

Book Review

On Focus: Blockchain Integration

Ivan Popchev

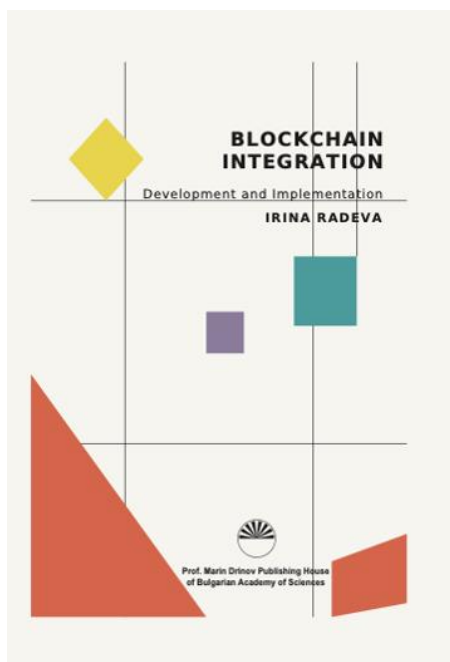
Bulgarian Academy of Sciences

E-mail: ivan.popchev@iict.bas.bg

Received: March 05, 2026

Accepted: March 27, 2026

Published: March 31, 2026



Printing office
of Prof. Marin Drinov Publishing House
of Bulgarian Academy of Sciences

www.press.bas.bg
ISBN 978-619-245-473-9

Blockchain is a distributed digital infrastructure that records transactions across a network of independent nodes without relying on a central authority. Yet this technical definition captures only part of the picture. The monograph under review argues that blockchain is equally a governance system — one that allocates authority, defines accountability, and shapes institutional trust through its very design. This perspective places blockchain integration at the centre of an important and timely debate. “This monograph addresses the central problem of blockchain integration, development and implementation, as well as the governance decisions embedded in these processes. Technical performance alone does not determine adoption outcomes. Rather, the infrastructural potential of blockchain depends on the interaction between design choices and governance arrangements, regulatory frameworks, and institutional requirements. The monograph demonstrates that evaluating blockchain requires examining three interconnected dimensions: technical architect-

tures (e.g. consensus mechanisms, data structures and cryptographic protocols); governance mechanisms (e.g. authority allocation, accountability structures and dispute resolution); and social-institutional contexts (e.g. regulatory environments, organisational practices and stakeholder expectations)” [1].

Blockchain technology has evolved far beyond its origins as a distributed ledger for cryptocurrency. Today it is present in central bank digital currencies, supply chain management, digital identity systems, healthcare, agriculture, and public administration. This rapid expansion creates a fundamental challenge: how should blockchain systems be evaluated, designed, and integrated into institutional environments where technical performance alone cannot guarantee

success? The conventional approach considers blockchain a purely technological infrastructure, focusing on throughput, latency, and consensus efficiency. Yet practice demonstrates that many technically sound implementations fail when they cannot align with governance requirements, regulatory frameworks, and stakeholder expectations. The published monograph offers a comprehensive and original response to this challenge by proposing a socio-technological framework that treats technical and institutional dimensions as interdependent rather than merely interacting.

The monograph comprises seven chapters organized around three themes. Chapters I–II address blockchain as socio-technological infrastructure, Chapters III–V cover development through decentralised applications, wallets, and interdisciplinary ecosystems, and Chapters VI–VII focus on evaluation frameworks and future directions. This structure reflects the author’s central thesis that integration, development, and implementation are not sequential technical stages but governance decisions that encode authority, accountability, and legitimacy into the architecture.

