APTISI Transactions on Management (ATM)
Vol. 10, No. 2, May 2026, pp. 191∼202
E-ISSN: 2622-6804 | P-ISSN: 2622-6812, DOI: 10.33050

Blockchain Financial Identity for Inclusive Access in Developing Nations

Sutama Wisnu Dyatmika[1*], Untung Rahardja[2], Muhtarom Muhtarom[3], Dwi Nur Ramadhan[4], Po Abbas Sunarya[5], Lily Maria Evans[6]
[1]Faculty of Economics and Business, University of PGRI Adi Buana Surabaya, Indonesia
[1]Faculty of Economics and Business, Universitas Airlangga, Indonesia
[2]Faculty of Computing, University of Technology Malaysia, Malaysia
[3]Faculty of Law, Social and Political Sciences, Universitas Terbuka, Indonesia
[4, 5]Faculty of Economics and Business, University of Raharja, Indonesia
[6]Department of Management, Pandawan Incorporation, New Zealand
[1]sutama@unipasby.ac.id, [2]urahardja@gmail.com,[3]muhtarom@ecampus.ut.ac.id, [4]dwi.nur@raharja.info, [5]abas@raharja.info, [6]evans@pandawan.ac.nz
***Corresponding Author**

Article Info

Article history:

Submission February 11, 2026
Revised February 26, 2026
Accepted April 10, 2026
Published May 21, 2026

Keywords:

Blockchain
Self-Sovereign Identity
Financial Inclusion
Digital Identity
Developing Nations

ABSTRACT

The absence of formal financial identity remains a significant barrier to financial inclusion in developing nations, limiting access to essential financial services. Traditional centralized identity systems are often vulnerable to data breaches, fraud, and institutional control, resulting in low public trust. **This study aims** to explore how blockchain-based identity systems, particularly through the concept of Self-Sovereign Identity (SSI), can address these limitations. **The research adopts** a qualitative case study approach by analyzing multiple blockchain-based digital identity initiatives across developing regions. **The findings** reveal that blockchain-enabled SSI enhances data security, transparency, and user autonomy, while improving accessibility to financial services. **The key contribution** of this study lies in identifying the integration of decentralized identity frameworks as a sustainable solution to strengthen financial inclusion and institutional trust. However, challenges such as infrastructure limitations, scalability issues, and regulatory uncertainty remain critical barriers. This study provides both theoretical insights and practical implications for policymakers, developers, and financial institutions in implementing secure and inclusive digital identity systems.

Corresponding Author:

DOI: https://doi.org/10.33050/atm.v10i2.2621

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 [2]. Without an officially recognized identity, people are unable to open bank accounts, access credit, or engage with regulated financial services. This situation perpetuates economic inequality and limits opportunities for social

and economic mobility [3]. 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. These systems tend to be controlled by governments or private entities, which not only limits transparency but also undermines individuals' control over their personal data. As a result, trust in centralized systems remains low, especially in regions with weak governance or limited digital infrastructure [4, 5].

This study seeks to explore how blockchain-based identity systems can overcome the limitations of traditional, centralized models. This study distinguishes itself from prior research by not only examining the technical capabilities of blockchain-based identity systems but also integrating socio-technical, institutional, and regulatory perspectives within the context of developing nations. This study seeks to explore how blockchain-based identity systems can overcome the limitations of traditional, centralized models [6]. Unlike previous research that predominantly focuses on the technological architecture of blockchain-based identity systems or isolated case implementations, this study integrates socio-technical, institutional, and regulatory perspectives within the context of developing nations [7].

While existing literature primarily examines the technological features of blockchain and Self-Sovereig n Identity (SSI), this research fills a gap by providing a comparative multi-case analysis that highlights cross-contextual patterns and challenges [4]. Moreover, the study contributes by linking SSI with financial inclusion outcomes and aligns the analysis with broader development goals, particularly in relation to sustainable digital infrastructure and institutional trust. While previous studies predominantly focus on technological architecture or isolated case implementations, this research provides a comparative multi-case analysis that highlights cross-contextual patterns and challenges [8, 9]. Furthermore, this study contributes by linking blockchain-based SSI with financial inclusion outcomes and aligning the analysis with broader development goals, particularly in relation to sustainable digital infrastructure and institutional trust. By synthesizing these dimensions, this research offers a more comprehensive and contextualized framework for understanding the role of blockchain in financial identity systems. The key research questions addressed in this paper are:

- How does a blockchain-based identity system address the weaknesses of conventional identity frameworks?
- What are the primary technical and social challenges in implementing blockchain for financial identity in developing nations?
- What are the potential long-term benefits of adopting blockchain-based financial identity systems for both individuals and the wider economy?

