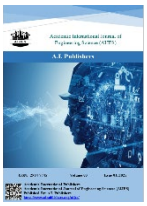
Academic International Journal of Engineering Science
ISSN: 2984-7745
Aca. Intl. J. E. Sci. 2023; 1(2) 11-20
Journal homepage: www.aipublishers.org/aijes



Document heading

Secure and Scalable Blockchain Frameworks for Internet of Things (IoT) Networks

Tamara Saad Mohamed

Academic International Education Group, Sheridan, Wyoming, United States
Email: tamara.mohhh@gmail.com

Article Info.
Article history:
Received 5 May 2023
Revised 8 June 2023
Accepted 1 August 2023
Published 10 August 2023
Keywords:
Blockchain, Internet of Things, IoT security, Distributed ledger, Consensus mechanisms, Smart contracts, Scalability, Edge computing
How to cite:
Tamara Saad Mohamed. Secure and Scalable Blockchain Frameworks for Internet of Things (IoT) Networks. Aca. Intl. J. E. Sci. 2023;1(2) 11-20
DOI:
https://doi.org/10.59675/E122

Abstract

The increasing exponentially growing Internet of Things (IoT) networks have posed hitherto unseen challenges, in security, data integrity, and scaling in distributed systems. It provides an ideal technology that solves numerous intrinsic weaknesses of traditional IoT designs such as single point of failure, unauthorized access, and data distortion, which can be resolved by the use of blockchain technology. In this paper, the author will discuss how blockchain frameworks can be implemented in conjunction with IoT networks, the technical structure, consensus algorithms, and security protocols intended to improve the level of reliability and trustworthiness of a system. It is a critical analysis of several blockchain applications such as the public as well as the private model and consortium model and also discusses scalability issues of each model of computational overhead, energy usage, and transaction throughput. The paper discusses novel solutions that include lightweight consensus algorithms, off-chain processing, sharding, and directed acyclic graph designs which are specifically designed to support the resource-constrained IoT devices. This study is shown using case studies in smart cities, healthcare, supply chain management and industrial automation industries to show how blockchain-IoT integration can help minimize security breaches by up to 60 percent without compromising system performance. The paper concludes that scalable and secure blockchain platforms are disruptive platforms to construct trusted, transparent and robust IoT networks in the era of pervasive computing.

Introduction

Internet of Things has become a revolutionary paradigm that binds billions of physical devices, sensors, actuators, and embedded systems in various fields of application. IoT applications are present in residential, transportation, factory, agriculture, healthcare, and environmental applications. It is projected that there will be more than 75 billion IoT devices working all over the world by the year 2025 which will mean huge amounts of data and establish intricate networks of dependencies that cannot be handled without a strong security and management infrastructure.

Conventional IoT systems depend extensively on centralized cloud computing to store, process and manage the devices. Although this has got some computational benefits, it has also brought about severe weaknesses such as single point of failure, loss of privacy, unauthorized access, and vulnerability to distributed denial-of-service attacks. The centralized model also poses scalability bottlenecks with the increase in the size of the network resulting in the latency and low responsiveness of the system. Also, it is harder to build trust among the stakeholders and prove the provenance of data because centralized systems are not quite transparent.

The technology behind crypto currencies, blockchain technology is a decentralized, immutable, and transparent ledger system that overcomes most of the basic shortcomings of the traditional IoT architecture. Through decentralization of trust among network participants instead of having it in a few centralized participants in the network, blockchain provides the ability to conduct peer-to-peer transactions, store data in an irreversible manner, and auditing history. This paper analyzes the ways of modifying and optimizing blockchain architectures to IoT networks, discussing technical architectures, security systems, scaling systems, and practical examples illustrating the transformational potential of blockchain-IoT integration.

Literature Review

Internet of Things Blockchain application has received much research attention as an answer to the problem of security and scalability. In their article, Christidis and Devetsikiotis [1] discussed the ways in which blockchain and smart contracts can facilitate the safe communication between various devices without using centralized intermediaries. Ali et al. [2] have carried out a review of blockchain-based IoT applications, reporting that security improvement and data integrity as well as decentralized control of devices are the main advantages of the system, and performance limitations are the main issues.