Chapter I „*Blockchain as Infrastructure*“ establishes the conceptual foundation by arguing that blockchain cannot be understood solely as distributed ledger technology. The author introduces a three-layer analytical framework: the technical layer (processing infrastructure), the governance layer (access and decision-making rules), and the social-institutional layer (integration with existing organisations and regulations). This framework is grounded in Elinor Ostrom’s institutional analysis of commons governance and infrastructure studies that emphasise embedding, path dependency, and layering as stability mechanisms. A significant contribution is the treatment of blockchain architectures as constitutional specifications – systems that structurally allocate authority, define accountability, and establish legitimacy through their technical design [2].

The chapter traces the evolution of consensus mechanisms across five generations (2008–2024). Each generation embeds a distinct theory of legitimate authority. Proof-of-Work equates computational expenditure with validation rights, Proof-of-Stake allocates influence by economic commitment, and Byzantine Fault Tolerance distributes decision power among predetermined validators. Regional and sectoral comparisons across the EU, China, the United States, and the Global South reveal that adoption depends on institutional embedding rather than technological superiority. The chapter concludes with a four-stage adoption model providing criteria for evaluating when blockchain implementations achieve infrastructure transition [3, 4].

Chapter II „*Blockchain Integration Frameworks*“ examines the mechanisms through which blockchain systems connect with external data, storage, and institutional infrastructures. The author demonstrates that integration frameworks are not neutral technical tools but governance instruments that redistribute authority and accountability at system boundaries. Four integration domains are analysed in detail. Oracles and off-chain data integration mediate between on-chain execution and real-world information. Distributed file systems combine on-chain cryptographic integrity with off-chain storage, creating dependencies between verifiability and organisational commitments.

