Blockchain: Literature Review

May 31, 2024

Abstract

This literature review provides an overview of the research on Blockchain. The review covers the following areas: Decentralized Financial Governance Applications, Blockchain-Enhanced IoT Security, Interoperable Atomic Ledger Models, Blockchain Transaction Scalability, and Blockchain-Based Consensus Systems. The review concludes by discussing the implications of the research for advancing blockchain technology across various sectors.

1 Introduction

Blockchain technology has revolutionized multiple sectors by providing decentralized, transparent, and secure frameworks for conducting transactions and managing data. The significance of blockchain lies in its ability to eliminate intermediary institutions, thereby economizing processes and enhancing security. This review aims to analyze the current state of research across five key areas: Decentralized Financial Governance Applications, Blockchain-Enhanced IoT Security, Interoperable Atomic Ledger Models, Blockchain Transaction Scalability, and Blockchain-Based Consensus Systems.

2 Background

Since its inception with Bitcoin, blockchain technology has attracted significant interest across various fields. It primarily gained prominence due to its promise of decentralized governance and tamper-proof transactions. As research in blockchain technology has matured, new applications and challenges have emerged, requiring a detailed examination of current research trends and future directions.

3 Literature Review

3.1 Decentralized Financial Governance Applications

Decentralized financial governance applications highlight blockchain's potential to revolutionize traditional financial systems [Witt et al., 2024, Rehak, 2024]. Decentralized Autonomous Organizations (DAOs) leverage blockchain to optimize human cooperation, exemplified by the Network Nervous System's (NNS) on-chain governance framework [Liu and Zhang, 2024]. Blockchain's integration in real estate investments via smart contracts and tokenization has been shown to mitigate administrative overhead and fraud [Joshi and Choudhury, 2024]. Additionally, blockchain enhances security and trust in trade finance through immutable and transparent transactions [Wu et al., 2024]. However, challenges remain in addressing potential power centralization [Rehak, 2024] and the feasibility of replacing existing financial systems [Zhao and Si, 2023]. Despite these concerns, blockchain's principles of decentralization, transparency, and trust continue to transform financial processes [Kumar, 2022, Shahrukh et al., 2023b].

3.2 Blockchain-Enhanced IoT Security

Blockchain's application in IoT security focuses on decentralized, immutable, and transparent properties to secure data exchanges [Zhang et al., 2022, Rahman et al., 2022]. Innovations include scalable decentralized ledger systems for large-scale networks [Xue et al., 2023] and secure data exchange architectures using BigchainDB, Tendermint, and IPFS [Kumar et al., 2023]. Lightweight consensus mechanisms address IoT's low computational power needs [Moudoud et al., 2022]. Despite potential benefits, challenges in scalability and resource demands persist, as seen in the convergence of blockchain with biometric recognition and distributed ledgers like IOTA [Ghafourian et al., 2023, Mamache et al., 2022]. Blockchain also ensures data integrity and security in healthcare IoT systems [Nabil et al., 2021, Zaman et al., 2021]. Furthermore, blockchain enhances trustless real-time transactions and data exchanges in data marketplaces and energy systems [Xu and Chen, 2021, Cioara et al., 2020], strengthening security and efficiency in decentralized IoT applications [Kiwelekar et al., 2021, Cioara et al., 2020].

3.3 Interoperable Atomic Ledger Models

Interoperable atomic ledger models offer mechanisms for secure and trusted smart contract execution in decentralized systems [Dargaye et al., 2024]. These models facilitate collaborative business processes across organizations, focusing on both entire process model execution and specific task monitoring [Köpke and Trattnig, 2023]. Byzantine Fault Tolerant Conflict-Free Replicated Data Types (BFT CRDTs) provide strong eventual consistency for distributed ledgers [Frey et al., 2024]. Multi-authority attribute-based encryption ensures privacy and interoperability in transaction systems [Marangone et al., 2023]. Leaderless architectures like DAG-based ledgers offer flexibility and performance but come with increased complexity [Camargo et al., 2023]. Interoperability is crucial for expanding blockchain applications in the financial sector, using protocols combining Trusted Execution Environments (TEE) with blockchains [Homoliak et al., 2023]. Effective blockchain programming languages must support policy specifications, access authorization, and workflow composition [Bernauer et al., 2023]. Platforms such as OpenDSU address interoperability needs across different blockchain solutions [Ursache et al., 2022].

