity ecosystem [9].

Refugee and Migrant Identity Systems

Both groups are issued little official documentation and are met with extensive administrative challenges in the host country. Cheesman issues a critique on the use of SSI in refugee management stating that it constitutes a self sovereign identity, however, it is ineffective if hosting organizations or governments restrict the individual to a set of automated predetermined procedures. Corte-Real et al [10]. speak of blockchain as a method of providing health records which is portable, verifiable, and greatly assists migrants in receiving continuous medical care [11]. But, Madon and Schoemaker's analysis of UNHCR's PRIMES system presents an alternative to the aid distribution problem through identity digitization [12]. Despite the positive side of enhanced access using technology, sensitive health data put the subjects of digital surveillance at risk and introduce concern about the misuse of such sensitive information.

Case Study: VerifiD Project

VerifiD stems from the UBC Blockathon for social good which aimed at using blockchain technology to solve humanitarian issues. We will discuss how VerifiD was used in combination with proof-of-concept system design and deployment strategies focusing on the homeless population in Vancouver.

Objectives and Design

VerifiD set out to develop a self-sovereign, portable identity platform that would help service-scarce homeless folks as they

seek social support services.

Decentralized Identity Verification
All participants would set up a digital profile based on a permissioned blockchain. Service providers like shelters and clinics would have to issue verification credentials to confirm the person's identity and service history which would all be stored on-chain and off-chain references.

Pre Certification by Community
Understanding the requirement of community trust, VerifiD employed peer verification. Non-profit shelters and healthcare providers were allowed to act as trusted introducers and give initial proofs of identity. By doing so, the model aimed to solve the problem of homeless people, who do not possess government-issued IDs that act as a restriction.

Tokenized Incentives
Users and service providers received incentives for engaging through the self-contained token economy. For example, a user could receive a token for credentialing themselves at a healthcare clinic. They would, in turn, be able to redeem tokens for hygiene items or transit cards, thus increasing usage of the platform.

Implementation Approach at UBC Blockathon
During an interdisciplinary hackathon, developers, social workers, and students collaborated over the weekend with the aim of creating a minimum viable product (MVP). A Hyperledger Fabric network was used for the project, selected for its permissioned architecture and enterprise level features:

- User App Interface: A mobile prototype enabled users to view and manage their VerifiD profiles, manage their credentials, and choose when to share information.
- Issuer Portal: Social service organizations and shelters could issue and validate credentials using a web-based dashboard.
- Smart Contracts: Branded chain code handled the issuance, verification, and token economy balance logic alongside credential issuance.

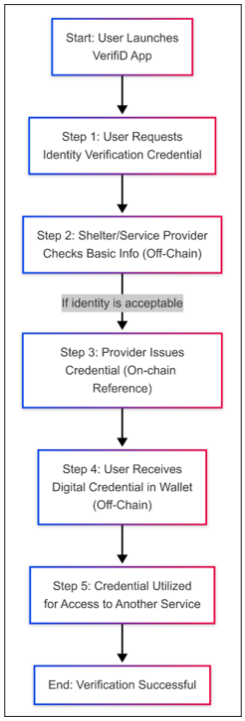

Figure 1: User Verification Process

A basic KYC (Know Your Customer) layer was added in compliance with Canadian regulations, as the team was aware that further alignment with regulations would be necessary for larger scale production deployment.

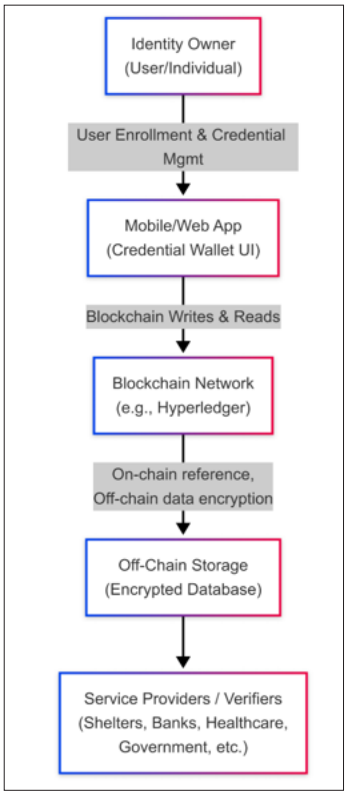

Figure 2: High Level System Architecture

Challenges and Lessons Learned
Data Privacy Concerns
Although participants and social service providers had the capability to store sensitive information off-chain, there was concern regarding the potential misuse or breach of the data. Ensuring that access to data was truly user controlled proved important, particularly from the perspective of a social service agency, but increased the technical challenges.

