A Survey on Blockchain based Crowd funding Platform

Vishal V. Mahale, Kshitija S. Gholap, Harshada D. Patil, Maya B. Bhor

Department of Computer Engineering, Sandip Institute of Engineering and Management, Nashik, Maharashtra, India

Corresponding author: Vishal V. Mahale, Email: vishal.mahale@siem.org.in

In this paper, we examine the use of blockchain technology to improve crowdfunding platforms by addressing issues like transparency, security, and centralization. Blockchain enables automation of processes such as fund collection and reward distribution through smart contracts, reducing fraud and enhancing transparency. We review trends like equity, donation-based, real estate, and reward-based crowd funding, showing how blockchain enhances security. In this paper we present study of existing blockchain based crowdfunding platform and we compare the using evaluation parameter like scalability, accessibility, time complexity, performance.

Keywords: Crowdfunding, Blockchain Technology, Smart Contracts, Decentralized Funding, Security, Transparency.

2025. In Puneet Kumar Gupta (ed.), *Computational Models for Intelligence and Automation*, 36–47. Computing & Intelligent Systems, SCRS, India. DOI: https://doi.org/10.56155/978-81-975670-1-8-4

1 Introduction

A smart contract is a self-executing program stored on a block chain. It automatically run itself when the term and condition is fulfil. This paper presents a comprehensive review of existing crowdfunding platforms and their limitations, highlighting the need for a secure, transparent, and decentralized approach. The authors also identify the challenges and limitations of existing smart contract-based crowdfunding platforms and propose a novel approach that addresses these issues [1]. These contracts are written in programming languages such as solidity which is used for Ethereum and are designed to be immutable and secure once deployed.This paper reviews existing access control mechanisms in block chain-enabled supply chains, highlighting their limitations in ensuring secure and authorized data access.The review highlights the advantages of Access Chain, including improved security, transparency, and efficiency, and discusses its potential applications in various supply chain scenarios [2].

Smart contracts operate based on predefined conditions such that when certain conditions are fulfil. The contract executes the agreed-upon actions, such as transferring funds or verifying transactions. In their 2022 paper, Y. Verginadis et al. propose a context-aware policy enforcement framework tailored for Platform-as-a-Service (PaaS) environments, focusing on enhancing access control mechanisms. They validate the framework's effectiveness through a series of experiments, demonstrating its ability to improve decision-making in complex cloud ecosystems, especially by balancing flexibility with security enforcement [3]. They are widely used in decentralized finance (DeFi), supply chain management, and digital identity verification due to their transparency, security, and efficiency. In the 2022 study, M. Tuler De Oliveira et al. introduce Smart Access, an attribute-based access control (ABAC) system designed for secure medical record management using block chain-based smart contracts. The paper demonstrates how the system enhances both security and flexibility in managing medical records, providing a decentralized and transparent solution while protecting patient privacy [4].

The generation life cycle of smart contract is shown in Figure 1.

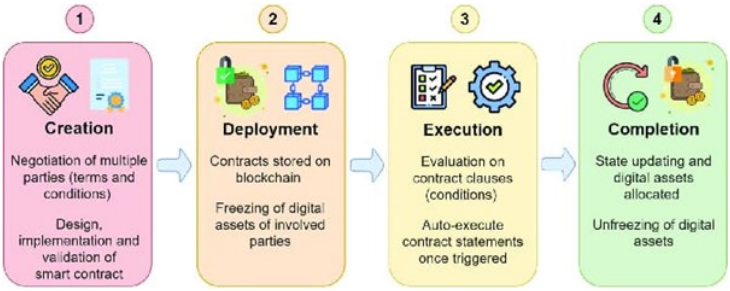

Figure 1: Life cycle of smart contract of crowdfunding platform.

A smart contract is like a digital agreement that automatically works when certain condition are met. It runs on blockchain a secure, decentralized digital ledger and does not need the middleman.In the 2022 study, M. Tuler De Oliveira et al. introduce Smart Access, an attribute-based access control (ABAC) system designed for secure medical record management using block chain-based smart contracts.The review highlights the advantages of the proposed framework, including improved security, privacy, and efficiency, and discusses its potential applications in healthcare scenarios [5].

