

Blockchain: Aspects of Interdisciplinary Applications

Ivan Popchev

Bulgarian Academy of Sciences, Sofia, Bulgaria

Email: ivan.popchev@iict.bas.bg

Abstract: Blockchain technology has expanded beyond cryptocurrency into a wide range of institutional domains. This expansion creates an evaluation challenge: technical performance alone cannot guarantee adoption success. This communication identifies four common mechanisms that appear when blockchain is applied across different institutional environments: authority redistribution, accountability reconfiguration, the tension between immutability and adaptability, and the decentralization paradox. These mechanisms demonstrate that blockchain functions as a socio-technological infrastructure that makes governance choices visible. To address the evaluation challenge, the Hybrid Socio-Technological Evaluation (HSTE) framework is presented. HSTE integrates four independent evaluation dimensions – technical performance, governance quality, institutional fit, and sustainability – through a five-stage workflow with exclusionary rule-gates that prevent technical performance from overriding institutional requirements. A formal model complements the framework by specifying the conditions for constitutional legitimacy. It defines two primary dimensions – technical assurance and governance assurance – and shows that legitimate equilibrium requires both sufficient integrity and proportional balance between them. The analysis is based on the monograph "Blockchain Integration: Development and Implementation."

Keywords: *blockchain, evaluation framework, governance, Hybrid Socio-Technological Evaluation, interdisciplinary applications, socio-technological infrastructure*

1. Introduction

Blockchain technology has evolved beyond its origins as a distributed ledger for cryptocurrency. It is now present in a wide range of institutional domains, from finance and healthcare to public administration and digital identity. This creates

an important question. How should blockchain implementations be evaluated when they operate across diverse institutional environments?

The conventional approach focuses on technical performance: throughput, latency, and consensus efficiency. But many technically sound implementations fail in practice. They cannot align with governance requirements and stakeholder expectations. This leads to a different approach.

A socio-technological approach treats technical and institutional dimensions as interdependent. Blockchain is not only a technical infrastructure. It is a governance system that allocates authority and shapes institutional trust through its design.

This communication examines two aspects of this approach. First, it presents blockchain applications across several domains and identifies common mechanisms. Second, it describes the Hybrid Socio-Technological Evaluation (HSTE) framework and a formal model for assessing legitimate equilibrium. The analysis is based on [1], [2].

2. Blockchain governance dynamics in interdisciplinary domains

The monograph examines blockchain applications across several institutional domains. The analysis reveals four common mechanisms that appear regardless of the specific application area.

The first mechanism is authority redistribution. In every domain, blockchain shifts decision-making power among participants. In healthcare, patients gain cryptographic control over their records [3], [4]. In digital identity systems using Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs), authority is redistributed among issuers, holders, and verifiers [5]. In CBDC pilots, wallet design determines how monetary policy is enforced and who has access to financial services [6], [7]. Each case shows that blockchain does not simply automate existing processes. It changes who decides.

The second mechanism is accountability reconfiguration. Blockchain creates new forms of accountability while weakening others. Blockchain platforms that integrate smart contracts with IoT sensor data [8], [9] enforce traceability and compliance verification automatically. It strengthens accountability across supply chains. But it also gives more power to those who write the smart contract rules. In public administration, land registries on blockchain in several countries improve auditability [1, Ch. V, pp. 167–170]. Yet auditability alone does not create institutional trust. Accountability requires legal frameworks and oversight, not only technical records.

The third mechanism is the tension between immutability and adaptability. Blockchain records are designed to be permanent. But institutions need to adapt.

Health records require rectification rights under GDPR. Electoral systems require ballot secrecy [10]. Immutable contracts may perpetuate errors that cannot be corrected. This tension is present in every domain. It cannot be resolved by technical means alone.

The fourth mechanism is the decentralization paradox. Technically decentralised systems tend to reconcentrate authority at the governance layer [1, Ch. V, pp. 179–188]. Someone needs to define the protocol rules, manage upgrades, and resolve disputes. This governance function often becomes centralised even when the technical infrastructure is distributed.

