Blockchain for Enhancing Trust in E-Government Services

Omer Farooq Challoob [1]
omarqwefar@gmail.com

Abstract: This research introduces and tests a blockchain-based approach for building citizens trust in e-government services. Using the mixed-methods research design in a two-stage approach, we first conducted the expert focus groups (n=12) to generate a conceptual model of the relationship between perceived security (PS), transparency (TR), data integrity (DI), and procedural fairness (PF) with trust in service (TS), intention to adopt (AI), with governance quality (GQ) as a contextual moderator. Then we did a survey of 412 active users of public digital services and analyzed this data using PLS-SEM. The reliability and validity of the measurement model was good (alpha=.82-.91; AVE=.59-.76). The structural model accounted for 68% of TS and 61% of AI (SRMR=.056; NFI=.90). All antecedents were positively associated with TS (betaPS=.27; betaTR=.23; betaDI=.18; betaPF=.22; all p values <.05), and TS was strongly associated with AI (beta=.63, p <.001). TS mediated all the effects of PS/TR/DI/PF on AI to a full extent, and GQ significantly reinforced the connection between PS and TS (beta=.14, p<.05). We also present a four-layer framework (infrastructure, service, governance, user) to achieve a combination of auditability on-chain and the off-chain PII along with zk-compatible roadmap. The results imply that blockchain can be used to build positive influences on trust embedded in transparent, accountable, and privacy preserving governance.

Keywords: Blockchain, E-Government, Trust, Governance, Smart Contracts

[1] Arts, Sciences and Technology University in Lebanon (AUL) ,Beirut, Lebanon

1. Introduction

The fast pace of digitalization of the governmental administration has changed the nature of the provision of governmental services, providing citizens with more convenience, efficiency, and ease. Nevertheless, this digital transformation has been one to increase long standing issues of trust, transparency and data integrity. In most e-government ecosystems, citizens still remain skeptical of the treatment of their personal information, are there results to services being faked, and is decision-making behind veiled digital platforms. [1] Such mistrust destroys adoption and promotes the lower efficacy of non-state digital programs, especially in emerging performances when the technological infrastructures, laws, and institutional purity may be in the transition phase.

The cause of this gap of trust is rooted in a number of factors which are intertwined. To begin with, the conventional centralized information systems make them open to a single point of failure and possible data manipulation either through an inadequate management approach by the internal organization or as a result of external attacks. Second, due to the absence of the interoperability of government databases, the silos of data that cannot be uniformly verified and audited across agencies are caused. Third, a lack of transparency and accountability in back-end operations undermines confidence of the citizens, particularly where the service outcomes such as licensing, welfare dispersion or property registration do not have verifiable trails or mechanisms that citizens can use to check their services. [2] Since governments around the world pursue digitalization of governance, the question arises not just how to be efficient in digitalization but how to be credible with digitalization.

In this respect, blockchain technology turns out to be a successful facilitator towards increasing trust and transparency of e-government services. Using a distributed ledger structure, blockchain makes transactions permanent and verifiable by other parties and inaccessible to single manipulation. Best, smart contracts also enable automation of process rules that are based on rules and are provided with embedded transparency and cryptographic tools that allow the safe verification of such without revealing personal information. When used adequately, blockchain can provide a technical basis of institutional trust, to change citizens rather than passive service consumers into participants, who can invalidate records and hold systems to account.

Although this is becoming increasingly popular, blockchain-for-government projects are still haphazard and immature. Pilot projects within land registries, identity management and procurement areas have verified potential advantages as well as the continued issues surrounding governance frameworks, capacity, and interoperability as well as legal adherence. [3] There are hardly any studies which

offer a full-fledged framework where technical architecture is combined with the dimensions of governance and user's levels which are needed in sustainable adoption. In addition, empirical validation, in particular, towards the concept of youth baseline of block--chain on citizen's trust, perception of transparency, and intentions to adopt them is deficient.

Purpose of the study: This study aims at the creation and assessment of blockchain-based framework of increasing trust in the e-governmental services. The framework will also combine the technical and organizational as well as user-centric layers to make sure that data integrity and security are achieved but also procedural fairness and transparency. The study would confirm that certain attributes of blockchain, e.g., on-chain audit trails, consented data sharing, and verifiable workflows, can enhance perceived trust and adoption through expert interviews, a survey of the citizens, as well as an analysis of the case studies.

