

BLOCKCHAIN-BASED IDENTITY MANAGEMENT IN GOVERNMENT SERVICES: A CONCEPTUAL ANALYSIS OF SMART CONTRACTS FOR SECURING DIGITAL IDENTITIES

Yazeed Al Moaiad¹
Faculty of Computer and Information
Al-Madinah International University
Kuala Lumpur, Malaysia
yazeed.alsayed@mediu.edu.my

Arwa Mohammed Badhawi²
Faculty of Computer and Information
Al-Madinah International University
Kuala Lumpur, Malaysia
CM355@lms.mediu.edu.my

Abstract— Digital identity is a foundational capability of digital government, yet prevailing centralized identity systems concentrate sensitive citizen data, create single points of failure, and often provide limited interoperability and user control. This paper presents a qualitative conceptual analysis of blockchain-based identity management for government services, emphasizing the role of smart contracts in secure and automated identity verification. A concept-centric review of academic literature, international standards, and policy reports was used to identify the principal constructs, risks, and design requirements of decentralized identity. The synthesis informed a layered reference architecture comprising a citizen identity wallet, government credential issuers, a permissioned consortium blockchain, smart-contract services, and encrypted off-chain storage. The framework uses decentralized identifiers and verifiable credentials to separate proof from disclosure, while smart contracts coordinate registration, credential status, consent, authorization, and immutable audit events. Comparative analysis indicates that the proposed model can reduce centralized attack surfaces, strengthen traceability, support selective disclosure, and improve cross-agency interoperability. These benefits remain conditional on secure contract engineering, key recovery, privacy-preserving storage, scalable governance, and legal recognition. The study contributes an integrated socio-technical framework and a staged adoption roadmap for public institutions. Because the analysis is conceptual, the framework requires validation through prototypes, performance testing, security assessment, and citizen-centered usability studies before production deployment.

Keywords— blockchain; digital identity; smart contracts; government services; self-sovereign identity; decentralized identifiers; verifiable credentials; e-government

I. Introduction

Digital identity is the electronic representation through which a person, organization, or device is recognized and authorized in an online environment. For citizens, it increasingly serves as the gateway to taxation, health care, social protection, licensing, education, and other government services. The expansion of digital government therefore makes identity management not merely an information-technology function, but a public trust infrastructure. A failure of that infrastructure may exclude legitimate users, expose personally identifiable information, enable fraud, or undermine confidence in digital institutions [1, 8].

Most government identity systems remain centralized: a public authority or contracted identity provider issues credentials, stores identity attributes, and makes authentication decisions. Central control can simplify administration and accountability, but it also concentrates risk. Large repositories become attractive targets; service availability depends on a limited number of systems; and citizens have little visibility into how their data are reused across agencies [3, 17]. Federated identity reduces repeated authentication through trusted identity providers, yet it still enables intermediaries to observe user activity and leaves interoperability dependent on institutional agreements.

Blockchain-based identity management proposes a different trust arrangement. Instead of treating a blockchain as a database for personal information, it can function as a tamper-evident coordination layer for decentralized identifiers (DIDs), credential status, cryptographic proofs, and audit events. Personal data remain with the holder or in encrypted off-chain repositories, while government bodies continue to perform lawful identity proofing and issue authoritative credentials.

Smart contracts then enforce transparent rules for registration, consent, verification, authorization, and revocation [7, 20, 28].

A. Research Problem and Objectives

The central problem is the absence of an integrated conceptual model that connects blockchain mechanisms with the security, privacy, interoperability, and governance requirements of government identity services. Technical discussions often emphasize ledger properties, while identity studies focus on credentials or self-sovereignty without specifying how smart contracts should coordinate the full identity life-cycle. This paper addresses four objectives: (1) analyze how blockchain can improve government identity management; (2) clarify the security and automation role of smart contracts; (3) compare the resulting approach with centralized identity; and (4) propose a government-oriented conceptual architecture.