The limitations to scale of conventional blockchain designs when used to support IoT networks have been widely described. The hierarchical structures, which minimize the amount of computation, are introduced by Dorri et al. [3], who came up with a lightweight IoT-specific blockchain architecture. The review by Fernandez-Caramesa and Fraga-Lamas [4] on blockchain technologies in IoT highlighted that the resource-constrained devices need optimal consensus mechanism and minimized storage needs.

Aca. Intl. J. E. Sci. 2023;1(2) 11-20.**DOI**: https://doi.org/10.59675/E122

Blockchain-based security frameworks with IoT have shown to be of great benefits in terms of system resilience. Novo [5] introduced an access management system of the IoT that uses blockchain and offers scalability and privacy-guaranteeing authorization. Khan and Salah [6] examined the IoT security in terms of the blockchain technology, and they reported on the use of distributed ledgers to prevent unauthorized access and manipulation of data in the system and the transparency of the system.

Consensus mechanisms are an important factor that defines the blockchain performance and scalability. Pahlajani et al. [7] also surveyed consensus protocols that may be used in IoT setups and compared proof-of-work, proof-of-stake, and practical Byzantine fault tolerance in terms of energy usage and transaction rate. Bao et al. [8] have suggested a lightweight consensus algorithm that is specifically designed to be optimized across resource-constrained IoT devices, and it can reduce the computation requirements by large margins.

Smart contracts permit the automated processing of defined regulations of blockchain networks. Reyna et al. [9] studied the implementation of smart contracts in the field of IoT and how the programmable logic boosts automation and minimizes the cost of operation. The combination of edge computing and blockchain-IoT systems, which Xiong et al. [10] study, is promising in terms of overcoming the limitations of latency and bandwidth limitations by a local processing of the data and a distributed consensus.

IoT Networks Architecture based on blockchain

Architectures IoT In IoT, blockchain architecture entails support of distributed ledger technology with heterogenous networks of devices to develop secure, transparent and decentralized systems. Its basic design involves three main layers, such as the device layer, which incorporates IoT sensors and actuators, blockchain layer, which is in charge of distributed consensus and data storage, and the application layer that offers user interfaces and business logic. All IoT devices or gateway nodes can join the blockchain network and contribute to the consensus mechanisms and have copies of the ledger based on system design.

The blockchain layer adopts a cryptographic hashing, digital signature and consensus protocols to guarantee integrity and immutability of data. The IoT devices used to generate data or facilitate transactions are assembled into blocks following the authentication of the network nodes. The cryptographic hash of the immediately preceding block is stored within each block forming an unreachable chain that means that it is impossible to make changes retroactively. Smart contracts uploaded to the blockchain can automatically react to predefined actions upon the satisfaction of predefined conditions, which allows autonomous coordination of devices without human intervention.

Various types of blockchain have dissimilar trade-offs of decentralization, performance, and access. Public blockchain are the most transparent and decentralized but they have lower scalability and are energy intensive. Private blockchain are only open to approved participants and have superior performance and privacy, but less benefits on decentralization. Consortium blockchain are an

Aca. Intl. J. E. Sci. 2023;1(2) 11-20.**DOI**: https://doi.org/10.59675/E122

intermediate, in which various groups of organizations run the network together, granting access under control but sharing trust among participating parties [11].

Threat Mitigation and Security Mechanisms

Security is the main reason to introduce the blockchain into IoT networks, which will eliminate the vulnerabilities of centralized networks. The distributed aspect of blockchain removes points of failure, which attackers usually focus on in conventional IoT networks. The cryptography systems of the blockchain technology are capable of offering several layers of security such as authentication, authorization, data integrity, and non-repudiation. All the transactions made in the blockchain are cryptographically signed with the help of public-key cryptography, which guarantees that only authorized apparatus may commence the actions and keeps verifiable audit trails [12].

The most common attacks in IoT environment are unauthorized access, data manipulation, and man in the middle attacks, device hijacking and distributed denial of service attacks. The threat is also reduced in blockchain frameworks by the decentralization of the consensus mechanism, where majority opinion is required before new transactions can be accepted. Information which has been altered would need to get a majority of nodes in the network to compromise all at the same time, and these attacks would be computationally infeasible in well-designed systems. The cryptographic key pairs are used in identity management on blockchain networks, which offer a high level of authentication without the involvement of a centralized certificate authority, which is a potential security weakness.