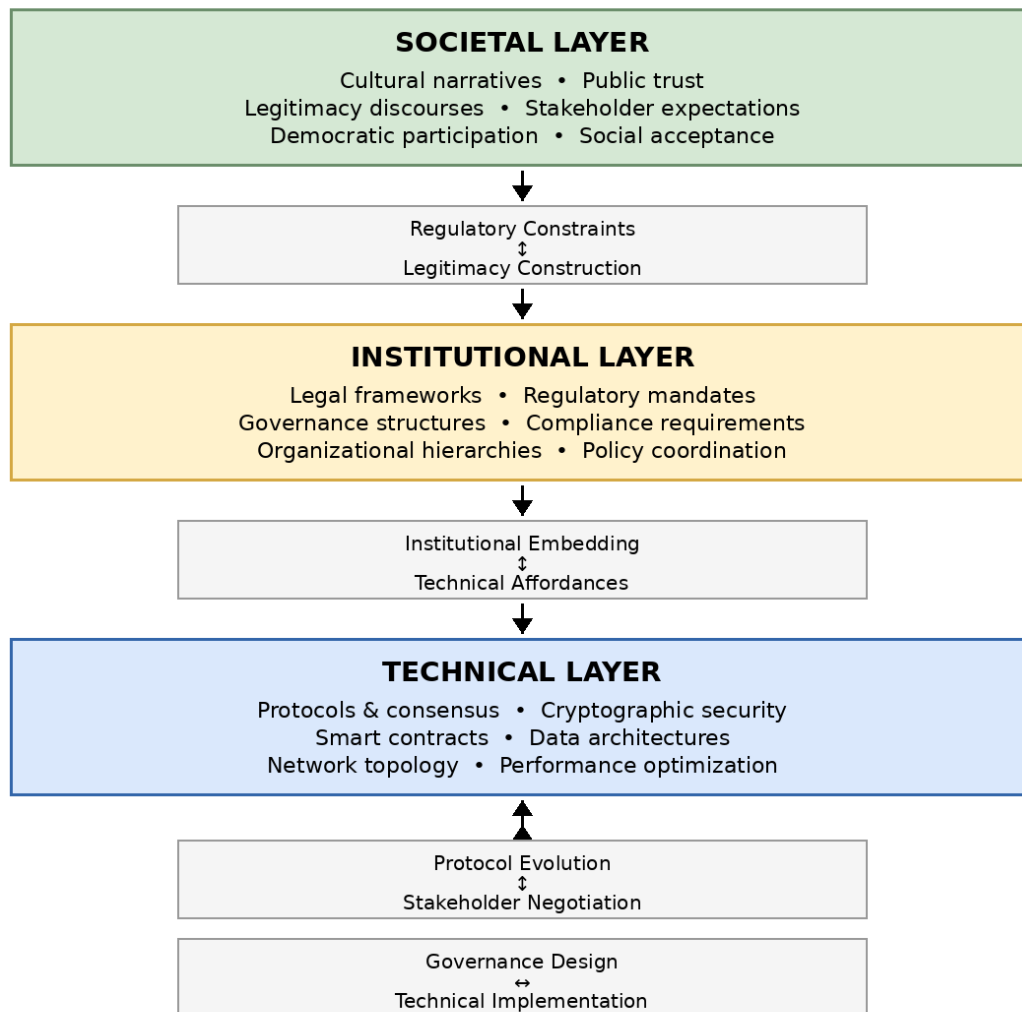


Fig. 1 Blockchain as socio-technological infrastructure

Cross-chain protocols negotiate between blockchain sovereignty and ecosystem coordination, while integration middleware and modular design shape user experience and access patterns. The chapter's sectoral analysis reveals that integration choices reflect institutional requirements. Finance prioritises oracle resilience, healthcare emphasises privacy-preserving middleware, agriculture adopts IoT integration for compliance verification, and government requires authenticated systems for legal enforceability [3, 5, 6].

Chapter III „Decentralised Applications (dApps)“ analyses decentralised applications (dApps) as institutional architectures rather than mere software products. The author argues that smart contracts and integration mechanisms act as constitutional instruments, allocating power, defining accountability, and setting conditions for participation. Architecture is treated as governance encoding, with authority distribution examined across operational domains. The chapter presents empirical validation through the SCPDx (Smart Crop Production Data Exchange) platform, which integrates blockchain technology with IoT sensors and distributed file storage [7].