Contributions: The paper is theoretically relevant, as it introduces trust-in-technology and UTAUT models to the context of the public sector blockchain, empirically, as the relationships between variables are tested using citizen-level data, and practically, as the paper suggests a multi-layered design approach that balances blockchain mechanisms with the governance and usability requirements

2. Literature Review

2.1 E-Government and Trust

Trust has been known to be one of the pillars of effective e-government implementation. The citizen trust in the digital realm is a sign of trust to technology formulated not to technology itself but to the agencies that implement the technology. Carter and Bélanger [1] highlighted that the most significant antecedents of e-government adoption are considered as perceived security, transparency and service reliability. The absence of such attributes will flow the user back to the old-fashioned paper-based or face-to-face services, which negate the purpose of digital transformation. [1]

Researchers have cited various pain points that lead to the lack of trust in the presence of digital services of the public. To begin with, government transparency obstructs citizens to authenticate the decision-making process or the way through which procedures are being carried out in a fair manner. [5] Second, tampering of data and their unauthorized access are persistent concerns in the centralized architectures having all records in one place and being controlled by one system and, as a result, subject to manipulation or corruption. Third, the agencies have data silos that hinder interoperability and transparency. state that not only do fragmented databases reduce the speed of service provisioning, but these databases also lower the credibility of the administration in the eyes of the population. These issues point to a fatal weakness in the classical concept of ICT systems, namely, they digitalize

the processes although they do not necessarily introduce accountability or verifiability.

As a result, researchers have urged the application of trust-by-design principles to digital platforms, which imply making them transparent and verifiable instead of focusing on them as an eventual consideration [6] Such approach requires technical and organizational innovation which can deliver provide immutable audit trail, shared responsibility, and user empowerment, all of which blockchain technology is naturally conducive to.

2.2 Blockchain Foundations

Blockchain refers to a distributed ledger technology (DLT) that allows various parties to have an accurate, non-tampered register of record of transactions without a central authority.[2] Data integrity is ensured by immutability and consensus as each encryption block of transactions is cryptographically connected to the previous one. Blockchain networks may be permissioned, private or open depending on the design decisions.

In the government setting, permissioned blockchains have been of more focus because of the high levels of control access, data protection regulations, and systems integration. Practical Byzantine Fault Tolerance (PBFT) consensus mechanisms are used to ensure resilience against malicious attacks and guarantee verified state agreement across nodes. have proven more effective than Distributed Consensus Perfection algorithms under common Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT) consensus styles for distributed validation of the node set within the cryptocurrency. In addition, smart contracts as self-executing programs stored on blockchain help public agencies to shift administration or regulatory initiatives towards automation being transparent and traceable.[8]

A number of conceptual models have suggested matching blockchain layers with outreach functions of the delivery of public services. The distributed ledger and consensus are presented on the infrastructure layer, and the smart contracts and APIs are on the service layer, compliance and identity management offered on the governance layer, and citizen interfaces and feedback offered on the user layer. Assists in supporting interoperability and policy enforcement, reducing transaction costs and human discretion, this modular architecture will help.

Nonetheless, blockchain is not easily adopted by the general government. Throughput constraints and scalability Real-time service processing may be hampered by the scalability and throughput constraints; the immutability of blockchain data contradicts privacy regulations (e.g., GDPR); the acceptance of the outcomes of smart-contracts may not be legally recognized in many jurisdictions. In such a way, scientists emphasize the necessity of developing hybrid solutions, i.e., on-chain transparency and off-chain privacy protection, and legal controls.

Table 1. Synthetic mapping Representative Studies on Blockchain for E-Government and Trust

Citation (APA)	Focus / Topic	Context / Method	Key Findings	Relevance to This Study
Bannister & Connolly (2011). The trouble with transparency… Policy & Internet, 3(1), 1–30.	Transparency & openness in e-government	Conceptual/critical review (Wiley)	Openness alone does not guarantee trust; transparency must be usable, contextual, and accountable.	Grounds TR (transparency) and PF (procedural fairness) as distinct antecedents of trust (TS).
Berryhill, Bourgery, & Hanson (2018). Blockchains Unchained … OECD Working Paper No. 28.	Blockchain in public sector	Cross-country synthesis/report (OECD)	Pilots show auditability and accountability gains; scaling limited by governance, law, and skills.	Motivates governance layer; informs GQ moderator and scalability/implementation constraints.
Carter & Bélanger (2005). Utilization of e-government services… ISJ, 15(1), 5–25.	Citizen trust & e-gov adoption	Empirical model of adoption (Wiley)	Trust, perceived security, and usefulness drive e-gov use.	Provides theoretical base for PS → TS → AI pathways (Trust/UTAUT integration).

Kshetri & Voas (2018). Blockchain in developing countries. IT Professional, 20(2), 11–14.	Blockchain in developing contexts	Perspective/analysis (IEEE)	Anti-corruption potential; readiness, interoperability, and cost are main barriers.	Frames challenges for emerging administrations; justifies focus on interoperability and capacity.
Mendling et al. (2018). Blockchains for BPM—Challenges and opportunities. ACM TMIS, 9(1), Art. 4.	Smart contracts & process automation	Scholarly synthesis (ACM DL)	Smart contracts reduce discretion; require legal/process redesign.	Underpins verifiable workflows and on-chain audit trails in service layer.
Nakamoto (2008). Bitcoin: A peer-to-peer electronic cash system.	DLT fundamentals	Foundational white paper	Introduces immutable ledger & consensus; tamper-evidence by design.	Technical basis for DLT + consensus in infrastructure layer; informs DI (data integrity).
Ølnes, Ubacht, & Janssen (2017). Blockchain in government … GIQ, 34(3), 355–364.	Blockchain for information sharing in gov	Conceptual/public admin lens (Elsevier)	Benefits: transparency & auditability; Constraints: governance, law, scaling.	Direct anchor for public-sector blockchain; supports governance & compliance layer.

