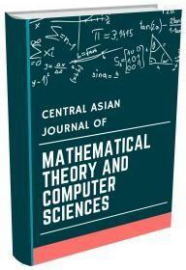

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 05 Issue: 03 | July 2024 ISSN: 2660-5309

Article

Secure Storage of Smart Contracts on Blockchain Platforms: A Systematic Review

Nsreen Ghni Khudur[1*]

1. Department of Programming, M.S.C of Software Engineering, Ferdowsi University
* Correspondence: nsreenghni@gmail.com

Abstract: The rapid evolution and adoption of blockchain technology have brought to the forefront the significance of smart contracts – self-executing contracts with terms directly encoded into the blockchain. Despite their utility, these smart contracts face numerous security challenges, particularly in the realm of secure storage. Addressing these challenges is crucial for maintaining data privacy, integrity, and robust access control mechanisms within blockchain platforms. This systematic review was conducted following the guidelines by Kitchenham and Charters, focusing on peer-reviewed journal articles and conference papers published between 2014 and 2024. The study selection process involved an extensive search of electronic databases such as IEEE Xplore, ACM Digital Library, Springer Link, and ScienceDirect. Researchers screened titles and abstracts, eliminating studies that did not specifically address the secure storage of smart contracts. Selected studies underwent a detailed evaluation based on predefined criteria, focusing on research objectives, methodologies, comprehensive topic coverage, and rigorous data collection and analysis techniques. Key information was then extracted, and a thematic analysis was performed to identify and categorize emerging themes for 220 papers from all total papers publishing 11,224 papers. The review revealed that public blockchains have garnered the most research attention due to their open and decentralized nature, followed by private and consortium blockchains. Critical themes identified include data privacy and confidentiality, integrity and immutability, access control and authorization, and performance and scalability considerations. Each theme underscores the multifaceted security challenges inherent in the storage of smart contracts. The findings highlight the need for continuous innovation and improvement in securing smart contracts, essential for the advancement of blockchain technology. The lack of standardized guidelines and adaptive security measures poses significant challenges. Future research should focus on developing streamlined, less complex solutions that integrate robust security mechanisms while maintaining functionality and efficiency. This systematic review provides valuable insights, guiding future research and development efforts aimed at enhancing the safety and reliability of blockchain applications.

Keywords: Smart Contracts, Blockchain Security, Data Privacy, Access Control, and Secure Storage

Citation: Khudur, N. G. Secure Storage of Smart Contracts on Blockchain Platforms: A Systematic Review. Central Asian Journal of Mathematical Theory and Computer Sciences 2024, 5(3), 169-192.

Received: 24th Jun 2024
Revised: 1st Jul 2024
Accepted: 8th Jul 2024
Published: 15th Jul 2024

1. Introduction

Smart contracts are self-executing scripts that are stored and run on blockchain platforms, enabling the transparent and automated execution of predefined processes [1,3]. These decentralized scripts allow for the programmability of digital assets, opening new application possibilities that were previously inaccessible [1,3]. Smart contracts have gained significant traction, with billions of dollars in value currently controlled by these blockchain-based applications [5,6]. Blockchain technology, the underlying infrastructure

for smart contracts, is a distributed ledger system that maintains a continuously growing list of records, called blocks, which are linked and secured using cryptography [6]. This decentralized architecture provides transparency, immutability, and security, making blockchain a suitable platform for the deployment of smart contracts [2,6]. The rise in popularity of blockchain has led to the development of various blockchain-based platforms, each with its own unique features and capabilities for hosting and executing smart contracts [1,6]. The secure storage of smart contracts on blockchain platforms is a critical concern, as vulnerabilities or threats in the storage mechanisms can compromise the integrity and reliability of these self-executing scripts [4,6].

Researchers and practitioners have identified various security challenges, including code-level vulnerabilities, storage-related issues, and potential attacks on the underlying blockchain infrastructure [4,6,3]. Addressing these security considerations is essential for the widespread adoption and trust in smart contract-based applications [4,6]. The secure storage of smart contracts on blockchain platforms is of paramount importance due to the critical role these self-executing scripts play in various applications [3,6]. Smart contracts are responsible for managing and automating the execution of complex business logic, often involving the transfer of valuable digital assets [1,6]. Any vulnerabilities or threats in the storage mechanisms of these contracts can lead to severe consequences, such as the loss or misappropriation of funds, breaches of data privacy, and the disruption of essential services [4,6].

Blockchain platforms, which serve as the infrastructure for smart contracts, are designed to provide a high degree of security, transparency, and immutability [2,6]. However, the secure storage of smart contracts on these platforms is not a trivial task, as it requires addressing various security challenges, including code-level vulnerabilities, storage-related issues, and potential attacks on the underlying blockchain infrastructure [3,4,6]. Failure to address these security concerns can undermine the trust and adoption of smart contract-based applications, limiting their potential to transform various industries [4,6]. Ensuring the secure storage of smart contracts is crucial for maintaining the integrity, reliability, and trustworthiness of blockchain-based systems [2,6]. This includes implementing robust access control mechanisms, secure data storage and retrieval processes, and comprehensive security monitoring and incident response capabilities [4,6]. Addressing these security considerations is essential for the widespread adoption and successful deployment of smart contract-based applications across diverse domains [4,6].

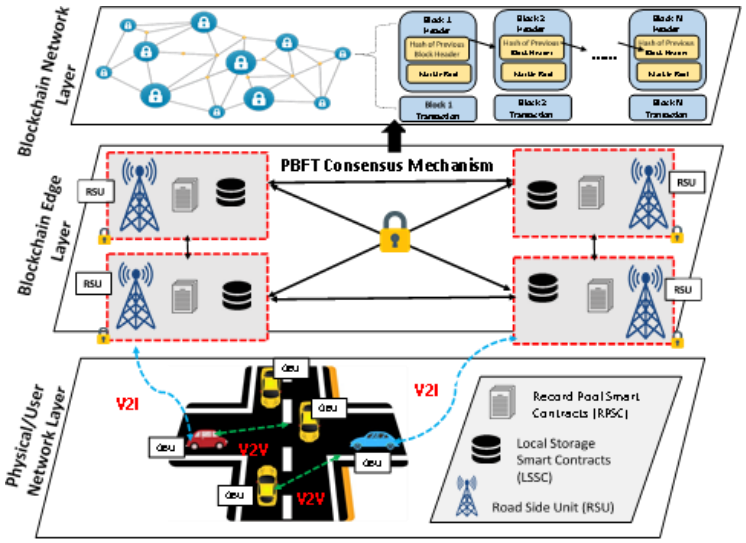

Figure 1. Overview of design architecture.

The blockchain network is typically represented as a decentralized peer-to-peer system, where nodes are interconnected to maintain consensus across the network about the state of the distributed ledger [7]. This network structure is crucial for ensuring the integrity and reliability of the blockchain-based system. The sequence of blocks (Block 1, Block 2, Block N) shown in the figure (1) represents the blockchain, where each block contains a set of transactions. The Practical Byzantine Fault Tolerance (PBFT) consensus mechanism ensures that all honest nodes in the network agree on the same sequence of blocks, even in the presence of faulty or malicious nodes [7]. This consensus mechanism is essential for maintaining the consistency and security of the blockchain. Roadside Units (RSUs) are nodes with local storage capabilities that play a critical role in local data aggregation and processing within the blockchain network. Additionally, the network utilizes specialized smart contracts, such as Local Storage Smart Contracts (LSSC) and Record Pool Smart Contracts (RPSC), to handle specific tasks, including local data storage, operations, and the secure management of a pool of records, likely transactions or data exchanges. These components contribute to the overall security and efficiency of the blockchain-based system.

The primary research question guiding this systematic review is: What are the key security considerations and challenges associated with the storage of smart contracts, including vulnerabilities, threats, and mitigation strategies? The objective of this study is to comprehensively examine the existing literature on the secure storage of smart contracts on blockchain platforms, with a focus on identifying and analyzing the critical security issues, potential threats, and proposed mitigation approaches. By synthesizing the current state of research in this domain, the study aims to provide a thorough understanding of the security landscape surrounding smart contract storage, inform the development of more secure blockchain-based applications, and highlight areas for future research and improvement.

2. Materials and Methods

The research methodology for this systematic review on the secure storage of smart contracts on blockchain platforms was designed following the guidelines provided by Kitchenham and Charters [8].

Literature search strategy

The literature search was conducted using various electronic databases, including IEEE Xplore, ACM Digital Library, Springer Link, and ScienceDirect. The relevant data was extracted from the selected articles, including the research objectives, methodologies, key findings, and proposed solutions for secure smart contract storage. The data was organized and tabulated to facilitate the analysis and synthesis of the findings. The quality of the included studies was assessed using a standardized checklist, such as the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, focusing on the study design, data collection, analysis, and reporting of the results. The extracted data was then synthesized and analyzed to identify common themes, patterns, and trends in the secure storage of smart contracts on blockchain platforms. The analysis included a comparison of the different approaches, techniques, and solutions proposed in the literature. Finally, the findings of the systematic review were reported in a structured format, following the guidelines for systematic reviews. The report includes a summary of the research objectives, methodology, key findings, and implications for research and practice. The systematic review will be disseminated through publication in a peer-reviewed journal or conference proceedings.

Databases and search terms used

The search terms used included "blockchain", "smart contracts", "secure storage", "systematic review", and their combinations. The search was limited to peer-reviewed journal articles and conference papers published between 2014 and 2024 to ensure the inclusion of the most recent and relevant research in the field.

Inclusion and exclusion criteria

The retrieved articles were then screened based on predefined inclusion and exclusion criteria. The inclusion criteria focused on articles that specifically addressed the secure storage of smart contracts on blockchain platforms, while the exclusion criteria eliminated articles that did not focus on this topic, were not written in English, or were duplicate publications.

Study selection process

The initial step in the study selection process involved a comprehensive search for relevant literature on the secure storage of smart contracts on blockchain platforms. The researchers scanned the titles and abstracts of potentially relevant studies to identify those that focused on the secure storage of smart contracts, including aspects such as data privacy, integrity, and access control. Studies that did not directly address the secure storage of smart contracts or were not related to blockchain platforms were excluded from further consideration.