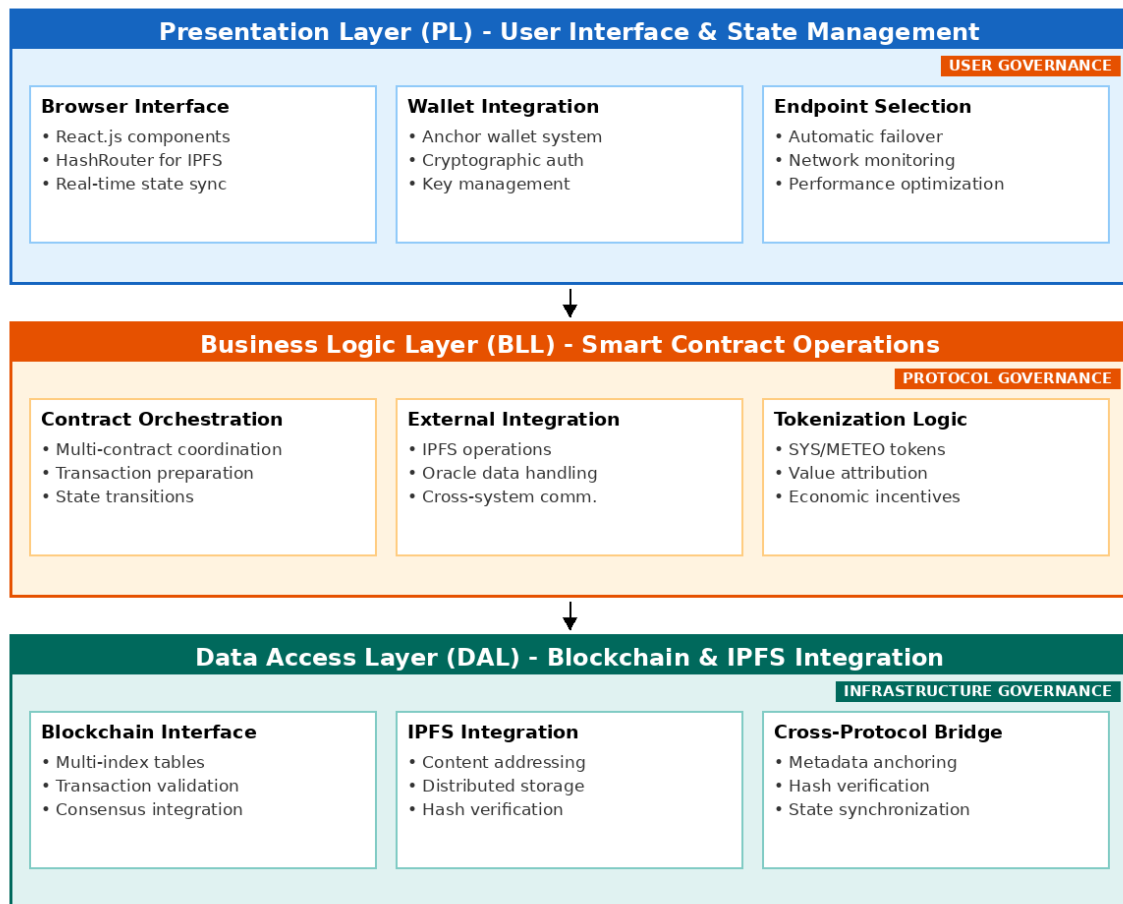


Fig. 2 SCPDX governance architecture

This platform demonstrates how smart contract modularity enables adaptive governance through separation of concerns. It allows incremental updates, targeted security audits, and domain-specific oversight rules while preserving system coherence. The analysis identifies three types of participation gates – technical (cryptographic authentication), administrative (institutional approval), and contractual (smart contract permissions) – that determine who may participate and under what conditions. The chapter concludes that preventive governance, based on transparency and traceability, is more sustainable than reactive arbitration. [3, 8].

Chapter IV „Blockchain Wallets“ examines blockchain wallets as interfaces that mediate user participation in blockchain systems. The author traces the evolution of wallets from simple key management tools to multi-purpose gateways and programmable policy engines. Four design axes are identified: custody models (self-custodial, custodial, and hybrid); device environments (hardware, mobile, and browser-based); operational scope (single-chain, multi-chain, and cross-chain); and security architectures [9].

Each axis represents a trade-off between autonomy and convenience, accessibility and protection, sovereignty and compliance. The chapter demonstrates that wallet architecture embeds institutional logic through design choices. Recent developments including account abstraction, multi-party computation, and integration with decentralised identity standards are reshaping the governance landscape. Central bank digital currency wallet pilots are examined to show how wallet design can incorporate monetary policy and oversight mechanisms.

Chapter V „*Blockchain in Interdisciplinary Applications and Digital Ecosystems*“ explores the use of blockchain technology across multiple interdisciplinary domains: healthcare, agriculture, cultural heritage, public administration, knowledge systems, digital identity, and monetary systems. The analysis identifies common patterns in how blockchain redistributes governance functions across these areas. Three original frameworks are developed. First, an evidence-based triad for knowledge systems comprising provenance, traceability, and evaluation establishes the conditions under which blockchain functions as a constitutional layer for evidence. Second, an analytical approach to digital identity governance analyses authority redistribution across issuers, holders, and verifiers. Third, a formal equilibrium model specifies how technical assurance (cryptographic guarantees) and governance assurance (institutional procedures) jointly produce system legitimacy [10, 11]. The model defines the conditions under which systems can be both verifiable and correctable. This discussion provides the theoretical bridge between the concrete development discussions in Chapters III–IV and the evaluation framework presented in Chapter VI.