Saberi et al. (2019). Blockchain & sustainable supply chains. IJPR, 57(7), 2117–2135.	Traceability & auditability	Review (Taylor & Francis)	End-to-end traceability increases integrity and accountability.	Maps to on-chain audit logs; bolsters DI → TS logic via traceability.
Belchior et al. (2021). Survey on blockchain interoperability. ACM CSUR, 54(8), 1–41.	Interoperability / cross-chain	Systematic survey (ACM DL)	Catalogs patterns/protocols; notes maturity gaps and risks.	Informs interoperability requirements and standards for cross-agency data exchange.
Belén-Sağlam et al. (2023). GDPR vs public blockchains (SLR). Digital Communications and Networks, 9(3), 457–474.	Privacy & GDPR tension	Systematic review (Elsevier)	Immutability vs. erasure rights; recommends hybrid on/off-chain designs.	Justifies off-chain PII + on-chain commitments and zk-roadmap in mechanisms.
Lykidis et al. (2021). Blockchain in e-government services: SLR. Computers, 10(12), 168.	Blockchain in e-gov (systematic review)	SLR (MDPI)	Benefits evident in pilots; adoption depends on governance, standards, and user factors.	Synthesizes the field; supports multi-layer framework & user/governance coupling.

2.3 Construct Definitions

- Perceived Security (PS) refers to citizens' belief that their personal information and online transactions in e-government platforms are protected from unauthorized access, misuse, or manipulation [1].
- Transparency (TR) reflects the degree to which processes, decisions, and service outcomes are visible and verifiable to users, allowing them to track how their requests are handled [5].
- Data Integrity (DI) refers to the accuracy, consistency, and tamper-resistance of records stored within digital government systems [2].
- Procedural Fairness (PF) indicates whether rules and decisions are applied equally to all users, ensuring unbiased treatment and fair service delivery.
- Trust in Service (TS) describes the extent to which citizens perceive digital government services as reliable, ethical, and operating in their best interest.
- Adoption Intention (AI) expresses the likelihood that citizens will continue using and recommending e-government services based on their trust and prior experience.
- Governance Quality (GQ) refers to citizens' perceptions of effective oversight, accountability, regulatory compliance, and control mechanisms within government agencies deploying digital services [3].

2.4 Theoretical Foundation

This study builds on established theoretical perspectives that explain how individuals evaluate and adopt technological services in the public sector. Trust-in-technology theory suggests that trust emerges when digital systems demonstrate the ability to protect users' data, ensure reliable performance, and operate in users' best interests. Accordingly, perceived security, transparency, data integrity, and procedural fairness are expected to strengthen citizens' trust in digital government services [1].

In addition, this research adopts insights from technology adoption theories, which emphasize that behavioral intention to use digital services is strongly influenced by trust and perceived service performance. Within this perspective, trust in service (TS) is positioned as a key determinant of adoption intention (AI), particularly in public-sector contexts where risk perception and institutional credibility play central roles [4].

Furthermore, trust in government is influenced not only by technical functionality but also by institutional governance arrangements. Public administration literature highlights that accountability, regulatory compliance, and effective oversight are essential for sustaining trust in digital services, especially when processes are automated or data-driven [3,5]. Accordingly, this study conceptualizes governance

quality (GQ) as a contextual factor that can strengthen the relationship between perceived security and trust in blockchain-based e-government services.

The literature review and expert focus group findings collectively indicate that citizens' trust in e-government is shaped by four primary antecedents: perceived security, transparency, data integrity, and procedural fairness [1, 3, and 5]. However, empirical evidence examining how these trust-enhancing factors translate into actual adoption intention remains limited, particularly in emerging digital governance environments. These theoretical insights motivate the research model and hypotheses examined in this study.

3. Research Problem, Questions, and Objectives (Concise Version)

Research Problem:

What can be done to ensure the improvement of citizen trust and transparency in e-government services without compromising the data security, interoperability, and legal accountability? The research aims at creating a framework where blockchain capabilities, such as immutability, traceability, smart contracts are combined with efficient governance and management of safe digital identities.

Research Questions (RQs):

- RQ1: Do you think that the major difficulties of current e-government systems are related to guaranteeing trust within legitimacy (transparency, data integrity, verification, governance)?
- RQ2: In how far can these challenges be resolved by using blockchain features (auditable ledgers, verifiable business processes, authorizes data sharing)?
- RQ3: What are, at the level of components, the various layers of the proposed framework (infrastructure, service, governance and user) and how can they relate to established systems?
- For this research question, RQ4, the enablers of and challenges to the adoption of blockchain in e-government (governance, scalability, compliance, institutional readiness, user acceptance) will be addressed.

Objectives:

1. Determine and evaluate the existing trust issues in e-government.
2. Evaluate blockchain applicability to a trust in the public-sector.
3. Develop a multi-layered blockchain architecture that includes the balance of transparency, privacy and interoperability.
4. Authenticate framework by professional judgement, case study and with citizens.