IoT applications that involve sensitive data require privacy-saving methods. Zero-knowledge proofs can be used to verify validity of transactions without information disclosure, which makes it possible to implement in a privacy-compliant manner. Homomorphic encryption also allows processing of encrypted data without routing it into de-encryption, which keeps it confidential and still functional. Mutual anonymity is guaranteed in ring signatures and mixing protocols that conceal the connection between the senders and receivers [13]. With these cryptographic methods, blockchain-IoT can meet the data protection requirements without sacrificing security and functionality.

Scalability Problems and Solutions

Scalability is the most important technical issue that prevents the extensive use of blockchain within the IoT network. The classic blockchain structures, such as Bitcoin and Ethereum, support between 7-15 transactions per second, which is minimal compared to the IoT environment where thousands of devices work out streams of data. Consensus mechanisms, and especially proof-of-work, have a computationally expensive nature, which forms bottlenecks that get bigger as the network grows. Moreover, the system of each node storing entire blockchain copies causes storage constraints on the IoT equipment with finite resources [14].

A number of new strategies are used to solve the limitations of scalability in blockchain-IoT systems. Lightweight consensus algorithms including proof-of-authority, proof-of-elapsed-time and

delegated proof-of-stake have much lower computational costs than proof-of-work without compromise in security. Such protocols either rely on trusted validators or hardware attestation to construct consensus with low power usage, which is appropriate to IoT devices with limited computational capabilities [15].

Scalability is made possible by off-chain processing and layer-2 solutions through the implementation of transactions that are not stored in the principal blockchain, but instead, periodically anchored by summaries to the primary ledger. State channels enable the devices to have various transactions in private, with final state recorded on-chain. The use of micropayments between IoT devices allows high-frequency payments without blockchain congestion due to the use of payment channels, and Lightning Network-style architectures. Sidechains introduce parallel blockchain networks, which process a certain type of transaction, periodically synchronizing with the main chain to ensure security and distribute computing resources [16].

Sharding helps to divide the blockchain network into smaller groups, which can process transactions parallel to each other, and significantly boost the total throughput. Every shard is in possession of part of the ledger and processes a subset of transactions, and cross shard communication protocols make the system consistent. The directed acyclic graph of structures such as the Tangle of IOTA provides a replacement of a linear blockchain structure, as it creates a networked transaction graph in which each new transaction serves to validate older ones, which also removes the need to mine a blockchain and allows scaling to a greater extent. Such alternative architectures do not provide as much security as they offer higher performance and can be used in particular IoT applications with varying trust models [17].

Intelligent Contracts and IoT Management

Smart contracts are self-executing programs that are deployed on blockchain networks and which are able to enforce predetermined rules and conditions automatically without the intervention of intermediaries. Smart contracts in the IoT can be used to organize autonomous devices, allocate resources automatically, and manage the system based on rules. Smart contracts may respond to certain conditions or events, detected by IoT sensors, by automatically executing functions, including actuator settings, triggering maintenance tasks or even transacting money. This automation lowers the costs of operation, completely removes the human error and allows complex multi-device coordination that would prove too challenging to achieve manually [18].

Smart contracts within the IoT settings need to be dealt with in a distinctive way, in terms of devices heterogeneity, resources, and real-time demands. Conventional smart contracts systems, such as Ethereum, cannot run on edge devices with small processing power. Lightweight smart contract systems are designed to run the code and state management operations with resource-constrained system environments, which means that they can be deployed to the IoT gateway and embedded systems. IoT applications can be simplified using domain-specific languages and simplified execution environments that eliminate overhead, but still provide the necessary functionality.

Aca. Intl. J. E. Sci. 2023;1(2) 11-20.**DOI**: https://doi.org/10.59675/E122

Smart contract code security vulnerabilities are grave threats because once a smart contract has been deployed it cannot be changed and the contract usually operates valuable assets or essential infrastructure. The all-too-common weaknesses are reentrancy attacks, integer overflow errors, access control weaknesses, and logic errors that can be used by attackers. Formal verification methods refer to mathematical proofs to confirm the correctness of the contract whereas automated security auditors identify typical vulnerability patterns. Examples of best practices in the development of smart contracts are rigorous testing, security audits, modularity, and mechanisms of upgrades that enable correction of severe vulnerabilities without full restart [19].