After the initial screening, the researchers obtained the full-text versions of the selected studies and conducted a more detailed review. During this stage, the researchers carefully evaluated each study based on a set of predefined criteria to ensure the inclusion of high-quality and relevant information. The criteria included:

1. Clear definition of research objectives or questions related to the secure storage of smart contracts.
2. Appropriate research methodologies, such as systematic reviews, empirical studies, or theoretical analyses.
3. Comprehensive coverage of the topic, including discussions of challenges, solutions, and future research directions.
4. Rigorous data collection and analysis techniques.
5. Alignment with the overall scope of the systematic review on the secure storage of smart contracts on blockchain platforms.

The researchers then selected the studies that met these inclusion criteria, ensuring that the final set of studies provided the most relevant and valuable information for the systematic review.

Data extraction and synthesis

After the final selection of studies, the researchers conducted a thorough data extraction process to gather the key information relevant to the secure storage of smart contracts on blockchain platforms. This included extracting details such as the study objectives, research methodologies, key findings, and proposed solutions or approaches. The researchers paid particular attention to the specific challenges and requirements identified in the studies, as well as the technical approaches and mechanisms discussed for ensuring the secure storage of smart contracts. This data extraction process allowed the researchers to build a comprehensive understanding of the current state of research in this domain and the various aspects that needed to be addressed.

With the key information extracted from the selected studies, the researchers conducted a thematic analysis to identify the main themes and categories emerging from

the literature. This involved carefully reviewing the findings, identifying common patterns, and grouping related concepts and approaches. The researchers organized the findings into several broad categories, such as data privacy and confidentiality, integrity and immutability, access control and authorization, and performance and scalability considerations. Within each category, the researchers further analyzed the specific techniques, mechanisms, and trade-offs discussed in the studies, highlighting the strengths, limitations, and potential areas for future research. This thematic analysis and categorization of the findings enabled the researchers to synthesize the existing knowledge, identify the key challenges and solutions, and provide a structured and comprehensive overview of the secure storage of smart contracts on blockchain platforms.

Overview of Smart Contract Storage on Blockchain Platforms

Smart contracts are self-executing digital agreements that are stored and executed on blockchain platforms. The storage and execution of smart contracts on blockchain platforms have several unique characteristics [9]. One of the key features of smart contract storage on blockchains is the immutability of the contract code. Once a smart contract is deployed on the blockchain, its code cannot be modified, ensuring the integrity and transparency of the agreement [10]. This immutability is achieved through the distributed consensus mechanism of the blockchain, where all nodes in the network validate and store the contract code. Another important aspect of smart contract storage is the decentralized nature of the blockchain. Smart contracts are not stored on a central server but are distributed across the entire network of nodes. This decentralization eliminates the need for a trusted third party to manage the contracts, reducing the risk of tampering or unauthorized access [11]. The storage of smart contracts on blockchain platforms also enables automatic execution of the contract terms when predefined conditions are met. This automation reduces the need for manual intervention and the associated costs, improving the efficiency of contract-based transactions [12]. Furthermore, the transparency of the blockchain allows all participants to view the smart contract code and the associated transactions, enhancing trust and accountability in the system [13]. This transparency is particularly beneficial in industries where transparency and traceability are crucial, such as supply chain management and financial services. In summary, the storage of smart contracts on blockchain platforms offers several advantages, including immutability, decentralization, automation, and transparency, which make them a valuable tool for various applications [14].

3. Research database

The search results across multiple research databases reveal significant academic interest in blockchain technology, particularly focusing on keywords such as "Blockchain," "Smart Contracts," and "Distributed Ledger Technology." IEEE Xplore leads with the highest number of papers on "Blockchain" (3,254) and "Smart Contracts" (841), reflecting its strong engineering and technology research focus. The ACM Digital Library also shows considerable research activity, with 2,158 papers on "Blockchain" and 689 on "Smart Contracts," indicating robust interest in both theoretical and practical aspects of these technologies among computer science researchers. ScienceDirect, although slightly lower in volume, still presents a substantial contribution with 1,923 papers on "Blockchain" and 543 on "Smart Contracts," underscoring its relevance in scientific and applied research contexts. Overall, these results highlight the widespread and multidisciplinary research efforts being made to explore, develop, and secure blockchain platforms and their components.

Table 1. Paper Search Results

Research Database	Search Keywords	Number of Papers
ACM Digital Library	Blockchain	2,158
	Smart Contracts	689
	Distributed Ledger Technology	496
IEEE Xplore	Blockchain	3,254
	Smart Contracts	841
	Distributed Ledger Technology	712
ScienceDirect	Blockchain	1,923
	Smart Contracts	543
	Distributed Ledger Technology	608
Total number of papers		11,224
Total number of papers considered for the study		220

Distribution Based on contract platforms

The distribution of blockchain research papers by platform demonstrates pronounced trends in the field, with Ethereum significantly leading at 164 papers. This considerable focus on Ethereum underlines its dominant role in facilitating programmable smart contracts and decentralized applications, making it the centerpiece of blockchain innovation and implementation. The large volume of research highlights Ethereum's extensive adoption across diverse sectors such as finance, supply chain management, healthcare, and beyond, driven by its robust development framework and continuous enhancements, including the anticipated shift to Ethereum 2.0 for improved scalability and security. Hyperledger Fabric follows with 57 papers, indicating its prominent position in enterprise applications where permissioned blockchain solutions are critical for operational efficiency, data privacy, and security. This platform's modularity makes it attractive for enterprise use cases like supply chain optimization and healthcare data management, drawing substantial academic and industry research interest.

Table 2. Blockchain papers are organized based on their platforms.

Platform	Number of Papers	References
Ethereum	164	[15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [68]. [69], [72], [75]. [76], [77], [79], [80]. [83], [84]. [87]. [88], [89]. [91]. [95]. [99]. [100]. [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111], [112], [113]. [114], [115], [116]. [117], [118], [119], [120]. [121], [122]. [123]. [124], [125]. [126]. [127]. [128]. [129]. [130], [131], [132], [133], [134], [135], [136], [137]. [138], [139]. [140]. [141], [142]. [143]. [144]. [145]. [146]. [147], [148], [149], [150], [151], [152], [153], [154]. [155], [156]. [157]. [158]. [159]. [160]. [161], [162], [163], [164].
Hyperledger Fabric	57	[25], [34], [35], [36]. [68]. [69]. [74]. [75]. [76]. [77]. [79]. [80]. [88]. [91]. [104]. [110]. [135]. [136]. [139]. [156]. [158]. [159]. [165], [166], [167], [168]. [169]. [170]. [171]. [172]. [173]. [174]. [175]. [176]. [177]. [178]. [179]. [180]. [181]. [182]. [183]. [184]. [185]. [186]. [187]. [188]. [189]. [190]. [191]. [192]. [193]. [194]. [195]. [196]. [197]. [198].
Bitcoin	39	[27], [28], [29], [30], [31], [32], [33], [68], [69]. [70]. [71]. [72]. [73]. [74]. [75]. [76]. [77]. [78]. [79]. [80]. [81] [82], [83]. [84]. [85]. [86]. [87]. [88]. [89]. [90]. [91] [92], [93]. [94]. [95]. [96]. [97] [98], [99]

R3 Corda	19	[25], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46]. [69]. [75]. [77]. [88]. [91]. [`35]. [136]. [153].
NXT	9	[25], [42], [43], [44], [45], [46], [47], [48], [49].
IOTA	7	[65], [66], [67], [69], [209], [210], [211],
FISCO BCOS	6	[215]. [216]. [217]. [218]. [219]. [220].
Counterparty	7	[19], [24], [50], [51], [52], [53], [54].
MultiChain	5	[69], [78], [135], [199], [200],
RChain	5	[19], [56], [57], [58], [59].
EOS/ EOS.IO	4	[118]. [214]. [204]. [139].
Stellar	4	[68], [135]. [203], [204],
Cosmos	4	[78], [88], [131], [201],
RootStock (RSK)	4	[19], [55], [56], [24].
Exergy	4	[19], [56], [57], [58].
BigChainDB	4	[62]. [63], [64], [69],
Quorum	3	[124], [77], [69],
IBM Blockchain	3	[69], [88]. [202].
Ripple	3	[70], [153], [205],
Qtum	2	[118], [207],
NEO	2	[118], [139],
Cardano	2	[204], [213],
Exonum	2	[206], [77],
ARK	2	[208], [118],
Ethermint	2	[135], [136],
Nebulas	2	[212], [154],
Polkadot	2	[213], [88],
Tezos	1	[59].
Kadena	1	[60].
EOS	1	[61].

Bitcoin, with 39 papers, continues to be a fundamental subject of study, reflecting its foundational impact on the blockchain landscape. Research on Bitcoin often delves into its security mechanisms, economic implications, and proof-of-work consensus algorithm that underpins many subsequent blockchain innovations. Other platforms, including R3 Corda (19 papers), NXT (9 papers), IOTA (7 papers), and several with fewer publications like Cosmos, RootStock, and Stellar (each with 4 papers), capture attention for their specialized applications. R3 Corda’s emphasis on financial services, IOTA’s tailored design for IoT applications, and Stellar's focus on cross-border payments highlight the diverse potential and ongoing innovation within the blockchain space. Despite fewer papers, these platforms signify important niches and evolving technologies within the

broader blockchain research community, showcasing a rich landscape of both well-established and emerging blockchain solutions.

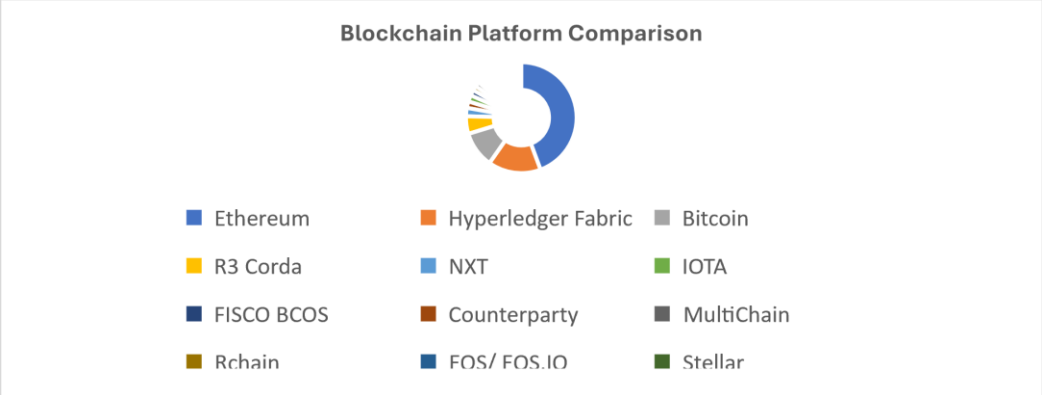

Figure 2. Platform distribution

Distribution Based on Blockchain Types

The distribution of blockchain research papers based on blockchain types reveals distinct areas of focus within the academic community. Public blockchains, which are open and decentralized platforms accessible to anyone, lead the research interest with 110 papers, indicating a strong emphasis on exploring their broad applications, security measures, and scalability challenges. Private blockchains, characterized by restricted access and typically used within organizations, follow with 70 papers, reflecting significant interest in their use for secure, internal operations and efficiency. Consortium blockchains, which are controlled by a group rather than a single entity and used for collaborative efforts between multiple organizations, have 40 papers, showing a more specialized but important focus area that balances decentralization with controlled access for business partnerships and industry collaborations. This distribution highlights the diverse applications and ongoing innovations in different types of blockchain systems.