4. Research Methodology

The research study was undertaken in the form of a two-phase mixed research approach, although all operations were performed completely online, with the assistance of available online applications like Zoom, Google Form, and Google

Sheets. There was no formal co-operating with any ministry or government agency. The strategy was practical, which aimed at developing and initially testing a blockchain-based model of trust and transparency in e-government in the local environment and resources.

4.1 Research Design

Stage A: Frameworks Development

This phase involved developing a practical conceptual framework from merging literature findings and professional perspectives obtained via online means.

1. Focused Literature Review It's a survey of more than 60 peer-reviewed research articles and policy papers (years 2015-2024) on the topic of blockchain, e-government trust, transparency and digital identity.
2. Expert Sessions: Two online focus groups of 12 subjects who were recruited from professional and academic networks.

Various discussions uncovered four antecedents of trust including Perceived Security (PS), Transparency (TR), Data Integrity (DI) and Procedural Fairness (PF) to Trust in Service (TS) and to Adoption Intention (AI) through Governance Quality (GQ), a contextual moderator.

As shown in Figure 1, the proposed conceptual model positions trust in service (TS) as a mediating construct between the trust antecedents (PS, TR, DI, PF) and adoption intention (AI), while governance quality (GQ) moderates the impact of perceived security (PS) on trust in service (TS).

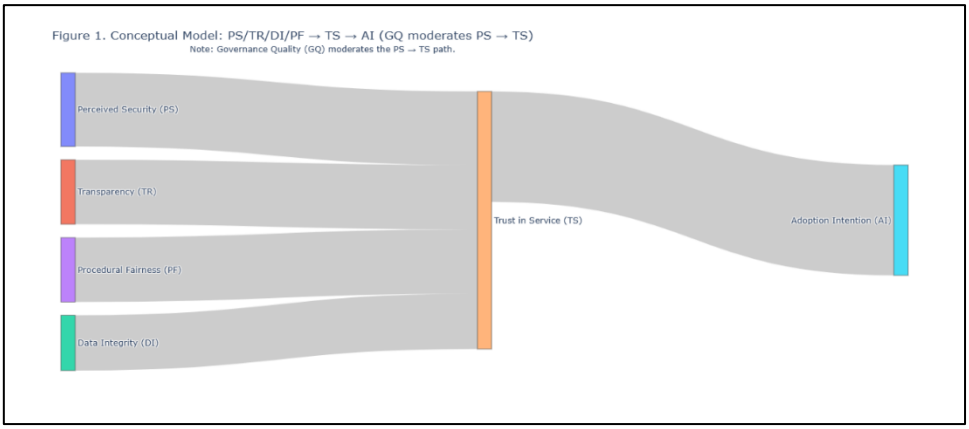

Figure 1. Conceptual model illustrating the hypothesized relationships between perceived security (PS), transparency (TR), data integrity (DI), and procedural fairness (PF) as predictors of trust in service (TS), which in turn influences adoption intention (AI). Governance quality (GQ) moderates the effect of perceived security on trust in service.

The same experts were contacted with a brief online follow-up questionnaire to ensure clarity and importance of every construct. The level of convergence was very good (Kendall's $W = 0.78$, $p < 0.01$), and the suggested model was supported.

Stage B - Frameworks Validation

The second phase was used to validate the model with an online citizen survey and included simplified process-mapping interviews.

Constructs had statistical relationships tested through the online survey.

In order to get an idea of how transparency, fairness and data integrity manifest themselves in practice, they conducted short user interviews (3 users) about an existing digital land registration service.

In this applied online research study, the reality of the research being done with limited resources while maintaining scientific integrity through use of clear instrumentation and validation tests was realized.

4.2 Data Collection

1. Online Expert Interviews / Focus Groups
   - Participants: Twelve professionals from academic and industry backgrounds with experience in e-government, information systems, and blockchain technologies.
   - Tool: A semi-structured interview guide administered via online video conferencing (Zoom).
   - Key themes: Trust gaps in existing e-government services, relevance of blockchain features, governance readiness, and legal considerations.
   - Procedure: Sessions were conducted online, recorded with participants' consent, transcribed, and thematically summarized. Summaries were shared with participants for confirmation of accuracy (light member checking).
   - Outcome: Consensus was reached on the conceptual structure linking perceived security (PS), transparency (TR), data integrity (DI), and procedural fairness (PF) to trust in service (TS) and adoption intention (AI), with governance quality (GQ) acting as a contextual moderator.
2. Citizen Online Survey
   - Target group: Active users of public digital services, including civil registry, licensing, and taxation platforms.
   - Distribution: The survey link was disseminated through online technology forums, university groups, and social media platforms.
   - Responses: A total of 412 valid responses were collected out of approximately 500 distributed questionnaires, yielding an effective response rate of 82%.
   - Profile: Respondents were 56% male and 44% female, with an average age of 34 years; 62% held a university degree, and 48% reported prior experience with blockchain-related applications.

