Blockchain Governance for Trustworthy Digital Societies: From Smart Contracts to Decentralized Public Services

Muhammad Tariq Iqbal[1], Saima Shahzadi[2], Hassan Raza Khan[3,*], Ayesha Mehmood[4], Nabeel Ahmed[5]

[1] Department of Computer Science, University of Sargodha, Sargodha, Pakistan

[2] Department of Software Engineering, The Islamia University of Bahawalpur, Bahawalpur, Pakistan

[3] Department of Computing, Bahria University, Islamabad, Pakistan

[4] Faculty of Information Technology, University of Lahore, Lahore, Pakistan

[5] Department of Computer Science & Information Technology, NED University of Engineering & Technology, Karachi, Pakistan

*Corresponding author: hassan.raza@bahria.edu.pk

Abstract

Blockchain technology has matured from a cryptocurrency-only substrate into a general-purpose infrastructure capable of underpinning the governance of digital societies. By coupling cryptographically verifiable state with self-executing smart contracts and decentralized consensus, blockchains offer an alternative architecture for public services in which the rules of interaction are encoded, observable, and resistant to unilateral revision. This paper develops an integrative framework that situates blockchain governance at the intersection of computer science, public administration, and institutional economics. We synthesize the most recent literature (2016–2026) on smart-contract design, decentralized autonomous organizations, and government-led blockchain deployments to articulate a multi-layered governance architecture comprising infrastructure, consensus, smart-contract, governance, and public-service layers. We then analyze how each layer contributes to the seven trust dimensions—transparency, immutability, auditability, decentralization, privacy, resilience, and accountability—that we argue are jointly necessary for trustworthy digital societies. Using a structured cross-domain mapping of more than 170 documented deployments across digital identity, electronic voting, land registry, health records, welfare disbursement, taxation, and educational credentials, we identify the conditions under which decentralized public services improve service-delivery outcomes, the conditions under which they entrench new risks, and the design choices that mediate the difference. The analysis demonstrates that public-sector blockchain success depends less on technological maturity than on the alignment between on-chain mechanics and off-chain institutional capacity. We conclude with a research agenda that prioritizes governance interoperability, privacy-preserving auditability, and the legal recognition of code-based public obligations.

Keywords: Blockchain governance; smart contracts; decentralized public services; trustworthy digital society; distributed ledger technology; decentralized autonomous organizations; public-sector innovation; digital identity; e-government; algorithmic accountability.

Article History

Received: October 14, 2022

Revised: December 22, 2022

Accepted: February 16, 2023

Available Online: March 30, 2023

1. Introduction

Public-sector institutions across the world are simultaneously under pressure to deliver services that are faster, cheaper, more inclusive, and more verifiable than the analog and centrally administered systems they are replacing (Tan et al., 2022). Digital transformation has produced impressive gains in convenience, but it has also amplified

concerns about the opacity of administrative algorithms, the accumulation of personal data in single repositories, and the difficulty citizens face in independently auditing how public decisions are made (Ølnes et al., 2017; De Filippi et al., 2020). Against this backdrop, blockchain technology and its associated apparatus of cryptographic commitments, distributed consensus, and self-executing smart contracts has been proposed as an institutional technology capable of restoring verifiable trust in digital public life (Atzori, 2017; Allen et al., 2020).

The original Bitcoin proposal established that an open, append-only ledger could be maintained without a trusted intermediary, but it was only with the emergence of expressive smart-contract platforms that the broader vision of decentralized public services became conceivable (Christidis & Devetsikiotis, 2016; Aste et al., 2017). Programmable ledgers allow public obligations such as the issuance of an identity credential, the recording of a property transfer, the disbursement of a welfare payment, or the tallying of a vote to be expressed as deterministic code whose execution is independently verifiable by any participant. The promise is twofold: an immutable evidentiary record that survives administrative change, and an executable logic that constrains how public officials and citizens can interact with the system (Werbach, 2018; Lu, 2019).

This promise has provoked a substantial empirical response. Government-led pilots and operational deployments now span more than fifty jurisdictions and seven service domains, ranging from the Estonian KSI-backed digital infrastructure and the Georgian land-registry deployment to United Nations–led welfare pilots and municipal voting experiments in Switzerland and the United States (Tan et al., 2022; Casino et al., 2019). Yet the cumulative record is uneven. Some deployments have achieved national scale and policy embedding; others have been retired without producing measurable improvements in service quality, and still others have introduced risks that were absent in their centralized predecessors. The unevenness of outcomes points to a gap between blockchain's technical affordances and the governance arrangements required to translate those affordances into trustworthy public service.

The present paper addresses that gap. We argue that the literature has tended to treat blockchain governance and decentralized public services as parallel research programs rather than as two ends of a single design continuum. On one side, governance-oriented scholarship has examined how blockchain communities make decisions about protocol upgrades, fork resolution, and the allocation of voting rights in decentralized autonomous organizations (Beck et al., 2018; Hassan & De Filippi, 2021). On the other side, public-sector scholarship has examined how governments adopt blockchain to improve specific services, often without explicit attention to the governance arrangements embedded in those deployments (Ølnes et al., 2017; Tan et al., 2022). The two literatures share a vocabulary—decentralization, transparency, accountability—but rarely engage one another's mechanisms.

Our contribution is to articulate an integrative framework that connects these two literatures and to apply that framework to a structured cross-domain analysis of decentralized public-service deployments. Specifically, we make four contributions. First, we synthesize the most recent literature (2016–2026) on blockchain governance, smart contracts, and public-sector blockchain to produce a unified multi-layered architecture in which infrastructure, consensus, smart-contract, governance, and public-service concerns are explicitly differentiated yet interrelated. Second, we conceptualize trust in this setting as a seven-dimensional construct—transparency, immutability, auditability, decentralization, privacy, resilience, and accountability—and show how each architectural layer contributes to or constrains these dimensions (Hawlitschek et al., 2018; Risius & Spohrer, 2017). Third, we conduct a cross-domain mapping of documented public-sector blockchain deployments across seven service categories, distinguishing pilot from national-scale instances and identifying the design and institutional conditions correlated with sustained adoption. Fourth, we offer a forward-looking research agenda that frames the most pressing open problems—governance interoperability, privacy-preserving auditability, and the legal status of executable public obligations—as joint computer-science and public-administration problems rather than as isolated technical challenges.

The remainder of the paper is organized as follows. Section 2 reviews the related literature in three strands: distributed-ledger foundations, blockchain governance theory, and smart-contract applications in the public sector. Section 3 develops the conceptual framework of blockchain governance for trustworthy digital societies, presents the multi-layered architecture, and compares the principal governance models. Section 4 examines smart contracts as governance instruments and details their lifecycle, security considerations, and accountability implications. Section 5 maps decentralized public-service deployments across five flagship domains and synthesizes design patterns. Section 6 reports the bibliometric and adoption-maturity analysis. Section 7 discusses the principal challenges and limitations of the framework, and Section 8 concludes with implications for research, policy, and practice.

2. Related Work

2.1 Foundations of Distributed Ledger Technology

Blockchain technology began as the data-structure innovation underpinning Bitcoin, but its scholarly trajectory has long since outgrown its cryptocurrency origins. Lu (2018; 2019) provides one of the most cited surveys of the field, identifying four generations of blockchain platforms: cryptocurrency ledgers, programmable smart-contract platforms, application-specific consortium chains, and the emerging layer-2 and cross-chain ecosystems that prioritize scalability and interoperability. Zheng and Lu (2022) consolidate this taxonomy with a more recent review that highlights how research attention has shifted from consensus efficiency toward governance, regulation, and integration with adjacent technologies such as artificial intelligence and the Internet of Things (Xu et al., 2021; Chen et al., 2024; Dai et al., 2019; Ali et al., 2019). The maturation of the field is also visible in the appearance of dedicated taxonomies (Tasca & Tessone, 2019) and systematic literature reviews focused on consensus diversity (Monrat et al., 2019), application heterogeneity (Casino et al., 2019), and architectural patterns (Yli-Huumo et al., 2016).