Obstructions Due to Compliance
Canada has approached the matter of digital identity in a positive manner. However, the compliance requirements for ID on the blockchain are still in development. Consequently, the VerifiD project had to work under vague legal conditions, especially concerning personal data handling as well as the use of tokenized engagement methods.

User Problems With Adoption
A major problem was that a significant number of homeless people do not have regular access to smartphones and the internet. This greatly diminishes the effectiveness of a must mobile dependent solution. The team thought about other options like using physical NFC cards that could be associated with on chain credentials. However, cost, card loss, and scalability raised concerns.

Involvement of the Community
Working with regional shelters and non profit organizations showed the significance of building together. It is critical to engage the stakeholders robustly when new technology is introduced, or else the resulting system may be ineffective to the needs and

constraints of the homeless population. Trust building and defining use cases with social workers, service providers, and potential users broadly is critical.

Through all these barriers, the VerifiD project showed how a blockchain-based identity can integrate numerous identity proofs and records to provide services to an ultra-sensitive segment of the population.

Additional Considerations and Ethical Implications

The problem that most literature and the VerifiD case study point out is the digital divide. Those who have no reliable access to the internet or smartphones may find it hard to engage in a blockchain-enabled identity ecosystem [3, 8]. The homeless population faces even worse challenges like low digital skills, lack of stable housing, and strong do not trust "formal" systems. Failure to address these issues will put these people in a highly vulnerable state where they will be more marginalized as major services move towards a more digital world which they cannot access.

Sovereignty Over One's Data and Consent

The essence of self-sovereign identity (SSI) is that a user has control over their identity data and is able to give well-informed consent before receiving their data shared through credentials. Still, the epistemic tension between service providers and users as a dependency relationship needs to be tackled such that coercive consent is avoided [10]. In cases where social services or help rely on the sharing of data, there may be a presumption that more information will be given, which the user is not comfortable with. Ethical design must always be aimed at preventing user exploitation while ensuring transparency over data and granting the users simple, straightforward ways to decide how the data is altered or removed.

Regulatory and Legal Complexity

The challenges related to the regulation of identity blockchain seems to be most problematic in Canada. The country seems to be having issues with an amalgamation of e-signatures, data protection, and token economies legislations from various jurisdictions. Compliance with PIPEDA while dealing with federal and provincial WIP law offending regulations was one of the consequences of the VerifiD project. The situation is further complicated by the cross border character of blockchain networks. Different jurisdictions contain nodes capable of replicating or validating data, therefore, ascertaining liability frameworks and legal ambiguity is essential to safeguarding users and adopting innovative technologies.

Ethical Use of Biometric Data

Some problems stemming from surveillance and data permanence are present in VerifiD and other blockchain based identity systems that utilize biometric identifiers such as fingerprints and face scans. When sensitive data gets compromised, it can never truly be altered out eliminating passwords. Once a person is deemed as marginalized changing anything becomes a problem. Life-long vulnerability is an issue some deemed leaders must step up against. Biometric governance is tricky to combine with privacy, encryption, and design in a way that brings forth the best resolution and ensures the governing body is never stumped on how the data is gained, held, or used.

Interoperability and Scalability

For blockchain-based identity solutions to deliver maximum social value, they need to be integrated with governmental databases, institutions, and healthcare services. These aspects may hinder the integration process. Additionally, factors related to public blockchains' scalability and efficient use of resources, like high fees relating to transactions and low block throughput, block large scale implementation. Permissioned or hybrid blockchains like the ones used by VerifiD are more easily scalable but are more closed in regard to the number and type of participants.

Future Research Directions

Methods for ensuring User Adoption

There has been ongoing research in the efficient onboarding and adoption processes of currently underserved users. Community training, the design of user interfaces, and even new access devices like biometric key fobs and NFC cards need more study in how they accept and implement these changes. Moreover, supporting more than one language and using cultural design elements can greatly assist in the integration of refugees and migrants.