These four mechanisms — authority redistribution, accountability reconfiguration, immutability-adaptability tension, and the decentralization paradox — appear across all examined domains. They demonstrate that blockchain is not a neutral technical tool. It is a socio-technological infrastructure that makes governance choices visible. The challenge is not whether to adopt blockchain but how to evaluate its governance consequences. This is the task addressed in the following section.

3. The HSTE evaluation framework

The Hybrid Socio-Technological Evaluation (HSTE) framework is a method for evaluating blockchain implementations that considers both technical and institutional dimensions [1, Ch. VI, pp. 224–278]. It addresses a specific problem. Existing evaluation methods focus on technical performance. They measure throughput, latency, and security. But they do not assess how a blockchain implementation allocates authority, handles disputes, or fits within existing institutions. HSTE fills this gap.

HSTE defines four evaluation pillars — independent dimensions that together provide a complete assessment. The term ‘pillar’ reflects the idea that each dimension supports the evaluation structure. If anyone is missing, the evaluation is incomplete. Pillar A covers technical performance: throughput, latency, energy efficiency, fault tolerance, and interoperability. Pillar B covers governance quality: decision rights, accountability, transparency, inclusiveness, and dispute resolution. Pillar C covers institutional fit: regulatory compliance, alignment with existing institutions, stakeholder legitimacy, and public trust. Pillar D covers sustainability and risk: systemic resilience, economic viability, and crisis adaptability.

The framework works in five stages. In Stage 1, rule-gates are defined. These are non-negotiable requirements. For example, ballot secrecy in elections or rectification rights in health records. A system that fails a rule-gate is rejected. Technical performance in other areas does not change this result.

In Stage 2, weights are assigned to criteria based on the specific domain. Healthcare may prioritise privacy. Finance may prioritise auditability. In Stage 3,

the scores from all four pillars are combined into a weighted composite index. Stage 4 tests the result. If small changes in weights reverse the ranking, the evaluation is unstable. Stage 5 is a deliberative checkpoint. Minority concerns and governance risks are recorded.

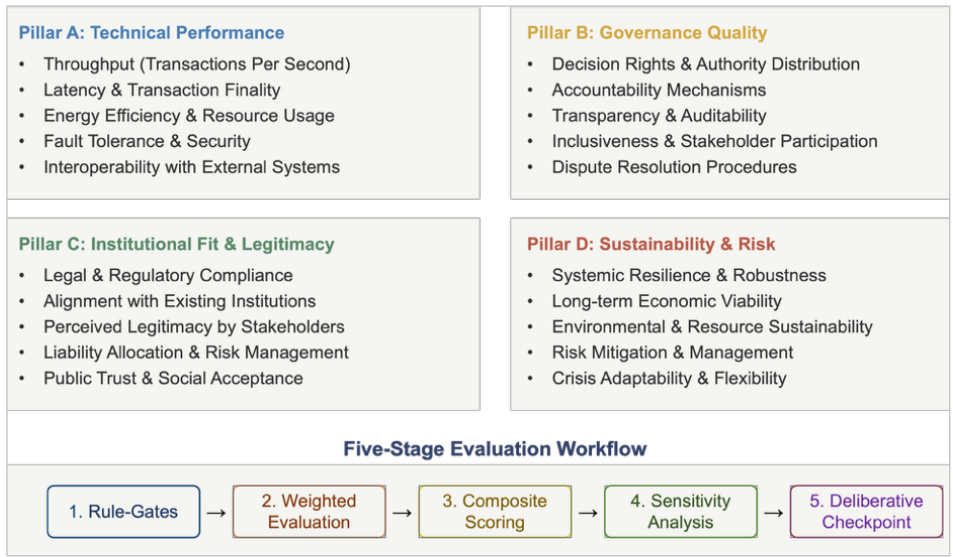


Fig. 1. HSTE Framework.

A ten-step protocol makes the framework operational: (1) define scope, (2) identify design axes, (3) establish rule-gates, (4) construct scoring matrices, (5) apply scenario planning [11], (6) conduct Delphi deliberation [12], (7) perform cost-benefit analysis [13], (8) conduct risk-benefit analysis [14], (9) compile a decision dossier, (10) formulate a decision with monitoring [1, Ch. VI, pp. 254–276].