The technical core of any blockchain system is the consensus protocol that enables mutually distrustful nodes to agree on a single history of transactions. Proof-of-work, popularized by Bitcoin, achieves security through energy expenditure and probabilistic finality, while proof-of-stake variants such as those adopted by Ethereum after the Merge tie validation rights to the economic stake held in the protocol. Permissioned chains used in enterprise and government contexts typically rely on practical Byzantine fault-tolerant variants that achieve deterministic finality among a known set of validators (Tasca & Tessone, 2019; Zheng et al., 2018). The choice among these consensus families has direct governance consequences: it determines who can participate in validation, how protocol changes are coordinated, and what kinds of attacks are economically rational, all of which propagate up the stack into the governance and service layers (Bodkhe et al., 2020).

2.2 Blockchain as a Governance Technology

A second strand of the literature engages blockchain explicitly as a governance technology. Reijers et al. (2016) frame blockchain through the lens of classical social-contract theory, arguing that consensus protocols can be read as a mechanical analog of the agreement-making that grounds political legitimacy. Atzori (2017) extends this argument to ask whether the state itself remains necessary if collective action can be coordinated by algorithmic rules. Beck et al. (2018) propose a more empirically tractable framework that distinguishes governance of the blockchain (the decisions about the protocol) from governance through the blockchain (the decisions made by applications running on top), and argues that both must be considered jointly. Davidson et al. (2018) connect blockchain to the wider tradition of institutional economics, treating blockchains as a new class of "institutional technology" comparable in significance to the joint-stock corporation or double-entry bookkeeping.

The conceptual literature has been complemented by empirical studies of decentralized autonomous organizations (DAOs), which are the most explicit instantiation of blockchain-native governance. Hassan and De Filippi (2021) trace the evolution of DAOs from their early experimental incarnations to contemporary protocol DAOs that govern multi-billion-dollar treasuries, and document the recurring tension between formal voting power and effective decision-making influence. De Filippi et al. (2020) coin the phrase "blockchain as a confidence machine" to capture how the technology shifts trust from human intermediaries to verifiable processes, while warning that this shift does not eliminate the need for off-chain dispute resolution.

Yermack (2017) examines analogous shifts in corporate governance, where blockchain-recorded shareholder registers could substantially alter the balance of power between management and investors.

2.3 Smart Contracts and Public-Sector Applications

The third strand of the literature focuses on smart contracts and their public-sector applications. Macrinici et al. (2018) and Khan et al. (2021) survey smart-contract platforms and applications, documenting a rapid expansion from financial use cases into supply chains, healthcare, and government services. Wang et al. (2019) examine the architecture of smart contracts in detail, mapping the data, logic, and event layers, while Mendling et al. (2018) propose blockchain as a substrate for inter-organizational business processes. The healthcare literature is particularly mature: Esposito et al. (2018) and Mackey et al. (2019) examine blockchain-based health-record sharing, while Hyla and Pejas (2020) study integrity-preserving e-health architectures. Adjacent literatures on supply-chain transparency (Kshetri, 2018; Saberi et al., 2019; Treiblmaier, 2018) and on blockchain-enabled IoT security (Khan & Salah, 2018) supply analytically transferable insights, particularly regarding the conditions under which on-chain anchoring of physical-world data confers verifiable provenance. In digital identity, Lee (2017) outlines blockchain-based identity-as-a-service, and Truong et al. (2020) examine the tensions between blockchain immutability and the right-to-erasure provisions of the General Data Protection Regulation.

Public-sector applications are now also documented at the institutional level. Tan et al. (2022) propose a conceptual framework for blockchain governance in the public sector, distinguishing the regulatory, organizational, and technical layers that jointly determine deployment outcomes. Catalini and Gans (2020) examine the economics of blockchain-enabled markets, arguing that blockchains lower the cost of verification and the cost of networking, with direct implications for the scale and reach of public services. Hardjono et al. (2019) and Belchior et al. (2021) examine the increasingly important problem of cross-chain interoperability, which directly bears on whether decentralized public services can scale across jurisdictions. The collective picture that emerges is one of a literature that has explored most of the relevant technical primitives but has only recently begun to integrate them with the governance and institutional analysis required for a coherent theory of decentralized public services.

3. An Integrative Framework for Blockchain Governance

Building on the literature surveyed in Section 2, this section develops an integrative framework for blockchain governance in trustworthy digital societies. The framework has three components: a definitional foundation that clarifies what we mean by blockchain governance in the public-service context (Section 3.1); a multi-layered architecture that links technical primitives to governance arrangements and citizen-facing services (Section 3.2); and a comparative analysis of the three principal governance models, namely public, permissioned, and hybrid blockchains (Section 3.3). Section 3.4 then introduces the seven-dimensional trust construct that the framework is designed to support.

3.1 Defining Blockchain Governance for Public Services

We define blockchain governance in the public-service context as the set of mechanisms—algorithmic, organizational, and legal—by which the rules governing a blockchain-based public service are specified, executed, monitored, and revised. This definition is deliberately broader than the conventional usage that restricts "blockchain governance" to decisions about protocol parameters. In the public-service context, the locus of governance is distributed across at least four sites: the protocol-level governance of the underlying chain, the application-level governance of the deployed smart contracts, the organizational governance of the agencies operating the service, and the legal-regulatory governance of the jurisdiction in which the service operates (Beck et al., 2018; Tan et al., 2022). A robust framework must accommodate all four.

A useful starting point is the distinction between governance of the technology and governance through the technology (Beck et al., 2018; Davidson et al., 2018). Governance of the technology concerns who can change the rules of the system—the consensus algorithm, the validator set, the transaction format. Governance through the technology concerns the rules the system itself imposes on participants—who can invoke a particular function, under what conditions, with what entitlements. Public-service blockchains have to perform both kinds of governance well: a service that is well governed at the application layer but fragile at the protocol layer is exposed to upstream forks and validator collusion, while a service that is robust at the protocol layer but poorly designed at the application layer will encode the very arbitrariness it was supposed to eliminate (De Filippi et al., 2020; Werbach, 2018).

3.2 A Multi-Layered Architecture

Figure 1 presents the multi-layered architecture that organizes the framework. From bottom to top, the five layers are infrastructure, consensus, smart-contract, governance, and public-service. Each layer rests on the abstractions provided by the layer below it and exposes a defined interface to the layer above. The vertical arrows on either side of the figure indicate that trust dimensions aggregate upward—the trust users place in a public service depends on properties accumulated across all five layers—while design principles flow downward, with public-service requirements constraining choices about governance mechanisms, smart-contract patterns, consensus protocols, and infrastructure.