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 aims to highlight solutions that can enhance data security, empower individuals with control over their digital identities, and foster trust in financial systems [10, 11]. The findings will be particularly relevant to policymakers, technology developers, and financial institutions working toward the creation of more secure, transparent, and equitable identity ecosystems. Furthermore, this study aligns with the global development agenda, particularly SDG 9, which emphasizes strengthening digital infrastructure and promoting innovation, and SDG 16, which focuses on building trustworthy, transparent, and inclusive institutions. The integration of blockchain-based identity systems supports these goals by providing secure digital foundations and enhancing institutional accountability [12, 13].

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. Without verifiable identity, individuals are unable to open bank accounts, access credit, apply for insurance, or participate fully in the formal economy [14]. This absence not only limits their economic opportunities but also increases vulnerability to exploitation and systemic inequality. 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) [15, 16]. The barriers are not only technical or bureaucratic, but also social: marginalized populations, rural communities, women, and stateless persons may have less awareness of or access to identity documentation, face higher costs (travel, fees), or distrust institutions.

2.2. Principles of 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 [17]. 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) [18].

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 a small set of authorities controlling identity issuance, verification, storage, and often have centralized databases that are points of weakness (for hacking, misuse, or corruption). Blockchain (or other distributed ledger technologies) are often seen in the literature as enablers for SSI by providing features like immutability, decentralization, Verifiable Credentials (VCs), and public/private key infrastructure [19].

To better understand the technical architecture behind SSI systems, it is important to examine the core components that make up a decentralized identity framework. Figure 1 below illustrates the conceptual structure of a distributed ledger used for SSI, highlighting key layers such as the Consensus Layer, Identity Layer (DIDs and VCs), and Node Validators. This structure enables secure and scalable identity management while ensuring user control over personal data [20, 21].

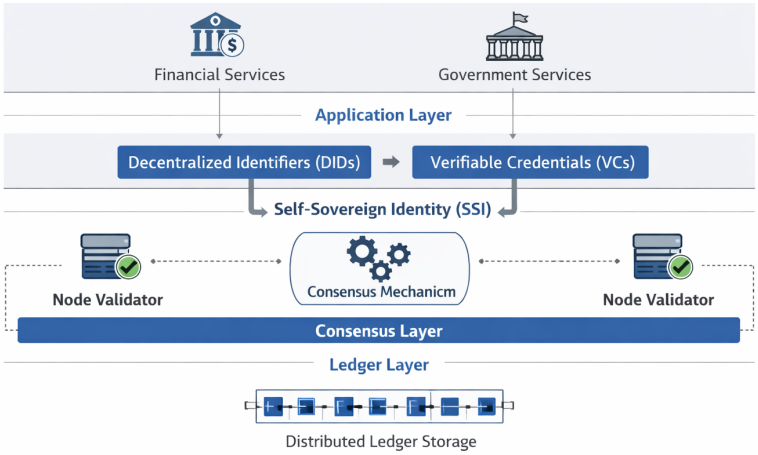

Figure 1. Conceptual Architecture of Distributed Ledger for Self-Sovereign Identity Systems

As illustrated in Figure 1, the distributed ledger architecture forms the backbone of SSI systems. The decentralized nature of this architecture ensures that identity management is not controlled by a single authority, but rather distributed across multiple nodes, each validating transactions through a consensus mechanism. The Identity Layer, represented by Decentralized Identifiers (DIDs) and VCs, allows users to retain full control over their identity data while ensuring secure and verifiable interactions [22]. This structure supports the core principles of SSI, such as privacy, user consent, and data integrity, which are essential for promoting financial inclusion in developing nations [23].

From a technical perspective, blockchain-based identity systems can be implemented using different architectural models, including permissioned and permissionless ledgers, depending on governance and scalability requirements [24]. In many SSI implementations, permissioned blockchains such as Hyperledger Indy are commonly used due to their support for identity-specific functionalities and controlled access. These systems often rely on consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA), which offer higher efficiency and lower energy consumption compared to Proof of Work

(PoW). Furthermore, SSI frameworks are typically built upon DIDs and VCs, following standards proposed by the World Wide Web Consortium (W3C) [25, 26]. DIDs enable unique, user-controlled identifiers that are anchored on the blockchain, while VCs allow secure and selective sharing of identity attributes without exposing unnecessary personal data [27]. This combination of blockchain architecture, consensus protocols, and SSI standards forms the technical backbone that ensures trust, security, and interoperability across identity ecosystems. To illustrate the underpinning architecture of the distributed ledger that enables SSI, Figure 1 shows a network of interconnected nodes sharing a common ledger [28].

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. 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.

Table 1. Comparison Between Traditional Identity Systems and Self-Sovereign Identity (SSI)

Aspect	Traditional Identity Systems	Self-Sovereign Identity (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. This structural shift mitigates vulnerabilities such as data breaches and unauthorized access while fostering interoperability across institutions and borders [29]. 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 [30].