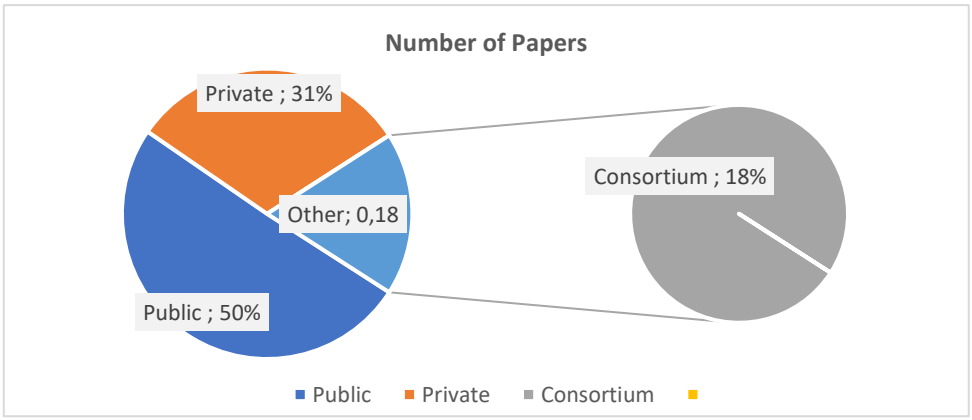

Figure 3. Blockchain Types distribution

Storage techniques for smart contracts

The distribution of research papers on storage techniques for smart contracts highlights the varying approaches to managing data within blockchain ecosystems. On-chain storage, which involves storing data directly on the blockchain, accounts for 48 papers. This method ensures immutability and transparency but often suffers from high costs and scalability issues due to the limited and expensive nature of blockchain storage space. As a result, the relatively lower volume of research on on-chain storage reflects these challenges, prompting researchers and developers to explore more efficient alternatives.

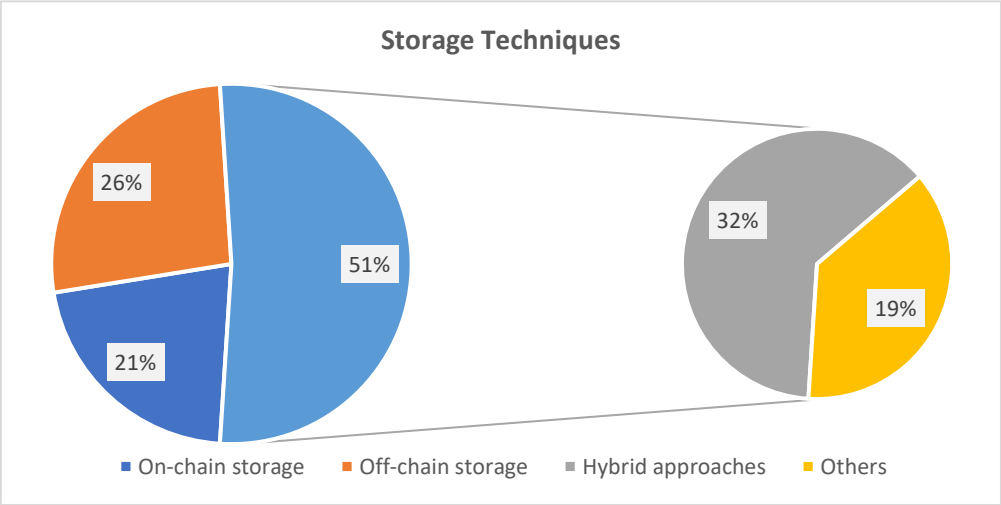

Figure 4. Storage techniques for smart contracts distribution

Off-chain storage emerges as a more extensively studied area with 58 papers, indicating a growing interest in methods that store data outside the blockchain while maintaining a reference or hash of the data on-chain. Off-chain solutions aim to address the limitations of on-chain storage by reducing costs and improving scalability, making them suitable for applications requiring large data storage without compromising security and integrity. Hybrid approaches, combining both on-chain and off-chain storage, lead the research with 72 papers. These approaches seek to balance the benefits of both methods, leveraging the security and immutability of on-chain storage while utilizing off-chain storage for data-intensive operations. The significant focus on hybrid approaches underscores the ongoing effort to optimize storage strategies, ensuring efficiency, cost-effectiveness, and security. Additionally, there are 42 papers categorized under "Others," which might explore novel or less conventional storage techniques, reflecting the diversity and innovation in research aimed at enhancing smart contract functionality.

Vulnerabilities in smart contract storage

The analysis of vulnerabilities in smart contracts reveals that unauthorized access is the most frequently addressed issue, appearing in 103 papers. This high frequency underscores the critical nature of securing access controls within smart contracts to prevent malicious exploitation. Unauthorized access can lead to severe consequences such as unauthorized transactions, data breaches, and manipulation of contract logic. Effective countermeasures include implementing robust authentication protocols, regular security audits, and employing multi-factor authentication approaches to ensure that only authorized entities can interact with sensitive contract functions.

Reentrancy attacks and storage overflow or underflow vulnerabilities also emerge as prominent concerns, discussed in 97 and 87 papers, respectively. Reentrancy attacks exploit the ability of external contacts to recursively call functions within the initial contract, often leading to unauthorized multiple operations such as repeated fund withdrawals. On the other hand, storage overflow or underflow vulnerabilities occur when arithmetic operations exceed the allocated storage limits, causing unexpected behavior and potential loss of funds. To combat these issues, developers employ techniques such as reentrancy guards, using the latest Solidity versions with automatic checks, and leveraging mathematical libraries that handle overflow or underflow scenarios gracefully.

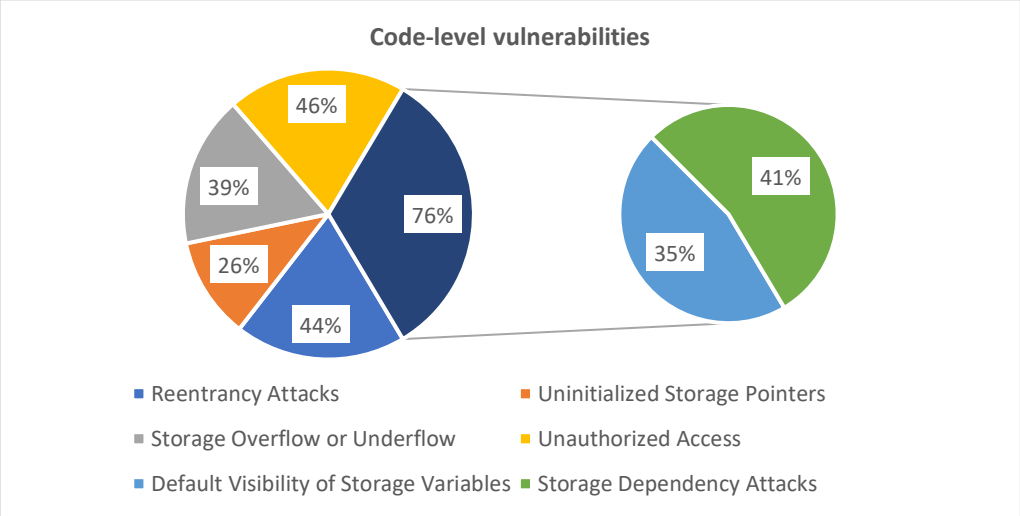

Figure 5. Code-level vulnerabilities distribution

Other significant vulnerabilities include storage dependency attacks and default visibility of storage variables, with 92 and 78 papers focusing on them, respectively. Storage dependency attacks exploit the dependencies in the storage layout of smart contracts, while issues with default visibility stem from improperly configured visibility states, making sensitive functions or variables accessible unintentionally. Addressing these vulnerabilities involves strategic planning and adherence to best coding practices, such as explicitly defining visibility for all functions and variables and thoroughly assessing storage layouts. Uninitialized storage pointers are also discussed in 58 papers, reflecting the importance of ensuring all storage variables are properly initialized to avoid unpredictable behaviors. Collectively, these papers provide a comprehensive understanding of prevalent vulnerabilities and the necessary steps to enhance the security and robustness of smart contracts.

4. Results

Emerging Trends and Future Directions

a. Advancements in secure storage solutions for smart contracts

Recent advancements in secure storage solutions for smart contracts have focused heavily on leveraging blockchain technology to enhance data integrity, confidentiality, and robustness against unauthorized access. In their implementation of a private blockchain using the Multichain open-source platform, Ismailisufi et al. [200] demonstrated how a tailored blockchain setup can provide a secure, decentralized ledger that mitigates many traditional storage vulnerabilities. The use of private blockchain networks enables better control over access permissions and data management, ensuring that only authorized entities can interact with the smart contracts and stored data. Additionally, [201] explored the underpinnings of building custom blockchain

solutions, emphasizing the importance of adaptability and flexibility in designing secure storage frameworks that can cater to specific application needs.