The key idea of HSTE is that evaluating blockchain implementations is not just performance measurement. It is a process that examines how technical design choices affect governance. Who gets authority? Who is accountable? How is legitimacy established?

4. Formal model of constitutionalization through code

The HSTE framework defines what should be evaluated and how the evaluation is conducted. The formal model presented in this section complements it. It specifies the mathematical conditions under which a blockchain implementation achieves constitutional legitimacy [1, Ch. V, pp. 194–219]. HSTE is a practical evaluation tool. The formal model is its analytical basis.

Two terms require clarification. Constitutional legitimacy means that a system’s design choices are recognised as accountable, transparent, and accepted

by its participants. It is not enough that a system works technically. It also needs to be accepted as a proper way to allocate authority and resolve disputes. Constitutionalization through code is the process by which technical design decisions acquire the force of institutional rules. When a smart contract defines who can participate and under what conditions, it performs a constitutional function.

The model defines two primary dimensions. Technical assurance $T \in [0,1]$ represents the strength of coded guarantees: immutability, cryptographic integrity, and automation. Governance assurance $G \in [0,1]$ represents institutional guarantees: legal frameworks, oversight, and participation rights. Their joint effect defines the constitutional performance function:

$$R = aT + bG - cTG \quad (1)$$

where $a > 0$ measures technological efficiency, $b > 0$ measures institutional oversight, and $c > 0$ measures coordination friction. The term $-cTG$ is important. It means that as both T and G increase, their interaction creates complexity costs. A system cannot simply maximise both dimensions independently. It needs to balance them.

Four evidentiary parameters capture how legitimacy is produced. Encoding (ϵ) translates governance rules into executable code. Anchoring (α) commits records cryptographically. Governed supersession (σ) enables lawful correction without erasure. Evidentiary independence (ι) allows verification without issuer presence. These combine into two derived measures.

Verifiability measures whether claims can be independently checked:

$$V = \frac{1}{2}(\alpha + \iota) \quad (2)$$

A system where records cannot be verified by third parties has low V . Rectifiability measures whether errors can be corrected through legitimate procedures:

$$Q = \sigma \quad (3)$$

A system that cannot correct its own records — even when they contain errors — has low Q . Both must be high. The integrity function captures this:

$$S = \min(V, Q) \quad (4)$$

The minimum operator is significant. A system with perfect verifiability ($V = 1$) but no ability to correct errors ($Q = 0$) yields $S = 0$. It is not legitimate even with strong technical performance. Similarly, a system that can correct records but cannot verify them is also not legitimate.

The model adds a second condition. The partial derivatives of R must exhibit negative feedback:

$$\left(\frac{\partial R}{\partial T}\right) \times \left(\frac{\partial R}{\partial G}\right) < 0 \quad (5)$$

This condition means that the two dimensions must constrain each other. When T increases, G should moderate it, and vice versa. Without this balance, the system enters one of two deviation zones.

In the drift zone, both T and G are weak. The system lacks both technical reliability and institutional oversight. It is neither verifiable nor accountable. In the lock zone, both T and G are excessive. The system becomes rigid. Over-regulation combined with over-automation prevents adaptation. Neither zone produces legitimacy.

