Journal of Orange Technology (JOT)
Vol. 2, No. 2, April, 2026, pp. 105−116
E-ISSN: XXXX-XXXX | P-ISSN: XXXX-XXXX, DOI:10.34306

Blockchain for Financial Identity in Developing Nations

Sri Watini[1], Ora Plane Maria Daeli[2], Syahyono[3], Ramzi Zainum Ikhsan[4*], Oliver Sauntos[5]
[1]Early Childhood Education Programs, University of Panca Sakti Bekasi, Indonesia
[2]Faculty of Teacher Training and Education, University of Raharja, Indonesia
[3]Department of Management, Universitas Islam 45 Bekasi, Indonesia
[4]Alfabet Inkubator Group, Indonesia
[5]Pandawan Incorporation, New Zealand
[1]srie.watini@gmail.com, [2]ora.maria@rahara.info, [3]syahyono@unisbekasi.ac.id, [4]ramzi.zainum@raharja.info,
[5]oliversauntos@pandawan.ac.nz
***Corresponding Author**

Article Info

Article history:

Submission February 4, 2026
Revised February 23, 2026
Accepted March 9, 2026
Published March 30, 2026

Keywords:

Blockchain
Self-Sovereign Identity
Financial Inclusion
Digital Identity
Developing Nations

ABSTRACT

The absence of formal financial identity remains a major barrier to financial inclusion in developing nations. Existing centralized identity systems are often vulnerable to fraud, data breaches, and third-party control, leading to low public trust and limited access to financial services. Blockchain technology offers a decentralized alternative through the concept of Self-Sovereign Identity (SSI), which enables individuals to own and control their personal data securely. **This study aims** to examine how blockchain-based identity systems can address the weaknesses of traditional identity frameworks and to identify the key technical and social challenges in their implementation within developing economies. **Using a qualitative**, case study-based approach, the research analyzes several blockchain-driven digital identity projects across diverse regions. **The findings** indicate that blockchain-enabled SSI improves data security, transparency, and user trust, while enhancing access to financial services. However, challenges related to infrastructure limitations, scalability, and regulatory uncertainty remain significant obstacles. **Overall, blockchain** has the potential to serve as a foundational technology for creating inclusive, secure, and sustainable financial identity systems in developing nations, while offering practical insights for policymakers, regulators, and financial institutions worldwide.

DOI: https://doi.org/10.34306/jot.v2i2.87

1. INTRODUCTION

In many developing nations, the absence of a formal financial identity remains a major barrier to financial inclusion [1]. The lack of adequate civil registration systems prevents millions of individuals from obtaining verifiable identification, thereby excluding them from participating in the formal economy. Without an officially recognized identity, people are unable to open bank accounts, access credit, or engage with regulated financial services [2, 3]. This condition not only restricts individual participation in economic activities but also perpetuates systemic inequality, limiting opportunities for upward social and economic mobility [4]. As a result, large segments of the population remain financially underserved, reinforcing cycles of poverty and marginalization.

The challenge of financial exclusion is further exacerbated by structural inefficiencies within existing identity systems [5]. In many cases, administrative barriers, high costs of registration, and geographical limita-

tions hinder access to official identification. Marginalized populations, including those in rural areas, women, and informal workers, are disproportionately affected by these limitations [6]. Consequently, the inability to establish a verifiable identity becomes not only a technical issue but also a socio-economic constraint that impacts access to essential services such as healthcare, education, and social welfare programs [7, 8]

Existing centralized identity systems, while designed to provide verification and security, often suffer from inherent vulnerabilities such as fraud, data breaches, and misuse of personal information by third parties [9]. These systems are typically controlled by governments or private entities, which can create power imbalances and reduce transparency in how personal data is managed. Moreover, centralized databases are highly attractive targets for cyberattacks, increasing the risk of large-scale data exposure [10]. As a result, trust in centralized identity systems remains low, particularly in regions where governance structures are weak or where past incidents of data misuse have undermined public confidence [4].

In response to these challenges, this study seeks to explore how blockchain-based identity systems can overcome the limitations of traditional, centralized models [11]. The key research questions addressed in this paper are: (1) How does a blockchain-based identity system address the weaknesses of conventional identity frameworks? (2) What are the primary technical and social challenges in implementing blockchain for financial identity in developing nations? and (3) What are the potential long-term benefits of adopting blockchain-based financial identity systems for both individuals and the wider economy? By addressing these questions, the study aims to provide a comprehensive understanding of both the opportunities and constraints associated with this emerging technological approach [12, 13].

The scope of this paper focuses on the application of blockchain and SSI principles to promote financial inclusion. By examining the integration of decentralized technologies in identity management, this research highlights solutions that can enhance data security, empower individuals with greater control over their digital identities, and foster trust in financial systems [14]. The findings are expected to be particularly relevant to policymakers, technology developers, and financial institutions working toward the creation of more secure, transparent, and equitable identity ecosystems [15]. Furthermore, this study aligns with the global development agenda, particularly Sustainable Development Goal (SDG) 9, which emphasizes strengthening digital infrastructure and promoting innovation, and SDGs 16, which focuses on building trustworthy, transparent, and inclusive institutions [16]. The integration of blockchain based identity systems thus represents a strategic pathway toward achieving inclusive and accountable digital transformation [17].