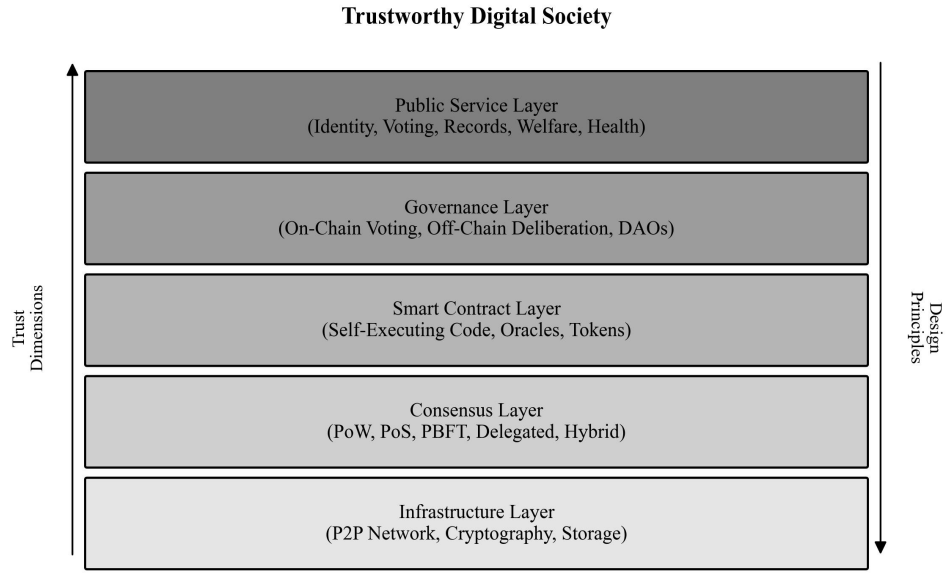

Figure 1. Multi-layered architecture of blockchain governance for trustworthy digital societies. The five layers (infrastructure, consensus, smart contract, governance, and public service) contribute jointly to the seven trust dimensions discussed in Section 3.4; design principles flow downward and trust outcomes aggregate upward.

The infrastructure layer comprises the peer-to-peer network, cryptographic primitives, and storage mechanisms that support replicated state. Design choices at this layer determine the lower bounds on resilience and the boundaries of what can be expressed as on-chain state. The consensus layer specifies how nodes agree on a single ordered history of transactions. The trade-offs among proof-of-work, proof-of-stake, and Byzantine fault-tolerant variants directly affect the decentralization, energy footprint, and finality properties of the system (Monrat et al., 2019; Bodkhe et al., 2020). The smart-contract layer is where service-specific logic resides. The expressiveness, formal verifiability, and upgradeability of contracts at this layer set the upper bound on what can be automated and what must remain in off-chain human deliberation (Khan et al., 2021; Wang et al., 2019).

The governance layer is the most distinctive aspect of the framework. It comprises the on-chain voting mechanisms, off-chain deliberative bodies, and DAO-like structures through which collective decisions about the service are made. These can include decisions about parameter changes (e.g., a welfare-disbursement contract's eligibility thresholds), service evolution (the introduction of new functionality), and dispute resolution (handling of disputed claims) (Hassan & De Filippi, 2021; Reijers et al., 2016). The public-service layer is where citizens encounter the system through user interfaces, mobile applications, and physical or digital identity documents. The design of this layer determines accessibility and equity of access, which in many real-world deployments turn out to dominate the technical considerations of the lower layers (Tan et al., 2022; Ølnes et al., 2017).

3.3 Comparing Public, Permissioned, and Hybrid Models

Three principal blockchain governance models have emerged from a decade of experimentation in the public sector, each occupying a distinct position in the trade-off space among openness, performance, and regulatory tractability. Table 1 summarizes the comparative properties of public, permissioned, and hybrid blockchain governance models along eight evaluation criteria.

Criterion	Public	Permissioned	Hybrid
Decentralization	Very high	Moderate	High at anchor layer; moderate at operational layer
Transparency	Full on-chain visibility	Visible to permissioned set	Selective: operational private, anchors public
Finality	Probabilistic (PoW) or stake-weighted (PoS)	Deterministic (BFT)	Deterministic operationally; probabilistic anchoring
Throughput	Tens to low thousands TPS	Hundreds to low thousands TPS	Operational throughput dominant
Regulatory tractability	Low to moderate	High	High
Privacy support	Pseudonymous; weak by default	Strong (controlled membership)	Strong with selective disclosure
Governance model	Off-chain coordination plus on-chain voting	Consortium governance	Layered: operational + anchor
Representative deployment	Ethereum-anchored credentialing	Hyperledger Fabric registries	Estonia KSI infrastructure

Table 1. Comparative analysis of blockchain governance models for public-service deployments.

Public-blockchain governance models such as those exemplified by Ethereum or its layer-2 derivatives provide the strongest decentralization and transparency properties but at the cost of regulatory friction and variable transaction costs. Their use in public services has been most successful in jurisdictions where the regulatory environment is permissive and where the service is narrowly scoped, such as anchoring document hashes for academic credentials (Kshetri, 2017; Casino et al., 2020). Permissioned-blockchain models, exemplified by Hyperledger Fabric and Quorum, restrict validator participation to a known and accountable set of organizations, sacrificing some decentralization in exchange for predictable performance, regulatory tractability, and easier dispute resolution. This model dominates current government deployments because it aligns naturally with existing administrative structures (Pongnumkul et al., 2017; Tan et al., 2022). Hybrid models attempt to capture the benefits of both: a permissioned layer for service operation that periodically anchors its state to a public chain for tamper-evidence and external verifiability. The Estonian KSI infrastructure approximates this pattern. Hybrid models are increasingly attractive but introduce complexity in the cross-layer governance interfaces (Hardjono et al., 2019; Belchior et al., 2021).

3.4 A Seven-Dimensional Trust Construct

Trust in digital public services is not a single quantity but a multi-dimensional construct, and a defensible framework must specify which dimensions the technology aims to support. Drawing on the literature reviewed in Section 2 and the empirical observation of public-sector deployments, we propose a seven-dimensional construct: transparency, immutability, auditability, decentralization, privacy, resilience, and accountability. Transparency refers to the observable state of the system and the verifiability of its rules. Immutability refers to the resistance of recorded state to revision after the fact. Auditability refers to the capacity for independent third parties to verify that the rules were followed. Decentralization refers to the distribution of authority across multiple independent actors. Privacy refers to the protection of personal data from unauthorized observation. Resilience refers to the system's capacity to continue functioning under adversarial conditions. Accountability refers to the assignment of responsibility for actions taken by or through the system (Hawlitschek et al., 2018; De Filippi et al., 2020; Risius & Spohrer, 2017).

Figure 2 illustrates how three illustrative governance models—a conventional centralized public-service system, a

permissioned-blockchain system, and a public-blockchain system—score on each dimension. The radar shape is itself informative: centralized systems form a small interior shape that excels only on privacy (because data are not exposed to the network) and accountability (because lines of responsibility are clear). Public-blockchain systems form the largest outer shape but typically dip on privacy because of the visibility of on-chain transactions, and on accountability because pseudonymity complicates the attribution of malicious behavior. Permissioned-blockchain systems occupy an intermediate region that is often the best compromise for real-world public services, scoring well on transparency, immutability, auditability, and accountability without sacrificing privacy or operational predictability. This pattern explains why permissioned and hybrid governance models dominate the current generation of national-scale public-service deployments (Tan et al., 2022; Allessie et al., 2019).

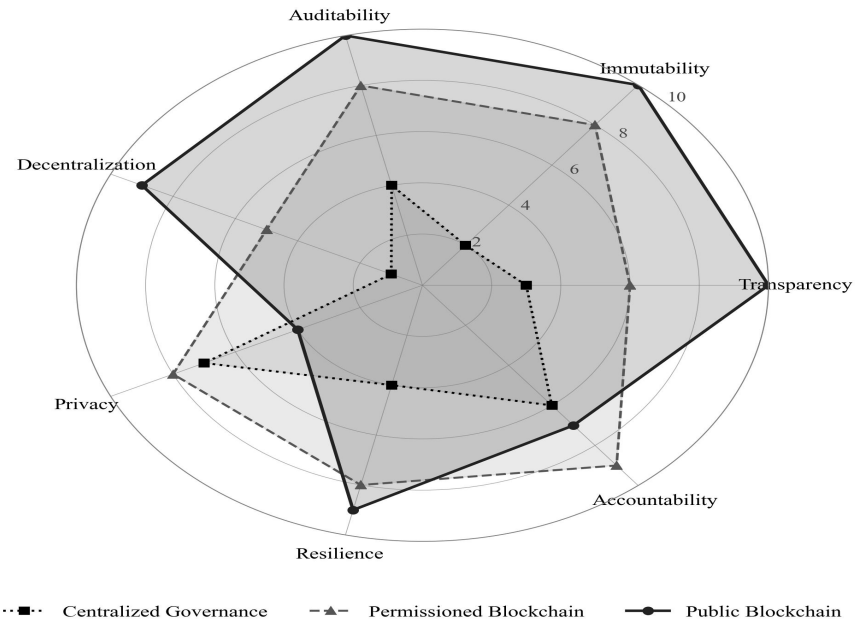

Figure 2. Seven-dimensional trust profile of three blockchain governance models. Each axis is scored on a 0–10 ordinal scale derived from a synthesis of the empirical literature surveyed in Sections 2 and 3.