Chapter VI „*Design and Evaluation Frameworks for Blockchain Integration*“ introduces the Hybrid Socio-Technological Evaluation (HSTE) framework, which represents one of the monograph's most significant analytical contributions. The HSTE framework integrates four evaluation pillars: technical performance, governance quality, institutional fit and legitimacy, and sustainability and risk.

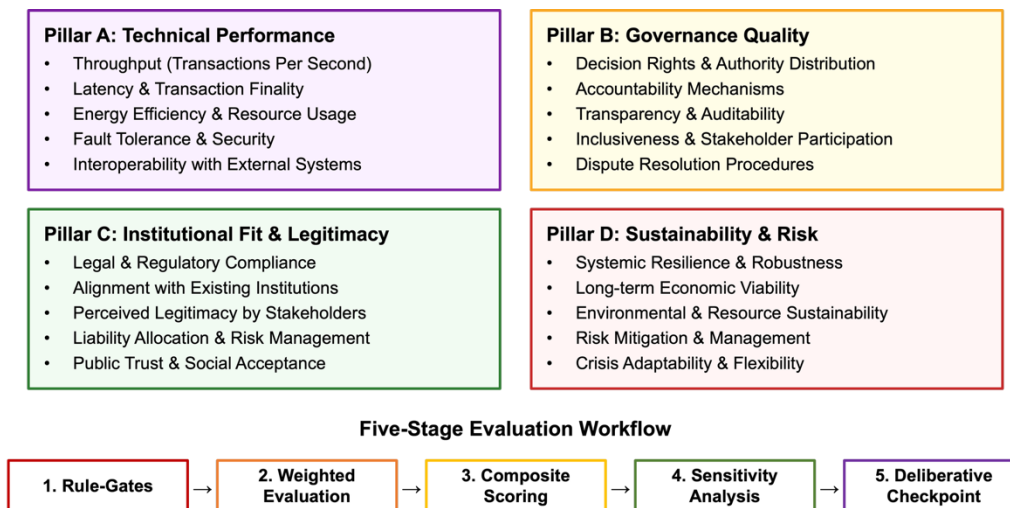


Fig. 3 Hybrid socio-technological evaluation framework

The framework's key contribution is its use of exclusionary rule-gates. Certain criteria – ballot secrecy in elections, rectification rights in health records, transparent liability allocation in finance – are treated as non-negotiable requirements. Systems that fail these gates are excluded from assessment regardless of their technical capabilities. A ten-step protocol structures the evaluation process through scope definition, rule-gate establishment, weighted scoring, scenario planning, cost-benefit and risk-benefit analyses, evidence synthesis, and continuous monitoring. The author demonstrates that HSTE transforms blockchain evaluation from performance measurement into constitutional specification. Technical architectures are judged for how they allocate authority, institutionalise legitimacy, and manage systemic risks [1, 12, 13, 14].

Chapter VII „*Future Directions and Challenges*“ examines blockchain’s possible futures not as prediction but as structured analysis of constitutional choices that integration makes visible. The author identifies two competing development paths – institutionalist embedding versus autonomous consolidation – and clarifies that policy frameworks rather than academic consensus currently shape blockchain’s trajectory [15, 16].