2. LITERATURE REVIEW

2.1. Financial Exclusion and Identity Barriers

In developing countries, financial exclusion is often rooted in a lack of formal identity. Many people are excluded from civil registration systems; births may go unrecorded, or people may lack official documentation such as national ID cards or birth certificates [18]. Without verifiable identity, individuals are unable to open bank accounts, access credit, apply for insurance, or participate fully in the formal economy. This absence not only limits their economic opportunities, but also increases vulnerability to exploitation and systemic inequality [16]. Literature shows that identity gaps lead to higher transaction costs, risk of fraud, and inefficiencies: banks and financial institutions are reluctant to serve customers whose identity credentials cannot be reliably verified (due to the risk of money laundering, fraud, or regulatory non-compliance) [17]. The barriers are not only technical or bureaucratic, but also social: marginalized populations, rural communities, women, stateless persons may have less awareness of or access to identity documentation, face higher costs (travel, fees), or distrust institutions [19].

2.2. Principles of Self-Sovereign Identity (SSI)

SSI is an identity model in which individuals fully own, control, and manage their digital identity, rather than relying on centralized authorities or intermediaries [20, 21]. Core principles identified in the literature include: user ownership and control over personal data; privacy, including selective disclosure (only sharing what is necessary); interoperability across different systems; portability, so identity credentials can move across platforms or borders; persistence (the identity endures over time); consent, meaning users explicitly decide how and when identity data is used; minimal disclosure of personal data; and preservation of security and integrity (e.g. using cryptographic methods) [22]. SSI differs from traditional identity models (centralized government registries, federated identity via corporations or banks, etc.) in that traditional systems typically have a single or small set of authorities controlling identity issuance, verification, storage, and

often have centralized databases that are points of weakness (for hacking, misuse, or corruption) [23, 24]. Blockchain (or other distributed ledger technologies) are often seen in the literature as enablers for SSI by providing features like immutability, decentralization, verifiable credentials, and public / private key infrastructure. To illustrate the underpinning architecture of the distributed ledger that enables SSI, Figure 1 shows a network of interconnected nodes sharing a common ledger [25].

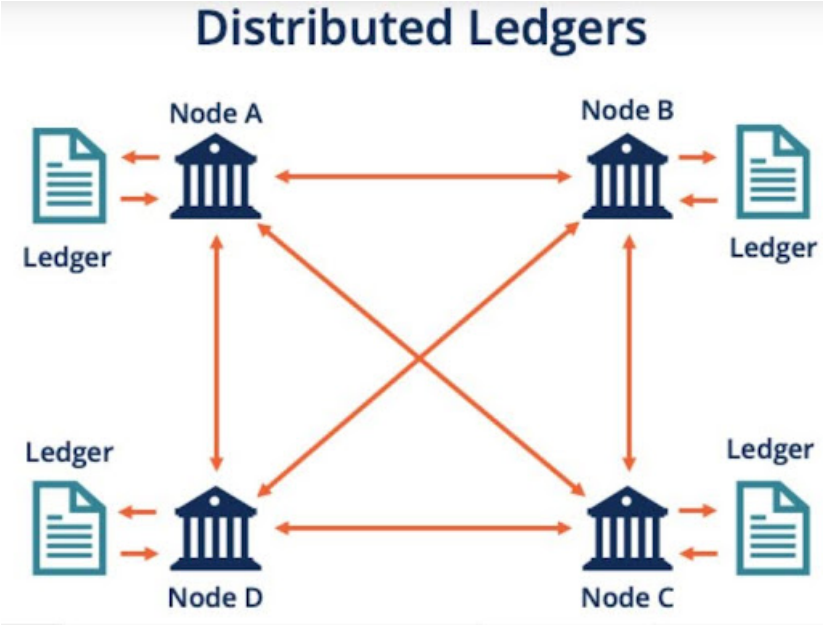

Figure 1. Distributed-ledger network showing interconnected nodes each storing a synchronized ledger

The diagram in Figure 1 depicts the core architecture of a distributed ledger system: multiple peer nodes maintain synchronized copies of the ledger, communicate via a peer-to-peer network, and jointly validate updates through a consensus mechanism [26, 27]. This structure eliminates a single point of control, increases resilience and trust, and forms the technical foundation upon which SSI systems can be built. In an SSI context, credentials can be anchored in such a ledger, while individuals retain control of their identity data and selectively disclose only what is required [28]. By leveraging the decentralized, tamper-resistant, and transparent features of distributed ledger technology, the model addresses many of the identity-barriers described earlier by enabling verifiable identity without relying on a central registry. This allows credentials to be anchored in a decentralized registry, while private or sensitive data remain under the control of the individual [29].

Before delving into practical implementations, it is essential to understand how SSI fundamentally differs from traditional identity frameworks. While conventional systems rely heavily on centralized authorities such as governments or financial institutions to issue, verify, and manage identity data, SSI introduces a decentralized model that places control directly in the hands of individuals [30, 31]. This paradigm shift enhances privacy, interoperability, and user empowerment while significantly reducing risks associated with centralized data storage. The comparison in Table 1 summarizes the key distinctions between traditional identity systems and SSI [32].

Table 1. Comparison Between Traditional Identity Systems and SSI

Aspect	**Traditional Identity Systems**	**SSI**
Control of Data	Centralized — controlled by governments or institutions.	Decentralized — controlled by individuals through private keys

Data Storage	Stored in centralized databases vulnerable to breaches.	Stored across distributed ledgers; sensitive data kept with the user.
Privacy	Limited; personal data often shared broadly without consent.	High; selective disclosure and user consent mechanisms.
Interoperability	Restricted between systems and jurisdictions.	Designed for interoperability across platforms and borders.
Security Risks	Single point of failure; prone to hacking and corruption.	Distributed and tamper-resistant through cryptographic verification.
User Empowerment	Users depend on third parties for verification and access.	Users manage their own digital identity and credentials.