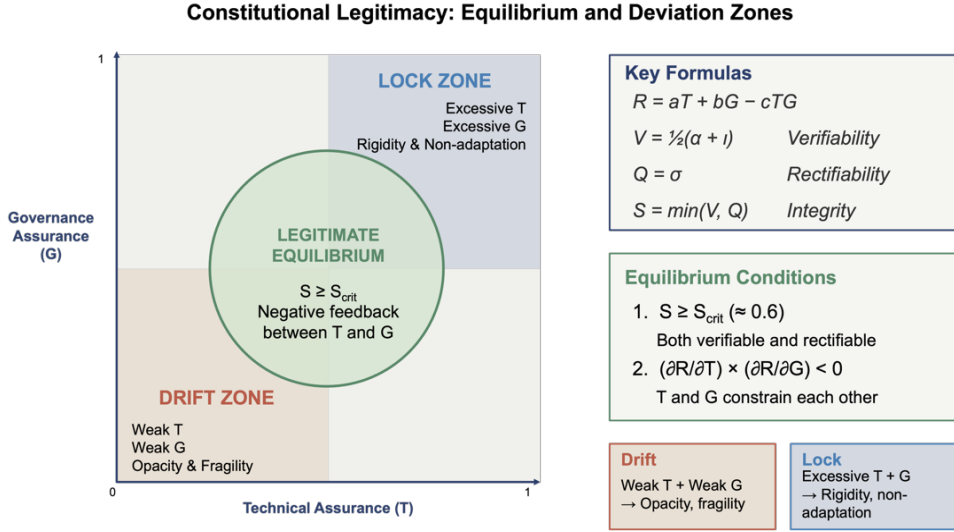


Fig. 2. Constitutional legitimacy zones in the $T \times G$ space.

Legitimate equilibrium requires both conditions simultaneously: $S \geq S_{crit}$ (approximately 0.6) and negative feedback between T and G . This equilibrium is not automatic. It needs to be designed and maintained. Protocol upgrades modify T . Procedural reforms modify G . Each adjustment shifts the system's position. The model is a diagnostic tool. It shows whether a system is legitimate and what adjustments are needed [1, Ch. V, pp. 198–204].

5. Conclusion

The socio-technological approach presented here offers a different way to assess blockchain implementations. Instead of measuring only technical performance, evaluation should consider governance consequences – who gains authority, who becomes accountable, and how legitimacy is established. The HSTE framework and the formal model offer practical and analytical tools for this task. They can be applied by regulators, system designers, and policymakers in any domain where blockchain is considered for institutional use.

Future work can extend these results in several directions. The threshold S_{crit} can be calibrated for specific institutional contexts through empirical studies. The interaction between the four governance mechanisms offers opportunities for more detailed analysis. The formal model may also find application in other socio-technological systems where design choices encode governance decisions. As blockchain adoption grows across sectors, the need for systematic evaluation becomes urgent. The HSTE framework and the formal model provide the necessary tools.

References

1. Radeva, I.: Blockchain Integration: Development and Implementation. 1st edn. Prof. Marin Drinov Publishing House of Bulgarian Academy of Sciences, Sofia (2024).
2. Radeva, I.: Blockchains: Practical Approaches. Engineering Sciences 59(2), 79–92 (2022).
3. Wang, M., Guo, Y., Zhang, C., Wang, C., Huang, H., Jia, X.: MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain. IEEE Transactions on Services Computing 16(1), 438–451 (2023).
4. Haleem, A., Javaid, M., Singh, R.P., Suman, R., Rab, S.: Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks 2, 130–139 (2021).
5. Preukschat, A., Reed, D.: Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. Manning (2021).
6. Bank for International Settlements: Central Bank Digital Currencies: Ongoing Policy Perspectives. BIS (2024).
7. European Central Bank: Progress on the Investigation Phase of a Digital Euro – Third Report. ECB, Frankfurt (2023).
8. Popchev, I., Doukovska, L., Radeva, I.: A Prototype of Blockchain/Distributed File System Platform. In: IEEE International Conference on Intelligent Systems IS'22, pp. 1–7. IEEE, Warsaw (2022).
9. Popchev, I., Radeva, I., Doukovska, L.: Oracles Integration in Blockchain-Based Platform for Smart Crop Production Data Exchange. Electronics 12(10), 2244 (2023).
10. Barelli, R., D'Onghia, M., Longari, S.: Toward Secure Electronic Voting: A Survey on E-Voting Systems and Attacks. IEEE Access 13, 89600–89626 (2025).
11. Schoemaker, P.J.H.: Scenario Planning: A Tool for Strategic Thinking. Sloan Management Review 36, 25–40 (1995).
12. Linstone, H., Turoff, M.: The Delphi Method: Techniques and Applications. Addison-Wesley (1975).
13. Boardman, A.E., Greenberg, D.H., Vining, A.R., Weimer, D.L.: Cost-Benefit Analysis: Concepts and Practice. 5th edn. Cambridge University Press (2018).
14. Stirling, A.: Risk, precaution and science: towards a more constructive policy debate. EMBO Reports 8(4), 309–315 (2007).