They are most commonly used on blockchain platforms like Ethereum. Because the blockchain is decentralized where smart contracts offer a high level of security and transparency. This paper reviews existing electronic portfolio management systems, highlighting their limitations in ensuring security, trust, and privacy. The review highlights the advantages of the proposed scheme, including decentralized control, immutability, transparency, and tamper-resistance, and discusses its potential applications in various industries, such as education and employment [6].

Block chain is a revolutionary technology that acts as a secure, transparent, and decentralized digital ledger. Blockchain is the chain of the block where the blocks contains the information like hash, relevant information and previous block hash. In their 2022 paper, S. Namane and I. B. Dhaou explore blockchain-based access control techniques for Internet of Things (IoT) applications, focusing on enhancing security and privacy in decentralized environments. The authors review the limitations of traditional access control methods, such as centralized management and single points of failure, and propose block chain as a viable alternative. The paper highlights several block chain-based models and techniques, evaluating their effectiveness in addressing scalability, privacy, and trust issues within IoT ecosystems [7].

Each and every block is interconnected with each other. Unlike traditional systems controlled by a single authority, block chain operates across a network of computers, ensuring that no single person or organization has complete control. This decentralized nature makes it highly secure and resistant to fraud. This paper reviews existing security mechanisms for Internet of Medical Things (IoMT), highlighting their limitations in ensuring secure and authorized access to medical data. The review highlights the advantages of the proposed schema, including decentralized control, context-aware access control, and tamper-resistance, and discusses its potential applications in healthcare scenarios, such as remote patient monitoring and telemedicine [8].

Every transaction is verified by multiple computers in the network, making it nearly impossible to alter past records. Block chain technology is widely used in crypto currencies like Bitcoin and Ethereum, but its applications extend far beyond digital money. It is transforming industries such as finance, supply chain management, healthcare, and even voting systems by providing secure, transparent, records. It contain blocks which contain the group of information. Where the blockchain are used in cryptocurrencies like bitcoin and Ethereum ,smart contract. In their 2022 paper, I. H. Abdulqadder and S. Zhou introduce Slice Block, a novel framework for context-aware authentication handover and secure network slicing in edge-assisted software-defined networking (SDN) and network function virtualization (NFV) environments, tailored for 6G networks. Slice Block integrates context-aware mechanisms to ensure seamless authentication handover across network slices while enhancing security and performance. The authors validate the system's efficiency through simulations, demonstrating its potential to improve security and optimize network resource allocation in edge-assisted 6G networks [9].

A crowdfunding platform is an online space where individuals, businesses, or organizations can raise money by collecting small contributions from a large number of people. Instead of relying on traditional funding methods like banks or big investors, crowdfunding allows anyone to support a project, business idea, or personal cause. These platforms operate in different ways, such as donation-based crowdfunding, where people contribute without expecting anything in return, or reward-based crowdfunding, where backers receive a product or service in exchange for their support. By connecting fundraisers with a global audience, crowdfunding platforms make it easier to turn ideas into reality without depending on traditional financial institutions. . In their 2021 paper, E. Psarra et al. propose a context-aware attribute-based access control (ABAC) framework for accessing electronic health records (EHRs) during critical incidents The authors

emphasize the importance of balancing timely access to critical medical data with privacy and security concerns. Through case studies and simulations, the paper demonstrates how the context-aware ABAC model can adapt dynamically to real-time situations, improving decision-making and access control in critical healthcare environments [10].

The remainder of the paper is organized as follow : Section II provides a comprehensive literature survey of existing crowdfunding system using smart contract .Section III provides discussion of state of art systems and section IV concludes the paper.

2 Related Work

This paper reviews existing crowdfunding platforms, highlighting their limitations and the potential of blockchain and smart contracts for enhanced security, transparency, and efficiency. The authors propose a blockchain-based crowdfunding model that addresses these issues through automated transactions, which enhances trust and reduces costs [11]. The limitations of traditional access control mechanisms in blockchain-enabled supply chains are examined, leading to the development of Access Chain, a decentralized and scalable framework that utilizes smart contracts for fine-grained data access [12].

Y. Verginadis et al. (2022) propose a context-aware policy enforcement framework for Platform-as-a-Service (PaaS) environments, combining role-based access control (RBAC) with context-aware policies to adapt to real-time changes [13]. M. Tuler De Oliveira et al. (2022) introduce Smart Access, an attribute-based access control (ABAC) system leveraging blockchain for secure medical record management, addressing privacy and scalability challenges [14].