As illustrated in Table 1, SSI frameworks redefine the traditional balance of power in identity management by decentralizing control and enhancing user autonomy [33]. This structural shift mitigates vulnerabilities such as data breaches and unauthorized access while fostering interoperability across institutions and borders. However, the transition to SSI also introduces new responsibilities for users, including secure key management and digital literacy, which must be addressed to ensure inclusivity and long-term adoption [34, 35]. Literature also highlights several challenges: key management (if a private key is lost, identity may be irretrievable), usability and accessibility for people with low digital literacy, regulatory and legal frameworks (governments may resist relinquishing control or require oversight), infrastructure issues (internet access, devices), and trust (both of the technology, and of verifiers to accept credentials that do not come from centralized or well-known authorities) [36, 37].

2.3. Existing Blockchain-Based Identity Projects

There are many pilot projects and implementations in real-world settings which attempt to use blockchain/SSI (or related decentralized identity technologies) to overcome identity barriers. Bhutan has launched a National Digital Identity (NDI) that follows SSI principles, allowing citizens to control their credentials via a mobile wallet. Citizens can decide what data to share, and credentials are cryptographically anchored to blockchain. The system was built initially with Hyperledger Indy and later moved to Polygon and CREDEBL. It has been integrated with banks, telecoms, and government portals, and is used for KYC, SIM activations, and other services. In addition, the study "Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity" found that SSI can make KYC processes more efficient, compliant with privacy regulations, and more convenient, while reducing data silos and dependency on centralized systems. Furthermore, several survey papers review blockchain-based identity management systems. For example, "Blockchain-based identity management systems: A review" outlines how identity management solutions are evolving with blockchain, highlighting benefits such as user control and decentralization, as well as recurring challenges including legal compliance, scalability, and trust verification.

3. RESEARCH METHODS

3.1. Research Approach

This study adopts a qualitative, case study-based approach, as the topic of blockchain for financial identity in developing nations is exploratory and complex, requiring an in-depth and contextual understanding of how such systems operate in real-world environments, the challenges encountered, and the factors influencing their success or failure. Qualitative methods enable the collection of rich, descriptive data from various stakeholders, allowing for a comprehensive interpretation of social, technical, and institutional dimensions that are often not captured through purely quantitative approaches. This approach is particularly suitable for examining emerging technologies like blockchain-based identity systems, where standardized evaluation frameworks are still evolving, and where contextual factors such as regulatory conditions, infrastructure readiness, and user

trust play a critical role in adoption. The study relies on secondary data sources, including academic literature, technical reports, policy documents, and documented case studies, which are systematically analyzed using thematic analysis to identify key patterns, challenges, and best practices across different implementations. In addition, a comparative perspective is employed to examine multiple cases, enabling a broader understanding of similarities and differences in implementation strategies and outcomes, thereby strengthening the robustness and generalizability of the findings. To illustrate the workflow of such systems in practice, a schematic overview is provided below, highlighting the interaction between users, identity providers, verification entities, and blockchain infrastructure within a decentralized identity ecosystem.

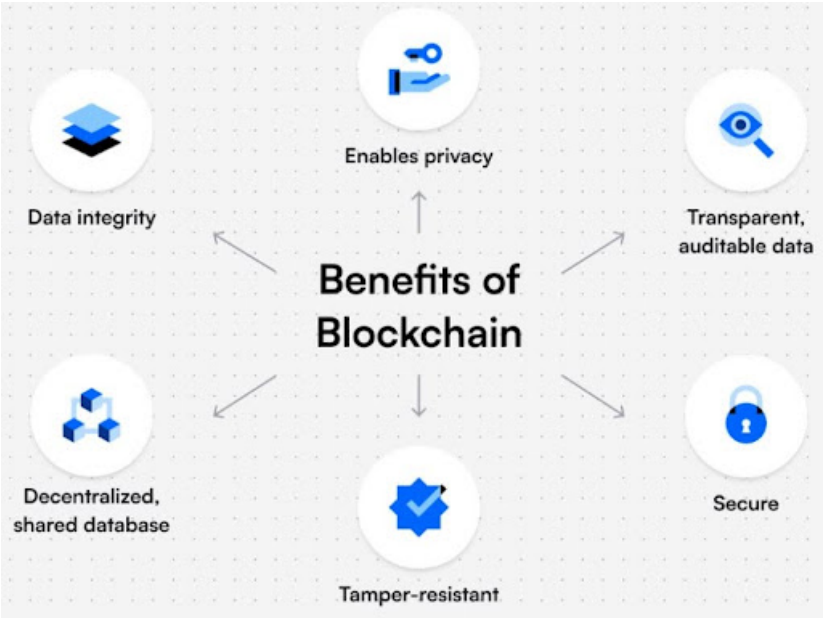

Figure 2. Workflow of a blockchain-based digital identity system for financial inclusion in developing nations, illustrating the sequence.

Figure 2 depicts the full lifecycle of the blockchain-based financial identity system from issuer registration through user verification and certificate issuance highlighting the socio-technical, institutional, and regulatory layers embedded in the implementation process. Moreover, this methodological choice aligns with contemporary scholarship: [9] (2022) emphasize that case studies are most fitting when the line between the phenomenon studied and the real-life context in which it occurs becomes difficult to define clearly. By selecting multiple case studies, this research design further strengthens analytic generalization through pattern comparison across different settings. Given that blockchain identity systems encompass socio-technical interactions, institutional limitations, regulatory pressures, and human behaviors, the qualitative case study method enables not just an account of what occurs, but an exploration of why and how revealing processes, emergent adaptations, contingent factors, and context-specific dynamics.