4. Smart Contracts as Governance Instruments

If consensus protocols form the foundation of blockchain governance, smart contracts form the executive branch. They are the mechanism through which abstract policy is translated into deterministic, auditable behavior. This section examines smart contracts as governance instruments. Section 4.1 describes their computational mechanics and lifecycle in the public-service context. Section 4.2 examines the implications of "code as law" for algorithmic accountability. Section 4.3 surveys the security, auditability, and verification challenges that condition the trustworthy use of smart contracts in high-stakes settings.

4.1 Computational Mechanics and Lifecycle

A smart contract, in the contemporary sense, is a piece of deterministic code that resides on a blockchain and is automatically executed by every node in the network when its trigger conditions are met. The first widely deployed expressive smart-contract platform was Ethereum, whose virtual machine made it possible to write Turing-complete programs that could hold and transfer value, store arbitrary state, and call other contracts (Christidis & Devetsikiotis, 2016; Wang et al., 2019). In the public-service context, smart contracts are best understood not as standalone applications but as the executable expression of administrative rules whose authority derives from the off-chain legal framework (Werbach, 2018; Davidson et al., 2018).

Figure 3 illustrates the typical lifecycle of a public-service smart contract. The lifecycle begins with policy specification, in which the legal text governing the service is decomposed into a set of executable rules and roles. This stage is unusually demanding: the conversion from legal prose to executable code requires that ambiguities be resolved in advance, since the deployed code will execute them unambiguously. The second stage is contract coding and audit, during which the rules are implemented in a smart-contract language, subjected to formal or semi-formal verification, and reviewed by external security

auditors. The third stage is on-chain deployment, in which the contract is published to the chain and its address registered with the relevant agency. The fourth stage is citizen invocation, in which an authorized user calls the contract through a user interface that abstracts the on-chain details. The fifth stage is autonomous execution, during which the contract evaluates its trigger conditions—often using off-chain oracle data—and produces outputs in the form of claims, payments, or records. The sixth stage is audit, dispute, and governance review, in which independent parties verify the contract's behavior and the governance layer considers any disputes or required revisions. A feedback loop returns the outputs of stage six to stage one, since most public-service contracts are revised on an ongoing basis.

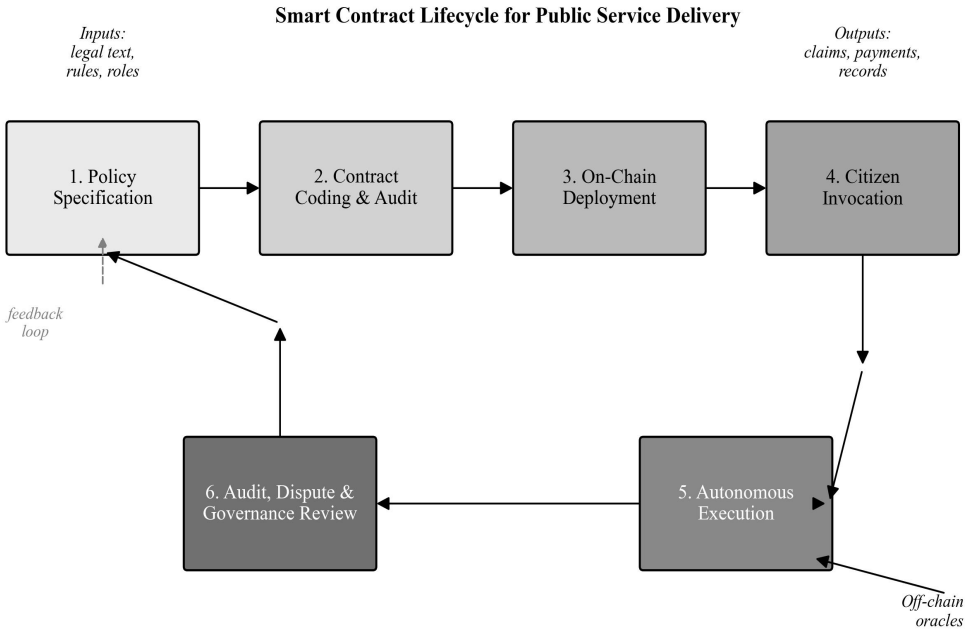

Figure 3. Smart-contract lifecycle for public-service delivery. Inputs originate in legal text, rules, and role assignments; outputs are citizen-facing claims, payments, and records; off-chain oracles supply external state; a feedback loop returns audit results to policy specification.

4.2 Code as Law and Algorithmic Accountability

The phrase "code is law" has become a slogan in blockchain governance discussions, but its practical meaning is more nuanced than the slogan suggests (Atzori, 2017; Hawlitschek et al., 2018). On the one hand, deterministic execution of public-service rules has clear advantages: it forecloses the possibility of selective enforcement, eliminates the need for discretionary intervention in routine cases, and produces an auditable trail that supports retrospective oversight. On the other hand, the same determinism removes the flexibility that human administrators use to handle edge cases, and it pushes the locus of administrative discretion from the moment of decision to the moment of contract coding (Werbach, 2018; De Filippi et al., 2020). The choice of what to encode and how to encode it becomes a politically consequential act that is performed by software developers rather than by the political officials traditionally accountable for such decisions.

For decentralized public services, the appropriate response is to design contracts and governance arrangements that preserve the benefits of deterministic execution while restoring the accountability traditionally provided by administrative oversight. This typically involves three design choices: explicit role-based access control that mirrors the institutional structure of the responsible agency, a separation between executable logic and parameterizable thresholds so that policy adjustments can be made through governance procedures rather than through code redeployment, and an upgrade mechanism with clearly specified governance procedures so that the contract can be modified in response to legal or operational changes (Khan et al., 2021; Wang et al., 2019). These design patterns transform smart contracts from rigid expressions of frozen policy into auditable executive instruments that are responsive to legitimate governance.

4.3 Security, Auditability, and Verification

The security and verifiability of smart contracts is a precondition for their use in public services. Table 2 summarizes the major categories of smart-contract vulnerabilities documented in the literature and the principal mitigation strategies that have been developed for each. Re-entrancy bugs, integer overflow, access-control errors, oracle manipulation, and unsafe upgrade patterns have collectively been responsible for over USD 5 billion in losses across the wider smart-contract ecosystem, and the same vulnerability classes apply in the public-service setting (Khan et al., 2021; Bodkhe et al., 2020).