B. Contributions

The paper makes three contributions. First, it synthesizes identity, blockchain, smart-contract, and digital-government literature into a single socio-technical design view. Second, it proposes a layered architecture that deliberately separates encrypted identity data from on-chain proofs and status records. Third, it derives a practical adoption roadmap and risk-control set, thereby avoiding the assumption that decentralization alone guarantees security, privacy, or institutional legitimacy.

II. Related Work and Theoretical Foundation

A. Digital Identity Models

Centralized identity places issuance, storage, and validation under one authority. It offers direct operational control but creates a single point of compromise and encourages duplication when agencies maintain separate databases. Federated identity links multiple services to trusted identity providers and improves user convenience, but it retains intermediary dependence and may permit cross-service tracking. Self-sovereign identity (SSI) shifts control toward the credential holder: authoritative issuers sign digital credentials, users store them in a wallet, and verifiers request only the evidence required for a transaction [2, 20, 24, 30].

SSI does not eliminate government authority. In a public-sector context, government agencies remain responsible for identity proofing, credential issuance, regulatory supervision, and redress. What changes is the technical distribution of control. The citizen can present a reusable, cryptographically verifiable credential without requiring every service provider to retrieve the same record from a central database.

Table 1 Comparison of identity-management models.

Aspect	Centralized	Federated	Blockchain-based
Primary control	Authority	Identity provider	Holder + issuers
Failure concentration	High	Moderate	Distributed
Privacy control	Low	Moderate	High if well designed
Interoperability	Limited	Agreement-based	Standards-based
Trust basis	Institutional	Intermediary	Institutional + cryptographic

B. Blockchain, DIDs, and Verifiable Credentials

A blockchain is a distributed ledger in which validated records are linked cryptographically and replicated across participating nodes. Its relevance to identity lies in integrity, shared state, and auditability rather than in public disclosure of personal information [21, 23]. Public blockchains maximize openness but may conflict with government privacy and governance requirements. Private blockchains provide stronger administrative control but can reproduce centralization. Consortium networks offer a middle path in which approved institutions share validation and governance; accordingly, they are often the most plausible design for cross-agency public services [6, 23].

DIDs are globally unique identifiers controlled through cryptographic keys rather than a conventional centralized directory. Verifiable credentials are digitally signed claims—such as residency, professional status, or eligibility—that can be validated cryptographically. Together, these standards allow an issuer to remain authoritative, a holder to control presentation, and a verifier to establish authenticity without direct database-to-database disclosure [24, 28]. Selective-disclosure techniques can further restrict the evidence to the minimum required attributes.

C. Smart Contracts as Policy Mechanisms

Smart contracts are deterministic programs executed by blockchain nodes when predefined conditions are satisfied. In identity management, they can record credential status, verify signatures, enforce authorization policies, capture consent, and generate auditable events [5, 7]. Their value is consistency: the same policy logic can be executed across agencies without relying on manual interpretation for every request. Their weakness is also consistency: an error in code can be repeated automatically and at scale. Secure development, independent audit, formal verification of critical properties, controlled upgrades, and emergency suspension are therefore essential [5].

D. Research Gap

Prior work establishes the promise of blockchain, SSI, and verifiable credentials, but government deployment introduces requirements that cannot be resolved by cryptography alone. Public institutions must preserve legal accountability, provide inclusive access and recovery, support inter-agency governance, minimize personal-data exposure, and maintain continuity of service. The gap addressed here is an integrated framework in which technology, policy, and institutional roles are designed together rather than treated as separate implementation concerns.

III. Research Methodology

A. Design

The study adopts a non-experimental, qualitative, and conceptual research design. Conceptual research is appropriate when an emerging field contains relevant constructs and mechanisms but lacks a stable, widely validated implementation model. The method emphasizes relationships among concepts and the explanatory coherence of the resulting framework rather than statistical hypothesis testing [12, 13, 14].