3.2. Case Study Selection

To ensure balanced and insightful findings, the research will select three to five case studies. The selection criteria include:

- Geographic diversity: projects will be chosen from distinct developing regions (for example, Sub-Saharan Africa, South Asia, Southeast Asia, Latin America) to capture variation in socio-cultural, regulatory, and infrastructural conditions.
- Project maturity: only projects that have been operational for at least 1–2 years, so that observable outcomes, challenges, and lessons learned can be identified.
- Scale and scope variation: include both small-scale pilot initiatives and larger system implementations; include projects led by NGOs or multilateral organizations, as well as those by government or private sector; possibly involving different blockchain platforms, SSI models, or identity architectures.

This diversity helps in distinguishing which factors are context-specific and which may generalize across settings. In forming this selection strategy, this research draws on recent methodological literature. Mtisi (2022), for example, underscores that purposive or criterion sampling is essential in qualitative case study research to select cases that are "information-rich" and relevant to the phenomenon under study, rather than relying on random sampling. Additionally, utilizing multiple case studies allows for comparison across contexts and helps identify both consistent themes and contextual divergence, supporting greater analytic credibility.

3.3. Data Collection

Data will be collected from multiple sources for each case to allow triangulation and enhance validity. The methods and sources include documentary materials such as project reports, white papers, policy documents, technical specifications, and evaluation reports, which provide insights into system architecture, timelines, and outcomes. In addition, academic and technical literature including peer-reviewed articles, conference papers, and theses will be used to analyze and contextualize blockchain-based identity systems and similar SSI frameworks. Media and public sources, such as news articles, blogs, press releases, community forums, and regulatory announcements, will also be examined to capture public perception, controversies, and implementation challenges. Furthermore, semi-structured interviews will be conducted with carefully selected informants, including project leaders, technical architects, regulatory stakeholders, and end-users or community representatives. These interviews will explore key aspects such as motivations, system design, user experience, adoption barriers, trust and privacy concerns, institutional dynamics, and system evolution over time.

For each case study, the research aims to involve approximately 5–10 informants representing diverse roles, including implementers, policymakers or regulators, and users. Informants will be selected purposively based on their direct involvement or experience with the system. Interviews may be conducted either in person or remotely, recorded with consent, transcribed verbatim, and anonymized to ensure confidentiality. Data collection will follow an iterative process and continue until saturation is reached, meaning that additional interviews or documents no longer yield new themes or insights. This determination will be guided by continuous monitoring of emerging codes and thematic patterns. As noted by [19] (2021), saturation should be aligned with the research questions, theoretical framework, and analytical strategy of the study, [22] (2024) suggest that near saturation can sometimes be achieved earlier depending on coding structure and interview design. Where feasible, field observations will also be conducted through visits to project sites or user communities to examine real-world implementation contexts, including infrastructure conditions and user interactions, thereby enriching the overall data with contextual depth.

3.4. Data Analysis

Thematic analysis will serve as the primary analytic method in this study, following a structured and systematic multi-step process designed to ensure analytical rigor, depth, and interpretive clarity. The process begins with familiarization, which involves repeated and immersive engagement with transcripts, documents, media materials, and observation notes. During this stage, the researcher documents initial impressions, recurring patterns, and emerging ideas through reflective memos, facilitating a deeper understanding of the data context and its relevance to the research questions. This is followed by generating initial codes, where meaningful data fragments are systematically labeled according to key concepts such as trust, interoperability, privacy, user behavior, and governance. Coding may be conducted manually or supported by qualitative data analysis software such as NVivo or Atlas.ti to enhance organization, traceability, and consistency. Subsequently, related codes are grouped to identify broader patterns and to search for themes, leading to the development of a preliminary codebook for each case study. These candidate themes are then critically reviewed and refined to ensure internal coherence, conceptual clarity, and distinct boundaries between themes, while also being validated against the entire dataset rather than relying solely on coded segments. Following this, themes are clearly defined and named through a process of refining their scope, selecting representative data extracts, and assigning meaningful and analytically precise labels. The final stage involves producing the thematic report, where findings are presented through a coherent narrative supported by illustrative quotations, cross-case comparisons, and explicit linkages to the research questions and existing literature, thereby ensuring both descriptive richness and analytical depth.

To enhance the trustworthiness and credibility of the analysis, multiple validation strategies are systematically applied throughout the research process. Triangulation is employed to cross-verify findings across diverse data sources, including interviews, documents, media content, and observations, thereby reducing potential bias and strengthening the reliability of interpretations. Member checking is conducted by sharing

preliminary themes and interpretations with selected informants to ensure that the findings accurately reflect participants' perspectives and lived experiences. An audit trail is maintained to document all stages of the analytical process, including coding decisions, theme development, and reflective memos, ensuring transparency, accountability, and replicability. In addition, reflexivity is continuously practiced, with the researcher critically reflecting on personal assumptions, positionality, and potential biases to minimize subjective influence on data interpretation. Furthermore, to complement the thematic analysis and to provide a clearer conceptual understanding of the relationships examined in this study, a visual framework is incorporated, illustrating how the key elements of the blockchain-based identity system interact within a broader analytical structure. This framework not only supports the interpretation of findings but also strengthens the integration between empirical results and theoretical insights presented in the subsequent sections.