Another notable advancement includes the 'Blockchain as a Service' (BaaS) models introduced by [202], which offer scalable and secure storage solutions tailored for IoT environments. Their work highlights how BaaS platforms simplify the deployment of blockchain networks, providing pre-configured infrastructure that enhances security through well-defined protocols and configurations. This approach not only addresses common storage vulnerabilities in smart contracts but also delivers enhanced data integrity and transparency, crucial for applications requiring stringent security standards. Furthermore, [203] demonstrated the practical application of blockchain-based storage in universal loyalty platforms, showing how these advancements can be directly applied to real-world scenarios to secure user data and transaction histories effectively. These advancements collectively underline the potential of blockchain technology in fortifying smart contract storage against evolving security threats.

b. Integration with other technologies

Recent advancements in the integration of blockchain technology with other security-enhancing technologies, such as Trusted Execution Environments (TEEs) and Multi-Party Computation (MPC), have significantly improved the security and privacy of smart contracts. [1] evaluated the suitability of adopting blockchain for various applications and emphasized the importance of integrating TEEs to ensure that even if the underlying hardware is compromised, sensitive data and computation can remain secure. TEEs provide a secure enclave where code can be executed isolated from the main operating system and other processes, thereby protecting the execution of smart contracts from being tampered with or observed by malicious actors. This integration enhances the robustness and integrity of blockchain applications, paving the way for more secure decentralized applications in sectors requiring high levels of confidentiality and trust.

Furthermore, [2] explored the challenges and opportunities of integrating MPC with blockchain technology for business process management. MPC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private, which is highly relevant for smart contracts that handle sensitive information. For instance, [4] proposed using MPC to manage untrusted business process monitoring and execution through blockchain, ensuring that data privacy is maintained even in decentralized environments. This approach allows for complex calculations to be performed securely and privately, without any party gaining access to the data of others. By incorporating these computational techniques, blockchain-based systems can adopt more sophisticated and secure architectures that meet the demands for higher privacy and compliance in various industries, including finance, healthcare, and supply chain management. These integrations not only fortify the security landscape of smart contracts but also open new avenues for their application and scalability in real-world scenarios.

5. Discussion

The systematic review on the secure storage of smart contracts on blockchain platforms offers a comprehensive analysis of the literature to identify critical security issues, potential threats, and mitigation strategies. The primary goal is to inform the development of more secure blockchain applications and highlight future research areas. Smart contracts, as self-executing contracts with the terms of the agreement directly

written into code, are subject to various security challenges, making a thorough examination of their secure storage vital. To achieve this, the researchers implemented a meticulous study selection process. Initially, a comprehensive search of relevant literature was conducted, focusing on titles and abstracts related to secure storage, data privacy, integrity, and access control within blockchain platforms. Studies that did not specifically address these aspects were excluded.

The selected studies were then thoroughly reviewed based on predefined criteria, including clear research objectives, appropriate methodologies, comprehensive coverage of the topic, and rigorous data collection and analysis techniques [85, 86]. Following the selection process, extensive data extraction was carried out. The researchers gathered key information, emphasizing the challenges, requirements, and technical approaches for ensuring the secure storage of smart contracts. This process included examining study objectives, research methodologies, key findings, and proposed solutions. The extracted information was then synthesized, allowing the researchers to build a detailed understanding of the current research landscape and identify various critical aspects that need addressing [87, 88, 89].

Subsequently, a thematic analysis was conducted to identify common patterns and categorize the findings into several broad themes. These include data privacy and confidentiality, integrity and immutability, access control and authorization, and performance and scalability considerations. Each category represents a crucial aspect of the secure storage of smart contracts, highlighting the multifaceted nature of the security challenges present in blockchain platforms [90, 91]. The literature search strategy was robust and comprehensive, utilizing electronic databases such as IEEE Xplore, ACM Digital Library, Springer Link, and ScienceDirect. The search terms included "blockchain", "smart contracts", "secure storage", and "systematic review". The researchers focused on peer-reviewed journal articles and conference papers published between 2014 and 2024 to ensure contemporary relevance. A standardized checklist, such as the PRISMA guidelines, was used to assess the quality of the included studies, focusing on study design, data collection, analysis, and reporting [8]. The review's findings reveal that public blockchains receive the most research attention, followed by private and consortium blockchains. Public blockchains are open to all and decentralized, which makes them a significant focus due to their broad applications and security challenges. Private blockchains, with restricted access, are explored for their use in secure, internal operations. Consortium blockchains, managed by a group of entities, are noted for their role in collaborative business efforts, highlighting a balance between decentralization and controlled access [91, 92, 93]. In summary, the systematic review underscores the importance of secure storage for smart contracts and provides a structured understanding of the associated security landscape. The synthesis and analysis of existing research allows for the identification of key themes and challenges, setting a foundation for future research and development in secure blockchain applications. The study emphasizes the need for continuous innovation and improvement in securing smart contracts, given their critical role in blockchain ecosystems.

6. Conclusion

The research methodology followed a systematic review approach based on guidelines by Kitchenham and Charters. The study selection process was rigorous, involving a thorough screening and detailed evaluation of articles based on predefined criteria. Data extraction focused on gathering key information related to study objectives, methodologies, findings, and proposed solutions. Thematic analysis was conducted to identify and categorize common themes and patterns. By synthesizing the existing research, this study has provided valuable insights into the secure storage of smart contracts on blockchain platforms. It underscores the multifaceted nature of security challenges and the critical aspects that must be addressed to enhance the safety and

reliability of blockchain applications. The findings are expected to guide future research and drive improvement in securing smart contracts, ultimately contributing to the advancement of blockchain technology in various sectors. Integrating robust security mechanisms while maintaining the functionality and efficiency of smart contracts remains a challenge. Future research needs to focus on developing more streamlined and less complex solutions. As blockchain technology evolves, so do the potential security threats. Continuous monitoring and adaptation of security measures are necessary to counter emerging threats effectively. The lack of standardized guidelines and regulations for securing smart contracts poses a significant challenge. Future work should aim at establishing clear regulatory frameworks and standards.

REFERENCES

1. Lo, S. K., et al. "Evaluating Suitability of Applying Blockchain." 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS), 2017, pp. 158-61. https://doi.org/10.1109/ICECCS.2017.26
2. Mendling, J., et al. "Blockchains for Business Process Management-Challenges and Opportunities." ACM Transactions on Management Information Systems (TMIS), vol. 9, no. 1, 2018, pp. 1-16. https://doi.org/10.1145/3183367
3. Wöhrer, M., and U. Zdun. "Design Patterns for Smart Contracts in the Ethereum Ecosystem." 2018 IEEE International Conference on Software Architecture Companion (ICSA-C), 2018, pp. 68-75. https://doi.org/10.1109/ICSA-C.2018.00023
4. Weber, I., et al. "Untrusted Business Process Monitoring and Execution Using Blockchain." International Conference on Business Process Management, 2016, pp. 329-47. https://doi.org/10.1007/978-3-319-45348-4_19
5. Xu, X., et al. "A Taxonomy of Blockchain-Based Systems for Architecture Design." 2017 IEEE International Conference on Software Architecture (ICSA), 2017, pp. 243-52. https://doi.org/10.1109/ICSA.2017.33
6. Xu, X., et al. Architecture for Blockchain Applications. Springer, 2019. https://doi.org/10.1007/978-3-030-03035-3
7. Firdaus, M., and K.-H. Rhee. "On Blockchain-Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks." Applied Sciences, vol. 11, no. 1, 2021, p. 414. https://doi.org/10.3390/app11010414
8. Kitchenham, Barbara, and Stuart M. Charters. "Guidelines for Performing Systematic Literature Reviews in Software Engineering." Jan. 2007, vol. 2, no. 3.
9. Zheng, Z., et al. "An Overview on Smart Contracts: Challenges, Advances and Platforms." Future Generation Computer Systems, vol. 105, 2020, pp. 475-91. https://doi.org/10.1016/j.future.2019.12.019
10. Bashir. Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained. Packt Publishing, 2018.
11. Norta, A. "Designing a Smart-Contract Application Layer for Transacting Decentralized Autonomous Organizations." International Conference on Advances in Computing and Data Sciences, 2016, pp. 595-604. https://doi.org/10.1007/978-981-10-3520-2_58
12. Mancini-Griffoli, T., et al. "Casting Light on Central Bank Digital Currency." International Monetary Fund, 2018.
13. Shapiro, E. "Point: Foundations of E-Democracy." Communications of the ACM, vol. 61, no. 8, 2018, pp. 18-28. https://doi.org/10.1145/3208095
14. Gupta, S. S. Blockchain. John Wiley & Sons, Inc., 2017.
15. Parjuangan, S., and Suhardi. "Systematic Literature Review of Blockchain Based Smart Contracts Platforms." 2020 International Conference on Information Technology Systems and Innovation (ICITSI), 2020, pp. 381-86. https://doi.org/10.1109/ICITSI50517.2020.9264908
16. Alharby, M., et al. "Blockchain-Based Smart Contracts: A Systematic Mapping Study of Academic Research (2018)." 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB), 2018, pp. 1-6. https://doi.org/10.1109/ICCBB.2018.8756390