Blockchain Integration and Edge Computing

Instead of sending all the data to centralized clouds, edge computing architectures compute data locally close to the IoT devices and cut down on latency and bandwidth usage and enhance privacy. Harnessing blockchain and edge computing results in hybrid solutions that can use the security features of distributed registry with the performance features of local processing. Edge nodes are capable of keeping copies of blockchain, consensus mechanisms and running smart contracts and processing streams of IoT data at the edge. The architecture allows real-time decision-making of time-sensitive applications such as autonomous vehicles and industrial automation [20].

The allocation of blockchain functionality to edge infrastructure must take care of resource allocation and topology of the network. Hierarchical blockchain structures distribute devices with various roles according to their calculation abilities, with edge servers endowed with plenty resources serving as full nodes in the blockchain where limited-resource IoT devices act as lightweight clients. Fog computing offers cloud services at the network boundaries, offering a middle computing tier that consolidates data of a group of devices on the IoT prior to recording in blockchain. This is a tiered solution that maintains security, performance and resource efficiency on a heterogeneous network of devices.

The consensus mechanisms in edge based blockchain systems should consider the network dynamics such as the movement of devices, intermittent connectivity, and changing computational resources. Adaptive consensus protocols change validation requirements according to network conditions ensuring safety and the performance is optimized. Geographic partitioning allows the local consensus of transactions in a region, and the occasional global synchronization of the entire system makes it consistent. These optimizations can make blockchain-IoT systems run successfully in a wide range of different deployment settings ranging between stable data centers and dynamic edge networks [21].

Case Study and Industry Applications

The Smart City projects across the globe are embracing blockchain-IoT models of infrastructure control, energy supply and municipal services. The smart city platform in Barcelona incorporates the implementation of blockchain in secure data exchange between the transportation systems,

Aca. Intl. J. E. Sci. 2023;1(2) 11-20.**DOI**: https://doi.org/10.59675/E122

environmental sensors, and utility systems. The decentralized structure allows the transparent governance and ensures the privacy of citizens with the help of cryptographic methods. The application of energy trading enables households that have solar panels to sell their surplus energy to their neighbors via smart contracts executed through blockchain technology and therefore avoids intermediary costs and allows the creation of peer-to-peer energy markets [22].

The blockchain-IoT integration is used in healthcare monitoring systems to ensure the safety of patient data and coordinate medical devices. RPM devices constantly record vital signs, the integrity of which is maintained by blockchain, and audit trails should be immutable to avoid compliance with the regulation. Smart contracts can be used to make emergency response process automatically in case of critical conditions detected by sensors and to notify medical staff as soon as possible without ignoring privacy-saving access control. Pharma supply chains use blockchain-IoT tracking to curb fake drugs, sensors track temperatures, humidity, and location during the supply chain and documented provenance records are tamper-proof records [23].

Applications of industrial automation and Industry 4.0 use blockchain to have secure machine-to-machine communication and autonomous manufacturing coordination. IoT sensors installed on production equipment capture operation data on blockchain networks, which can be used to predict and ensure maintenance and quality with verifiable provenance. The supply chain applications can monitor raw materials and finished products using IoT devices with blockchain technology, which introduces end-to-end visibility that minimizes fraud and enhances efficiency. Smart contracts automatically pay and update inventory when shipments arrive at their destinations and this helps to reduce the administrative overhead and speed up business processes [24].

New Technologies and Future Trends

Cryptography quantum-resistant is currently a needed requirement since quantum computing development poses a threat to the existing blockchain security pillars. Post-quantum security is provided by lattice-based cryptography, hash-based signatures, and multivariate polynomials systems, which are long-lasting solutions to the IoT applications. To deploy quantum resistant algorithms in resource constrained IoT devices, cryptographic operations have to be optimized to have the least amount of computational overhead and still ensure a security guarantee. The studies are concentrated on lightweight post-quantum encryption schemes that are particularly oriented to the IoT settings [25].

The combination of artificial intelligence with blockchain-IoT makes it possible to have intelligent data analytics, anomaly detection and adaptive security. Models of machine learning that run on edge nodes process IoT streams of data and detect trends that reveal indications of security risks or inefficiencies in the operation. Federated learning enables distributed networks of IoTs to model-train together without having to store sensitive information on a central server, and blockchain enables the aggregation of model updates securely. The AI-based smart contracts are able to dynamically tune system parameters on the basis of learned dynamics, thus creating self-optimizing IoT networks that adapt to changing environments [26].