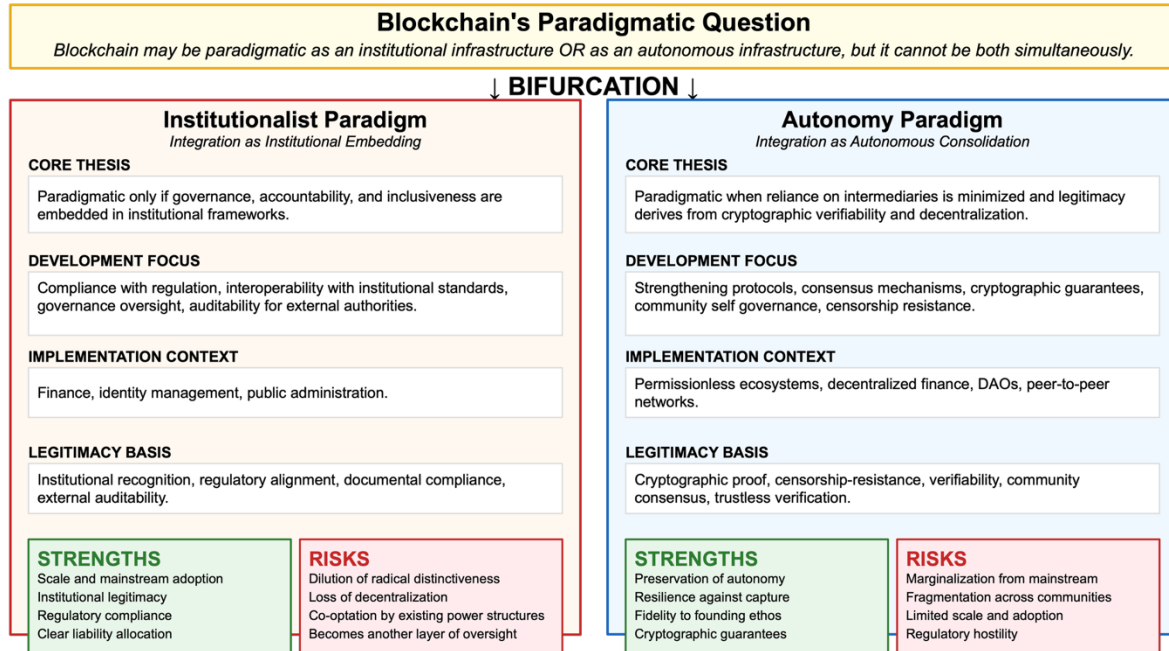


Fig. 4 Paradigm bifurcation and challenges

The author analyses risk management as constitutional practice, convergence with emerging technologies (Artificial Intelligence, Internet of Things), convergence with foundational infrastructures, and the principal challenges in blockchain development. The failure scenarios presented demonstrate the importance of multiple evaluation criteria: systems can be scalable but exclusionary, secure but captured, compliant but depoliticized, or immutable but containing false data. This concluding chapter reinforces the monograph’s central argument that blockchain’s challenges are not isolated technical problems but paradigmatic choices about authority, inclusiveness, and truth.

The monograph presents a comprehensive and analytically rigorous examination of blockchain integration, development, and implementation. All conceptual frameworks are supported with detailed analysis, formal models, and empirical evidence through the SCPDx platform. Each chapter is well supported with relevant references drawn from computer science, institutional economics, constitutional theory, and infrastructure studies. The interdisciplinary approach is a particular strength, demonstrating that blockchain evaluation requires methods from both informatics and institutional analysis.

Instead of a conclusion

Blockchain integration deserves focused attention. Today and in the future, blockchain is not merely a technical infrastructure but a socio-technological system. It encodes governance, allocates authority, and constructs legitimacy through its architectural design. The monograph convincingly demonstrates that the success of adoption depends not on technical performance metrics alone but on the construction of legitimacy through institutional embedding. This insight is of fundamental importance for researchers, practitioners, policymakers, and system

designers who must navigate the complex landscape of blockchain integration. As blockchain adoption accelerates across sectors and jurisdictions, the need for systematic evaluation frameworks becomes increasingly urgent. This monograph provides precisely such a framework.

The Prof. Marin Drinov Publishing House of Bulgarian Academy of Sciences should be congratulated with this publication. It is the first monograph devoted entirely to the socio-technological analysis of blockchain integration, development and implementation.