17. Sharma, P., et al. "A Review of Smart Contract-Based Platforms Applications, and Challenges." Cluster Computing, vol. 26, 2023, pp. 395-421. https://doi.org/10.1007/s10586-021-03491-1
18. Dhaiouir, S., and S. Assar. "A Systematic Literature Review of Blockchain-Enabled Smart Contracts: Platforms, Languages, Consensus, Applications and Choice Criteria." Research Challenges in Information Science, edited by F. Dalpiaz et al., vol. 385, Springer, 2020, pp. 155-70. https://doi.org/10.1007/978-3-030-50316-1_15
19. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper, 2014. https://ethereum.org/en/whitepaper/
20. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, no. 151, 2014, pp. 1-32.
21. Dannen, C. Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. Apress, 2017. https://doi.org/10.1007/978-1-4842-2535-6
22. Antonopoulos, A. M., and G. Wood. Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media, 2018.
23. Zheng, Z., et al. "Blockchain Challenges and Opportunities: A Survey." International Journal of Web and Grid Services, vol. 14, no. 4, 2018, pp. 352–375. https://doi.org/10.1504/IJWGS.2018.095647
24. Bartoletti, M., and L. Pompianu. "An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns." International Conference on Financial Cryptography and Data Security, Springer, Cham, 2017, pp. 494–509. https://doi.org/10.1007/978-3-319-70278-0_31
25. Macrinici, D., et al. "Smart Contract Applications within Blockchain Technology: A Systematic Mapping Study." Telematics and Informatics, vol. 35, no. 8, 2018, pp. 2337–2354. https://doi.org/10.1016/j.tele.2018.10.004
26. Triantafyllidis, C., and P. Moreno-Sanchez. "Towards Secure and Scalable Ethereum Smart Contracts." arXiv Preprint arXiv:1901.08755, 2019. https://doi.org/10.48550/arXiv.1901.08755
27. Andrychowicz, M., et al. "Secure Multiparty Computations on Bitcoin." 2014 IEEE Symposium on Security and Privacy, IEEE, 2014, pp. 443–458.
28. Kosba, A., et al. "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts." 2016 IEEE Symposium on Security and Privacy (SP), IEEE, 2016, pp. 839–858.
29. Bartoletti, M., et al. "A Proof-of-Stake Protocol for Consensus on Bitcoin Subchains." International Conference on Financial Cryptography and Data Security, Springer, Cham, 2017, pp. 568–584.
30. Bigi, G., et al. "Validation of Decentralised Smart Contracts through Game Theory and Formal Methods." Programming Languages with Applications to Biology and Security, Springer, Cham, 2015, pp. 142–161.
31. Wattenhofer, R. The Science of the Blockchain. Inverted Forest Publishing, 2016.
32. Judmayer, A., et al. Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms. Synthesis Lectures on Information Security, Privacy, & Trust, vol. 9, no. 1, 2017, pp. 1-123. https://doi.org/10.2200/S00773ED1V01Y201701SPT017
33. Antonopoulos, A. M. Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media, Inc., 2017.
34. Aleksieva, Veneta, and Hristo Valchanov. "Smart Contracts Based on Hyperledger Fabric Blockchain for the Purpose of Health and Life Insurance Services." AIP Conference Proceedings, vol. 2570, no. 1, Aug. 2022, p. 020002. https://doi.org/10.1063/5.0099626
35. Dhillon, Vikram, et al. "Blockchain-Based Smart Contracts: Technical and Usage Aspects." Blockchain and Distributed Ledger Technology Use Cases, edited by Horst Treiblmaier and Thomas Clausen, Springer, 2020, pp. 121-144. https://doi.org/10.1007/978-3-030-44337-5_7
36. Valeksieva, Veneta, and Hristo Valchanov. "Implementation of Smart Contract, Based on Hyperledger Fabric Blockchain." 2020 International Conference Automatics and Informatics (ICAI), IEEE, 2020, pp. 1-5. https://doi.org/10.1109/ICAI50593.2020.9311346
37. Brown, Richard Gendal. "The Corda Blockchain Platform: A Solution for Every Business?" Network Security, vol. 2019, no. 1, Jan. 2019, pp. 9–12. https://doi.org/10.1016/S1353-4858(19)30005-0
38. Frantz, Christopher K., and Marten Hansson. "Smart Contracts and Blockchain in the Enterprise." IEEE Software, vol. 38, no. 2, Mar. 2021, pp. 50–58. https://doi.org/10.1109/MS.2020.3024723

39. Koens, Twan, and Erik Poll. "Assessing Interoperability Solutions for Distributed Ledgers Through Cross-Ledger Transactions." Pervasive and Mobile Computing, vol. 59, Aug. 2019, pp. 116–136. https://doi.org/10.1016/j.pmcj.2019.05.002
40. Xu, Xiwei, et al. "A Taxonomy of Blockchain-Based Systems for Architecture Design." 2017 IEEE International Conference on Software Architecture (ICSA), IEEE, 2017, pp. 243–252. https://doi.org/10.1109/ICSA.2017.33
41. Zetzsche, Dirk A., et al. "The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II." _Journal of Financial Transformation_, vol. 52, Nov. 2020, pp. 35-45.
42. Alonso, Pedro, et al. "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues." _Telematics and Informatics_, vol. 36, Mar. 2019, pp. 55–81. https://doi.org/10.1016/j.tele.2018.11.006
43. Casino, Fran, et al. "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues." _Telematics and Informatics_, vol. 36, Mar. 2019, pp. 55–81. https://doi.org/10.1016/j.tele.2018.11.006
44. Salimitari, Maryam, and Mohsen Chatterjee. "A Survey on Consensus Protocols in Blockchain for IoT Networks." _arXiv preprint arXiv:1809.05613_, 2018
45. Vacca, Anna, et al. "A Systematic Literature Review of Blockchain and Smart Contract Development: Techniques, Tools, and Open Challenges." _Journal of Systems and Software_, vol. 174, Apr. 2021, p. 110891. https://doi.org/10.1016/j.jss.2020.110891
46. Wang, Huaiqing, et al. "A Survey on Blockchain for Internet of Things: Principles, Applications and Challenges." _IEEE Internet of Things Journal_, vol. 8, no. 24, Dec. 2021, pp. 17546-17578. https://doi.org/10.1109/JIOT.2021.3089590
47. Udokwu, Chibuzor, et al. "The State of the Art for Blockchain-Enabled Smart-Contract Applications in the Organization." _2018 Ivannikov ISPRAS Open Conference (ISPRAS)_, IEEE, 2018, pp. 137-144.
48. Zhang, Sheng, and Jong-Hyouk Lee. "Analysis of the Main Consensus Protocols of Blockchain." _ICT Express_, vol. 6, no. 2, 2020, pp. 93-97.
49. Leka, Ermal, et al. "Systematic Literature Review of Blockchain Applications: Smart Contracts." _2019 International Conference on Information Technologies (InfoTech)_, IEEE, 2019, pp. 1-3.
50. Salah, Khaled, et al. "Systematic Literature Review of Blockchain based Smart Contracts Platforms." _2020 International Conference on Information Technology Systems and Innovation (ICITSI)_, IEEE, 2020, pp. 1-7.
51. Mohanta, Bhasmee Karan, et al. "A Review of Smart Contract-Based Platforms, Applications, and Open Challenges." _IEEE Access_, vol. 9, 2021, pp. 103827-103846.
52. Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al. "Blockchain Smart Contracts: Applications, Challenges, and Future Trends." _Peer-to-Peer Netw. Appl._ 14, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0
53. DiMatteo, L. A., Cannarsa, M., & Poncibò, C. (Eds.). _The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms_. Cambridge University Press, 2019. https://doi.org/10.1017/9781108592239
54. Narayanan, Arvind, and Andrew Miller. "Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts." _Communications of the ACM_, vol. 60, no. 5, May 2017, pp. 78-84.
55. Gervais, Arthur, et al. "On the Security and Performance of Proof of Work Blockchains." _Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security_, 2016, pp. 3-16.
56. Atzei, Nicola, et al. "A Survey of Attacks on Ethereum Smart Contracts." _Principles of Security and Trust_, edited by Matteo Maffei and Mark Ryan, Springer Berlin Heidelberg, 2017, pp. 164-186.
57. Bartoletti, Massimo, and Livio Pompianu. "An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns." _Lecture Notes in Computer Science_, vol. 10323, 2017, pp. 494-509.
58. Clack, C. D., Bakshi, V. A., & Braine, L. "Smart Contract Templates: Foundations, Design Landscape and Research Directions." _arXiv preprint arXiv:1608.00771_, 2017. DOI: https://doi.org/10.48550/arXiv.1608.00771
59. Goodman, L. M. "The Tezos Self-Amending Crypto-Ledger." 2018. Retrieved from https://tezos.com/whitepaper.pdf

60. Bartoletti, M., Benetollo, L., Bugliesi, M., Crafa, S., Sasso, G.D., Pettinau, R., Pinna, A., Piras, M., Rossi, S., Salis, S., Spanò, A., Tkachenko, V., Tonelli, R., & Zunino, R. "Smart Contract Languages: a Comparative Analysis." _ArXiv_, abs/2404.04129, 2024.
61. Dhillon, Vikram et al. "Recent Developments in Blockchain." (2017).
62. Bhattacharyya, Abhisha et al. "Towards Detecting Semantic Events on Blockchains." _BlockSW/CKG@ISWC_, 2019.
63. El-Hindi, Muhammad et al. "BlockchainDB." _Proceedings of the VLDB Endowment_, 2019, n. pag.
64. McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., ... & Granzotto, A. "BigchainDB: A Scalable Blockchain Database (DRAFT)." _ascribe GmbH_, Berlin, Germany, 2016.
65. Sealey, Nathan et al. "IOTA Tangle 2.0: Toward a Scalable, Decentralized, Smart, and Autonomous IoT Ecosystem." _2022 International Conference on Smart Applications, Communications and Networking (SmartNets)_, 2022, pp. 01-08.
66. Alshaikhli, Mays et al. "Evolution of Internet of Things From Blockchain to IOTA: A Survey." _IEEE Access_ 10, 2022, pp. 844-866.
67. Silvano, Wellington Fernandes and Roderval Marcelino. "Iota Tangle: A cryptocurrency to communicate Internet-of-Things data." _Future Gener. Comput. Syst._ 112, 2020, pp. 307-319.
68. Ahmed, M., Elahi, I., Abrar, M., Aslam, U., Khalid, I. and Habib, M.A. "Understanding Blockchain: Platforms, Applications and Implementation Challenges." _Proceedings of the 3rd International Conference on Future Networks and Distributed Systems_, Paris, France, 2019.
69. Ismail, L., Hameed, H., AlShamsi, M., Alhammadi, M.S. and AlDhanhani, N. "Towards a Blockchain Deployment at UAE University: Performance Evaluation and Blockchain Taxonomy." UAE, 2019.
70. Tasatanattakool, P. and Techapanupreeda, C. "Blockchain: Challenges and Applications." _2018 IEEE International Conference on Information Networking (ICOIN)_, Thailand, 2018.
71. Xie, W., Zhou, W., Kong, L., Zhang, X., Min, X., Xiao, Z. and Li, Q. "ETTF: A Trusted Trading Framework Using Blockchain in E-commerce." _2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design_, China, 2018.
72. Anjum, A., Sporny, M. and Sill, A. "Blockchain Standards for Compliance and Trust." _IEEE Cloud Computing_, vol. 4, no. 4, 2017, pp. 84-90.
73. Urien, P. "Towards Secure Elements for Trusted Transactions in Blockchain and Blochchain IoT (BIoT) Platforms. Invited Paper." _2018 Fourth IEEE International Conference on Mobile and Secure Services (MobiSecServ)_, 2018.
74. Ahram, T., Sargolzae, A., Sargolzaei, S., Daniels, J. and Amaba, B. "Blockchain Technology Innovations." _IEEE Technology & Engineering Management Conference (TEMSCON)_, USA, 2017.
75. Saraf, C. and Sabadra, S. "Blockchain Platforms: A Compendium." _IEEE International Conference on Innovative Research and Development (ICIRD)_, Thailand, 2018.
76. Brinckman, A., Luc, D., Nabrzyski, J., Neidig, G.L. and Neidig, J. "A Comparative Evaluation of Blockchain Systems for Application Sharing Using Containers." _IEEE 13th International Conference on eScience_, 2017.
77. Teslya, N. and Ryabchikov, I. "Blockchain Platforms Overview for Industrial IoT Purposes." _2018 22nd Conference of Open Innovations Association (FRUCT)_, Russia, 2018.
78. Kan, L., Wei, Y., Muhammad, A.H., Siyuan, W., Gao, L.C. and Kai, H. "A Multiple Blockchains Architecture On Inter-Blockchain Communication." _2018 IEEE International Conference on Software Quality, Reliability and Security Companion_, China, 2018.
79. Teslya, N. and Ryabchikov, I. "Blockchain-based Platform Architecture for Industrial IoT." _21st Conference of Open Innovations Association (FRUCT)_, Finland, 2017.
80. Ma, Z., Huang, W., Bi, W., Gao, H. and Wang, Z. "A Master-Slave Blockchain Paradigm and Application in Digital Rights Management." _China Communications_, vol. 15, no. 8, 2018, pp. 174-188.
81. Salah, K., Alfalasi, A. and Alfalasi, M. "A Blockchain-based System for Online Consumer Reviews." _IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)_, 2019.