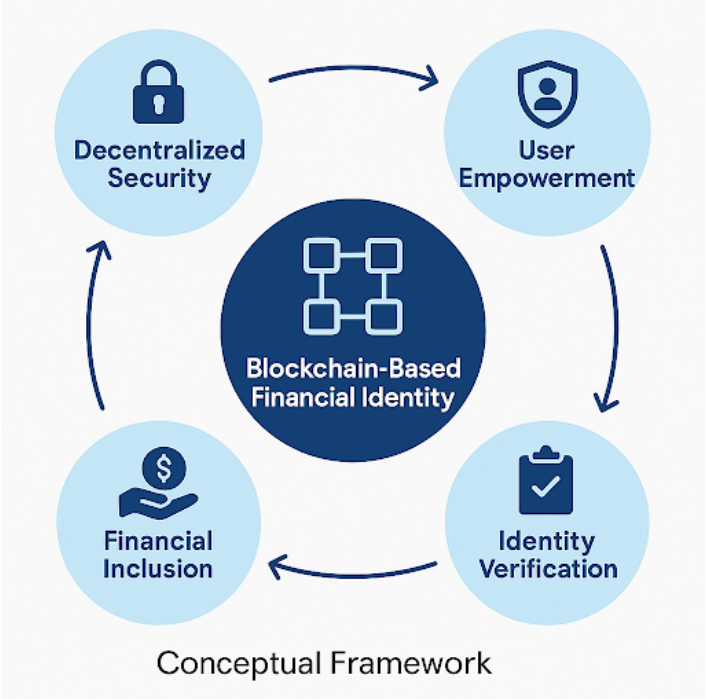

Figure 3. Conceptual Framework of Blockchain-Based Financial Identity System

This conceptual framework illustrates how decentralized security, user control, identity verification, and financial inclusion interact within a blockchain-enabled identity ecosystem. As shown in Figure 3, decentralized security forms the foundational layer by ensuring data integrity, immutability, and resistance to single points of failure. Building on this, user control enabled through SSI allows individuals to manage and selectively disclose their personal data, reinforcing privacy and autonomy. These two components collectively support a more reliable and efficient identity verification process, where credentials can be authenticated without reliance on centralized authorities. In turn, improved identity verification facilitates broader financial inclusion by lowering entry barriers to financial services such as banking, credit access, and digital transactions. The framework serves as a guiding structure that links the technological components of SSI with broader socioeconomic outcomes, demonstrating how technological design choices translate into real-world impacts. Furthermore, Figure 3 provides a holistic view of the interdependencies between technical, social, and institutional elements, supporting the analysis conducted in the subsequent Discussion section.

4. RESULTS AND DISCUSSION

4.1. Results

The analysis of selected case studies reveals several important findings regarding the implementation of blockchain-based financial identity systems in developing nations. First, blockchain-based identity solutions significantly enhance trust and transparency in identity verification processes. The decentralized nature of

blockchain reduces dependence on centralized authorities, which are often perceived as unreliable or vulnerable to data breaches. Second, the implementation of SSI demonstrates a strong impact on user control and data privacy. Users are able to selectively disclose their identity attributes, which minimizes unnecessary data exposure and strengthens personal data protection.

Third, blockchain-based systems contribute to improved access to financial services, particularly in onboarding processes such as Know Your Customer (KYC). Individuals who previously lacked formal identity are able to participate in digital financial ecosystems more easily. However, the results also indicate that adoption remains uneven due to several external constraints. Key barriers include limited digital infrastructure, low levels of digital literacy, and the absence of clear regulatory frameworks in many developing countries.

4.2. Discussion

4.2.1. The Blockchain Advantage

Blockchain's decentralized architecture eliminates a single point of failure, which represents a major vulnerability in traditional centralized identity systems. Systems such as Self-Sovereign Identity (SSI) built on blockchain distribute identity verification across multiple nodes, ensuring that no single authority holds complete control over data or decision-making processes. In addition, the immutability feature of blockchain ensures that once identity credentials are recorded, they cannot be altered or fraudulently tampered with, thereby creating a tamper-proof ledger that enhances data integrity and system reliability. Existing literature supports these advantages; for instance, [21] (2024), in their analysis of various SSI frameworks, highlight that decentralization and cryptographically verifiable credentials are fundamental to achieving transparency and trust in identity systems. Furthermore, SSI enhances user control and security by enabling individuals to gain ownership over their identity data and determine which attributes to share, with whom, and under what conditions. This reduces reliance on intermediaries and mitigates risks such as identity theft and unauthorized data exposure. Policy & Society (2022) argues that blockchain-based identity management provides a level of user autonomy that is not achievable in centralized databases, which are more vulnerable to breaches and misuse. Moreover, mechanisms such as verifiable credentials and decentralized identifiers (DIDs) reinforce security and privacy by design, further strengthening trust and reliability within the system.