References:

1. Radeva, I. Blockchain Integration: Development and Implementation, 1st Edn., Sofia: Printing office of Prof. Marin Drinov Publishing House of Bulgarian Academy of Sciences, 2024, 350. ISBN 978-619-245-473-9, <https://www.press.bas.bg/bg>
2. Wright A., P. D. Filippi (2018). Blockchain and the Law: The Rule of Code, 2nd Edn., Cambridge, MA: Harvard University Press, <https://www.hup.harvard.edu/catalog.php?isbn=9780674241596>
3. Popchev, I., L. Doukovska, I. Radeva (2022). A Framework of Blockchain/IPFS-based Platform for Smart Crop Production, In IEEE International Conference Automatics and Informatics, Varna, Bulgaria, 265-270. <https://doi.org/10.1109/ICAI55857.2022.9960070>.
4. Radeva, I. (2022). Blockchains: Practical Approaches, Engineering Sciences, 59(2), 79-92, <https://doi.org/10.7546/EngSci.LIX.22.01.01>.
5. Popchev, I., L. Doukovska, I. Radeva (2022). A Prototype of Blockchain/distributed File System Platform, In IEEE International Conference on Intelligent Systems IS'22, Warsaw, Poland: IEEE, 1-7. <https://doi.org/10.1109/IS57118.2022.10019715>.
6. Popchev, I., I. Radeva, V. Velichkova (2021). Blockchains in Enterprise Global Risk Management, In 2021 International Conference Automatics and Informatics (ICAI), 282-287. <https://doi.org/10.1109/ICAI52893.2021.9639500>.
7. Popchev, I., I. Radeva (2024). Decentralized Application (dApp) Development and Implementation, Cybernetics and Information Technologies, 24(2), 122-141, <https://doi.org/10.2478/cait-2024-0019>.
8. Popchev, I., I. Radeva, L. Doukovska (2023). Oracles Integration in Blockchain-Based Platform for Smart Crop Production Data Exchange, Electronics, 12(10), Art. no. 10, <https://doi.org/10.3390/electronics12102244>.
9. Popchev, I., I. Radeva, M. Dimitrova (2023). Towards Blockchain Wallets Classification and Implementation, In 2023 International Conference Automatics and Informatics (ICAI), 346-351. <https://doi.org/10.1109/ICAI58806.2023.10339101>.
10. Radeva, I., I. Popchev (2022). Blockchain-Enabled Supply-chain in Crop Production Framework, Cybernetics and Information Technologies, 22(1), 151-170, <https://doi.org/10.2478/cait-2022-0010>.
11. Ilieva, G., T. Yankova, I. Radeva, I. Popchev (2021). Blockchain Software Selection as a Fuzzy Multi-criteria Problem, Computers, 10(10), Art. no. 10, <https://doi.org/10.3390/computers10100120>.
12. Popchev I., I. Radeva (2024). Framework for Evaluation of Authentication and Proof-of-Event Mechanisms in Smart Contracts, In 2024 IEEE 12th International Conference on Intelligent Systems (IS), 1-10. <https://doi.org/10.1109/IS61756.2024.10705211>.
13. Greco, S., M. Ehrgott, J. R. Figueira, (Eds.) (2016). Multiple Criteria Decision Analysis. State of the Art Surveys, 2nd Edn., In International Series in Operations Research & Management Science, Springer New York, <https://doi.org/10.1007/978-1-4939-3094-4>.

14. Linstone, H., M. Turoff (1975). *The Delphi Method: Techniques and Applications*, Vol. 18, Addison-Wesley Publishing Company, Advanced Book Program, <https://doi.org/10.2307/3150755>.
15. Popchev, I., I. Radeva, L. Doukovska, M. Dimitrova (2023). A Web Application for Data Exchange Blockchain Platform, In 2023 International Conference on Big Data, Knowledge and Control Systems Engineering (BdKCSE), 1-7. <https://doi.org/10.1109/BdKCSE59280.2023.10339770>.
16. Radeva, I., I. Popchev, M. Dimitrova (2024). Similarity Thresholds in Retrieval-Augmented Generation, In 2024 IEEE 12th International Conference on Intelligent Systems (IS), 1-7. <https://doi.org/10.1109/IS61756.2024.10705214>.