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) [31, 32].

2.3. Existing Blockchain-Based Identity Projects

There are many pilot projects and real-world implementations that attempt to use blockchain/SSI (or related decentralized identity technologies) to overcome identity barriers. Some examples:

Bhutan: Bhutan has launched a National Digital Identity (NDI) that adheres to SSI principles, allowing citizens to control their credentials through a mobile wallet [33]. Citizens can decide what data to share, and credentials are cryptographically anchored to the 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, used for KYC (Know Your Customer), SIM activations, etc.

Digital KYC with SSI: 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 [34]. Reviews of blockchain identity management: There are several survey papers that examine many identity systems [35]. For example, "Blockchain-based identity management systems: A review outlines how

identity management solutions are evolving with blockchain, the benefits in terms of user control and decentralization, as well as recurring issues like legal compliance, scalability, and trust verification.

3. RESEARCH METHODOLOGY

3.1. Research Approach

This study adopts a qualitative, case study-based approach. Because the topic of blockchain for financial identity in developing nations is exploratory and complex, case studies allow for deep contextual understanding of how projects operate in real environments, what challenges arise, and what factors contribute to success or failure. Qualitative methods enable rich, descriptive data from stakeholders, enabling interpretation of social, technical, and institutional dimensions that are often not visible in purely quantitative work [36]. To illustrate the workflow of such systems in practice, a schematic overview is provided below.

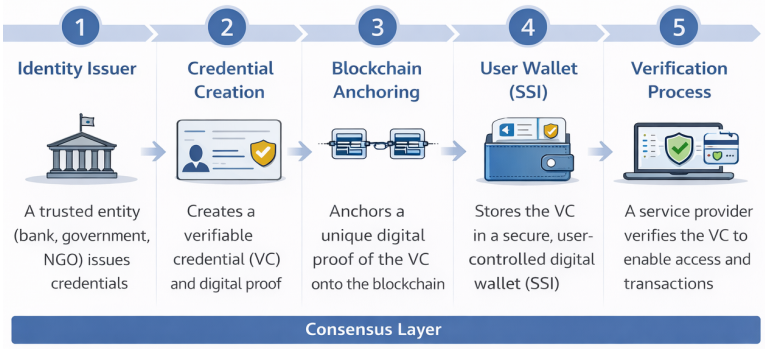

Figure 2. Blockchain-Based Identity Workflow for Financial Inclusion

Figure 2 illustrates the step-by-step workflow of a blockchain-based identity system designed to enhance financial inclusion. The process begins with the Identity Issuer, such as a bank, government, or NGO, creating a VC for the individual, which serves as digital proof of their identity. This credential is then anchored onto the blockchain, ensuring immutability and security through decentralized verification. The credential is stored in the User Wallet SSI, a secure, user-controlled digital wallet that allows individuals to maintain full control over their identity data. Finally, when needed, the Verification Process is carried out by a service provider to confirm the authenticity of the VC and grant access to financial services. This workflow showcases the integration of blockchain technology to create a secure, transparent, and efficient system for managing digital identities, especially in regions with limited access to traditional banking services [37].

Moreover, this methodological choice aligns with contemporary scholarship 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 [38]. 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 [39].

3.2. Case Study Selection

To ensure balanced and insightful findings, the research selects three to five case studies. The selection criteria include geographic diversity, project maturity, and variation in scale and scope to ensure a comprehensive understanding of different implementation contexts [40]. Geographic diversity is considered by selecting projects from distinct developing regions, such as Sub-Saharan Africa, South Asia, Southeast Asia, and Latin America, in order to capture variations in socio-cultural, regulatory, and infrastructural conditions [41]. Project maturity is also taken into account by including only initiatives that have been operational for at least one to two years, allowing observable outcomes, challenges, and lessons learned to be identified [42].

In addition, scale and scope variation is ensured by incorporating both small-scale pilot initiatives and larger system implementations, including projects led by non-governmental organizations, multilateral institutions, governments, and private sector entities, as well as those utilizing different blockchain platforms, SSI

models, and identity architectures [43]. To ensure balanced and insightful findings, the research selects three to five case studies. The selection criteria include geographic diversity, project maturity, and variation in scale and scope. These criteria ensure a comprehensive understanding of different implementation contexts [44]. Projects were chosen from distinct developing regions, Sub-Saharan Africa, South Asia, Southeast Asia, and Latin America, capturing socio-cultural, regulatory, and infrastructural variations. Additionally, only initiatives that have been operational for at least one to two years were included, ensuring the identification of observable outcomes and lessons learned [45].