The evidence base consists of peer-reviewed articles, books, standards, and institutional reports covering digital identity, e-government, blockchain architecture, smart-contract security, privacy, and SSI. The review was concept-centric: materials were analyzed for recurring constructs, architectural patterns, benefits, risks, and governance requirements rather than summarized publication by publication [19, 29]. No human participants or personal datasets were used.

B. Analytical Procedure

The procedure followed an input-process-output logic. Inputs included limitations of centralized identity, blockchain and smart-contract concepts, identity standards, and policy guidance. The process comprised literature synthesis, problem analysis, framework design, and conceptual evaluation. Outputs consisted of a reference architecture, a comparative assessment, and implementation recommendations. Figure 1 summarizes this sequence.

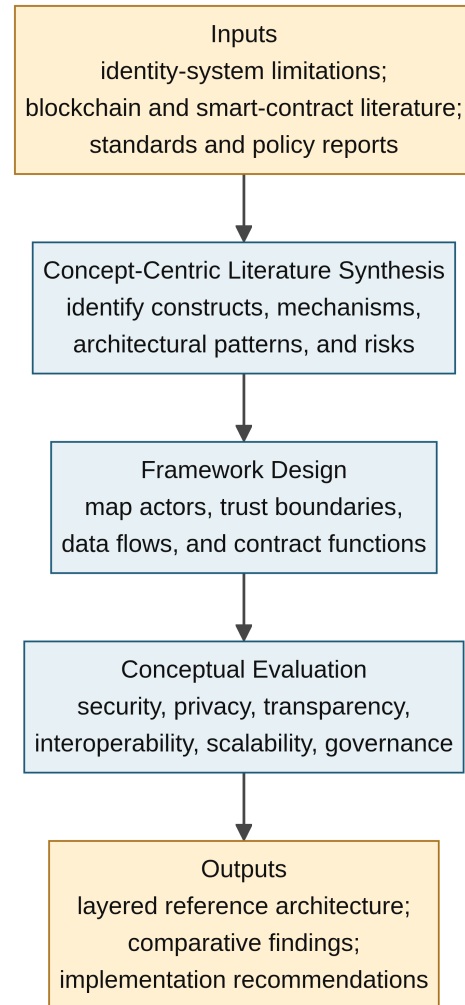


Figure 1 Conceptual research methodology.

C. Evaluation Criteria

The framework was assessed against six criteria derived from the literature: (1) resistance to unauthorized modification and service disruption; (2) privacy and data minimization; (3) transparency and auditability; (4) interoperability across agencies; (5) scalability and operational feasibility; and (6) governance and regulatory accountability. The assessment is analytical rather than empirical; statements therefore describe expected effects under specified design conditions, not measured performance.

IV. Proposed Conceptual Framework

A. Design Principles

The proposed framework is guided by seven principles: user control over credential presentation; government authority over lawful issuance and revocation; minimal disclosure; separation of personal data from ledger records; cryptographic verifiability; policy automation with human accountability; and interoperability through open identity standards. These principles prevent the common mistake of equating blockchain adoption with indiscriminate on-chain storage.

B. Layered Architecture

The architecture contains five interacting layers. The **user layer** is a citizen wallet that protects private keys and stores verifiable credentials. The **government-service layer** includes credential issuers and service providers. The **smart-contract layer** manages registration events, credential status, consent receipts, policy evaluation, and revocation. The **blockchain layer** is a permissioned consortium ledger operated by authorized government institutions. The **off-chain data layer** stores encrypted personal or biometric data under legally defined controls. Only hashes, DIDs, status references, and audit events are anchored on the ledger.