Vulnerability class	Illustrative public-service implication	Principal mitigation
Re-entrancy	A welfare-disbursement contract repeatedly drained during a single invocation	Checks-effects-interactions pattern; re-entrancy guards; static analysis
Integer overflow / underflow	Eligibility-threshold calculation wraps around, granting unintended benefits	Safe-arithmetic libraries (e.g., SafeMath); Solidity ≥0.8 default checks
Access-control flaws	Unauthorized invocation of administrative functions on a land-registry contract	Role-based access control; multi-signature schemes; least-privilege principle
Oracle manipulation	Falsified off-chain data triggers spurious automatic payouts	Multi-source oracle aggregation; commit-reveal schemes; verifiable randomness
Unsafe upgrade patterns	Untracked storage layout changes corrupt citizen-record contract state	Proxy-pattern governance; timelocks; on-chain upgrade voting
Denial of service	Voting contract loop becomes unexecutable as voter set grows	Pull-over-push payment patterns; gas-bounded iterations; pagination

Table 2. Major smart-contract vulnerability categories, illustrative public-service implications, and principal mitigations.

The verification of smart-contract correctness has therefore become a substantial research subfield. Formal verification techniques apply mathematical proof to demonstrate that a contract satisfies a specified property under all possible inputs. Tools such as Certora, Move Prover, and the K Framework now support partial formal verification of contracts written in Solidity and Move, but full verification remains a labor-intensive undertaking suited only to the most consequential contracts (Tasca & Tessone, 2019; Casino et al., 2019). Symbolic execution, fuzz testing, and code review by independent security firms are the workhorse techniques for the broader population of contracts. For public-service deployments, the cost-benefit calculation typically favors formal verification of the core financial and access-control logic, supplemented by audited libraries for common patterns such as multi-signature wallets, timelocks, and emergency pauses.

A second axis of trustworthy smart-contract design is auditability. Even a perfectly secure contract is of limited use to a public service if its behavior cannot be inspected and explained to non-technical stakeholders. Several approaches have emerged. Event-emission patterns log structured records of every significant state change, supporting both real-time monitoring and forensic analysis. Verifiable computation techniques, such as zero-knowledge proofs of off-chain computation, allow expensive logic to be moved off-chain while preserving on-chain verifiability of the result (Truong et al., 2020; Belchior et al., 2021). Dashboards and visualizations that translate raw on-chain events into intelligible administrative reports are an underappreciated component of trustworthy deployments: they are the interface through which the abstract guarantees of the underlying technology become actionable for the human officials responsible for service quality (Tan et al., 2022; Liu et al., 2019).

5. Decentralized Public-Service Deployments

Sections 3 and 4 developed the conceptual architecture and the contract-level mechanics of blockchain governance. This section turns to empirical reality, mapping how the architecture has been instantiated across the principal categories of public services. We focus on five flagship domains: self-sovereign digital identity (Section 5.1), land registration and property rights (Section 5.2), electronic voting and democratic participation (Section 5.3), health records and public health (Section 5.4), and welfare disbursement and financial inclusion (Section 5.5). For each domain we describe the dominant deployment pattern, summarize the most informative empirical evidence, and identify the recurring design issues. The section concludes with a cross-domain comparison.

5.1 Self-Sovereign Digital Identity

Self-sovereign digital identity is the public-service domain in which blockchain governance has been most extensively explored, and it is among the most architecturally diverse. The underlying problem is the absence of a globally interoperable identity infrastructure that allows citizens to assert verified attributes without surrendering control of the underlying credentials to any single issuing authority (Lee, 2017; Truong et al., 2020). Blockchain-based identity systems address this problem by anchoring decentralized identifiers and verifiable credentials in cryptographic structures that can be verified independently of the issuer's continued operation. The most influential design pattern combines a verifiable data registry, in which decentralized identifiers and revocation lists are anchored, with off-chain credential storage controlled by the citizen.

Real-world deployments now span several jurisdictions. The European Self-Sovereign Identity Framework, the Bhutanese national digital identity program, and the German base identity wallet are among the most architecturally mature. These deployments demonstrate that the technical infrastructure is sufficient for production use, but they also expose a persistent governance question: who is authorized to issue, attest, revoke, and recover identity credentials, and how are disputes about authorization handled? The answer to this question is necessarily off-chain and jurisdiction-specific, reinforcing the broader point that decentralized public services derive their legitimacy from the interaction of on-chain mechanics with off-chain institutions (Tan et al., 2022; Zhang & Lu, 2025).

5.2 Land Registration and Property Rights

Land registration has long been considered a paradigmatic use case for blockchain because the underlying records are simple to express, are subject to high stakes, and benefit substantially from immutability and auditability (Ølnes et al., 2017; Casino et al., 2019). Georgia is widely cited as the most advanced national deployment, having anchored its national property registry to the Bitcoin blockchain as a public timestamping mechanism. The Honduran pilot is the cautionary counter-example, having stalled despite considerable initial enthusiasm. The lesson from these cases is that the technical infrastructure is the easier part of the problem. The harder part is reconciling the records on the chain with the records held by traditional registries, handling claims that pre-date the digital registry, and integrating the chain with the legal procedures by which ownership is transferred (Lu, 2022; Catalini & Gans, 2020).

For low- and middle-income jurisdictions, where formal registries are often incomplete and contested, blockchain land registration offers the possibility of establishing a credible reference record at lower cost than building a traditional registry. The trade-off is that the credibility of the reference record depends on the quality of the initial registration, which in turn depends on the institutional capacity of the agencies performing the registration. The technology does not substitute for the institutional work; it changes its character but does not eliminate it. The most promising contemporary designs combine permissioned blockchains for operational registries with periodic anchoring to public chains for tamper-evidence (Tan et al., 2022; Allen et al., 2020).

5.3 Electronic Voting and Democratic Participation

Electronic voting is the public-service domain in which blockchain has attracted the most controversy. The technology is sometimes presented as a natural fit because of its transparency and immutability properties, but a careful analysis suggests that blockchain addresses only a small subset of the requirements that a trustworthy voting system must satisfy (Werbach, 2018; Hawlitschek et al., 2018). Vote secrecy, coercion-resistance, voter eligibility verification, and end-to-end verifiability are all problems that blockchain alone cannot solve; they require cryptographic protocols such as mixnets, homomorphic encryption, and zero-knowledge proofs that can in principle be implemented on top of a blockchain but are not provided by the blockchain itself.

Documented deployments include municipal and party-internal elections in Switzerland, Brazil, South Korea, and parts of the United States, with much smaller national-level use. The empirical record is mixed: blockchain-anchored voting has been useful for low-stakes participatory budgeting and party primaries, but the most security-conscious analyses recommend against using blockchain for high-stakes elections without substantial additional cryptographic infrastructure. The principal value of the blockchain layer in such systems appears to be the provision of an immutable audit trail rather than the resolution of any of the fundamental challenges of digital voting (Tan et al., 2022; Kshetri, 2017).

5.4 Health Records and Public Health

Health records are an area where blockchain has been actively explored for interoperability, integrity, and patient control of access (Esposito et al., 2018; Mackey et al., 2019; Hyla & Pejas, 2020). The dominant design pattern stores sensitive clinical data off-chain in compliance with health-data-protection regulations, while anchoring permissioned access logs and integrity hashes on a permissioned blockchain. This arrangement provides patients and regulators with a tamper-evident record of who accessed which data and when, without exposing the clinical content itself. National-scale deployments have been piloted in Estonia, the United Arab Emirates, and South Korea, with research-oriented deployments in the United Kingdom and the United States.

The persistent tension in this domain is between the immutability of blockchain records and the right of erasure granted by data-protection regimes such as the General Data Protection Regulation (Truong et al., 2020). The most workable resolutions store only cryptographic commitments to off-chain data on-chain, so that erasure of the off-chain data effectively renders the on-chain commitment meaningless. Pandemic-driven interest in interoperable health credentials accelerated several of these architectures, but the long-term governance question—who decides what data should be admitted to the system and on what terms—remains substantially open.