Based on these criteria, this study identifies and analyzes several representative blockchain-based identity initiatives across developing regions. Specifically, the selected cases include Bhutan's NDI system in South Asia, the ID2020 initiative implemented in Sub-Saharan Africa, and the Modular Open Source Identity Platform (MOSIP) adopted in countries such as the Philippines and Ethiopia. These cases represent diverse governance structures, technological frameworks, and socio-economic conditions, thereby enabling a robust cross-case comparative analysis of blockchain-based financial identity systems. This diversity helps distinguish which factors are context-specific and which may be generalized across different settings [46].

In forming this selection strategy, this research draws on recent methodological literature. For example, prior studies emphasize that purposive or criterion sampling is essential in qualitative case study research to select cases that are information-rich and directly relevant to the phenomenon under study, rather than relying on random sampling. Additionally, the use of multiple case studies allows for cross-context comparison, enabling the identification of both consistent patterns and contextual differences, thereby strengthening the analytical credibility of the research [47].

3.3. Data Collection

Data will be collected from multiple sources for each case to allow triangulation and deepen validity. The methods and sources include:

- Documentary sources project reports, white papers, policy documents, technical specifications, and evaluation reports. These provide background, architecture, timelines, and outcomes. Academic/technical literature, peer-reviewed articles, conference papers, and theses that evaluate or analyze the selected identity projects or similar blockchain / SSI systems.

- Media & public sources: news articles, blogs, press releases, community forums, regulatory announcements to capture public perception, controversies, or delays.

- Semi-structured interviews with carefully selected informants: project leads, technical architects, regulatory stakeholders, and end-users or community representatives. Interviews will focus on motivations, technical design, user experience, adoption obstacles, trust or privacy concerns, institutional dynamics, and adaptation over time.

- Informant sampling and number for each case, the aim is to interview 5–10 informants, covering diverse roles (implementer, policymaker/regulator, users). Informants will be chosen purposely for direct involvement or experience. Interviews may be conducted in person or remotely, recorded (with consent), transcribed verbatim, and anonymized.

- Saturation and iterative collection The collection will proceed until data saturation is achieved, when further interviews or documents yield minimal or no new themes. This decision will be informed by monitoring emerging codes and themes throughout the process. Emphasize that saturation should be operationalized in line with the research questions, theoretical framework, and analytic logic of the study.

Meanwhile, evidence shows that near saturation may be reached substantially earlier than full saturation under certain coding structures and with clear interview guides. Field observations (if feasible): Where possible, visits to project sites or user communities will be conducted to observe the deployment environment, how identity tools are used in practice, infrastructure conditions, and user interactions, adding contextual depth to interviews and documents.

3.4. Data Analysis

Thematic analysis will be the main analytic method, following a structured multi-step process:

- Familiarization repeated reading of transcripts, documents, media materials, and observation notes; initial impressions and possible coding ideas will be recorded in reflective memos.
- Generating initial codes applying codes (manually or using qualitative software such as NVivo or Atlas.ti) to data fragments related to research questions (e.g. trust, interoperability, privacy, user behavior, governance). Searching for themes: grouping related codes into candidate themes, forming a preliminary codebook per case.
- Reviewing themes, refining themes to ensure internal coherence and distinctness; validating themes against full datasets (not just coded fragments). Defining and naming themes: refining definitions and boundaries of themes, selecting representative data extracts, and creating clear labels.

producing the thematic report: writing a narrative of findings with illustrative quotes and comparing across cases; relating patterns back to research questions and literature.

To enhance trustworthiness:

- Triangulation cross-verifying findings across interviews, documents, media, and observations.
- Member checking: sharing preliminary themes with some informants for feedback.
- Audit trail keeping detailed logs of coding decisions, theme development, memos.
- Reflexivity researcher maintains reflective memos about personal assumptions or biases.

To complement the thematic analysis process described above and to clarify the conceptual relationships examined in this study, a visual framework is provided in Figure 3 to illustrate how the key elements of the blockchain-based identity system interact within the broader analytical structure.

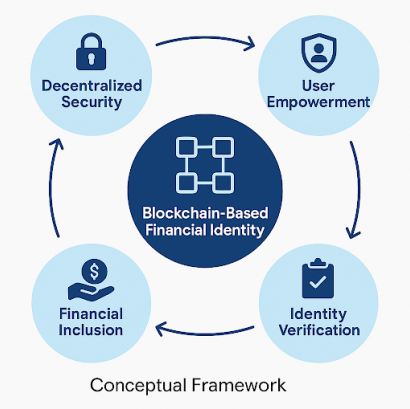

Figure 3. Conceptual Framework of Blockchain-Based Financial Identity System

This conceptual framework illustrates how decentralized security, user control, identity verification, and financial inclusion interact within a blockchain-enabled identity ecosystem. The framework serves as a guiding structure that links the technological components of SSI with broader socio-economic outcomes, supporting the analysis conducted in the subsequent Discussion section.