3.4 Blockchain Transaction Scalability

Scalability challenges in blockchain primarily involve transaction throughput and storage capacity. Sidechains and off-chain computation have been proposed but often fall short due to security and efficiency concerns [Motaqy et al., 2024, Ivanov et al., 2021]. DAGs offer potential solutions to Miner Extractable Value (MEV) and systemic centralization issues [Raikwar et al., 2023]. Layer 2 (L2) systems offload transactions to enhance scalability, though they introduce added complexities [Bottoni et al., 2022]. Addressing latency in Proof of Work (PoW) networks involves estimating optimal block sizes [Wilhelmi et al., 2022] and understanding miner financial incentives [Gebraselase et al., 2021]. Public blockchains face transaction gridlock and high fees, with sharding and optimizations being explored to improve scalability [Ivanov et al., 2021, Wang et al., 2020]. Protocols like Horizon enable cross-chain transactions and gas-efficient asset transfers [Lan et al., 2021], while selective deletion methods aim to manage blockchain size growth [Hillmann et al., 2021]. Permissioned blockchains like Hyperledger Fabric require careful management of configuration complexities despite offering transparency and security benefits [Hua et al., 2020]. Ongoing research is vital for achieving scalable blockchain systems.

3.5 Blockchain-Based Consensus Systems

Consensus mechanisms are foundational to blockchain's decentralized trust model. Cryptocurrencies underpin blockchain technology, which is integral to Industry 4.0's requirements for decentralization, transparency, and security [Witter and Vit, 2024]. Consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) are central, with PoS addressing PoW's inefficiencies [Chen et al., 2023, Fernandez-Carames and Fraga-Lamas, 2024]. Ethereum demonstrates the versatility of blockchain with its Turing-complete smart contracts [Masumori et al., 2024]. However, challenges like PoW's high energy consumption and the necessity for secure off-chain communication persist [Sober et al., 2024, 2022]. Emerging consensus models such as proof of reputation (PoR) and BFT protocols focus on enhancing scalability and energy efficiency [Aluko and Kolonin, 2021, Berger et al., 2023, Rezabek et al., 2023]. Developing quantum-resistant cryptosystems is a priority to counter future threats [Fernandez-Carames and Fraga-Lamas, 2024]. Innovations like optimistic rollups and sharded blockchains target efficiency and cost reduction [Capretto et al., 2024, Taherpour and Wang, 2023]. Cross-chain communication and throughput improvements, as seen in interchain timestamping and zero-knowledge proofs, are essential for enhanced interoperability and security [Tas et al., 2023, Ellul and Pace, 2023]. The rise of DeFi and blockchain's application across sectors underscore the transformative potential of consensus mechanisms [Junior and Laurindo, 2024, Shahrukh et al., 2023a, Mahdi et al., 2023]. Continuing advancements in algorithmic design and cross-chain interoperability drive blockchain's evolution [Zeggari et al., 2022, Georghiades et al., 2022, Li and Wu, 2022].

4 Discussion

The reviewed literature highlights blockchain technology's significant advancements and challenges across various applications. Decentralized financial governance showcases blockchain's potential in optimizing traditional financial systems, although concerns about power centralization and replacement feasibility persist. In IoT security, blockchain proves advantageous, yet scalability and resource demands remain critical challenges. Interoperable atomic ledger models facilitate secure, trusted decentralized processes but require ongoing efforts to manage complexity and interoperability. Scalability in blockchain transactions faces fundamental challenges, with various solutions proposed, each with its benefits and limitations. Lastly, consensus mechanisms are foundational to blockchain's operation, with ongoing advancements aimed at enhancing scalability, efficiency, and security.