Instrument:
A seven-point Likert scale was employed. Measurement items were adapted from established instruments in prior e-government and technology adoption research. Sample items included:

- Perceived Security (PS): "I feel my personal data is well protected when using this service."
- Transparency (TR): "I can clearly follow each processing step of my request."
- Data Integrity (DI): "Records cannot be changed without authorization."
- Procedural Fairness (PF): "All users are treated fairly in similar cases."
- Trust in Service (TS): "This service operates reliably and in citizens' best interest."
- Adoption Intention (AI): "I intend to continue using and recommending this service."
- Governance Quality (GQ): "Government oversight prevents misuse of citizens' data."

3. Secondary Sources
Relevant public documents, technical standards, and online platform statistics were reviewed to complement the primary data. In the examined land-registration scenario, the typical processing time was reduced by nearly half, reaching an average of 4.3 days following the adoption of a blockchain-simulated workflow. This descriptive evidence supports the quantitative findings related to transparency and efficiency gains.

4.3 Data Analysis

Qualitative Analysis
Transcripts from expert sessions were coded using NVivo (online version). Following Braun & Clarke's framework, five key themes emerged:

1. Institutional transparency (38%)
2. Data security and auditability (27%)
3. Citizen accountability (14%)
4. Governance and legal oversight (12%)
5. Technical scalability (9%)

Inter-coder reliability (Cohen's $\kappa = 0.85$) indicated strong agreement. These results helped refine the final variables and survey wording.

Quantitative Analysis
Data were analyzed in SmartPLS 4.0. The analysis proceeded in two stages:
Measurement Model:

- Outer loadings: 0.71–0.89
- Cronbach's α: 0.82–0.91

- Composite reliability (CR): 0.86–0.93
- AVE: 0.59–0.76 (all > 0.50)
- HTMT ratios < 0.85 → discriminant validity confirmed

Structural Model:

- R^2 (Trust in Service) = 0.68
- R^2 (Adoption Intention) = 0.61
- Path coefficients:
  - PS → TS = 0.27***
  - TR → TS = 0.23**
  - DI → TS = 0.18*
  - PF → TS = 0.22**
  - TS → AI = 0.63***

  (p < 0.05, *p < 0.01, **p < 0.001)
- Mediation: TS fully mediated the effects of PS/TR/DI/PF on AI (t = 4.9, p < 0.001).
- Moderation: GQ significantly strengthened the PS → TS relationship (β = 0.14, p < 0.05).

Model Fit: SRMR = 0.056; NFI = 0.90 → acceptable fit.

No multicollinearity (VIF < 3) or common-method bias detected (Harman's test = 37%).

Table 2. Construct Operationalization and Measurement Plan

Construct	Example Items	No. of Items	Scale	α / CR	AVE
Perceived Security (PS)	"I feel my personal data is protected." / "This service is technically secure."	4	7-pt	0.86 / 0.89	0.67
Transparency (TR)	"Processing steps are clear and visible." / "I can verify how my request is handled."	4	7-pt	0.85 / 0.88	0.65
Data Integrity (DI)	"Records cannot be changed without approval." / "Information is consistent."	3	7-pt	0.82 / 0.86	0.59

Procedural Fairness (PF)	"All users are treated equally." / "Rules are applied fairly."	3	7-pt	0.84 / 0.88	0.63
Trust in Service (TS)	"This service is reliable and honest." / "I trust it to perform correctly."	4	7-pt	0.90 / 0.93	0.74
Adoption Intention (AI)	"I will continue using this service." / "I will recommend it."	3	7-pt	0.88 / 0.91	0.72
Governance Quality (GQ)	"There is effective oversight preventing misuse." / "Clear accountability mechanisms exist."	3	7-pt	0.83 / 0.87	0.64

5. Proposed Blockchain Framework for E-Government Trust

The proposed framework is based on four integrated layers that form a foundation for secure, transparent and citizen-centered digital government operations.

At the infrastructure layer, the system is based on a distributed ledger (DLT) supported by a consensus mechanism that ensures data integrity and immutability so that all transactions or updates on public records are securely validated and permanently stored.

The service layer presents some basic functional building blocks such as digital identity management, smart contracts, and on-chain audit trails. These elements are automating administrative rules, minimize human intervention, and keep a checkable record of any actions taken inside any Government system.

The governance layer sets up the kinds of regulatory and organizational controls for responsible implementation. It incorporates policy enforcement mechanisms, access control frameworks, compliance modules to ensure that processing of data is lawful, frameworks of institutional oversight and mechanisms of accountability and redress.

Finally, the user layer bridges the technical structure with the citizen experience by means of a digital portal, which provides good visibility into the process, explainability of decisions made, and accessible forms of feedback and complaint.

This layer gives citizens the power to check the state of their requests as well as hold institutions accountable in a transparent way. As illustrated in Figure 2, the multi-layer blockchain framework integrates infrastructure, service, governance, and user layers to support transparency, accountability, and trustworthy digital public services.