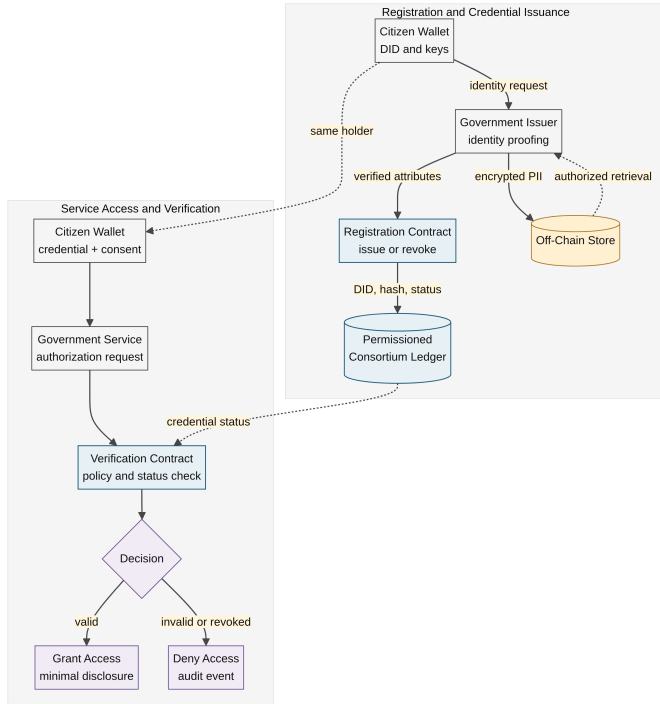


Figure 2 Proposed blockchain-based government identity architecture. Solid arrows represent operational messages; dotted arrows represent status, retrieval, or holder-continuity links.

C. Identity Lifecycle

Registration and issuance: A citizen submits identity evidence to an authorized government issuer. The agency performs identity proofing under existing law, encrypts sensitive records off-chain, and issues a signed credential to the citizen wallet. A registration contract anchors only the credential hash, issuer, status pointer, and timestamp.

Authentication and verification: When requesting a service, the citizen presents a credential or cryptographic proof and gives transaction-specific consent. The service invokes a verification contract, which validates the issuer, signature, expiration, revocation status, and relevant policy. The contract returns a decision without disclosing unrelated attributes.

Authorization and audit: Access rules are encoded as explicit policy conditions. A successful decision releases the service or a narrowly scoped data reference; a failed decision records an auditable reason code without publishing sensitive content. Every automated outcome remains subject to an accountable appeal and correction process.

Update, suspension, and revocation: Issuers update credential status when circumstances change or fraud is detected. The original credential need not be deleted from every service database because verifiers consult the authoritative status mechanism. Recovery procedures rebind a citizen to new keys after loss or compromise, using multi-party controls rather than a single administrator.

D. Smart-Contract Responsibilities

Table 2 Smart-contract functions and safeguards.

Function	Automated responsibility	Required control
Registration	Validate issuer and anchor credential metadata	Identity proofing remains off-chain
Verification	Check signature, issuer, status, and validity	Fail closed; log reason code
Authorization	Evaluate role, attribute, and consent policy	Least privilege and appeal
Consent	Record scope, purpose, and expiry	Revocable, human-readable terms
Revocation	Publish status change	Multi-party authorization
Audit	Emit immutable event reference	No personal data in logs

V. Conceptual Analysis and Findings

A. Security and Resilience

The framework reduces exposure to a single compromised authentication database by distributing trust across approved institutions and enabling services to verify credentials cryptographically. Tamper-evident status records improve detection of unauthorized changes, while signed credentials make forgery more difficult. Smart contracts can consistently enforce authorization rules and reduce discretionary errors. These gains do not remove endpoint risk: compromised wallets, issuer systems, contract code, or administrative keys may still undermine the system. Security therefore depends on layered controls, not the ledger alone [5, 7, 17].

B. Privacy and Data Protection

Privacy is strengthened when the ledger contains only non-sensitive proofs and when citizens disclose only the attributes required for a service. The hybrid storage model supports confidentiality, correction, and jurisdiction-specific retention while preserving a verifiable audit trail [25]. Nevertheless, hashes and metadata can still become identifying when correlated. DID rotation, pairwise identifiers, minimal event data, purpose limitation, encryption, and carefully designed access logs are necessary. A permanent ledger must never be used as a substitute for lawful records management.