Another study reviews access control for electronic health records (EHRs), proposing a machine learning and context-aware framework to enhance security and efficiency [15]. The review of electronic portfolio management systems identifies challenges in traditional methods and suggests a consortium blockchain-based scheme for improved security and transparency [16].

S. Namane and I. B. Dhaou (2022) explore blockchain-based access control techniques for IoT applications, proposing models that enhance security and privacy[17]. Additionally, a novel context-aware attribute-based access control framework for EHRs during critical incidents is introduced to balance timely access with privacy concerns[20].

In the context of IoT devices, the limitations of traditional access control methods are discussed, leading to a proposed blockchain-based consortium capability access control (IoT-CCAC) approach[21][22]. This highlights decentralized control, scalability, and fine-grained access control.

Furthermore, a smart contract-based dynamic consent management system is proposed to ensure compliance with GDPR while enhancing user control over personal data[23]. Lastly, this paper reviews existing access control mechanisms and suggests the integration of smart contracts and attribute-based controls for improved security in medical records and IoT systems [25] [26] [27] [28].

This paper reviews access control mechanisms in global healthcare systems, emphasizing their limitations in securing sensitive medical data due to centralized management and vulnerability to cyberattacks. It proposes a blockchain-based access control framework tailored for healthcare ecosystems, highlighting advantages like decentralization, immutability, and transparency. The framework's applications in telemedicine and health information exchange are discussed, emphasizing its potential to enhance security, privacy, and efficiency in data management [29].

The authors also examine access control in blockchain-enabled supply chains, critiquing traditional methods for their scalability and management challenges. They introduce the Access Chain framework, designed for secure data access in supply chains, emphasizing its benefits in improving security and trust in data management [30].

In a 2022 study, H. Abdul Qadder and S. Zhou present Slice Block, a framework for context-aware authentication in 6G networks, leveraging Directed Acyclic Graph (DAG) blockchain technology to ensure secure network slicing [31]. B. Annane et al. propose a context-aware Ciphertext Policy Attribute-Based Encryption scheme for the Internet of Medical Things (IoMT), addressing privacy concerns through decentralized access control [32].

M. M. Merlec et al. introduce SmartBuilder, a block-based visual programming framework that simplifies smart contract development [33]. R. Xu et al. propose a decentralized access control framework for IoT using blockchain and smart contracts, promoting security and efficiency [34].

The survey on context-aware access control mechanisms in cloud and fog networks discusses their significance and identifies open research issues, highlighting the need for ongoing research [35]. E. Psarra et al. propose an attribute-based access control framework for electronic health records, integrating contextual factors to enhance security during emergencies [36]. Lastly, a paper advocates for context-aware smart contracts that adapt to changing conditions in IoT systems [37]. In 2021, S. Al Garni et al. explored secured access control in IoT, proposing a distributed ledger solution for secure authentication [38].

The paper by M. Amine Bouras et al. introduces a consortium capability access control approach for IoT systems, known as IoT-CCAC. This decentralized mechanism leverages blockchain technology to enable collaborative access control among multiple organizations, ensuring data confidentiality and integrity. A hierarchical structure assigns capabilities based on device roles, with access control decisions made by a consortium of stakeholders, demonstrating the approach's feasibility through simulations [39].

Lastly, M. M. Merlec et al. propose a smart contract-based dynamic consent management system for personal data under the General Data Protection Regulation (GDPR). Their decentralized system allows individuals to grant or revoke consent for data usage dynamically, ensuring compliance with GDPR requirements. The authors demonstrate the system's effectiveness through case studies and simulations, emphasizing its potential to enhance data privacy while providing transparency and accountability [40].

In their 2021 paper "Blockchain-based Context-aware Authorization Management as a Service in IoT," T. Sylla et al. present a framework that utilizes blockchain to enhance authorization management in Internet of Things (IoT) environments. This decentralized, context-aware system improves security and privacy by adapting to the dynamic conditions of IoT networks, allowing for efficient access control without centralized authorities, demonstrating scalability across diverse scenarios [41].