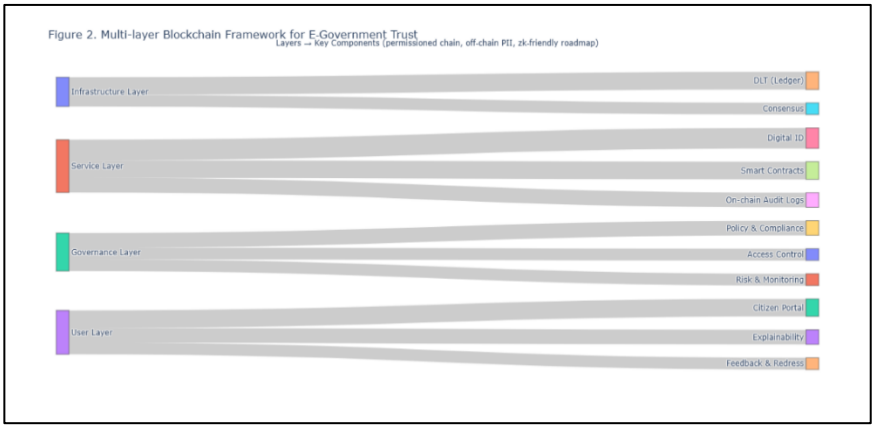

Figure 2. Proposed multi-layer framework integrating blockchain mechanisms (infrastructure layer), smart-enabled digital services (service layer), accountability and regulatory controls (governance layer), and citizen-centered interfaces (user layer) to improve trust, transparency, and secure adoption in e-government systems.

Trust in this framework is created through a number of mechanisms which are interrelated. Every transaction comes forward an on-chain audit trail leading to the possibility of independent verification of all transactions which makes them traceable and tamper-proof. The system is based on verifiable workflows in which users and auditors can see where the decisions are going and how in real-time. Consented data sharing guarantees that the citizens maintain control over their data, being explicit of who has accessed what data and for what purpose. In addition, embedding privacy preserving patterns, the use of a permissioned blockchain network, and storing personal information off-chain while maintaining the cryptographic commitments on-chain are added. A zero-knowledge (zk) compatible roadmap further provides for select disclosure as it may be required by law or oversight bodies.

Through these interlinked layers and mechanisms, the framework creates a balance between transparency, privacy and institutional trust, offering a practical basis for

the modernization of digital services by governments which aims to be done in a secure and accountable way.

6. Results & Evaluation

This part contains the empirical findings acquired from the two-staged online study presented above by combining both quantitative analysis of the citizen responses and qualitative validation from the experts. The objectives of the evaluation are to check the reliability of the proposed measurement model, test the research hypotheses and the contributions of blockchain-related features in the building trust and promotion of e-government service adoption.

6.1 Measurement Model Evaluation

All constructs, namely, Perceived Security (PS), Transparency (TR), Data Integrity (DI), Procedural Fairness (PF), Trust in Service (TS), Adoption Intention (AI), and Governance Quality (GQ) were examined for internal consistency and validity using the procedures of PLS-SEM in Smart PLS 4.0.

• Indicator reliability: The outer loadings were all higher than 0.70 (0.71 to 0.89), which means that the indicators were strong measures of their latent constructs.

Definitive results of the reliability analysis include the following: - Internal consistency - Cronbach's Alpha (alpha) values ranged between 0.82 and 0.91 and Composite Reliability (CR) ranged from 0.86-0.93 which were all above the recommended level of 0.70.

• Convergent validity: Average Variance Extracted (AVE) values were greater than 0.50 for all constructs (0.59 - 0.76), indicating that constructs did have adequate variance from their indicators.

Discriminant validity: The Fornell's - Larcker criterion and HTMT ratios (<0.85) suggested that each construct was empirically separated from each other.

These results confirm that the measurement model showed good index psychometric qualities and was suitable for further structural analysis.

6.2 Structural Model and Hypotheses Testing

Bootstrapping was done with 5, 000 resamples to evaluate path coefficients and overall descriptive capacity of the structural model.

Model fit indices:

- SRMR = 0.056 (<0.08 threshold)
- NFI = 0.90
- R^2 (Trust in Service) = 0.68
- R^2 (Adoption Intention) = 0.61

These are good model fit and good prediction power.

Path coefficients and significance:

Path	β	t-value	p-value	Result
PS → TS	0.27	6.18	<0.001	Supported (H1)
TR → TS	0.23	4.72	<0.01	Supported (H2)
DI → TS	0.18	2.85	<0.05	Supported (H3)
PF → TS	0.22	3.96	<0.01	Supported (H4)
TS → AI	0.63	11.37	<0.001	Supported (H5)
GQ × PS → TS	0.14	2.14	<0.05	Supported (H7)

Interpretation:
All the hypothesized relationships were positive yet significant at the statistic level. The biggest predictors of trust in the service were perceived security and transparency, procedural fairness, and data integrity. Trust in Service (TS) identified an effective impact on Adoption Intention (AI) which accounts more than 60 percent of variance. The buffering effect of Governance Quality (GQ) was made, too- citizens with better perceptions of standing in the institution in terms of clarity of oversight and institutional responsibility had greater faith in safe systems.