5 Conclusion

This literature review consolidates findings from key areas of blockchain research, emphasizing both the technology's potential and the challenges needing resolution. Future research should focus on addressing scalability issues, enhancing interoperability, and developing energy-efficient consensus mechanisms. Blockchain technology's ability to transform various sectors depends on overcoming these challenges and capitalizing on its core principles of decentralization, transparency, and security.

References

Oladotun Aluko and Anton Kolonin. Proof-of-reputation: An alternative consensus mechanism for blockchain systems, 2021. URL `https://arxiv.org/abs/2108.03542`.

Christian Berger, Signe Schwarz-Rüsch, Arne Vogel, Kai Bleeke, Leander Jehl, Hans P. Reiser, and Rüdiger Kapitza. Sok: Scalability techniques for bft consensus, 2023. URL `https://arxiv.org/abs/2303.11045`.

Alexander Bernauer, Sofia Faro, Rémy Hämmerle, Martin Huschenbett, Moritz Kiefer, Andreas Lochbihler, Jussi Mäki, Francesco Mazzoli, Simon

Meier, Neil Mitchell, and Ratko G. Veprek. Daml: A smart contract language for securely automating real-world multi-party business workflows, 2023. URL https://arxiv.org/abs/2303.03749.

Simone Bottoni, Anwitaman Datta, Federico Franzoni, Emanuele Ragnoli, Roberto Ripamonti, Christian Rondanini, Gokhan Sagirlar, and Alberto Trombetta. Qpq 1dlt: A system for the rapid deployment of secure and efficient evm-based blockchains, 2022. URL https://arxiv.org/abs/2208.07665.

Darcy Camargo, Luigi Vigneri, and Andrew Cullen. Managing write access without token fees in leaderless dag-based ledgers, 2023. URL https://arxiv.org/abs/2307.08627.

Margarita Capretto, Martin Ceresa, and Cesar Sanchez. Monitoring the future of smart contracts, 2024. URL https://arxiv.org/abs/2401.12093.

Junchao Chen, Suyash Gupta, Alberto Sonnino, Lefteris Kokoris-Kogias, and Mohammad Sadoghi. Resilient consensus sustained collaboratively, 2023. URL https://arxiv.org/abs/2302.02325.

Tudor Cioara, Claudia Pop, Razvan Zanc, Ionut Anghel, Marcel Antal, and Ioan Salomie. Smart grid management using blockchain: Future scenarios and challenges, 2020. URL https://arxiv.org/abs/2012.06256.

Zaynah Dargaye, Önder Gürcan, Florent Kirchner, and Sara Tucci-Piergiovanni. Towards secure and trusted-by-design smart contracts, 2024. URL https://arxiv.org/abs/2403.16903.

Joshua Ellul and Gordon J Pace. Active external calls for blockchain and distributed ledger technologies: Debunking cited inability of blockchain and dlt to make external calls, 2023. URL https://arxiv.org/abs/2302.01764.

Tiago M. Fernandez-Carames and Paula Fraga-Lamas. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks, 2024. URL https://arxiv.org/abs/2402.00922.

Davide Frey, Lucie Guillou, Michel Raynal, and François Taïani. Process-commutative distributed objects: From cryptocurrencies to byzantine-fault-tolerant crdts, 2024. URL https://arxiv.org/abs/2311.13936.

Befekadu G. Gebraselase, Bjarne E. Helvik, and Yuming Jiang. Effect of miner incentive on the confirmation time of bitcoin transactions, 2021. URL https://arxiv.org/abs/2111.02725.

Yanni Georghiades, Karl Kreder, Jonathan Downing, Alan Orwick, and Sriram Vishwanath. Scalable multi-chain coordination via the hierarchical longest chain rule, 2022. URL https://arxiv.org/abs/2112.11072.