4.2.2. The Challenges of Implementation

Despite its advantages, blockchain-based identity systems face significant technical, infrastructural, and regulatory challenges in developing nations. From a technical perspective, scalability remains a major concern, as expanding systems to accommodate large user bases and high transaction volumes often results in increased latency, higher transaction costs, and greater energy consumption. Public blockchain networks, in particular, experience throughput limitations when multiple users perform operations simultaneously, as highlighted in "Blockchain technology and application: an overview," which notes that performance tends to decline as data volume increases. In addition to technical constraints, infrastructural limitations such as unreliable internet connectivity, unstable power supply, and limited access to digital devices further hinder adoption in many developing regions. Beyond these issues, regulatory and governance challenges also present substantial barriers, as legal frameworks frequently lag behind technological developments in blockchain and Self-Sovereign Identity (SSI). Uncertainty regarding data ownership, liability, identity verification standards, smart contract enforceability, and privacy rights, including the "right to be forgotten," creates risks for stakeholders and slows implementation. The systematic review "Blockchain Implementation Challenges in Developing Countries" identifies regulatory gaps as a key factor contributing to stakeholder hesitation, while Policy & Society (2022) emphasizes that trust in such systems depends not only on technological robustness but also on regulatory legitimacy and institutional governance. These interconnected challenges demonstrate that, despite its potential, the successful implementation of blockchain-based identity systems requires alignment between technological capability, infrastructural readiness, and regulatory support, as summarized in Table 2.

Table 2. Key Challenges in Implementing Blockchain-Based Financial Identity

Category	Specific Challenges
Technical	Scalability issues, high transaction costs, and limited network infrastructure.

Infrastructural	Poor internet connectivity, lack of electricity, and limited access to digital devices.
Regulatory	Unclear legal frameworks, ambiguity in data ownership, and inconsistent privacy laws.
Social	Low digital literacy, public distrust of technology, and fear of surveillance.
Institutional	Resistance from centralized authorities and lack of coordination between institutions.

Table 2 highlights the multidimensional challenges involved in implementing blockchain-based financial identity systems, emphasizing that barriers extend beyond purely technical concerns. From a technical perspective, issues such as scalability limitations, high transaction costs, and insufficient network infrastructure can hinder system performance and widespread usability. On the infrastructural level, inadequate internet connectivity, unreliable electricity, and limited access to digital devices further restrict adoption, particularly in developing regions. The regulatory challenges identified in Table 2 underscore the absence of clear legal frameworks, uncertainty around data ownership, and inconsistent privacy regulations, all of which create risks and hesitation among stakeholders. Additionally, social factors including low digital literacy, lack of public trust, and concerns over surveillance pose significant obstacles to user acceptance. Finally, institutional barriers, such as resistance from centralized authorities and poor inter-organizational coordination, complicate implementation efforts. Overall, as reflected in Table 2, successfully addressing these challenges requires an integrated approach combining technological advancements with supportive policies, education initiatives, and strong collaboration across sectors to ensure sustainable and inclusive adoption.

4.2.3. The Future of Financial Identity

Beyond financial services, blockchain-based identity systems could unlock access to key services that are often out of reach for individuals without formal identity, such as healthcare, education, and participation in democratic processes (voting). The literature supports this potential: the Frontiers in Blockchain study (2024) shows that many SSI frameworks are designed to be interoperable and universally usable, which could allow identity solution portability across sectors, enabling access to social services and public programmes in addition to financial inclusion. Moreover, as countries increasingly digitize public services, a secure and verifiable identity infrastructure could reduce costs, fraud, and administrative friction in distributing welfare, verifying immunizations, issuing school certificates, or enabling remote voting. However, this future requires resolving challenges around regulation, infrastructure, and trust. For instance, developing nations might need to adapt governance models that balance decentralization with accountability and legal oversight.

5. MANAGERIAL IMPLICATIONS

The findings of this study provide important implications for policymakers, financial institutions, and technology developers involved in implementing blockchain-based financial identity systems. For policymakers, the results highlight the urgent need to establish clear and adaptive regulatory frameworks that address data ownership, privacy protection, and legal recognition of decentralized identities. Without regulatory clarity, adoption will remain limited due to uncertainty and risk perceptions among stakeholders. Governments should also invest in digital infrastructure, particularly in underserved areas, to ensure reliable internet connectivity and access to digital devices, which are critical for the successful deployment of blockchain-based identity solutions.

For financial institutions, this study suggests that adopting blockchain-based SSI can significantly enhance customer onboarding processes, particularly in KYC procedures. By leveraging verifiable credentials and decentralized identity verification, institutions can reduce operational costs, minimize fraud risks, and improve customer trust. However, managers must also consider user readiness, including digital literacy and trust in technology, by providing user-friendly interfaces and educational initiatives. Strategic partnerships with governments, fintech companies, and telecom providers are also essential to create interoperable ecosystems that support seamless identity verification across sectors.

For technology developers and system implementers, the study emphasizes the importance of design-

ing scalable, secure, and user-centric identity systems. Technical challenges such as scalability, transaction costs, and system performance must be addressed through appropriate blockchain selection, hybrid architectures, or layer-2 solutions. Additionally, developers should prioritize usability and accessibility to ensure inclusivity, especially for populations with limited technical knowledge. Collaboration across sectors is critical to align technological innovation with real-world needs, ensuring that blockchain-based identity systems are not only technically robust but also socially acceptable, institutionally supported, and sustainable in the long term.

6. CONCLUSION

Blockchain holds substantial potential to overcome identity barriers in developing nations by enabling verifiable financial identities for people who lack formal recognition. Its decentralized and immutable nature helps prevent a single point of failure or tampering, while combining it with SSI architectures empowers individuals with control, privacy, and consent over their personal data. This synergy offers a transformative foundation for creating financial identity systems that are inclusive, resilient, and user-centric.