C. Trust, Transparency, and Accountability

Traditional identity relies principally on institutional trust. The proposed framework combines that trust with cryptographic verification and shared auditability. Citizens and agencies can verify that a recognized issuer created a credential and that its status has not been altered. Transparent execution also makes policy behavior more inspectable. However, algorithmic execution does not define legitimate policy. Governments remain responsible for deciding who may issue credentials, how disputes are resolved, when contracts are upgraded, and how incorrect records are corrected [23, 28].

D. Interoperability and Scalability

DIDs and verifiable credentials provide common formats for exchanging proofs across heterogeneous services. A consortium ledger can offer a shared trust registry without forcing every agency to replace its internal systems. Scalability is improved by keeping high-volume personal data and routine application processing off-chain. The ledger should be limited to compact status and audit transactions. Performance still depends on consensus design, node distribution, credential-revocation strategy, contract efficiency, and service-level architecture.

Table 3 Conceptual comparison of traditional and proposed approaches.

Criterion	Traditional system	Proposed framework
Architecture	Centralized or siloed	Distributed consortium
Attack surface	Concentrated repository	Distributed trust; endpoint risks remain
Privacy control	Provider-directed	Holder-mediated selective disclosure
Data storage	Central identity data-base	Encrypted off-chain data; on-chain proofs
Auditability	Organization-specific logs	Shared tamper-evident events
Interoperability	Bilateral integration	DIDs and verifiable credentials
Governance	Single authority	Multi-institution policy and accountability

The comparison in Table 3 supports five principal findings. First, decentralization can improve resilience by reducing dependence on a single identity repository. Second, smart contracts are most useful as policy-execution and coordination mechanisms, not as repositories of personal data. Third, privacy gains depend on selective disclosure and off-chain storage rather than immutability itself. Fourth, standards-based credentials offer a credible path to cross-agency interoperability. Fifth, public-sector value is conditional on governance maturity, secure key management, and legally recognized accountability.

VI. Governance, Risks, and Design Controls

A. Smart-Contract Assurance

Contract defects can produce unauthorized access, denial of service, privacy leakage, or irreversible state changes. Critical contracts should

therefore use minimal functions, explicit invariants, role separation, independent review, static and dynamic analysis, formal verification where feasible, and staged deployment. Upgrade mechanisms must balance maintainability with protection against unilateral policy changes. Emergency pause and rollback procedures should require multi-party authorization and generate auditable records.

B. Key Management and Recovery

User control is meaningful only when citizens can safely protect and recover cryptographic keys. A government identity service cannot assume that every citizen will maintain a hardware wallet or understand key custody. Recovery may combine device-bound keys, trusted recovery contacts, in-person re-proofing, threshold signatures, and time-delayed administrative assistance. No recovery actor should be able to impersonate a citizen alone. Inclusive alternatives are also required for people with disabilities, limited connectivity, or low digital literacy.

C. Data Governance and Legal Alignment

A permissioned ledger needs a formal governance charter defining node operators, issuer accreditation, technical standards, liability, incident response, audit rights, change management, and dispute resolution. Privacy-by-design should be translated into enforceable data rules: purpose limitation, data minimization, lawful basis, transparent consent, access control, correction, retention, and breach notification [9, 10, 22, 25]. Legal analysis must address whether digital credentials and smart-contract decisions are recognized in each jurisdiction and how citizens can challenge an automated outcome.

D. Operational Trade-offs

Blockchain adds value when multiple institutions need a shared, independently verifiable trust state. It may add unnecessary complexity when a single agency controls all participants and conventional signed databases already meet the requirement. A disciplined decision process should therefore compare the proposed ledger with public-key infrastructure, federated identity, and other distributed architectures. Selection criteria should include threat model, number of trust domains, transaction volume, latency, integration cost, governance capacity, and long-term maintainability.