Interoperability standards make different blockchain systems and IoT standards interoperable, avoiding vendor lock in and making applications cross-platform. The cross-chain communication protocols enable the transfer of assets and data between the various blockchain networks. APIs and middleware layers Standardized APIs and middleware layers, given the complexity of blockchain, provide an interface through which IoT applications can connect to a variety of ledger technologies. The common standards of blockchain-IoT integration are being developed by industry consortia to encourage the ecosystem development and widespread adoption [27].

Zero-knowledge rollups and proofs of validity provide scalability benefits, which consist of bundling many transactions and providing cryptographic evidence to the base blockchain. These layer-2 solutions enable security guarantees and minimize by a significant amount the on-chain data requirements. Secure multi-party computation and trusted execution environments are privacy-preserving computation methods that can be used to execute confidential smart contracts on sensitive IoT data. The innovations are aimed at solving the outstanding issues regarding privacy, scalability, and performance that continue to curtail the deployment of blockchain-IoT in the challenging applications [28].

Conclusion

This paper on safe and scalable blockchain infrastructures on Internet of Things networks reveals how distributed ledger technology is changing the connected device ecosystems by solving the inherent security, faith, and scalability risks and threats of their traditional centralized structures. With a combination of cryptographic security, decentralized consensus protocols, and smart contract automation with IoT infrastructure, blockchain frameworks assist in transparent, tamper-proof, and autonomous coordination of devices in various areas of use. Combining blockchain-IoT integration with the ability to remove single points of failure and retain data integrity, as well as the ability to have verifiable audit trails, is an essential enabler to trusted pervasive computing environments [29].

The results, nevertheless, point out to the fact that effective large-scale implementation needs to be accompanied by solving significant problems of computational performance, energy usage, transaction rate, and system resources. Recent developments such as lightweight consensus, off-chain execution, sharding, incorporating edge computing, and directed acyclic graph designs are successful in resolving most of the scalability issues but preserve security guarantees. The contribution of standardization organizations, industry consortia, and regulation frameworks to the development of interoperability protocols and security standards cannot be overestimated to facilitate the large-scale use in the context of heterogeneous IoT ecosystems [30].

With the growing adoption of Internet of Things worldwide in smart cities, in healthcare, industrial automation, and critical infrastructure, secure and scalable blockchain solutions will gain more and more prominence in proving system reliability, trustworthiness, and resilience. The current study focused on resolving the technical issues that still lack resolution and the exploration of quantum-resistant cryptography, integration of artificial intelligence, and cross-chain interoperability will

spearhead the next generation of blockchain-powered IoT systems that self-manage performance, security, and adjust to the operational needs of pervasive computing.

Questions for Discussion

1. What are the ways in which IoT/blockchain integration can be used to improve security and privacy in smart city deployment and still ensure system performance?
2. How can the trade-offs among decentralization, scalability and energy efficiency of blockchain systems in resource limited IoT devices be measured?
3. What are some of the ways to use emerging technologies such as quantum-resistant cryptography, artificial intelligence, and cross-chain protocols to make blockchain-IoT ecosystems more reliable and interoperable with each other?