Policy and Governance Frameworks

Trust frameworks for the management of a person's digital identity have not been fully developed by Public-Private partnerships. Governments may provide a commanding atmosphere that has sufficient rules and standards while the creativity of the private sector can provide friendly user support services. Further research is needed to provide new models of co-governance and analyze how adaptable they are to local societal realities without imposing strict top-down community approved frameworks.

AI Technologies Integration

There is AI supervised machine learning that can help with risk analysis, fraud detection, and credentialing. Yet, identity management solutions that are AI enabled are not without troubles, especially algorithmic bias discrimination against already disadvantaged populations. The merging of blockchain based identities with Zero-Knowledge Proofs (ZKPs) possess identity attributes of promisingpy privacy-preserving data verification while limiting sensitive user information disclosure. How the integration of ZKPs into AI solutions without compromising efficiency, security, and privacy remains a question to explore for future research.

Longitudinal Impact Studies

While some initial pilot projects such as VerifiD have been encouraging, more robust longitudinal impact studies are needed in the case of social impacts of blockchain identity systems. Such studies may look at measuring recidivism of the homeless, employment longitudinal studies, or continuity of care. Both the policymakers and the technology experts can measure user satisfaction, costs, and the effectiveness of scalability and durability of the systems and solutions put in place [13].

Conclusion

The implementation of systems of digital identity management using the blockchain technology may provide a different solution to the problem of identity abuse of the most vulnerable groups. Decentralized holders of credential and user attribute containers remarkabley improve resource manageability, reduce service providers' workload, and aid in establishing trust between citizens and the government. The VerifiD project is a part of the UBC Blockathon for Social Good that demonstrates the power of well organized community initiatives in solving issues like homelessness through the provision of secure portable identity systems.

Still, there is some optimism, but the challenges posed to achieving it are equally profound. The other side of the coin of these new technologies is the reality and danger of the digital divide, determining regulatory frameworks, ethical data usage, and determining user adoption. Attempts to find solutions that are workable will need policies, technological changes, input from various players, and multidisciplinary approaches. Only in that way social good guarantees from the blockchain-based digital identity systems will be met. As the borders of research and practice are broadened, there is growing necessity of cooperation between the government and non-profit organizations together with the technological experts in order to package the best solutions and no community is left out in the race towards a digital identity.

References

1. A Gelb, A Diofasi (2017) Identification for development: The biometrics revolution. CGD Working Paper 315: 1-35.
2. C Allen (2016) The path to self-sovereign identity GitHub Essay https://github.com/ChristopherA/self-sovereign-identity
3. M Tobin, D Reed (2017) The inevitable rise of self-sovereign identity. The Sovrin Foundation 1-24.
4. E Abebe, S Ryan, M De Filippi (2021) Digital identity under decentralized governance: A critical analysis in Proc. IEEE Int Conf Blockchain (ICBC) 50-57.
5. M Tobin, D Reed (2017) The inevitable rise of self-sovereign identity. The Sovrin Foundation 1-24.
6. World Bank (2018) The global Findex database: Measuring financial inclusion and the fintech revolution. The World Bank Washington DC Tech Rep https://openknowledge.worldbank.org/entities/publication/ed800062-e062-5a05-acdd-90429d8a5a07.
7. P Gans, J Ubacht, M Janssen (2022) Hybrid governance in self-sovereign identity: Balancing community empowerment and institutional oversight. Gov Inf Quart 39: 4101652.
8. R Khurshid, A Gadnis (2019) Blockchain for homeless: A case study for portable identity management. JMIR Mhealth Uhealth 7: 8-12378.
9. R Khurshid, K Rajeswaren, M. Andrews (2020) Evaluating the feasibility of block chain based digital ID in a homeless community. IEEE Access 8: 139217-139228.
10. S Boysen Verified.Me and the future of digital identity in Canada Canadian Banking Insights Report Toronto 15-28.
11. M Cheesman (2020) Self sovereignty for refugees? The contested horizons of digital identity Geoforum 111: 134-144.
12. M Corte Real, G Batista, A Dias, H Gamboa (2022) Using block chain to provide healthcare continuity for migrant populations in Proc. IEEE Conf Emerging Tech for Healthcare (CE-TH) 109-115.
13. S Madon, E Schoemaker (2021) UNHCR's PRIMES: Dilemmas in implementing digital identity for refugees. Dev Policy Rev 39: 229-247.