4. RESULTS AND DISCUSSION

4.1. The Blockchain Advantage

4.1.1. Decentralization and Immutability

Blockchain's decentralized architecture eliminates a single point of failure, a major vulnerability in traditional centralized identity systems. Systems like SSI built on blockchain distribute identity verification

across multiple nodes, meaning no single authority holds all the power or data. The immutability feature of blockchain ensures that once identity credentials are recorded, they cannot be altered or fraudulently tampered with, giving a tamper-proof ledger. Literature confirms these advantages in its analysis of various SSI frameworks. They observe that decentralization and cryptographically VCs are central to achieving transparency and trust in identity systems [48].

4.1.2. User Control and Security

With SSI, users gain ownership and control over their identity data. They decide which attributes to share, with whom, and under what conditions. This reduces intermediaries and thereby mitigates risks such as identity theft or unauthorized data exposure. Argues that in blockchain-based identity management, users obtain autonomy over their personal data in ways incompatible with centralized databases, which are prone to breaches and misuse. Moreover, mechanisms such as VCs and DIDs reinforce security and privacy [49].

4.2. The Challenges of Implementation

4.2.1. Scalability and Infrastructure

Despite its advantages, blockchain identity systems face serious technical and infrastructural challenges in developing nations. Scaling up to handle large user bases or many transactions often results in high latency, higher transaction fees, and energy costs. Public blockchains in particular struggle with throughput when many users attempt operations simultaneously. For example, "Blockchain technology and application: an overview" highlights how public blockchains experience delays as more data accumulates, slowing down transaction speed. Also, in many developing areas, reliable internet connectivity, stable power supply, and access to devices are not universal, which limits adoption [50].

4.2.2. Regulatory and Governance Hurdles

Legal and regulatory frameworks often lag behind technological developments in blockchain and SSI. Unclear laws about data ownership, liability, identity proofing, smart contract enforceability, and privacy (including "right to be forgotten") pose real risks and barriers to adoption. The systematic review "Blockchain Implementation Challenges in Developing Countries" notes that the lack of effective regulations and legal uncertainty contributes to stakeholder hesitation. Similarly stresses that trust in such systems is not only about technology but also about regulatory legitimacy and institutional governance [51].

Despite the advantages of blockchain technology, its implementation in developing nations faces multifaceted challenges spanning technical, infrastructural, and social dimensions. Governance challenges remain significant, as many developing countries lack the regulatory frameworks necessary to oversee decentralized technologies effectively. Governments may be reluctant to relinquish control over identity systems, raising concerns about data sovereignty, accountability, and privacy. Furthermore, institutional adoption of blockchain-based identity systems can be hindered by a lack of technical expertise and trust in emerging technologies.

Financial institutions may resist adopting blockchain-based systems due to unclear regulations and concerns over data security and privacy. In addition, limited digital literacy, inadequate infrastructure, and resistance to technological change can hinder adoption, particularly among rural and low-income communities. Therefore, supportive policies, capacity-building initiatives, and inclusive technology design are essential to ensure equitable implementation. Table 2 summarizes these key obstacles.

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.

Addressing these challenges requires not only technological innovation but also supportive policy frameworks, capacity-building programs, and cross-sector collaboration to foster sustainable adoption.

4.3. 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 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. 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. 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. For instance, developing nations might need to adapt governance models that balance decentralization with accountability and legal oversight.

5. MANAGERIAL IMPLICATIONS

The implementation of SSI systems presents significant opportunities and challenges for organizations, particularly in the fintech sector. For managers, adopting blockchain-based identity solutions requires a strategic shift toward decentralized data management, where user control and privacy are prioritized. Organizations must ensure that their technological infrastructure is robust enough to handle the demands of blockchain, including secure storage and verification of credentials. Furthermore, implementing SSI demands a comprehensive approach to governance, where collaboration with regulatory bodies is crucial to address legal uncertainties and ensure compliance with data privacy laws. Managers should focus on developing clear internal policies and procedures that promote transparency and trust, while also aligning their strategies with emerging regulatory standards. As digital identity systems gain prominence in financial services, managers must ensure that their organizations are not only technologically equipped but also legally prepared to integrate these systems seamlessly into existing financial frameworks. Ultimately, the successful implementation of blockchain-based identity systems will depend on the ability of organizations to balance innovation with regulatory compliance, while ensuring that customer trust and security remain central to the deployment strategy.

6. CONCLUSION

Blockchain offers strong potential to address identity barriers in developing nations by enabling verifiable financial identities for individuals without formal recognition. Its decentralized and immutable characteristics reduce risks of tampering and single points of failure. When integrated with SSI, it empowers users with control, privacy, and consent over their personal data, creating a more inclusive, resilient, and user-centric financial identity system.