82. Averin, A. and Averina, O. "Review of Blockchain Technology Vulnerabilities and Blockchain-System Attacks." _2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)_, 2019.
83. Platt, S. and Oliver, M. "Towards Blockchain for Decentralized Self-Organizing Wireless Networks." _2019 IEEE Globecom Workshops (GC Wkshps)_, Spain, 2019.
84. Rankhambe, B.P. and Khanuja, H.K. "A Comparative Analysis of Blockchain Platforms – Bitcoin and Ethereum." _2019 5th International Conference on Computing Communication Control andAutomation (ICCUBEA)_, India, 2019.
85. Agbezoutsi, K.E., Urien, P. and Dandjinou, T.M. "Towards Blockchain Services For Mobile Money Traceability And Federation." _2019 3rd Cyber Security in Networking Conference (CSNet)_, France, 2019.
86. Dai, X., Xiao, J., Yang, W., Wang, C. and Jin, H. "Jidar: A Jigsaw-like Data Reduction Approach without Trust Assumptions for Bitcoin System." _IEEE 39th International Conference on Distributed Computing Systems (ICDCS)_, China, 2019.
87. Zhang, S. and Lee, J.-H. "Eclipse-based Stake-Bleeding Attacks in PoS Blockchain Systems." _Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure_, New Zealand, 2019.
88. Jabbar, K. and Work, P.B. "Infrastructural Grind: Introducing Blockchain Technology in the Shipping Domain." _Cyber Infrastructures_, USA, 2018.
89. Zhao, W., Yang, S. and Luo, X. "On Consensus in Public Blockchains." _Proceedings of the 2019 International Conference on Blockchain Technology_, USA, 2019.
90. Tosh, D.K., Shetty, S., Liang, X., Kamhoua, C.A., Kwiat, K.A. and Njilla, L. "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack." _17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing_, USA, 2017.
91. Henry, R., Herzberg, A. and Kate, A. "Blockchain Access Privacy: Challenges and Directions." _IEEE Security & Privacy_, 2018.
92. Kim, S., Lee, C.S. and Kahng, H.K. "New Function and Configuration of Future Network for Blockchain Platform Operation." _International Conference on Advanced Communications Technology (ICACT)_, Korea, 2019.
93. Halunen, K., Vallivaara, V. and Karinsalo, A. "On the Similarities Between Blockchains and Merkle-Damgard Hash Functions." _IEEE International Conference on Software Quality, Reliability and Security Companion_, Finland, 2018.
94. Di Pietro, R., Salleras, X., Signorini, M. and Waisbard, E. "A Blockchain-based Trust System for the Internet of Things." _Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies_, USA, 2018.
95. Bartoletti, M., Lande, S., Pompianu, L. and Bracciali, A. "A General Framework for Blockchain Analytics." _ACM ScalablE and Resilient InfrAstructures for distributed Ledger_, USA, 2017.
96. Bello, G. and Perez, A.J. "Adapting Financial Technology Standards to Blockchain Platforms." _ACM Southeast Conference_, USA, 2019.
97. Ølnes, S. and Jansen, A. "Blockchain Technology as Infrastructure in Public Sector – an Analytical Framework." _Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age_, Norway, 2018.
98. Yamada, Y., Nakajima, T. and Sakamoto, M. "Blockchain-LI: A Study on Implementing Activity-based Micro-pricing Using Cryptocurrency Technologies." _Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media_, China, 2016.
99. Khairuddin, I.E., Sas, C. and Speed, C. "BlocKit: A Physical Kit for Materializing and Designing for Blockchain Infrastructure." _Proceedings of the 2019 on Designing Interactive Systems Conference_, 2019.
100. Han, S., Xu, Z. and Chen, L. "Jupiter: A Blockchain Platform for Mobile Devices." _2018 IEEE 34th International Conference on Data Engineering_, Hong Kong, China, 2018.
101. Alruwaili, A. and Kruger, D. "Intelligent Transaction Techniques for Blockchain Platforms." _2019 IEEE International Conference on Computing, Electronics & Communications Engineering (iCCECE)_, USA, 2019.

102. Sukhodolskiy, I. and Z., S. "A Blockchain-Based Access Control System for Cloud Storage." _2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)_, 2018.
103. Cheng, J.-C., Lee, N.-Y., Chi, C. and Chen, Y.-H. "Blockchain and Smart Contract for Digital Certificate." _Proceedings of IEEE International Conference on Applied System Innovation_, Taiwan, 2018.
104. Kirkman, Stephen S. "A Data Movement Policy Framework for Improving Trust in the Cloud Using Smart Contracts and Blockchains." _2018 IEEE International Conference on Cloud Engineering_, USA, 2018.
105. Elsden, C., Lustig, C., Nissen, B., Dunphy, P., Jabbar, K., Speed, C. and Vines, J. "HCI for Blockchain: Studying, Designing, Critiquing and Envisioning Distributed Ledger Technologies." 2018.
106. Yavuz, E., Koç, A.K., Çabuk, U.C. and Dalkılıç, G. "Towards Secure E-Voting Using Ethereum Blockchain." _2008 6th IEEE International Symposium on Digital Forensic and Security (ISDFS)_, 2018.
107. Suankaewmanee, K., Hoang, D.T., Niyato, D., Sawadsitang, S., Wang, P. and Han, Z. "Performance Analysis and Application of Mobile Blockchain." _2018 International Conference on Computing, Networking and Communications (ICNC): Mobile Computing and Vehicle_, USA, 2018.
108. Liu, C., Chai, K.K., Zhang, X., Lau, E.T. and Chen, Y. "Adaptive Blockchain-Based Electric Vehicle Participation Scheme in Smart Grid Platform." _IEEE Access_, vol. 6, 2018, pp. 25657-25665.
109. Dai, M., Zhang, S., Wang, H. and Jin, S. "A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain." _IEEE Access_, vol. 6, 2018, pp. 22970-22975.
110. Pongnumkul, S., Siripanpornchana, C. and Thajchayapong, S. "Performance Analysis of Private Blockchain Platforms in Varying Workloads." _2017 26th International Conference on Computer Communication and Networks (ICCCN)_, Canada, 2017.
111. Zhao, S., et al. "Research on the Blockchain-based Integrated Demand Response Resources Transaction Scheme." 2018 International Power Electronics Conference (IPEC-Niigata 2018 -ECCEAsia), Japan, 2018.
112. Özyılmaz, K.R. and A. Yurdakul. "Work-in-progress: Integrating Low-power IoT Devices to a Blockchain-based Infrastructure." 2017 IEEE International Conference on Embedded Software (EMSOFT), Turkey, 2017.
113. Qiu, H., et al. "ChainIDE: A Cloud-based Integrated Development Environment for Cross-blockchain Smart Contracts." 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), France, 2019.
114. Huang, Z., et al. "Development of Reliable Wireless Communication System for Secure Blockchain-based Energy Trading." 16th International Joint Conference on Computer Science and Software Engineering (JCSSE), Thailand, 2019.
115. Hasegawa, Y. and H. Yamamoto. "Highly Reliable IoT Data Management Platform Using Blockchain and Transaction Data Analysis." 2020 IEEE International Conference on Consumer Electronics (ICCE), USA, 2020.
116. Im, H., et al. "Privacy and Ledger Size Analysis for Healthcare Blockchain." International Conference on Information Networking (ICOIN), Spain, 2020.
117. Masood, A.B., et al. "Realizing an Implementation Platform for Closed Loop Cyber-Physical Systems Using Blockchain." 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Malaysia, 2019.
118. Ray, P.P., et al. "Blockchain for IoT-based Healthcare: Background, Consensus, Platforms, and Use Cases." IEEE Systems Journal, India, 2019.
119. Wang, Y., et al. "Cloud-Assisted EHR Sharing with Security and Privacy Preservawith via Consortium Blockchain." IEEE Access, 2019.
120. Tripathi, A.K., et al. "Business Service Management using Blockchain." 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), India, 2019.
121. Lei, K., et al. "Towards Decentralized Equilibrium Asset Trading Based on Blockchain." 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), China, 2019. https://doi.org/10.1109/HPCC/SmartCity/DSS.2019.00196
122. Amrutiya, V., et al. "Trustless Two-Factor Authentication Using Smart Contracts in Blockchains." International Conference on Information Networking (ICOIN), Malaysia, 2019. https://doi.org/10.1109/ICOIN.2019.8718107