References

1. Christidis K, Devetsikiotis M. Blockchain and smart contracts for the Internet of Things. **IEEE Access**. 2016; 4:2292–2303.
2. Ali MS, Vecchio M, Pincheira M, Dolui K, Antonelli F, Rehmani MH. Applications of blockchain in the Internet of Things: a comprehensive survey. **IEEE Commun Surv Tutor**. 2019;21(2):1676–1717.
3. Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: the case study of a smart home. In: **Proc IEEE Int Conf Pervasive Comput Commun Workshops**; 2017. p. 618–623.
4. Fernández-Caramés TM, Fraga-Lamas P. A review on the use of blockchain for the Internet of Things. **IEEE Access**. 2018;6:32979–33001.
5. Novo O. Blockchain meets IoT: an architecture for scalable access management in IoT. **IEEE Internet Things J**. 2018;5(2):1184–1195.
6. Khan MA, Salah K. IoT security: review, blockchain solutions, and open challenges. **Future Gener Comput Syst**. 2018;82:395–411.
7. Pahlajani S, Kshirsagar A, Pachghare V. Survey on private blockchain consensus algorithms. In: **Proc 1st Int Conf Innov Inf Commun Technol**; 2019. p. 1–6.
8. Bao Z, Shi W, He D, Chood KKR. IoTChain: a three-tier blockchain-based IoT security architecture. **arXiv**. 2018;arXiv:1806.02008.
9. Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT: challenges and opportunities. **Future Gener Comput Syst**. 2018;88:173–190.
10. Xiong Z, Zhang Y, Niyato D, Wang P, Han Z. When mobile blockchain meets edge computing. **IEEE Commun Mag**. 2018;56(8):33–39.
11. Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: a survey. **Int J Web Grid Serv**. 2018;14(4):352–375.
12. Kshetri N. Can blockchain strengthen the Internet of Things? **IT Prof**. 2017;19(4):68–72.
13. Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: a new blockchain-based access control framework for the Internet of Things. **Secur Commun Netw**. 2016;9(18):5943–5964.
14. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. **Telematics Inform**. 2019;36:55–81.
15. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling blockchain: a data processing view of blockchain systems. **IEEE Trans Knowl Data Eng**. 2018;30(7):1366–1385.
16. Decker C, Wattenhofer R. A fast and scalable payment network with Bitcoin duplex micropayment channels. In: **Proc Int Symp Self-Stabilizing Systems**; 2015. p. 3–18.
17. Popov S. **The Tangle** [Internet]. White paper. 2018. Available from: https://www.iota.org

18. Huh S, Cho S, Kim S. Managing IoT devices using blockchain platform. In: **Proc 19th Int Conf Adv Commun Technol**; 2017. p. 464–467.
19. Mohamed TS, Aydin S, Alkhayyat A, Malik RQ. Kalman and Cauchy clustering for anomaly detection-based authentication of IoMTs using extreme learning machine. **IET Commun**. 2025;19(1):e12467.
20. Samaniego M, Deters R. Blockchain as a service for IoT. In: **Proc IEEE Int Conf Internet Things IEEE Green Comput Commun**; 2016. p. 433–436.
21. Pan J, Wang J, Hester A, Alqerm I, Liu Y, Zhao Y. EdgeChain: an edge-IoT framework and prototype based on blockchain and smart contracts. **IEEE Internet Things J**. 2019;6(3):4719–4732.
22. Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. In: **Proc 18th IEEE Int Conf High Perform Comput Commun**; 2016. p. 1392–1393.
23. Uddin MA, Stranieri A, Gondal I, Balasubramanian V. A survey on the adoption of blockchain in IoT: challenges and solutions. **Blockchain Res Appl**. 2021;2(2):100006.
24. Leng K, Bi Y, Jing L, Fu HC, Van Nieuwenhuyse I. Research on agricultural supply chain system with double chain architecture based on blockchain technology. **Future Gener Comput Syst**. 2018;86:641–649.
25. Fernández-Caramés TM, Froiz-Míguez I, Blanco-Novoa O, Fraga-Lamas P. Enabling the Internet of Mobile Crowdsourcing Health Things: a mobile fog computing, blockchain and IoT-based continuous glucose monitoring system for diabetes mellitus research and care. **Sensors (Basel)**. 2019;19(15):3319.
26. Salah K, Rehman MH, Nizamuddin N, Al-Fuqaha A. Blockchain for AI: review and open research challenges. **IEEE Access**. 2019; 7:10127–10149.
27. Belchior R, Vasconcelos A, Guerreiro S, Correia M. A survey on blockchain interoperability: past, present, and future trends. **ACM Comput Surv**. 2021;54(8):1–41.
28. Buterin V. An incomplete guide to rollups [Internet]. 2021. Available from: https://vitalik.ca/general/2021/01/05/rollup.html
29. Weber I, Gramoli V, Ponomarev A, Tran AB, Rimba P, Xu X. On availability for blockchain-based systems. In: **Proc IEEE 36th Symp Reliable Distrib Syst**; 2017. p. 64–73.
30. Dorri A, Kanhere SS, Jurdak R. Towards an optimized blockchain for IoT. In: **Proc IEEE/ACM 2nd Int Conf Internet-of-Things Design Implement**; 2017. p. 173–178.