Similarly, I.-H. Chuang et al. introduce TIDES, a trust-aware economic framework for IoT data management, in their 2020 article "TIDES: A Trust-aware IoT Data Economic System with Blockchain-enabled Multi-access Edge Computing." By integrating blockchain with multi-access edge computing (MEC), TIDES addresses issues of data integrity and resource utilization, promoting transparent transactions and localized processing, and showing potential for enhancing trust and efficiency in IoT [42].

N. Chendeb and colleagues, in their work on secure healthcare systems, propose a framework combining blockchain and IoT to address challenges in data integrity, privacy, and access control. This integration ensures tamper-proof management of healthcare data and secure communica-

tion among stakeholders, thus enhancing the security of patient information and streamlining operations [43].

Additionally, a paper discusses limitations in existing role-based access control (RBAC) systems, proposing a blockchain-enabled approach that employs smart contracts for dynamic access control. This method enhances flexibility, scalability, and security, making it applicable to various domains, including cloud computing and social networks, while addressing challenges like performance and interoperability [44].

A performance analysis of Hyperledger Besu evaluates its scalability and throughput, examining factors such as network size and transaction volume. The findings highlight optimization opportunities for developers and users of this private blockchain platform, alongside comparisons to other blockchain technologies [45].

Another comprehensive survey reviews the integration of blockchain with IoT, discussing benefits like enhanced security and trust while identifying challenges in scalability and interoperability across domains such as smart homes and industrial automation. Future research directions are also suggested, focusing on merging blockchain with emerging technologies like edge computing [46].

Furthermore, a paper proposes a blockchain-based capability-based access control (CBAC) strategy for space situation awareness (SSA). This decentralized approach addresses traditional access control limitations, promoting secure and dynamic data sharing while highlighting challenges related to performance and standardization [47].

Lastly, a survey of IoT access control mechanisms outlines the unique challenges of these environments, exploring various models such as discretionary and role-based access control. The authors discuss the potential of integrating blockchain and edge computing to address specific issues such as scalability and privacy [48].

Additional studies explore blockchain applications in crowdfunding, detailing how it enhances security and transparency, and in electronic bidding, proposing a smart contract framework that improves trust and efficiency in the bidding process [49] [50].

3 Discussion

This literature survey highlights the transformative potential of smart contract systems in addressing key challenges in funding mechanisms. Traditional funding method often rely on intermediaries, leading to inefficiencies, increased costs, and risk such as fraud and poor fund management. In contrast , smart contracts enhances trust and transparency by ensuring that all term and transaction are recorded immutably, allowing stakeholders to verify information without relying on intermediaries.

The review of crowdfunding literature reveal that the integration of blockchain technology can significantly improve funding processes across various sectors, including technology, finance, social enterprise. The decentralized nature of smart contract not only streamline transaction but also reduces costs associated with traditional funding approaches. Furthermore, the ability to quick raise funds through online platform offers entrepreneurs a valuable marketing avenue, fostering grater engagement and visibility for the projects.

Overall, the funding suggest the adopting smart contact based funding system can lead to more efficient ,secure, and transparent funding solution ,ultimately benefiting both funders and project initiators .Future research should explore the practical implication and scalability of these

Table 1: Literature Review Summary

PROPOSED SYSTEM	YEAR	KEY FOCUS	DISADVANTAGES
Optimized gas fees and transaction speed using layer-2 scaling.[1]	2023	Crowdfunding Platform using Smart Contracts	High gas fees and slow transaction speed.
Improved scalability with efficient resource allocation.[2]	2023	Access control in blockchain supply chain	Limited scalability and high resource consumption.
Streamlined policy enforcement with dynamic access control systems.[3]	2022	Policy enforcement for PaaS-enabled access control	Complexity in context-aware policy enforcement mechanisms.
Privacy-preserving techniques like zk-SNARKs for secure medical record access.[4]	2022	Medical records access via smart contracts	Challenges in integrating smart contracts with healthcare data while maintaining privacy.
Adaptive control mechanisms with real-time patient data integration.[5]	2022	Predictive access control in healthcare	Inability to handle dynamic changes in patient conditions.
Consortium blockchain for efficient data management at scale.[6]	2022	Electronic portfolio management using blockchain	Inability to scale for large-scale academic data.
Consortium blockchain for efficient data management at scale.[7]	2022	Electronic portfolio management using blockchain	Inability to scale for large-scale academic data.
Simplified encryption protocols for seamless integration with IoT devices.[8]	2022	CP-ABE for IoT security	Complexity in implementing attribute-based encryption for IoT devices.
Secure network slicing with seamless authentication handover using blockchain.[9]	2022	Authentication in 6G networks with blockchain	Network slicing complexities and authentication handover issues in 6G environments.
Scalable and dynamic context-aware access control systems for emergencies.[10]	2022	Context-aware access control for healthcare	Difficulties in scaling access control mechanisms during critical incidents.
Improved decentralization and capability management via consortium blockchain.[11]	2021	Blockchain-based access control for IoT	Issues with decentralized capability access control.
Enhanced security using blockchain-backed cryptography and smart contracts.[12]	2021	Secured access control in IoT	Inadequate security measures for IoT-based smart contracts.
Smart contracts enabling real-time consent revocation in GDPR-compliant frameworks.[13]	2021	Dynamic consent management under GDPR	Challenges in handling consent revocation in a decentralized manner.
Context-aware contracts capable of handling dynamic changes in IoT systems.[14]	2021	Context-aware smart contracts for IoT	Difficulty in dynamic IoT device interaction with blockchain smart contracts.
Immediate access for emergency medical records via decentralized attribute-based access control systems.[15]	2022	Medical records access via smart contracts	Lack of real-time access for emergency medical services.