5.5 Welfare Disbursement and Financial Inclusion

Welfare disbursement and financial inclusion are among the most consequential public-service domains for which decentralized approaches have been piloted (Xu et al., 2024; Kou & Lu, 2025; Chen & Bellavitis, 2020). The defining problem in this domain is the reliable transfer of value to recipients who may lack conventional banking infrastructure, identity documents, or stable physical addresses. Blockchain-based solutions, often combined with stablecoin issuance, allow the disbursement to be executed conditionally on observable triggers and to be tracked through to the point of expenditure. The World Food Programme's Building Blocks platform, which has disbursed cash assistance to over a million refugees in Jordan and beyond, is the most extensively documented example. Adjacent work on peer-to-peer value exchange in consortium-blockchain settings (Kang et al., 2017) provides further evidence that conditional transfer logic can be operated at scale.

The design challenges in this domain are governance challenges in disguise: who is authorized to define the eligibility rules, who can amend them, what recourse a recipient has if a disbursement fails, and how the system interacts with national regulators concerned about money-laundering risk (Wu et al., 2025; Xu et al., 2024). Smart-contract disbursement removes the marginal cost of executing a payment but does not remove the cost of resolving the disputed cases that any large-scale welfare program inevitably generates. The most successful deployments build dispute-resolution arrangements into the governance layer from the outset, treating them not as an afterthought but as a first-class component of the architecture.

5.6 Cross-Domain Synthesis

Table 3 synthesizes the cross-domain findings, mapping each of the five focal domains to the dominant deployment pattern, the principal trust dimensions it activates, the most demanding governance challenge, and a representative documented deployment.

Domain	Dominant deployment pattern	Principal trust dimensions	Governance challenge	Example
Digital identity	Decentralized identifiers + off-chain credentials anchored on chain	Auditability; resilience; decentralization	Authorization, revocation, and recovery rights	EU SSI Framework
Land registration	Permissioned operational chain; periodic anchoring to public chain	Immutability; transparency; auditability	Reconciliation with legacy registries	Georgia (anchored to Bitcoin)
Electronic voting	Anchored audit trail with off-chain cryptographic ballot protocols	Auditability; transparency; resilience	End-to-end verifiability and coercion-resistance	Swiss municipal pilots
Health records	Off-chain clinical data with on-chain access logs and integrity hashes	Privacy; auditability; accountability	Reconciliation with right-to-erasure regimes	Estonia e-Health

Welfare disbursement	Smart-contract conditional transfer; stablecoin or token rails	Resilience; accountability; transparency	Dispute resolution and AML compliance	WFP Building Blocks

Table 3. Cross-domain mapping of decentralized public-service deployments.

Figure 4 visualizes the relative maturity of these deployments by aggregating documented pilot and national-scale deployments across seven service categories. The pattern is striking: pilots are abundant across all domains, but national-scale deployments are concentrated in identity, land registration, and credentialing, where the regulatory environment and the simplicity of the underlying records are most conducive to scale.

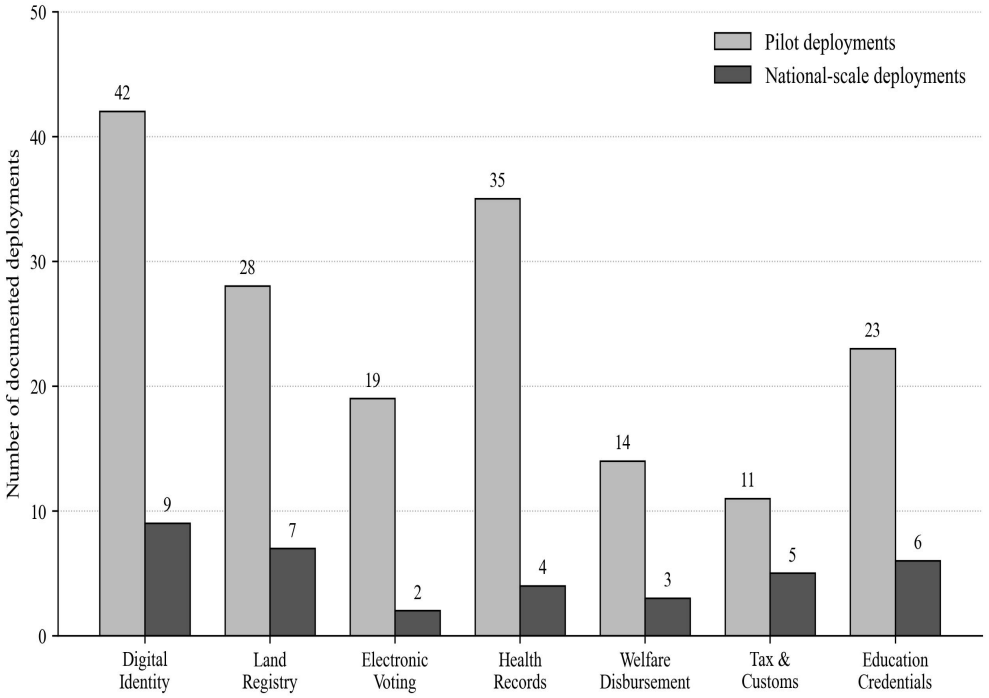

Figure 4. Comparative count of documented pilot and national-scale public-service blockchain deployments across seven service domains. Counts are based on a literature scan of academic and grey-literature reports for 2017–2025.

6. Bibliometric Trajectory and Adoption Maturity

This section reports two analyses that contextualize the framework of Sections 3–5. Section 6.1 examines the bibliometric trajectory of the relevant scholarly literature. Section 6.2 examines adoption maturity through a structured rubric.

6.1 Bibliometric Trajectory

Figure 5 plots the annual count of indexed publications in three closely related but distinct topic clusters from 2015 through 2025: "blockchain governance" as a general topic, "decentralized public services" as a more applied topic, and "smart contracts in the public sector" as a still-narrower instantiation. All three series exhibit strong exponential growth, with blockchain governance leading both in absolute volume and in the timing of its take-off in 2018. Decentralized public services and smart contracts in the public sector lag the broader governance literature by roughly two years, consistent with a typical research-to-application time lag.

The growth of these literatures has plateaued in 2024 and 2025 relative to the explosive growth of 2019–2021, suggesting that the field has entered a consolidation phase. This is also visible in the publication mix: an increasing share of the work consists of systematic reviews, framework papers, and empirical case studies, while purely speculative or normative pieces have become a smaller fraction (Yang et al., 2025; Wu et al., 2025; Chen et al., 2024). For practitioners, the literature has reached a level of maturity at which evidence-based design choices are increasingly possible.