However, significant challenges remain. Scaling blockchain systems to national or regional levels often leads to high costs, latency, and computational demands, issues that are amplified in regions with limited infrastructure and unstable connectivity. Additionally, regulatory uncertainty, unclear data ownership, and lack of standardized identity frameworks hinder adoption by governments and financial institutions, highlighting the need for alignment between technological innovation and institutional readiness.

Despite these barriers, blockchain-based identity systems can unlock broader access to services such as banking, healthcare, education, and social programs. To realize this potential, stakeholders must collaborate: regulators need clear and balanced legal frameworks, financial institutions must invest in secure and scalable infrastructure, and developers should enhance interoperability and efficiency. With the right combination of

policy, technology, and collaboration, blockchain can drive inclusive growth and support global development goals related to innovation and institutional accountability.

7. DECLARATIONS

7.1. About Authors

Sutama Wisnu Dyatmika (SW) https://orcid.org/0000-0003-1811-2337
Untung Rahardja (UR) https://orcid.org/0000-0002-2166-2412
Muhtarom Muhtarom (MM) https://orcid.org/0009-0002-1497-9574
Dwi Nur Ramadhan (DR) https://orcid.org/0009-0004-2941-2364
Po Abbas Sunarya (PA) https://orcid.org/0000-0002-3869-2837
Lily Maria Evans (LE) https://orcid.org/0009-0005-9759-710X

7.2. Author Contributions

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

REFERENCES

[1] C. Sakyi-Nyarko, A. H. Ahmad, and P. M. Akolgo, "Digital financial inclusion–trade," *Trade and Investment in Africa: A Research Companion*, 2025.
[2] A. Jaya, F. Saputra, D. N. Ramadhan, T. Green *et al.*, "Optimization of digital business to support msmes growth in the industry 4.0 transformation," *Journal of Computer Science and Technology Application*, vol. 3, no. 1, pp. 1–10, 2026.
[3] N. Udohaya, "Financial inclusion," in *Impact Investing and Financial Inclusion: Examining the Innovations that Empower the Underserved*. Springer, 2025, pp. 323–445.
[4] S. Jha and R. C. Dangwal, "Fintech services and financial inclusion: a systematic literature review of developing nations," *Journal of Science and Technology Policy Management*, vol. 16, no. 7, pp. 1167–1198, 2025.
[5] P. H. P. Tan, A. Rizky, Q. Aini, D. N. Ramadhan, and T. Green, "Utilizing the alphasign website to create blockchain-based or online digital signatures," *Blockchain Frontier Technology*, vol. 5, no. 1, pp. 25–36, 2025.
[6] O. A. Bello, "The role of data analytics in enhancing financial inclusion in emerging economies," *International Journal of Developing and Emerging Economies*, vol. 11, no. 3, pp. 90–112, 2024.
[7] D. Bennet, S. A. Anjani, O. P. Daeli, D. Martono, and C. S. Bangun, "Predictive analysis of startup ecosystems: Integration of technology acceptance models with random forest techniques," *CORISINTA*, vol. 1, no. 1, pp. 70–79, 2024.
[8] A. A. Al-Qudah, M. Al-Okaily, and M. P. P. Yadav, "The growth of fintech and blockchain technology in developing countries: Uae's evidence," *International Journal of Accounting & Information Management*, vol. 33, no. 2, pp. 383–406, 2025.
[9] N. Lutfiani, A. Ivanov, N. P. L. Santoso, S. V. Sihotang, and S. Purnama, "E-commerce growth plan for msmes' sustainable development enhancement," *CORISINTA*, vol. 1, no. 1, pp. 80–86, 2024.
[10] O. Okusi, C. Ikemefuna, and E. Chukwuani, "Integrating zero trust architectures and blockchain protocols for securing cross-border transactions and digital financial identity systems," *International Journal of Computer Applications Technology and Research*, vol. 14, no. 6, pp. 163–180, 2025.
[11] D. Robert, F. P. Oganda, A. Sutarman, W. Hidayat, and A. Fitriani, "Machine learning techniques for predicting the success of ai-enabled startups in the digital economy," *CORISINTA*, vol. 1, no. 1, pp. 61–69, 2024.
[12] P. Vasishta, A. Dhiman, S. Smith, and A. Singla, "How can defi improve the quality, affordability, access and usage of financial services? a systematic literature review," *Journal of Economic and Administrative Sciences*, 2025.

[13] C. Lukita, N. Lutfiani, A. R. S. Panjaitan, U. Rahardja, M. L. Huzaifah *et al.*, "Harnessing the power of random forest in predicting startup partnership success," in *2023 Eighth International Conference on Informatics and Computing (ICIC)*. IEEE, 2023, pp. 1–6.