system in diverse funding environment.

Considering the limitation of state of art system, in future the below prototype model as shown in fig 2 can be cosnsider.

Figure 2: Flow diagram of crowdfunding platform.

4 Conclusion and Future Scope

This survey highlights the transformative impact of blockchain technology and smart contracts on crowdfunding platforms by addressing issues such as high fees, lack of transparency, and fraud. By enabling decentralized fund management and conditional fund release, these innovations enhance security and eliminate intermediaries, fostering trust among investors and project creators.

The potential applications span multiple sectors, including finance, healthcare, and supply chain management, offering a transparent and efficient fundraising solution. Looking ahead, advancements in artificial intelligence, machine learning, and IoT integration promise to further enhance smart contract funding, enabling real-time asset monitoring and automated decision-making. Additionally, cross-chain interoperability will expand the system's capabilities, paving the way for new use cases and driving growth in the crowdfunding landscape.

References

[1] Raunak Sulekh, Manas Katiyar, Devang Trivedi, "Crowdfunding Platform using Smart Contracts", Volume 8, Issue 6, June 2023, ISSN No:-2456-2165

[2] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, "Access Chain: An access control framework to protect data access in blockchain enabled supply chain," Future Gener. Computer. Syst., vol. 148, pp. 380–394, Nov. 2023.

[3] Y. Verginadis et al., "Context-aware policy enforcement for PaaSenabled access control," IEEE Trans. Cloud Comput., vol. 10, no. 1, pp. 276–291, Jan.–Mar. 2022.

[4] M. Tuler De Oliveira, L. H. A. Reis, Y. Verginadis, D. M. F. Mattos, and S. D. Olabarriaga, "Smart Access: Attribute-based access control system for medical records based on smart contracts," IEEE Access, vol. 10, pp. 117836–117854, 2022

[5] E. Psarra, D. Apostolou, Y. Verginadis, I. Patiniotakis, and G. Mentzas, "Context-based, predictive access control to electronic health records," Electronics, vol. 11, no. 19, p. 3040, 2022.

[6] M. M. Merlec, M. M. Islam, Y. K. Lee, and H. P. In, "A consortium blockchain-based secure and trusted electronic portfolio management scheme," Sensors, vol. 22, no. 3, p. 1271, Feb. 2022.

[7] S. Namane and I. B. Dhaou, "Blockchain-based access control techniques for IoT applications," Electronics, vol. 11, no. 14, p. 2225, 2022.

[8] B. Annane, A. Alti, and A. Lakehal, "Blockchain based context-aware CP-ABE schema for Internet of Medical Things security," Array, vol. 14, Jul. 2022, Art. no. 100150.

[9] I. H. Abdulqadder and S. Zhou, "Slice Block: Context-aware authentication handover and secure network slicing using DAG-blockchain in edge-assisted SDN/NFV-6G environment," IEEE Internet Things J., vol. 9, no. 18, pp. 18079–18097, Sep. 2022.

[10] E. Psarra, Y. Verginadis, I. Patiniotakis, D. Apostolou, and G. Mentzas, "Accessing electronic health records in critical incidents using contextaware attribute-based access control," Intell. Decis. Technol., vol. 15, no. 4, pp. 667–679, 2021.