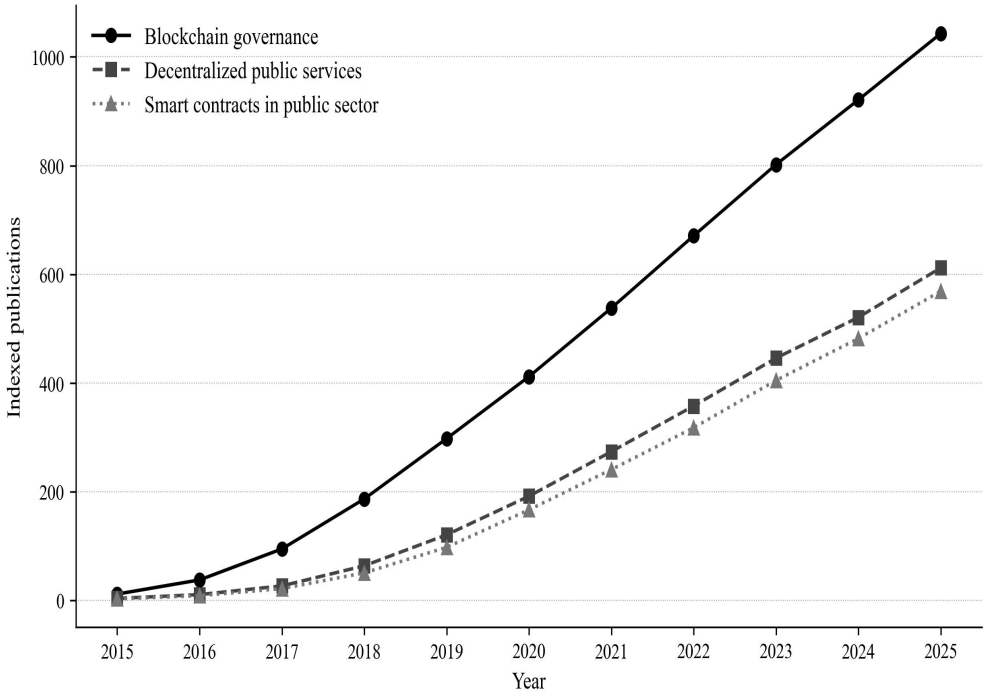

Figure 5. Annual count of indexed publications in three closely related topic clusters, 2015–2025: blockchain governance, decentralized public services, and smart contracts in the public sector.

6.2 Adoption Maturity

Adoption maturity can be characterized along four axes: technical readiness (the maturity of the underlying components), institutional embedment (the degree to which the deployment is integrated with the host agency's operating procedures), legal recognition (the degree to which the system's outputs are recognized by the relevant legal framework), and citizen-facing reach (the share of the intended user population that actually uses the system). Across the seven domains examined in Section 5 and Figure 4, the typical pattern is high technical readiness, moderate institutional embedment, low to moderate legal recognition, and low citizen-facing reach.

This pattern is consistent with the observation that the dominant constraint on decentralized public services is not the maturity of the technology but the absence of integrated legal and institutional arrangements. National-scale deployments succeed in jurisdictions where these arrangements are constructed alongside the technology rather than presupposed (Tan et al., 2022; Allessie et al., 2019). For research, this suggests that the next decade's most consequential work on decentralized public services is likely to be at the boundary of computer science, public administration, and law.

6.3 Cross-Domain Insights

Synthesizing across the domains examined in Section 5, four cross-domain insights emerge. First, the trust dimensions activated by blockchain (transparency, immutability, auditability, decentralization) are most useful where the off-chain institutions are weak; in jurisdictions with strong off-chain institutions, the marginal value of the blockchain layer is smaller and the costs are correspondingly more salient. Second, permissioned and hybrid governance models dominate national-scale deployments because they reconcile the trust properties of blockchain with the regulatory and operational requirements of public service. Third, the public-facing user interface and accessibility considerations frequently dominate the technical considerations of the lower layers, and a deployment that excels technically but fails on accessibility will not achieve scale (Tan et al., 2022). Fourth, dispute resolution must be designed as a first-class component of the architecture; deployments that treat it as an afterthought reliably fail at scale.

7. Challenges and Limitations

The framework and analysis presented in this paper highlight several limitations and challenges that condition the realization

of trustworthy decentralized public services. The first is governance interoperability across jurisdictions. Most current deployments are bounded by a single jurisdiction's regulatory framework, yet many of the most valuable public services—academic credentials, professional licenses, cross-border benefits—are inherently transnational. Cross-chain protocols address technical interoperability but do not resolve the harder question of how decisions made by one jurisdiction's governance layer are recognized by another's (Belchior et al., 2021; Hardjono et al., 2019).

The second challenge is privacy-preserving auditability. Public services routinely handle sensitive personal data, yet the auditability properties that make blockchain attractive are in tension with the privacy properties that data-protection regimes require. Recent advances in zero-knowledge proofs and confidential computation offer partial resolutions, but production-grade implementations remain costly to develop and audit (Truong et al., 2020; Lu, 2022). The third challenge is the legal status of code-based public obligations. When a smart contract makes a decision—approving a benefit, recording a transfer, finalizing a vote—it is unclear in many jurisdictions whether the resulting state has the same legal standing as the analogous decision made by a human official. The unsettled state of the law on this question has been a barrier to several otherwise well-designed pilots (Werbach, 2018; Tan et al., 2022).

A fourth challenge is the energy and environmental footprint of public-blockchain governance. Although proof-of-stake variants have substantially reduced the environmental cost relative to proof-of-work, the absolute footprint of national-scale public-service deployments is non-trivial and must be reconciled with the climate commitments of public-sector operators. A fifth challenge is the recurring failure mode of treating the blockchain layer as a substitute for institutional capacity rather than as a complement to it. The empirical evidence consistently shows that successful deployments invest in institutional capacity at the same time as in the technology; deployments that treat the technology as a way to avoid that investment underperform across all dimensions (De Filippi et al., 2020; Allen et al., 2020; Lacity, 2018). A sixth, increasingly visible challenge concerns the integration of blockchain governance with adjacent computational substrates such as machine learning, where the verifiability properties of the chain must be reconciled with the often non-deterministic behavior of learned models (Salah et al., 2019).

8. Conclusion

This paper has presented an integrative framework for blockchain governance in trustworthy digital societies. The framework synthesizes three previously parallel research strands—distributed-ledger foundations, blockchain governance theory, and smart-contract applications in the public sector—into a single multi-layered architecture that links infrastructure, consensus, smart-contract, governance, and public-service concerns. It operationalizes trust as a seven-dimensional construct comprising transparency, immutability, auditability, decentralization, privacy, resilience, and accountability, and shows how each architectural layer contributes to and constrains these dimensions. Through a structured cross-domain mapping of public-service deployments across seven service categories, the paper has documented both the considerable progress that has been made and the substantial distance that remains between the most mature pilots and routine, scaled, legally recognized operation.

Three substantive conclusions emerge from the analysis. First, blockchain governance is most valuable for public services where the off-chain institutional environment is weak, and least valuable where strong institutions already provide the trust properties that blockchain aims to mechanize. This is not a critique of the technology but an observation about its comparative advantage. Second, the choice of governance model—public, permissioned, or hybrid—is more consequential than is sometimes recognized in the technical literature, because each model embodies different assumptions about who participates in validation, who can amend the rules, and how the system interacts with the legal environment. Third, the most pressing open problems in the field—governance interoperability, privacy-preserving auditability, and the legal status of code-based public obligations—are not purely technical problems; they sit at the intersection of computer science, public administration, and law, and progress on them will require interdisciplinary collaboration.

The framework presented here has limitations. It is grounded in the literature published through early 2026, and the field continues to evolve rapidly. Future work should test the framework against new categories of deployments that are still emerging, including AI-augmented smart contracts that incorporate machine-learned components, decentralized physical infrastructure networks for public utilities, and Web 3.0-mediated public participation platforms (Yang et al., 2025; Zhang & Lu, 2025; Tanwar et al., 2020). It would also benefit from controlled empirical studies that quantitatively assess the effect of specific design choices on the trust dimensions identified here.

From a policy perspective, the analysis supports four recommendations. Public-sector organizations exploring blockchain should begin with the institutional question—what governance arrangements does the service require—rather than the technical question of which platform to deploy. Permissioned and hybrid governance models are likely to dominate near-term national-scale deployments, but they should be designed with explicit interfaces to the wider public-chain ecosystem so that interoperability is not foreclosed. Privacy-preserving cryptographic techniques should be treated as core requirements rather than optional enhancements, particularly in domains involving sensitive personal data. Finally, legal recognition of code-based public obligations should be addressed proactively through legislative and regulatory clarification rather than reactively through litigation. The trustworthy digital societies that blockchain governance can help to produce will not emerge from the technology alone; they will emerge from the deliberate integration of the technology with the institutions, laws, and norms that confer legitimacy on public action.