[14] D. Mhlanga, "The critical developmental importance of blockchain technology in africa," in *Financial Inclusion and Sustainable Development in Sub-Saharan Africa*. Routledge, 2025, pp. 136–152.

[15] R. Jaiswal and S. Gupta, "Global research trends on blockchain technology in finance: past, present and future," *International Journal of Electronic Finance*, vol. 14, no. 4, pp. 454–484, 2025.

[16] Q. Aini, I. Sembiring, A. Setiawan, I. Setiawan, and U. Rahardja, "Perceived accuracy and user behavior: Exploring the impact of ai-based air quality detection application (aiku)," *Indonesian Journal of Applied Research (IJAR)*, vol. 4, no. 3, pp. 209–224, 2023.

[17] H.-H. Ou, G.-Y. Chen, and I.-C. Lin, "A self-sovereign identity blockchain framework for access control and transparency in financial institutions," *Cryptography*, vol. 9, no. 1, p. 9, 2025.

[18] M. H. R. Chakim, Q. Aini, P. A. Sunarya, N. P. L. Santoso, D. A. R. Kusumawardhani, and U. Rahardja, "Understanding factors influencing the adoption of ai-enhanced air quality systems: A utaut perspective," in *2023 Eighth International Conference on Informatics and Computing (ICIC)*. IEEE, 2023, pp. 1–6.

[19] E. Chukwuma-Eke, O. Ogunsola, and N. Isibor, "Developing financial inclusion strategies through technology and policy to improve energy access for underserved communities," 2025.

[20] N. Del Sarto and P. K. Ozili, "Fintech and financial inclusion in emerging markets: a bibliometric analysis and future research agenda," *International Journal of Emerging Markets*, vol. 20, no. 13, pp. 270–290, 2025.

[21] R. Salam, Q. Aini, B. A. A. Laksminingrum, B. N. Henry, U. Rahardja, and A. A. Putri, "Consumer adoption of artificial intelligence in air quality monitoring: A comprehensive utaut2 analysis," in *2023 Eighth International Conference on Informatics and Computing (ICIC)*. IEEE, 2023, pp. 1–6.

[22] J. Mookerjee, M. K. Bhuriya, R. Josphin, and G. Radhakrishnan, "Digital banking and financial inclusion in rural economies," *South Eastern European Journal of Public Health*, vol. 26, no. 1, pp. 954–963, 2025.

[23] M. Annas, F. A. Ramahdan, T. Handra, A. H. D. Saputra, and H. Jensen, "Application of iot and ai based on esp32cam to support sustainable mobility in smart cities," *Blockchain Frontier Technology (B-Front)*, vol. 4, no. 2, pp. 121–131, 2025.

[24] Z. Shariff, M. Memon, A. Ali, A. Mubasher, and A. Hussain, "The role of blockchain technology in cryptocurrency adoption: A cross-national analysis of developing countries," *Periodicals of Management Studies*, vol. 5, no. 2, pp. 41–50, 2025.

[25] D. T. Abraha, "Blockchain-based solution for addressing refugee management in the global south: Transparent and accessible resource sharing in humanitarian organizations," *Frontiers in Human Dynamics*, vol. 6, p. 1391163, 2025.

[26] T. Mariyanti, I. Wijaya, C. Lukita, S. Setiawan, and E. Fletcher, "Ethical framework for artificial intelligence and urban sustainability," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 98–108, 2025.

[27] M. A. A. Syahid, Z. M. Zan, Y. Pon, T. S. T. M. Zukri, M. A. Ibrahim, and M. Z. Said, "The transformative role of digital technology in enhancing economic inclusivity within developing countries: A scoping review," *PaperASIA*, vol. 41, no. 3b, pp. 406–416, 2025.

[28] S. Pranata, F. Fanani, D. Hidayati, R. Lesmana, and Z. Ndlovu, "Implementation of smart contracts in tiktok influencer marketing," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 84–97, 2025.

[29] M. S. Thong, "Blockchain drive for financial inclusion," in *Blockchain for financial governance in malaysia and singapore: transforming regulatory and shariah compliance to drive financial inclusion*. Springer, 2025, pp. 139–176.

[30] N. K. A. Dwijendra, M. Zaidi, I. G. N. K. Arsana, S. E. Izzat, A. T. Jalil, M.-H. Lin, U. Rahardja, I. Muda, A. H. Iswanto, and S. Aravindhan, "A multi-objective optimization approach of smart autonomous electrical grid with active consumers and hydrogen storage system," *Environmental and Climate Technologies*, vol. 26, no. 1, pp. 1067–1079, 2022.

[31] D. Pramudito, J. Na'am, and F. Ernawan, "Exploring blockchain and ai in digital banking: A literature review on transactions enhancement, fraud detection, and financial inclusion," *Sistemasi: Jurnal Sistem Informasi*, vol. 14, no. 3, pp. 1448–1459, 2025.