Nevertheless, realizing that promise faces significant obstacles. Scaling blockchain to national or regional levels often brings prohibitive transaction costs, latency, and high computational demands problems that are magnified in areas with limited infrastructure, intermittent connectivity, or unreliable power. Socioeconomic and regulatory challenges further complicate deployment: ambiguity around data ownership, identity verification standards, and cross-jurisdictional governance discourage both governments and financial institutions from fully embracing such systems. These real-world constraints illustrate that technological innovation must be paired with institutional readiness.

Despite these challenges, the downstream impact of a robust blockchain-based financial identity system is far-reaching. Beyond banking and credit, it can unlock access to healthcare, education, social welfare programs, and digital voting through an interoperable identity ecosystem. To make this vision a reality, stakeholders must strike a careful balance between decentralization and accountability, embedding privacy, security, and legal legitimacy from the start. With the right combination of technological design, regulatory frameworks, infrastructure investment, and stakeholder collaboration, blockchain could become a powerful catalyst for closing identity and inclusion gaps. This direction also reinforces global objectives under SDG 9 and SDG 16, highlighting how secure digital identity infrastructure can contribute to innovation-led inclusion and more accountable institutions.

7. DECLARATIONS

7.1. About Authors

Sri Watini (SW) https://orcid.org/0000-0002-7757-0656

Ora Plane Maria Daeli (OP) https://orcid.org/0009-0005-5707-9332

Syahyono (MM) -

Ramzi Zainum Ikhsan (RZ) https://orcid.org/0009-0005-2253-6476

Oliver Sauntos (OS) -

7.2. Author Contributions

Conceptualization: RZ; Methodology: MM; Software: OP; Validation: SW and OS; Formal Analysis: MM and OS; Investigation: SW; Resources: RZ; Data Curation: OP; Writing Original Draft Preparation: SW and OP; Writing Review and Editing: OS and RZ; Visualization: LP; All authors, SW, OP, MM, RZ, and OS, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] S. Sindhu, "Blockchain-enabled decentralized identity and finance: Advancing women's socioeconomic empowerment in developing economies," *Journal of Women, Innovation, and Technological Empowerment*, vol. 1, no. 1, pp. 19–24, 2025.

[2] T. Gillpatrick, S. Boğa, and O. Aldanmaz, "How can blockchain contribute to developing country economies? a literature review on application areas," *Economics*, vol. 10, no. 1, pp. 105–128, 2022.

[3] T. S. Bahukeling, A. I. Suroso, A. Buono, and P. Nurhayati, "Enhancing msme digital marketing through public-private partnerships with fuzzy ahp," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 325–338, 2026.

[4] D. Mhlanga, "Block chain technology for digital financial inclusion in the industry 4.0, towards sustainable development?" *Frontiers in Blockchain*, vol. 6, p. 1035405, 2023.

[5] S. Wibowo, I. A. Widjaya, J. Zanubiya, R. Evans, U. Rahardja *et al.*, "Orange technology for humanistic innovation in higher education," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 4, no. 2, pp. 105–115, 2026.

[6] N. Y. Hussain, F. I. Babalola, E. Kokogho, and P. E. Odio, "Blockchain technology adoption models for emerging financial markets: Enhancing transparency, reducing fraud, and improving efficiency," *International Journal of Multidisciplinary Research and Growth Evaluation*, no. 01, 2024.

[7] J. Uddoh, D. Ajiga, B. P. Okare, and T. D. Aduloju, "Blockchain identity verification models: a global perspective on regulatory, ethical, and technical issues," *Shodhshauryam Int Sci Refereed Res J*, vol. 6, no. 2, pp. 162–72, 2023.

[8] A. Adegbite, "The role of blockchain technology in enhancing financial inclusion," *IOSR Journal of Economics and Finance*, vol. 15, no. 5, pp. 19–28, 2024.

[9] A. Begum, M. S. K. Munira, and S. Juthi, "Systematic review of blockchain technology in trade finance and banking security," *American Journal of Scholarly Research and Innovation*, vol. 1, no. 01, pp. 25–52, 2022.

[10] U. Rahardja, L. Sulistyo, D. Safarina, M. R. Kusuma, N. Silawati, and Z. Nanle, "Hibahqu education monitoring platform based on human-centric orange technology laravel 12 vue. js," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 6, no. 2, pp. 203–218, 2025.

[11] M. D. T. P. Nasution, Y. Rossanty, R. Harahap, A. R. Tanjung, and T. A. M. Nasution, "Technology-driven resource utilization and integration to enhance firm performance," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 268–283, 2026.

[12] S. C. Friday, C. I. Lawal, D. C. Ayodeji, and A. Sobowale, "Systematic review of blockchain applications in public financial management and international aid accountability," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 4, no. 1, pp. 1165–1180, 2023.

[13] E. K. Chowdhury, I. I. Khan, and B. K. Dhar, "Strategy for implementing blockchain technology in accounting: Perspectives of stakeholders in a developing nation," *Business Strategy & Development*, vol. 6, no. 3, pp. 477–490, 2023.

[14] H. O. Mbaidin, M. A. Alsmairat, and R. Al-Adaileh, "Blockchain adoption for sustainable development in developing countries: Challenges and opportunities in the banking sector," *International Journal of Information Management Data Insights*, vol. 3, no. 2, p. 100199, 2023.

[15] A. Kumar, S. K. Srivastava, and S. Singh, "How blockchain technology can be a sustainable infrastructure for the agrifood supply chain in developing countries," *Journal of Global Operations and Strategic Sourcing*, vol. 15, no. 3, pp. 380–405, 2022.