[11] M. Amine Bouras, B. Xia, A. Omer Abuassba, H. Ning, and Q. Lu, "IoT-CCAC: A blockchain-based consortium capability access control approach for IoT," PeerJ Comput. Sci., vol. 7, p. e455, Apr. 2021.

[12] S. Algarni et al., "Blockchain-based secured access control in an IoT system," Appl. Sci., vol. 11, no. 4, p. 1772, 2021.

[13] M. M. Merlec, Y. K. Lee, S.-P. Hong, and H. P. In, "A smart contract-based dynamic consent management system for personal data usage under GDPR," Sensors, vol. 21, p. 7994, Nov. 2021.

[14] L. Ngwira et al., "Towards context-aware smart contracts for blockchain IoT systems," in Proc. Int. Conf. Inf. Commun. Technol. Conver. (ICTC), 2021, pp. 82–87.

[15] M. Tuler De Oliveira, L. H. A. Reis, Y. Verginadis, D. M. F. Mattos, and S. D. Olabarriaga, "SmartAccess: Attribute-based access control system for medical records based on smart contracts," IEEE Access, vol. 10, pp. 117836–117854, 2022.

[16] Y. Verginadis et al., "Context-aware policy enforcement for PaaSenabled access control," IEEE Trans. Cloud Comput., vol. 10, no. 1, pp. 276–291, Jan.–Mar. 2022.

[17] E. Psarra, D. Apostolou, Y. Verginadis, I. Patiniotakis, and G. Mentzas, "Context-based, predictive access control to electronic health records," Electronics, vol. 11, no. 19, p. 3040, 2022.

[18] S. Namane and I. B. Dhaou, "Blockchain-based access control techniques for IoT applications," Electronics, vol. 11, no. 14, p. 2225, 2022.

[19] S. Salonikias et al., "Blockchain-based access control in a globalized healthcare provisioning ecosystem," Electronics, vol. 11, no. 17, p. 2652, 2022.

[20] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, "AccessChain: An access control framework to protect data access in blockchain enabled supply chain," Future Gener. Comput. Syst., vol. 148, pp. 380–394, Nov. 2023.

[21] H. Abdulqadder and S. Zhou, "SliceBlock: Context-aware authentication handover and secure network slicing using DAG-blockchain in edge-assisted SDN/NFV-6G environment," IEEE Internet Things J., vol. 9, no. 18, pp. 18079–18097, Sep. 2022.

[22] B. Annane, A. Alti, and A. Lakehal, "Blockchain based context-aware CP-ABE schema for Internet of Medical Things security," Array, vol. 14, Jul. 2022, Art. no. 100150.

[23] M. M. Merlec, Y. K. Lee, and H. P. In, "SmartBuilder: A block-based visual programming framework for smart contract development," in Proc. IEEE Int. Conf. Blockchain (Blockchain), 2021, pp. 90–94.

[24] R. Xu, Y. Chen, and E. Blasch, "Decentralized access control for IoT based on blockchain and smart contract," in Modeling and Design of Secure Internet of Things. Hoboken, NJ, USA: Wiley, 2020, pp. 505–528.

[25] A. S. M. Kayes et al., "A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues," Sensors, vol. 20, no. 9, p. 2464, 2020.

[26] E. Psarra, Y. Verginadis, I. Patiniotakis, D. Apostolou, and G. Mentzas, "Accessing electronic health records in critical incidents using contextaware attribute-based access control," Intell. Decis. Technol., vol. 15, no. 4, pp. 667–679, 2021.

[27] L. Ngwira et al., "Towards context-aware smart contracts for blockchain IoT systems," in Proc. Int. Conf. Inf. Commun. Technol. Conver. (ICTC), 2021, pp. 82–87

[28] S. Algarni et al., "Blockchain-based secured access control in an IoT system," Appl. Sci., vol. 11, no. 4, p. 1772, 2021.

[29] M. Amine Bouras, B. Xia, A. Omer Abuassba, H. Ning, and Q. Lu, "IoT-CCAC: A blockchain-based consortium capability access control approach for IoT," PeerJ Comput. Sci., vol. 7, p. e455, Apr. 2021.