Mahdi Ghafourian, Bilgesu Sumer, Ruben Vera-Rodriguez, Julian Fierrez, Ruben Tolosana, Aythami Moralez, and Els Kindt. Combining blockchain and biometrics: A survey on technical aspects and a first legal analysis, 2023. URL https://arxiv.org/abs/2302.10883.

Peter Hillmann, Marcus Knüpfer, Erik Heiland, and Andreas Karcher. Selective deletion in a blockchain, 2021. URL https://arxiv.org/abs/2101.05495.

Ivan Homoliak, Martin Perešíni, Patrik Holop, Jakub Handzuš, and Fran Casino. Cbdc-aquasphere: Interoperable central bank digital currency built on trusted computing and blockchain, 2023. URL https://arxiv.org/abs/2305.16893.

Song Hua, Shenbin Zhang, Bingfeng Pi, Jun Sun, Kazuhiro Yamashita, and Yoshihide Nomura. Reasonableness discussion and analysis for hyperledger fabric configuration, 2020. URL https://arxiv.org/abs/2005.11054.

Nikolay Ivanov, Qiben Yan, and Qingyang Wang. Blockumulus: A scalable framework for smart contracts on the cloud, 2021. URL https://arxiv.org/abs/2107.04904.

Shashank Joshi and Arhan Choudhury. Tokenization of real estate assets using blockchain, 2024. URL https://arxiv.org/abs/2405.01852.

Carlos Alberto Durigan Junior and Fernando Jose Barbin Laurindo. It strategic alignment in the decentralized finance (defi): Cbdc and digital currencies, 2024. URL https://arxiv.org/abs/2405.10678.

Arvind W. Kiwelekar, Pramod Patil, Laxman D. Netak, and Sanjay U Waikar. Blockchain-based security services for fog computing, 2021. URL https://arxiv.org/abs/2102.08896.

Mohit Kumar, Hritu Raj, Nisha Chaurasia, and Sukhpal Singh Gill. Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0, 2023. URL https://arxiv.org/abs/2307.13603.

Rishav Kumar. Role of blockchain in revolutionizing online transactional security, 2022. URL https://arxiv.org/abs/2206.04141.

Julius Köpke and Sebastian Trattnig. Transformation rules for the decentralization of a blockchain-extended global process model, 2023. URL https://arxiv.org/abs/2312.07388.

Rongjian Lan, Ganesha Upadhyaya, Stephen Tse, and Mahdi Zamani. Horizon: A gas-efficient, trustless bridge for cross-chain transactions, 2021. URL https://arxiv.org/abs/2101.06000.

Xiao Li and Weili Wu. Recent advances of blockchain and its applications, 2022. URL https://arxiv.org/abs/2208.07993.

Yulin Liu and Luyao Zhang. The economics of blockchain governance: Evaluate liquid democracy on the internet computer, 2024. URL https://arxiv.org/abs/2404.13768.

Syed Sarosh Mahdi, Zaib Ullah, Gopi Battineni, Muneer Gohar Babar, and Umer Daood. The telehealth chain: a protocol for secure and transparent telemedicine transactions on the blockchain, 2023. URL https://arxiv.org/abs/2310.18839.

Hamed Mamache, Gabin Mazué, Osama Rashid, Gewu Bu, and Maria Potop-Butucaru. Resilience of iota consensus, 2022. URL https://arxiv.org/abs/2111.07805.

Edoardo Marangone, Claudio Di Ciccio, Daniele Friolo, Eugenio Nerio Nemmi, Daniele Venturi, and Ingo Weber. Enabling data confidentiality with public blockchains, 2023. URL https://arxiv.org/abs/2308.03791.

Atsushi Masumori, Norihiro Maruyama, and Takashi Ikegami. Self-replicating and self-employed smart contract on ethereum blockchain, 2024. URL https://arxiv.org/abs/2405.04038.