123. Niya, S.R., et al. "A Blockchain-based Scientific Publishing Platform." UK, 2019. https://doi.org/10.1109/Blockchain.2019.00052
124. Yoo, J., et al. "Formal Modeling and Verification of a Federated Byzantine Agreement Algorithm for Blockchain Platforms." Korea, 2018. https://doi.org/10.1109/ICUFN.2018.8436655
125. Saleh, H., et al. "Platform for Tracking Donations of Charitable Foundations based on Blockchain Technology." 2019 Actual Problems of Systems and Software Engineering (APSSE), Russia, 2019. https://doi.org/10.1109/APSSE.2019.8915366
126. Bragagnolo, S., et al. "Towards Scalable Blockchain Analysis." 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Europe, 2019. https://doi.org/10.1109/WETSEB.2019.00009
127. Taş, R. and Ö.Ö. Tanrıöver. "Building A Decentralized Application on the Ethereum Blockchain." 2019 3rd IEEE International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2019. https://doi.org/10.1109/ISMSIT.2019.8932857
128. Teja, K., et al. "Secured Voting Through Blockchain Technology." 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), India, 2019. https://doi.org/10.1109/ICOEI.2019.8862703
129. Coblenz, M., et al. "Smarter Smart Contract Development Tools." 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Canada, 2019. https://doi.org/10.1109/WETSEB.2019.00010
130. Bai, L., et al. "BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT." IEEE Access, 2019. https://doi.org/10.1109/ACCESS.2019.2917545
131. Amoordon, A. and H. Rocha. "Presenting Tendermint: Idiosyncrasies, Weaknesses, and Good Practices." IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), China, 2019. https://doi.org/10.1109/IWBOSE.2019.8666558
132. Aldweesh, A., et al. "OpBench: A CPU Performance Benchmark for Ethereum Smart Contract Operation Code." 2019 IEEE International Conference on Blockchain (Blockchain), USA, 2019. https://doi.org/10.1109/Blockchain.2019.00032
133. Xu, J. and Y. Shi. "Research on an Innovative Digital Intelligent Ecological Model Based on the BlockChain Cloud in China." 2020 International Conference on Big Data and Informatization Education (ICBDIE), China, 2020. https://doi.org/10.1109/ICBDIE49879.2020.00057
134. Dingman, W., et al. "Classification of Smart Contract Bugs Using the NIST Bugs Framework." Hawaii, 2019. https://doi.org/10.1109/ICBC.2019.00032
135. Dib, O., et al. "Consortium Blockchains: Overview, Applications and Challenges." International Journal on Advances in Telecommunications, vol. 11, 2018, pp. 51-64. https://doi.org/10.30534/ijatcse/2018/0111.12018
136. Brotsis, S., et al. "On the Security of Permissioned Blockchain Solutions for IoT Applications." 2020 2nd International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined, Greece, 2020. https://doi.org/10.1109/CyberTrust49311.2020.9264840
137. Gao, Z., et al. "SmartEmbed: A Tool for Clone and Bug Detection in Smart Contracts through Structural Code Embedding." IEEE International Conference on Software Maintenance and Evolution (ICSME), 2019. https://doi.org/10.1109/ICSME.2019.00058
138. Xenakis, D., et al. "Blockchain-driven Mobile Data Access Towards Fully Decentralized Mobile Video Trading in 5G Networks." ICC 2020-2020 IEEE International Conference on Communications (ICC), 2020. https://doi.org/10.1109/ICC40277.2020.9149227
139. Benahmed, S., et al. "A Comparative Analysis of Distributed Ledger Technologies for Smart Contract Development." 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Canada, 2019. https://doi.org/10.1109/PIMRC.2019.8904235
140. Arias, E.J.G. "Towards Principled Compilation of Ethereum Smart Contracts (SoK)." 2019 10th IEEE IFIP International Conference on New Technologies, Mobility and Security (NTMS), France, 2019. https://doi.org/10.1109/NTMS.2019.8763847

141. Ashraf, I., et al. "GasFuzzer: Fuzzing Ethereum Smart Contract Binaries to Expose Gas-Oriented Exception Security Vulnerabilities." IEEE Access, vol. 8, 2020, pp. 99552-99564. https://doi.org/10.1109/ACCESS.2020.2997036
142. Ocheja, P., et al. "Connecting Decentralized Learning Records: A Blockchain Based Learning Analytics Platform." Proceedings of the 8th International Conference on Learning Analytics and Knowledge, Japan, 2018. https://doi.org/10.1145/3170358.3170381
143. Liu, H., et al. "Enabling Clone Detection For Ethereum via Smart Contract Birthmarks." 2019 IEEE/ACM 27th International Conference on Program Comprehension (ICPC), China, 2019. https://doi.org/10.1109/ICPC.2019.00028
144. Scholten, O.J., et al. "Ethereum Crypto-Games: Mechanics, Prevalence and Gambling Similarities." Spain, 2019. https://doi.org/10.1145/3337722.3341853
145. Walker, M.A., et al. "PlaTIBART: a Platform for Transactive IoT Blockchain Applications with Repeatable Testing." Proceedings of the 4th Workshop on Middleware and Applications for the Internet of Things, 2017. https://doi.org/10.1145/3152141.3152382
146. Martens, D. and W. Maalej. "ReviewChain: Untampered Product Reviews on the Blockchain." 2018 ACM/IEEE 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, Germany, 2018. https://doi.org/10.1145/3194113.3194118
147. Li, B. and Y. Wang. "RZKPB: A Privacy-preserving Blockchain-Based RZKPB: A Privacy-preserving Blockchain-Based." 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, China, 2018. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00215
148. Pittl, B., et al. "Bazaar-Blockchain: A Blockchain for Bazaar-based Cloud Markets." 2018 IEEE International Conference on Services Computing, 2018. https://doi.org/10.1109/SCC.2018.00042
149. Dittmann, G. and J. Jelitto. "A Blockchain Proxy for Lightweight IoT Devices." Crypto Valley Conference on Blockchain Technology (CVCBT), Switzerland, 2019. https://doi.org/10.1109/CVCBT.2019.000-6
150. Shbair, W.M., et al. "BlockZoom: Large-Scale Blockchain Testbed." 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019. https://doi.org/10.1109/BLOC.2019.8751461
151. Nguyen, V.-C., et al. "Digitizing Invoice and Managing VAT Payment Using Blockchain Smart Contract." Vietnam, 2019. https://doi.org/10.1109/RIVF.2019.8713687
152. Wang, Z., et al. "ArtChain: Blockchain-enabled Platform for Art Marketplace." 2019 IEEE International Conference on Blockchain (Blockchain), China, 2019. https://doi.org/10.1109/Blockchain.2019.00021
153. Clincy, V. and H. Shahriar. "Blockchain Development Platform Comparison." IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), USA, 2019. https://doi.org/10.1109/COMPSAC.2019.00209
154. Rot, A. and B. Blaicke. "Blockchain's Future Role in Cybersecurity. Analysis of Defensive and Offensive Potential Leveraging Blockchain-Based Platforms." 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), 2019. https://doi.org/10.1109/ACITT.2019.8779947
155. Yang, S., et al. "CoDAG: An efficient and compacted DAG-based blockchain protocol." 2019 IEEE International Conference on Blockchain (Blockchain), China, 2019. https://doi.org/10.1109/Blockchain.2019.00029
156. Zhu, S., et al. "Hybrid Blockchain Design for Privacy Preserving Crowdsourcing Platform." IEEE International Conference on Blockchain (Blockchain), USA, 2019. https://doi.org/10.1109/Blockchain.2019.00062
157. Tsai, W.-T. and E. Deng. "Application of Blockchain to Trade Clearing." 2018 IEEE International Conference on Software Quality, Reliability and Security Companion, China, 2018. https://doi.org/10.1109/QRS-C.2018.00047
158. Dinh, T.T.A., et al. "BLOCKBENCH: A Framework for Analyzing Private blockchains." Proceedings of the 2017 ACM International Conference on Management of Data, Singapore, 2017. https://doi.org/10.1145/3035918.3064031
159. Nathan, S., et al. "Blockchain Meets Database: Design and Implementation of a Blockchain Relational Database." Proceedings of the VLDB Endowment, USA, 2019. https://doi.org/10.14778/3352063.3352070
160. Rodríguez-Pérez, A., et al. "Bringing transparency and trust to elections: using blockchains for the transmission and tabulation of results." Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, Spain, 2019. https://doi.org/10.1145/3326365.3326406

161. Huang, D., et al. "Building Private Blockchains over Public Blockchains (PoP): An Attribute-Based Access Control Approach." Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, USA, 2019. https://doi.org/10.1145/3297280.3297299
162. Ma, F., et al. "EVM: From Offline Detection to Online Reinforcement for Ethereum Virtual Machine." 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER), China, 2019. https://doi.org/10.1109/SANER.2019.8667997
163. Rangelov, D., et al. "Experiences Designing a Multi-Tier Architecture for a Decentralized Blockchain Application in the Energy Domain." 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Germany, 2019. https://doi.org/10.1109/ICUMT.2019.8970808
164. Bhattacharya, R., et al. "A Blockchain based Peer-to-Peer Framework for Exchanging Leftover Foreign Currency." 2017 IEEE Computing Conference, UK, 2017. https://doi.org/10.1109/SAI.2017.8252163
165. Min, X., et al. "A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size." 2016 IEEE TrustCom/BigDataSE/ISPA, China, 2016. https://doi.org/10.1109/TrustCom.2016.0275
166. Biswas, S., et al. "A Scalable Blockchain Framework for Secure Transactions in IoT." IEEE Internet of Things Journal, vol. 6, no. 3, 2018, pp. 4650-4659. https://doi.org/10.1109/JIOT.2018.2836590
167. Mikula, T.J. and R. Hylsberg. "Identity and Access Management with Blockchain in Electronic Healthcare Records." 21st IEEE Euromicro Conference on Digital System Design, 2018. https://doi.org/10.1109/DSD.2018.00019
168. Hulea, M., et al. "Pharmaceutical Cold Chain Management Platform Based on a Distributed Ledger." 2018 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Romania, 2019. https://doi.org/10.1109/AQTR.2018.8451336
169. Bessani, A., et al. "A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform." 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2019. https://doi.org/10.1109/DSN.2018.00018
170. Lu, Z., et al. "A blockchain-based privacy-preserving authentication scheme for vanets." IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, vol. 27, no. 12, 2019, pp. 2792-2801. https://doi.org/10.1109/TVLSI.2019.2937013
171. Jogunola, O., et al. "Demonstrating Blockchain-Enabled Peer-to-Peer Energy Trading and sharing." IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 2019. https://doi.org/10.1109/CCECE.2019.8861682
172. Lu, L., et al. "Educoin: a secure and efficient payment solution for mooc environment." 2019 IEEE International Conference on Blockchain (Blockchain), China, 2019. https://doi.org/10.1109/Blockchain.2019.00022
173. Zhou, E., et al. "Ledgerdata refiner: a powerful ledger data query platform for hyperledger fabric." Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), China, 2019. https://doi.org/10.1109/IOTSMS48152.2019.8939229
174. Maddali, L.P., et al. "VeriBlock: A Novel Blockchain Framework based on Verifiable Computing and Trusted Execution Environment." 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), India, 2020. https://doi.org/10.1109/COMSNETS48256.2020.9027304
175. Xu, H., et al. "BDSS-FA: A Blockchain-Based Data Security Sharing Platform With Fine-Grained Access Control." IEEE Access, vol. 8, 2020, pp. 87552-87561. https://doi.org/10.1109/ACCESS.2020.2992903
176. Pallam, B. and M.M. Gore. "Boomerang: Blockchain-based Freelance Paradigm on Hyperledger." 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), India, 2019. https://doi.org/10.1109/ICCCNT45670.2019.8944516
177. Huang, B., et al. "BoR: Toward High-Performance Permissioned Blockchain in RDMA-Enabled Network." IEEE Transactions on Services Computing, vol. 13, no. 1, 2019, pp. 301-313. https://doi.org/10.1109/TSC.2019.2957693
178. Shi, Z., et al. "An Automated Customization and Performance Profiling Framework for Permissioned Blockchains in a Virtualized Environment." 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Australia, 2019. https://doi.org/10.1109/CloudCom.2019.00057