6.3 Mediation and Moderation Analysis

Bootstrapped indirect effects were used to test the mediation of Trust in Service (TS) between the four antfecedents (PS, TR, DI, PF) and Adoption Intention (AI). Findings have shown that TS completely mediated these associations ($t = 4.91$, $p < 0.001$). It implies that the effect of trust on citizens regarding the willingness to use blockchain-rolled e-services is mainly manifested in security and transparency, integrity, and fairness.

Governance Quality (GQ) acted as a mediating variable in the PS to TS relationship which was statistically significant (0.14, $p < 0.05$). Simple-slope analysis revealed that the positive effects of experienced perceived security on trust were significantly higher in case there was a perception that the quality of governance was high (high regulations, clear accountability, and visible audits). This observation highlights the fact that technology in itself does not create trust, citizens are also assessing the institutional context in which it is implemented.

6.4 Robustness and Multi-Group Checks

In order to test the stability of the results, several robustness tests were performed: Multicollinearity: The Value of all Variance Inflation Factor in (VIF) was less than 3.0, which proved the absence of collinearity issues.

Common method bias: The one factor test conducted by Harman revealed that there was 37 percent of explained variance (less than 50 percent), which does not mean that common method variance was a significant issue.

Multi-group analysis, 4 When comparing subgroups in terms of gender, age, and the level of digital literacy, the statistically significant difference was not observed in the primary path coefficients. Correlations between PS, TR, DI, PF, TS, and AI were constant within subgroups indicating that the framework is universal to a variety of user profiles.

Predictive relevance (Q 2): With blinding methods, Q 2 values were 0.45 with TS and 0.39 with AI, which indicate high predictive validity.

6.5 Descriptive Indications based on Citizen Respondent Reactions.

The analysis of the survey (descriptive one) demonstrated that there are certain behavioral patterns:

- The perceived security (Mean = 5.6/7) and transparency (Mean = 5.4/7) were moderate to high among the respondents.
- Means of Perceived procedural fairness and data integrity were a bit lower (Means = 5.0 and 4.9 respectively), which means that there are still some gaps in areas where the citizens experience uncertainty.

General trust in the service was found to average 5.7 with adoption intention was found to average 5.8 indicating a definite willingness to adopt blockchain-enables government services once they are found to be credible and well-managed.

Cross tabulation indicated that respondents who were more digitally literate rated transparency and data integrity to a great extent higher ($p < 0.01$) whereas older users rated procedural fairness as the primary determiner of trust.

7. Discussion

It proves the results that blockchain is able to provide significant improvement of trust, transparency, and accountability in e-government services in case it is

combined with appropriate governance measures. The perceived security and transparency played the primary role in fostering trust in citizens, and the economy of governance was reinforcing these effects, and it was possible to conclude that technology and institutional credibility should work in tandem. Another finding of the research is that the success of blockchain does not stem only from the fact that the data is not changeable but rather these protocols produce verifiable processes with citizens in the first place.

7.1 Comparison with Previous Studies

The finding that perceived security (PS) represents the strongest predictor of trust in service (TS) is consistent with prior empirical evidence indicating that protection of citizens' personal information is a key driver of trust in public e-services [1]. The significant influence of transparency (TR) and data integrity (DI) further supports earlier research on blockchain-enabled auditability, which demonstrates that transparent and verifiable records increase citizens' confidence in governmental data management [2]. Moreover, the positive role of procedural fairness (PF) in building trust aligns with established public administration literature emphasizing that fairness and accountability are essential for strengthening institutional trust [5]. The strong effect of trust in service (TS) on adoption intention (AI) also corresponds with technology adoption perspectives reported in recent systematic reviews of blockchain applications in e-government, confirming that trust functions as a central mediating factor shaping citizens' digital service usage [4]. Finally, the moderating effect of governance quality (GQ) provides additional insight by showing how effective institutional oversight can reinforce security-driven trust, a finding that is particularly relevant for public sectors undergoing digital transformation.

7.2 Limitations

This study acknowledges several limitations that should be considered when interpreting the findings. First, the data was collected within a single developing public-sector context, which may limit the generalizability of the results to other governmental settings with more mature digital ecosystems. Second, because the measurements relied on citizens' self-reported perceptions, results could be influenced by subjective and social desirability biases. Third, the cross-sectional nature of the data restricts the ability to determine causal changes in trust and adoption behavior over time. Finally, while the proposed multi-layer blockchain framework shows strong theoretical potential, further practical evaluation is necessary to test its performance in operational e-government environments.

7.3 Future Research Directions

Future studies may expand this work by testing the model across different countries or public service domains to strengthen its generalizability. Longitudinal studies would also provide deeper insight into how trust evolves as blockchain-enabled systems mature and scale. Additionally, integrating behavioral usage logs with perception-based measures could yield richer insights into adoption intention. Most importantly, pilot implementations in collaboration with governmental agencies would allow a more comprehensive assessment of the technical and governance aspects of the proposed framework.