[16] N. L. Eyo-Udo, M. O. Agho, E. C. Onukwulu, A. K. Sule, C. Azubuike, L. Nigeria, and P. Nigeria, "Advances in blockchain solutions for secure and efficient cross-border payment systems," *International Journal of Research and Innovation in Applied Science*, vol. 9, no. 12, pp. 536–563, 2024.

[17] O. Jutel, "Blockchain humanitarianism and crypto-colonialism," *Patterns*, vol. 3, no. 1, 2022.

[18] N. I. Susanthi, M. Ali, and A. H. Hernawan, "Digital learning platforms as facilitator for university-business collaboration in logistics management curriculum design," *International Journal of Cyber and*

IT Service Management (IJCITSM), vol. 6, no. 1, pp. 37–50, 2026.

[19] A. A. Ajayi, E. Igba, A. D. Soyele, and J. Enyejo, "Enhancing digital identity and financial security in decentralized finance (defi) through zero-knowledge proofs (zkps) and blockchain solutions for regulatory compliance and privacy," *Iconic Res. Eng. J*, vol. 8, no. 4, pp. 373–394, 2024.

[20] W. Usino, M. M. Sari, F. P. Oganda, O. P. M. Daeli, and E. Smith, "Artificial intelligence integration for sustainable business model innovation insights from global startups," *Sundara Advanced Research on Artificial Intelligence*, vol. 1, no. 2, pp. 82–89, 2025.

[21] N. Azizah, P. A. Sunarya, U. Rahardja, A. B. Mutiara, P. Prihandoko, and C. Pasha, "Improving smear-negative tuberculosis detection using data augmentation and faster r-cnn," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 6, no. 1, pp. 65–77, 2026.

[22] K. Coutinho, N. Khairwal, and P. Wongthongtham, "Towards a truly decentralized blockchain framework for remittance," *Journal of Risk and Financial Management*, vol. 16, no. 4, p. 240, 2023.

[23] R. E. Indrajit, M. V. A. Sin, E. A. Nabila, W. N. Wahid, and N. Septiani, "Optimizing business process efficiency through artificial intelligence integration in industry 4.0," *Sundara Advanced Research on Artificial Intelligence*, vol. 1, no. 2, pp. 47–55, 2025.

[24] D. Martinez, L. Magdalena, and A. N. Savitri, "Ai and blockchain integration: Enhancing security and transparency in financial transactions," *International Transactions on Artificial Intelligence*, vol. 3, no. 1, pp. 11–20, 2024.

[25] I. Staley and E. Amankwa, "Blockchain and decentralized finance in fintech startups in emerging markets: A systematic literature review of opportunities and challenges," *Journal of Applied Finance & Banking*, vol. 16, no. 2, pp. 81–108, 2026.

[26] K. D. Hartomo, M. Zaki, G. K. Hanum, N. Silawati, and A. Valerry, "Empirical studies on the relationship between wearable stress detection and workplace productivity," *Journal of Orange Technology*, vol. 1, no. 1, pp. 1–10, 2024.

[27] I. Christodoulou, I. Rizomyliotis, K. Konstantoulaki, A. Nazarian, and D. Binh, "Transforming the remittance industry: Harnessing the power of blockchain technology," *Journal of Enterprise Information Management*, vol. 37, no. 5, pp. 1551–1577, 2024.

[28] A. Al-Dmour, R. Al-Dmour, H. Al-Dmour, and A. Al-Adwan, "Blockchain applications and commercial bank performance: The mediating role of ais quality," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 10, no. 2, p. 100302, 2024.

[29] M. Pandey, M. Velmurugan, G. Sathi, A. R. Abbas, N. Zebo, and T. Sathish, "Blockchain technology: Applications and challenges in computer science," in *E3S web of conferences*, vol. 399. EDP Sciences, 2023, p. 04035.

[30] P. Vijayagopal, B. Jain, and S. Ayinippully Viswanathan, "Regulations and fintech: A comparative study of the developed and developing countries," *Journal of Risk and Financial Management*, vol. 17, no. 8, p. 324, 2024.

[31] A. Kumari and N. C. Devi, "The impact of fintech and blockchain technologies on banking and financial services," *Technology Innovation Management Review*, vol. 12, no. 1/2, 2022.

[32] L. Judijanto, M. Tubagus, R. Hasibuan, D. Mustajab, and A. Rosid, "Integration of blockchain technology in the financial system: assessing its impact on efficiency, security, and stability of financial markets," *INTERNATIONAL JOURNAL OF FINANCIAL ECONOMICS*, vol. 1, no. 9, pp. 41–53, 2025.

[33] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: an overview," *PeerJ Computer Science*, vol. 9, p. e1705, 2023.

[34] M. Campbell-Verduyn and F. Giumelli, "Enrolling into exclusion: African blockchain and decolonial ambitions in an evolving finance/security infrastructure," *Journal of Cultural Economy*, vol. 15, no. 4, pp. 524–543, 2022.

[35] M. Lee. (2025, Aug.) Blockchain revolution: Empowering developing countries. Accessed: 2026-03-27. [Online]. Available: https://onekey.so/blog/ecosystem/blockchain-revolution-empowering-developing-countries/

[36] K. Devi and D. Indoria, "Study on the waves of blockchain over the financial sector," in *List Forum für Wirtschafts-und Finanzpolitik*, vol. 48, no. 3. Springer, 2022, pp. 181–201.

[37] I. Bashir, *Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3*. Packt Publishing Ltd, 2023.