179. Ampel, B., et al. "Performance Modeling of Hyperledger Sawtooth Blockchain." 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), China, 2019. https://doi.org/10.1109/ISI.2019.8823470
180. Zhang, J., et al. "Performance Analysis of the Libra Blockchain: An Experimental Study." 2019 2nd International Conference on Hot Information-Centric Networking (HotICN), China, 2019. https://doi.org/10.1109/HotICN.2019.8818598
181. Fan, C., et al. "Towards A Scalable DAG-based Distributed Ledger for Smart Communities." IEEE 5th World Forum on Internet of Things (WF-IoT), Ireland, 2019. https://doi.org/10.1109/WF-IoT.2019.8767276
182. Foschini, L., et al. "Hyperledger Fabric Blockchain: Chaincode Performance Analysis." ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Ireland, 2020. https://doi.org/10.1109/ICC40277.2020.9148846
183. Goranović, A., et al. "Hyperledger Fabric Smart Grid Communication Testbed on Raspberry PI ARM Architecture." 15th IEEE International Workshop on Factory Communication Systems (WFCS), Sweden, 2019. https://doi.org/10.1109/WFCS.2019.8758017
184. Javaid, H., et al. "Optimizing Validation Phase of Hyperledger Fabric." 2019 IEEE 27th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), France, 2019. https://doi.org/10.1109/MASCOTS.2019.00041
185. Toapanta, S.M.T., et al. "A Hyperledger Technology Approach to Mitigate the Risks of the Database in Foreign Trade Management." 2020 3rd International Conference on Information and Computer Technologies (ICICT), USA, 2020. https://doi.org/10.1109/ICICT50521.2020.00061
186. Zheng, W., et al. "NutBaaS: A Blockchain-as-a-Service Platform." IEEE Access, vol. 7, 2019, pp. 134422-134433. https://doi.org/10.1109/ACCESS.2019.2941905
187. Mahesh, A.N., et al. "Conceptualizing Blockchain based Energy Market for Self-Sustainable Community." Proceedings of the 2nd Workshop on Blockchain-enabled Networked Sensor, 2019. https://doi.org/10.1145/3362744.3362754
188. Sivagnanam, S., et al. "Introducing the Open Science Chain - Protecting Integrity and Provenance of Research Data." Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (learning), 2019. https://doi.org/10.1145/3332186.3332218
189. Badra, S., et al. "Multi-tier Blockchain Framework for IoT-EHRs Systems." The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks, Egypt, 2019. https://doi.org/10.1016/j.procs.2019.09.037
190. Cluchet, P., et al. "PlasticCoin: an ERC20 Implementation on Hyperledger Fabric for Circular Economy and Plastic Reuse." IEEE/WIC/ACM International Conference on Web Intelligence-Companion, 2019. https://doi.org/10.1145/3358695.3360926
191. Oh, B. and D. Kim. "Serverless-Enabled Permissioned Blockchain for Elastic Transaction Processing." Proceedings of the 20th International Middleware Conference Demos and Posters, 2019. https://doi.org/10.1145/3366627.3368102
192. Kaijun, L., et al. "Research on agricultural supply chain system with double chain architecture based on blockchain technology." Future Generation Computer Systems, vol. 86, 2018, pp. 641-649. https://doi.org/10.1016/j.future.2018.04.061
193. Vukolić, M. "Rethinking Permissioned Blockchains." Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Zurich, 2017. https://doi.org/10.1145/3055518.3055526
194. Sinclair, D., et al. "Security Requirement Prototyping with Hyperledger Composer for Drug Supply Chain – A Blockchain application." Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, USA, 2019. https://doi.org/10.1145/3309074.3309083
195. Ban, T.Q., et al. "Survey of Hyperledger Blockchain Frameworks: Case Study in FPT University's Cryptocurrency Wallets." Proceedings of the 2019 8th International Conference on Software and Computer Applications, 2019. https://doi.org/10.1145/3316615.3316706
196. Ali, A.A., et al. "The Quest for Fully Smart Autonomous Business Networks in IoT Platforms." Proceedings of the 3rd Africa and middle east conference on software engineering, 2017. https://doi.org/10.1145/3195106.3195110

197. Ali, G.W.S., et al. "A Blockchain-based Decentralized Data Storage and Access Framework for PingER." 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), USA, 2018. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00166

198. Sukhwani, H., et al. "Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network)." 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), 2018. https://doi.org/10.1109/NCA.2018.8548322

199. Al-Zahrani, F.A. "Subscription-Based Data-Sharing Model Using Blockchain and Data as a Service." IEEE Access, vol. 8, 2020, pp. 115966-115981. https://doi.org/10.1109/ACCESS.2020.3004235

200. Ismailisufi, A., et al. "A Private Blockchain Implementation Using Multichain Open-Source Platform." 24th International Conference on Information Technology (IT), Montenegro, 2020. https://doi.org/10.1109/IT48387.2020.9070742

201. Mujagić, A., et al. "Building Own Blockchain." Middleware '19: Proceedings of the 20th International Middleware Conference Industrial Track, Davis, CA, USA, 2019. https://doi.org/10.1145/3366615.3369092

202. Samaniego, M. and R. Deters. "Blockchain as a Service for IoT." 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom), Canada, 2017. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.98

203. Agrawal, M., et al. "Blockchain-based Universal Loyalty Platform." 2019 IEEE International Conference on Advances in Computing, Communication and Control (ICAC3), India, 2019. https://doi.org/10.1109/ICAC347.2019.9036748

204. Lei, X., et al. "BFastPay: A Routing-free Protocol for Fast Payment in Bitcoin Network." CODASPY '21: Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, 2021. https://doi.org/10.1145/3422337.3447111

205. Adochiei, F.-C., et al. "Brain Mapping using a Blockchain Approach." The 7th IEEE International Conference on E-Health and Bioengineering, Romania, 2018. https://doi.org/10.1109/EHB.2018.8443456

206. Korepanova, D., et al. "Building a Private Currency Service Using Exonum." IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2019. https://doi.org/10.1109/BlackSeaCom.2019.8812771

207. Wang, H., et al. "Crowdchain: A Location Preserve Anonymous Payment System Based on Permissioned Blockchain." 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), China, 2019. https://doi.org/10.1109/SmartIoT.2019.00041

208. Turkanović, M., et al. "EduCTX: A Blockchain-Based Higher Education Credit Platform." IEEE Access, vol. 6, 2018, pp. 5112-5127. https://doi.org/10.1109/ACCESS.2018.2789929

209. Florea, B.C. "Blockchain and Internet of Things Data Provider for Smart Applications." 2018 7th Mediterranean Conference on Embedded Computing (MECO), 2018. https://doi.org/10.1109/MECO.2018.8406089

210. Annane, A.A. and A.L. Boubakeur. "Blockchain based context-aware CP-ABE schema for Internet of Medical Things security." Array, 2022. https://doi.org/10.1016/j.array.2022.100159

211. Oham, Chuka a., et al. "WIDE: A witness-based data priority mechanism for vehicular forensics." Blockchain: Research and Applications, 2022. https://doi.org/10.1016/j.bcra.2022.100057

212. Xin, K., et al. "Reciprocal Crowdsourcing: Building Cooperative Game Worlds on Blockchain." 2020 IEEE International Conference on Consumer Electronics (ICCE), China, 3030. https://doi.org/10.1109/ICCE46568.2020.9043189

213. Chowdhury, Oishi, et al. "The Rise of Blockchain Technology In Shariah Based Banking System." ICCA '22: Proceedings of the 2nd International Conference on Computing Advancements, 2022. https://doi.org/10.1145/3542163.3542171

214. Dernayka, I. and A. Chehab. "Blockchain Development Platforms: Performance Comparison." 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 2021. https://doi.org/10.1109/NTMS53355.2021.9593464

215. Duan, H., et al. "Metaverse for Social Good: A University Campus Prototype." Proceedings of the 29th ACM International Conference on Multimedia, 2021. https://doi.org/10.1145/3474085.3475235

216. Liu, Ruihuan a., et al. "Improving Vaccine Safety Using Blockchain." Computers & Industrial Engineering, 2023. https://doi.org/10.1016/j.cie.2023.108679

217. Xiaodong, Z., et al. "Research on Technical Architecture and Overall Scheme of Railway Block Chain Service Platform." ICBTA: International Conference on Blockchain Technology and Application, 2020. https://doi.org/10.1145/3445483.3445503

218. Campanile, Lelio 1., et al. "Designing a GDPR compliant blockchain-based IoV distributed information tracking system." Information Processing & Management, 2021. https://doi.org/10.1016/j.ipm.2021.102748

219. Tan, Liang, et al. "A blockchain-empowered access control framework for smart devices in green internet of things." ACM Transactions on Internet Technology, Volume 21, 2021. https://doi.org/10.1145/3452294

220. Yang, Guozheng, et al. "Distributed fusion cross-chain model and architecture." IET Blockchain, 2022. https://doi.org/10.1049/blc2.12004