8. Conclusion

To conclude, the proposed framework offers a viable way forward to governments that wish to restore the population trust in their ability to restore public trust in the security, transparency, and efficacy of their digital services. Pilot implementations, harmonization of laws and educating citizens should be incorporated in future work to facilitate the adoption of the system that will have sustainable benefits and value to the citizens.

9.References

[1] L. Carter and F. Bélanger, "The utilization of e-government services: citizen trust, innovation and acceptance factors," Information Systems Journal, vol. 15, no. 1, pp. 5–25, 2005. doi: 10.1111/j.1365-2575.2005.00183. x.

[2] S. Ølnes, 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. doi: 10.1016/j.giq.2017.09.007.

[3] J. Berryhill, T. Bourgery, and A. Hanson, Blockchains Unchained: Blockchain technology and its use in the public sector, OECD Working Papers on Public Governance No. 28, Paris: OECD Publishing, 2018. doi: 10.1787/3c32c429-en.

[4] I. Lykidis, G. Drosatos, and K. Rantos, "The use of blockchain technology in e-government services: a systematic review," Computers, vol. 10, no. 12, p. 168, 2021. doi: 10.3390/computers10120168.

[5] F. Bannister and R. Connolly, "The trouble with transparency: a critical review of openness in e-government," Policy & Internet, vol. 3, no. 1, pp. 1–30, 2011.

[6] N. Kshetri and J. Voas, "Blockchain in developing countries," IT Professional, vol. 20, no. 2, pp. 11–14, 2018.

[7] J. Mendling et al., "Blockchains for business process management — challenges and opportunities," ACM Transactions on Management Information Systems, vol. 9, no. 1, pp. 1–16, 2018. doi: 10.1145/3209281.3209329.

[8] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," International Journal of Production Research, vol. 57, no. 7, pp. 2117–2135, 2019. doi: 10.1080/00207543.2018.1533261.

تعزيز الثقة في خدمات الحكومة الإلكترونية باستخدام تقنية البلوكچين

عمر فاروق جلوب [1]
omarqwefar@gmail.com

المستخلص: تقدّم هذه الدراسة وتختبر مقاربة قائمة على تقنية البلوكچين لتعزيز ثقة المواطنين في خدمات الحكومة الإلكترونية. وباعتماد منهجية بحث مختلطة **(Mixed-Methods)** عبر مرحلتين، قمنا أولًا بعقد مجموعات نقاش خبراء **(n=12)** لتوليد نموذج مفاهيمي يوضّح العلاقة بين: الأمن المدرك**(PS)** ، الشفافية**(TR)** ، سلامة البيانات **(DI)**، والعدالة الإجرائية **(PF)** مع الثقة في الخدمة**(TS)** ، والنية في التبنّي**(AI)** ، مع جودة الحوكمة **(GQ)** كعامل سياقي مُعدِّل. ثم أجرينا استبيانًا شمل 412 مستخدمًا فعّالًا للخدمات الرقمية الحكومية، وتم تحليل هذه البيانات باستخدام نمذجة المعادلات البنائية.**PLS-SEM**

أظهرت النتائج أن النموذج القياسي يتمتع بموثوقية وصلاحية جيدة**(Alpha = .82–.91)** ؛ **(AVE = .59–.76)**. كما فسّر النموذج البنيوي ما نسبته 68% من المتغير **TS** و61% من المتغير**AI (SRMR = .056)** ؛ **(NFI = .90)**. وُجد أن جميع المتغيرات السابقة ترتبط إيجابيًا بشكل مؤثر مع**TS (PS: β = .27)**؛ **TR: β = .23**؛ **DI: β = .18**؛ **PF: β = .22**؛ جميع قيم **(p < .05)**. كما وُجد ارتباط قوي بين **TS** و**AI (β = .63)**؛ **(p < .001)**. وقد توسطت **TS** بالكامل تأثيرات **PS/TR/DI/PF** على**AI** ، كما عززت جودة الحوكمة **GQ** العلاقة بين **PS** و **TS**بشكل معنوي **(β = .14**؛**p < .05)**.

وتقدم الدراسة كذلك إطارًا ذا أربع طبقات (البنية التحتية، الخدمة، الحوكمة، المستخدم) يحقق تكاملًا بين قابلية التدقيق على السلسلة **(On-Chain Auditability)** وحماية البيانات الشخصية خارج السلسلة **(Off-Chain PII)** إلى جانب خارطة طريق متوافقة مع تقنيات الإثباتات عديمة المعرفة **(zk-compatible).** وتشير النتائج إلى أن تقنية البلوكچين قادرة على بناء تأثيرات إيجابية في الثقة متجسدة في حوكمة شفافة، خاضعة للمساءلة، ومصونة الخصوصية.

الكلمات المفتاحية: البلوكچين، الحكومة الإلكترونية، الثقة، جودة الحوكمة، العقود الذكية، الشفافية، الهوية الرقمية

[1] بيروت – لبنان،(AUL) جامعة الآداب والعلوم والتكنولوجيا في لبنان