Acknowledgements

The authors thank the anonymous reviewers for their careful reading and constructive feedback, which substantially improved both the structure of the argument and the clarity of the exposition. The authors also acknowledge the support of their respective institutions for providing the computing resources and library access that made this synthesis possible.

References

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2), 1676–1717. DOI: 10.1109/COMST.2018.2886932

Allen, D. W. E., Berg, C., Markey-Towler, B., Novak, M., & Potts, J. (2020). Blockchain and the evolution of institutional technologies: Implications for innovation policy. Research Policy, 49(1), 103865. DOI: 10.1016/j.respol.2019.103865

Allessie, D., Sobolewski, M., & Vaccari, L. (2019). Blockchain for digital government. Joint Research Centre Science for Policy Report EUR 29677 EN. DOI: 10.2760/942739

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. Computer, 50(9), 18–28. DOI: 10.1109/MC.2017.3571064

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation, 6(1), 45–62. DOI: 10.22495/jgr_v6_i1_p5

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. Journal of the Association for Information Systems, 19(10), 1020–1034. DOI: 10.17705/1jais.00518

Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. ACM Computing Surveys, 54(8), 168. DOI: 10.1145/3471140

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for Industry 4.0: A comprehensive review. IEEE Access, 8, 79764–79800. DOI: 10.1109/ACCESS.2020.2988579

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81. DOI: 10.1016/j.tele.2018.11.006

Casino, F., Politou, E., Alepis, E., & Patsakis, C. (2020). Immutability and decentralized storage: An offline-first approach for highly available IoT. IEEE Access, 8, 4737–4744. DOI: 10.1109/ACCESS.2019.2962017

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. Communications of the ACM, 63(7), 80–90. DOI: 10.1145/3359552

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 13, e00151. DOI: 10.1016/j.jbvi.2019.e00151

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715–1729. DOI: 10.1007/s10796-022-10248-7

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. DOI: 10.1109/ACCESS.2016.2566339

Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076–8094. DOI: 10.1109/JIOT.2019.2920987

Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. Journal of Institutional Economics, 14(4), 639–658. DOI: 10.1017/S1744137417000200

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust and challenges of governance. Technology in Society, 62, 101284. DOI: 10.1016/j.techsoc.2020.101284

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1), 31–37. DOI: 10.1109/MCC.2018.011791712

Hardjono, T., Lipton, A., & Pentland, A. (2019). Toward an interoperability architecture for blockchain autonomous systems. IEEE Transactions on Engineering Management, 67(4), 1298–1309. DOI: 10.1109/TEM.2019.2920154

Hassan, S., & De Filippi, P. (2021). Decentralized autonomous organization. Internet Policy Review, 10(2). DOI: 10.14763/2021.2.1556

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electronic Commerce Research and Applications, 29, 50–63. DOI: 10.1016/j.elerap.2018.03.005

Hyla, T., & Pejas, J. (2020). eHealth integrity model based on permissioned blockchain. Future Generation Computer Systems, 112, 1095–1104. DOI: 10.1016/j.future.2019.07.030

Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., & Hossain, E. (2017). Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Transactions on Industrial Informatics, 13(6), 3154–3164. DOI: 10.1109/TII.2017.2709784

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. DOI: 10.1016/j.future.2017.11.022

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Networking and Applications, 14(5), 2901–2925. DOI: 10.1007/s12083-021-01127-0

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1–34. DOI: 10.1186/s40854-024-00668-6

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038. DOI: 10.1016/j.telpol.2017.09.003

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80–89. DOI: 10.1016/j.ijinfomgt.2017.12.005

Lacity, M. C. (2018). Addressing key challenges to making enterprise blockchain applications a reality. MIS Quarterly Executive, 17(3), 201–222. DOI: 10.17705/2msqe.00002

Lee, J. H. (2017). BIDaaS: Blockchain Based ID As a Service. IEEE Access, 6, 2274–2278. DOI: 10.1109/ACCESS.2017.2782733

Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. Current Issues in Auditing, 13(2), A19–A29. DOI: 10.2308/ciia-52540

Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231–255. DOI: 10.1080/23270012.2018.1516523

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80–90. DOI: 10.1016/j.jii.2019.04.002

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876–1907. DOI: 10.1080/17517575.2021.2008513

Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., Obbad, K., Barkovich, R., & Palombini, M. (2019). 'Fit-for-purpose?'—challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine, 17, 68. DOI: 10.1186/s12916-019-1296-7

Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. Telematics and Informatics, 35(8), 2337–2354. DOI: 10.1016/j.tele.2018.10.004

Mendling, J., Weber, I., van der Aalst, W., vom Brocke, J., Cabanillas, C., Daniel, F., Debois, S., Di Ciccio, C., Dumas, M., Dustdar, S., et al. (2018). Blockchains for business process management—challenges and opportunities. ACM Transactions on Management Information Systems, 9(1), 4. DOI: 10.1145/3183367

Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134–117151. DOI: 10.1109/ACCESS.2019.2936094

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly, 34(3), 355–364. DOI: 10.1016/j.giq.2017.09.007

Pongnumkul, S., Siripanpornchana, C., & Thajchayapong, S. (2017). Performance analysis of private blockchain platforms in varying workloads. 26th International Conference on Computer Communication and Networks (ICCCN), 1–6. DOI: 10.1109/ICCCN.2017.8038517

Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in blockchain technologies & social contract theories. Ledger, 1, 134–151. DOI: 10.5195/ledger.2016.62

Risius, M., & Spohrer, K. (2017). A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. Business & Information Systems Engineering, 59(6), 385–409. DOI: 10.1007/s12599-017-0506-0

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. DOI: 10.1080/00207543.2018.1533261

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127–10149. DOI: 10.1109/ACCESS.2018.2890507

Tan, E., Mahula, S., & Crompvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for innovation. Government Information Quarterly, 39(1), 101625. DOI: 10.1016/j.giq.2021.101625

Tanwar, S., Bhatia, Q., Patel, P., Kumari, A., Singh, P. K., & Hong, W. C. (2020). Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward. IEEE Access, 8, 474–488. DOI: 10.1109/ACCESS.2019.2961372

Tasca, P., & Tessone, C. J. (2019). A taxonomy of blockchain technologies: Principles of identification and classification. Ledger, 4, 1–39. DOI: 10.5195/ledger.2019.140

Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Management, 23(6), 545–559. DOI: 10.1108/SCM-01-2018-0029

Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2020). GDPR-compliant personal data management: A blockchain-based solution. IEEE Transactions on Information Forensics and Security, 15, 1746–1761. DOI: 10.1109/TIFS.2019.2948287

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11), 2266–2277. DOI: 10.1109/TSMC.2019.2895123

Werbach, K. (2018). Trust, but verify: Why the blockchain needs the law. Berkeley Technology Law Journal, 33(2), 487–550. DOI: 10.15779/Z38H41JM9N

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1–2). DOI: 10.1080/17517575.2024.2448003

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452–10473. DOI: 10.1109/JIOT.2021.3060508

Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9). DOI: 10.1080/17517575.2024.2397630

Yang, L., Hou, Q., Zhu, X., Lu, Y., & Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. Enterprise Information Systems, 19(11), 2541199. DOI: 10.1080/17517575.2025.2541199

Yermack, D. (2017). Corporate governance and blockchains. Review of Finance, 21(1), 7–31. DOI: 10.1093/rof/rfw074

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. PLOS ONE, 11(10), e0163477. DOI: 10.1371/journal.pone.0163477

Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. Systems Research and Behavioral Science, 42(4), 996–1015. DOI: 10.1002/sres.3037

Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. DOI: 10.1080/17517575.2021.1939895

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375. DOI: 10.1504/IJWGS.2018.095647