[30] M. M. Merlec, Y. K. Lee, S.-P. Hong, and H. P. In, "A smart contract-based dynamic consent management system for personal data usage under GDPR," Sensors, vol. 21, p. 7994, Nov. 2021.

[31] T. Sylla et al., "Blockchain-based context-aware authorization management as a service in IoT," Sensors, vol. 21, no. 22, p. 7656, 2021.

[32] I.-H. Chuang et al., "TIDES: A trust-aware IoT data economic system with blockchain-enabled multi-access edge computing," IEEE Access, vol. 8, pp. 85839–85855, 2020.

[33] N. Chendeb, N. Khaled, and N. Agoulmine, "Integrating blockchain with IoT for a secure healthcare digital system," in Proc. 8th Int. Workshop Adv. ICT Infrastructure. Services, 2020, pp. 1–8.

[34] M. U. Rahman, B. Guidi, F. Baiardi, and L. Ricci, "Context-aware and dynamic role-based access control using blockchain" in Advanced Information Networking and Applications. Cham, Switzerland: Springer, pp. 1449–1460, 2020.

[35] C. Fan, C. Lin, H. Khazaei, and P. Musilek, "Performance analysis of Hyperledger Besu in private blockchain," in Proc. IEEE DAPPS, 2022,pp. 64–73.

[36] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," IEEE Internet Things J., vol. 6, no. 5, pp. 8076–8094,Oct. 2019.

[37] R.Xu, Y. Chen, E. Blasch, and G. Chen, "Exploration of blockchain enabled decentralized capability-based access control strategy for space situation awareness," Opt. Eng. vol. 58, no. 4, pp. 041609–041609, Feb. 2019.

[38] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," J. Netw. Comput. Appl., vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[39] Zhao, Hongjiang, and Cephas P. K. Coffie. "The Applications of Blockchain Technology in Crowdfunding Contract" SSRN Electronic Journal, 2018. DOI.org (Crossref), https://doi.org/10.2139/ssrn.3133176

[40] Yi-Hui Chen, Shih-Hsin Chen, Iuon-Chang Lin, "Blockchain based smart contract for bidding system" 2018 IEEE International Conference on Applied System Invention (ICASI), Apr 2018, 978- 1-5386-4342-6.

[41] Rootstock Platform Bitcoin Powered Smart Contract Whitepaper. [Online]. Available: https://www.rsk.co/wp-content/uploads/2019/ 02/RSK-White-Paper-Updated.pdf

[42] NXT Whitepaper. [Online]. Available: https://www.rsk.co/wpcontent/uploads/2019/02/RSK-White-Paper-Updated.pdf

[43] T. Min and W. Cai, ''A security case study for blockchain games,'' in Proc. IEEE Games, Entertainment, Media Conf. (GEM), Jun. 2019, pp. 1–8.

[44] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, ''A survey on blockchain: A game theoretical perspective,'' IEEE Access, vol. 7, pp. 47615–47643, 2019.

[45] Y. Zhang, S. Ma, J. Li, K. Li, S. Nepal, and D. Gu, ''SMARTSHIELD: Automatic smart contract protection made easy,'' in Proc. IEEE 27th Int. Conf. Softw. Anal., Evol. Renege. (SANER), Feb. 2020, pp. 23–34.

[46] C. G. Harris, ''The risks and challenges of implementing ethereum smart contracts,'' in Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC), May 2019, pp. 104–107.

[47] S. Kim and S. Ryu, ''Analysis of blockchain smart contracts: Techniques and insights,'' in Proc. IEEE Secure Develop. (SecDev). 2020, pp. 65–73.

[48] P. Otte, M. de Vos, and J. Pouwelse, ''Trust Chain: A sybil-resistant scalable blockchain,'' Future Gener. Comput. Syst., vol. 107, pp. 770–780, Jun. 2020.

[49] Y. Cai and D. Zhu, ''Fraud detections for online businesses: A perspective from blockchain technology,'' Financial Innov., vol. 2, no. 1, p. 20, Dec. 2016.

[50] M. Bellare, Z. Brakerski, M. Naor, T. Ristenpart, G. Segev, H. Shacham, and S. Yilek, ''Hedged public-key encryption: How to protect against bad randomness,'' in Proc. Int. Conf. Theory Appl. Crypto. Inf. Secure. Springer, 2009, pp. 232–249.