[32] Y. Shino, H. Kenta, and I. K. Mertayasa, "Media promotional for art in tangerang city with audio visual adobe creative," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 4, no. 2, pp. 192–204, 2022.

[33] J. Singh, G. S. Batra, and S. K. Chatrath, "Blockchain's role in social welfare, financial inclusion, and

public sector innovations in india: A multi-sector analysis of government-led initiatives," *Cities*, vol. 167, p. 106366, 2025.

[34] S. Abdallah-Ou-Moussa, M. Wynn, and O. Kharbouch, "Blockchain, cryptocurrencies, and decentralized finance: A case study of financial inclusion in morocco," *International Journal of Financial Studies*, vol. 13, no. 3, p. 124, 2025.

[35] A. Ali, M. H. Butt, and I. Senturk, "Decentralised finance as a catalyst for financial inclusion: Evidence from emerging economies," *Policy Journal of Social Science Review*, vol. 3, no. 7, pp. 292–303, 2025.

[36] A. Wu, "Enabling financial access via blockchain: The potential for decentralized finance to address inclusion challenges in latin america," in *Sustainable Digital Finance*. Springer, 2025, pp. 267–282.

[37] L. B. Malusare, "Blockchain technology and its impact on financial inclusion," *DIGITAL TRANSFORMATIONS THROUGH MULTIDISCIPLINARY RESEARCH*, p. 12, 2025.

[38] 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.

[39] S. Rasheed and S. Louca, "Blockchain-based implementation of national census as a supplementary instrument for enhanced transparency, accountability, privacy, and security," *Future Internet*, vol. 16, no. 1, p. 24, 2024.

[40] S. Mousa, "Unleashing the potential of industry 4.0 for financial inclusion," in *Financial Inclusion, Sustainability, and the Influence of Religion and Technology*. IGI Global Scientific Publishing, 2024, pp. 253–285.

[41] I. A. Adeniran, A. O. Abhulimen, A. N. Obiki-Osafiele, O. Osundare, E. Agu, and C. Efunniyi, "Global perspectives on fintech: Empowering smes and women in emerging markets for financial inclusion," *International Journal of Frontline Research in Multidisciplinary Studies*, vol. 3, no. 02, pp. 030–037, 2024.

[42] R. Ranasinghe, F. Rahmani, G. Gilbert, and E. Gharaie, "Exploring the factors influencing project management methodology implementation in local governments," *Administrative Sciences*, vol. 15, no. 9, p. 332, 2025.

[43] E. Ancona, D. Guerra, S. Armstrong, H. O. da Mata, C. Medeiros, J. Silva, and E. Dahlstrom, "Technical, legal and policy aspects of an international space traffic management framework," *Acta Astronautica*, vol. 232, pp. 356–363, 2025.

[44] S. Annamalah, K. L. Aravindan, S. Ahmed, and I. Sentosa, "Exploring the relevance and rigour of case study research in business: a contemporary perspective," *Journal of Sustainability Research*, vol. 7, no. 2, 2025.

[45] D. Scott and S. Gössling, "Beyond ambition: a review of tourism climate change declaration outcomes and prospects from baku," *Journal of Sustainable Tourism*, vol. 34, no. 2, pp. 512–533, 2026.

[46] S. Zacharias, H. W. Loescher, H. Bogena, R. Kiese, M. Schrön, S. Attinger, T. Blume, D. Borchardt, E. Borg, J. Bumberger *et al.*, "Fifteen years of integrated terrestrial environmental observatories (tereno) in germany: Functions, services, and lessons learned," *Earth's Future*, vol. 12, no. 6, p. e2024EF004510, 2024.

[47] L. Migliorini, M. Olcese, P. Cardinali, and F. Madera, "Exploring outdoor initiatives as tools for youth engagement, inclusion, and environmental awareness: a multi-case study from italy and france," *Children and Youth Services Review*, p. 108659, 2025.

[48] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A survey on decentralized identifiers and verifiable credentials," *IEEE Communications Surveys & Tutorials*, 2025.

[49] Y. Lee, H. Shin, and D. Choi, "A survey on credential revocation and did deactivation in self-sovereign identity systems," *IEEE Access*, 2025.

[50] D. Mhlanga, "Digital transformation of education, the limitations and prospects of introducing the fourth industrial revolution asynchronous online learning in emerging markets," *Discover education*, vol. 3, no. 1, p. 32, 2024.

[51] Organisation for Economic Co-operation and Development, "G7 mapping exercise of digital identity approaches," 2024, oECD policy report accessed 2026. [Online]. Available: https://www.oecd.org/en/publications/g7-mapping-exercise-of-digital-identity-approaches_56fd4e94-en.html