VII. Practical Implications and Adoption Roadmap

For government institutions, the framework suggests a staged rather than system-wide transition.

- 1) **Governance and use-case selection:** Establish accountable sponsors, select a bounded high-value service, define legal authority, and agree on credential semantics and node governance.
- 2) **Prototype and assurance:** Implement issuer, wallet, verifier, and contract components in a test environment. Conduct privacy threat modeling, contract audit, penetration testing, and accessibility review.
- 3) **Controlled pilot:** Enroll a limited population, retain a conventional fallback channel, monitor service quality, evaluate recovery and redress, and collect evidence on user trust and administrative cost.
- 4) **Interoperable scaling:** Expand only after performance, security, and legal controls meet predefined thresholds. Standardize interfaces, accredit additional issuers, and continuously audit both code and governance.

Policy makers should create legal clarity for decentralized credentials and smart-contract-supported decisions, adopt privacy-by-design obligations, mandate interoperability standards, and define liability across issuers, wallet providers, ledger operators, and service agencies. System designers should prioritize simple proofs, minimal on-chain data, human-readable consent, graceful failure, and appealability.

VIII. Limitations and Future Research

This study is conceptual and does not implement or empirically test the proposed architecture. It cannot quantify transaction throughput, latency, storage cost, attack resistance, user acceptance, or institutional readiness. The evidence synthesis is broad and concept-centered rather than a formal systematic review with exhaustive database screening. In addition, legal requirements differ across jurisdictions and may change as decentralized identity regulation develops.

Future research should implement a permissioned prototype and evaluate it against a centralized baseline. Important measures include

credential-issuance time, verification latency, revocation propagation, node-failure tolerance, contract execution cost, recovery success, privacy leakage, accessibility, and cross-agency integration effort. Security studies should test contract vulnerabilities, wallet compromise, issuer collusion, metadata correlation, and denial-of-service scenarios. Pilot studies should also examine citizen comprehension, trust, consent behavior, and the effectiveness of appeal mechanisms.

IX. Conclusion

Blockchain and smart contracts can support a more resilient, user-centered, and interoperable model of government digital identity when they are used as a shared trust and policy layer rather than as a public store of personal information. The proposed framework combines government-issued verifiable credentials, citizen-controlled presentation, a permissioned consortium ledger, carefully scoped smart contracts, and encrypted off-chain storage. Conceptual analysis indicates improved resistance to centralized compromise, stronger auditability, selective disclosure, and reusable cross-agency verification.

These advantages are conditional. Poorly designed smart contracts, weak key recovery, metadata leakage, unclear governance, or inadequate legal safeguards can reproduce or amplify existing harms. Responsible adoption therefore requires privacy-by-design, rigorous software assurance, open standards, accountable institutional roles, accessible recovery, and empirical validation. Under these conditions, blockchain-enabled identity can become a credible component of digital-government infrastructure rather than a technology-led replacement for governance.

X. References

- [1] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.
- [2] A. Al-Kuwaiti, K. Kyriakopoulos, and S. Hussein, "Blockchain for digital identity management: Opportunities and challenges," *Information Systems Frontiers*, vol. 23, no. 3, pp. 557–576, 2021.
- [3] C. Allen, "The path to self-sovereign identity," *Life With Alacrity*, 2016.
- [4] A. M. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and DApps*, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2023.
- [5] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts," in *Principles of Security and Trust*. Berlin, Germany: Springer, 2017, pp. 164–186.
- [6] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.
- [7] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [8] P. Dunleavy, H. Margetts, S. Bastow, and J. Tinkler, "New public management is dead—Long live digital-era governance," *Journal of Public Administration Research and Theory*, vol. 16, no. 3, pp. 467–494, 2006.
- [9] European Union Agency for Cybersecurity, *Decentralised Digital Identity and Trust Services*. Athens, Greece: ENISA, 2022.
- [10] European Union Agency for Cybersecurity, *Blockchain Security and Trust Mechanisms*. Athens, Greece: ENISA, 2023.
- [11] J. R. Gil-Garcia, S. S. Dawes, and T. A. Pardo, "Digital government and public management research," *Government Information Quarterly*, vol. 35, no. 4, pp. S1–S5, 2018.
- [12] S. Gregor, "The nature of theory in information systems," *MIS Quarterly*, vol. 30, no. 3, pp. 611–642, 2006.
- [13] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.
- [14] Y. Jabareen, "Building a conceptual framework: Philosophy, definitions, and procedure," *International Journal of Qualitative Methods*, vol. 8, no. 4, pp. 49–62, 2009.
- [15] M. Janssen and E. Estevez, "Lean government and platform-based governance—Doing more with less," *Government Information Quarterly*, vol. 30, no. 1, pp. S1–S8, 2013.
- [16] M. Janssen, Y. Charalabidis, and A. Zuiderwijk, "Benefits, adoption barriers and myths of open data and open government," *Information Systems Management*, vol. 29, no. 4, pp. 258–268, 2012.
- [17] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.
- [18] I. Mergel, N. Edelmann, and N. Haug, "Defining digital transformation: Results from expert interviews," *Government Information Quarterly*, vol. 36, no. 4, Art. no. 101385, 2019.
- [19] M. B. Miles, A. M. Huberman, and J. Saldaña, *Qualitative Data Analysis: A Methods Sourcebook*, 3rd ed. Thousand Oaks, CA, USA: Sage, 2014.
- [20] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.
- [21] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- [22] Organisation for Economic Co-operation and Development, *Digital Government Index 2021*. Paris, France: OECD Publishing, 2021.
- [23] S. Øines, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Information Quarterly*, vol. 34, no. 3, pp. 355–364, 2017.
- [24] A. Preukschat and D. Reed, *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Shelter Island, NY, USA: Manning, 2021.

- [25] A. Romanou, "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise," *Computer Law & Security Review*, vol. 34, no. 1, pp. 99–110, 2018.
- [26] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York, NY, USA: Penguin, 2016.
- [27] United Nations, *E-Government Survey 2022: The Future of Digital Government*. New York, NY, USA: United Nations Department of Economic and Social Affairs, 2022.
- [28] S. Wang, P. De Filippi, and A. Narayanan, "Self-sovereign identity," *Communications of the ACM*, vol. 64, no. 2, pp. 78–87, 2021.
- [29] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quarterly*, vol. 26, no. 2, pp. xiii–xxiii, 2002.
- [30] P. J. Windley, *Learning Digital Identity: A Hands-On Guide to Self-Sovereign Identity*. Sebastopol, CA, USA: O'Reilly Media, 2020.
- [31] Y. Al Moaiad, D. Alkhateeb, and M. Alökla, "Enhancing cybersecurity practices in Nigerian government institutions: An analysis and framework," *Journal of Electrical Systems*, vol. 20, no. 3, pp. 5964–5967, 2024.
- [32] Y. Al Moaiad, D. Alkhateeb, and M. Alökla, "Deep analysis of iris print and fingerprint for detecting drug addicts," *Journal of Electrical Systems*, vol. 20, no. 3, pp. 5639–5644, 2024.
- [33] Y. Al Moaiad, M. Alobed, and M. Alsakhnini, "Python solutions to address natural language challenges," *International Journal*, vol. 10, no. 3, pp. 3594–3603, 2024.
- [34] Y. Al Moaiad, M. Alobed, M. Alsakhnini, and A. M. Momani, "Challenges in natural Arabic language processing," *Edelweiss Applied Science and Technology*, vol. 8, no. 6, pp. 4700–4705, 2024.