Zahra Motaqy, Mohamed E. Najd, and Ghada Almashaqbeh. chainboost: A secure performance booster for blockchain-based resource markets, 2024. URL https://arxiv.org/abs/2402.16095.

Hajar Moudoud, Soumaya Cherkaoui, and Lyes Khoukhi. An iot blockchain architecture using oracles and smart contracts: the use-case of a food supply chain, 2022. URL https://arxiv.org/abs/2201.11370.

Shirajus Salekin Nabil, Md. Sabbir Alam Pran, Ali Abrar Al Haque, Narayan Ranjan Chakraborty, Mohammad Jabed Morshed Chowdhury, and Md Sadek Ferdous. Blockchain-based covid vaccination registration and monitoring, 2021. URL https://arxiv.org/abs/2109.10213.

Ziaur Rahman, Xun Yi, Sk. Tanzir Mehedi, Rafiqul Islam, and Andrei Kelarev. Blockchain applicability for the internet of things: Performance and scalability challenges and solutions, 2022. URL https://arxiv.org/abs/2205.00384.

Mayank Raikwar, Nikita Polyanskii, and Sebastian Müller. Fairness notions in dag-based dlts, 2023. URL https://arxiv.org/abs/2308.04831.

Rainer Rehak. A trustless society? a political look at the blockchain vision, 2024. URL https://arxiv.org/abs/2405.06097.

Filip Rezabek, Kilian Glas, Richard von Seck, Achraf Aroua, Tizian Leonhardt, and Georg Carle. Multilayer environment and toolchain for holistic network design and analysis, 2023. URL https://arxiv.org/abs/2310.16190.

Md. Raisul Hasan Shahrukh, Md. Tabassinur Rahman, and Nafees Mansoor. Aid nexus : A blockchain based financial distribution system, 2023a. URL https://arxiv.org/abs/2311.08372.

Md. Raisul Hasan Shahrukh, Md. Tabassinur Rahman, and Nafees Mansoor. Exploration of hyperledger besu in designing private blockchain-based financial distribution systems, 2023b. URL https://arxiv.org/abs/2311.08483.

Michael Sober, Max Kobelt, Giulia Scaffino, Dominik Kaaser, and Stefan Schulte. Distributed key generation with smart contracts using zk-snarks, 2022. URL https://arxiv.org/abs/2212.10324.

Michael Sober, Giulia Scaffino, and Stefan Schulte. Cross-blockchain communication using oracles with an off-chain aggregation mechanism based on zk-snarks, 2024. URL https://arxiv.org/abs/2405.08395.

Amirhossein Taherpour and Xiaodong Wang. Hybridchain: Fast, accurate, and secure transaction processing with distributed learning, 2023. URL https://arxiv.org/abs/2310.08839.

Ertem Nusret Tas, Runchao Han, David Tse, Fisher Yu, and Kamilla Nazirkhanova. Interchain timestamping for mesh security, 2023. URL https://arxiv.org/abs/2305.07830.

Cosmin Ursache, Michael Sammeth, and Sînică Alboaie. Opendsu: Digital sovereignty in pharmaledger, 2022. URL https://arxiv.org/abs/2209.14879.

Xiangyu Wang, Ting Yang, and Yu Wang. State sharding model on the blockchain, 2020. URL https://arxiv.org/abs/2010.16034.

Francesc Wilhelmi, Sergio Barrachina-Muñoz, and Paolo Dini. End-to-end latency analysis and optimal block size of proof-of-work blockchain applications, 2022. URL https://arxiv.org/abs/2202.01497.

Leon Witt, Armando Teles Fortes, Kentaroh Toyoda, Wojciech Samek, and Dan Li. Blockchain and artificial intelligence: Synergies and conflicts, 2024. URL https://arxiv.org/abs/2405.13462.

M. Witter and A. Rodrigo De Vit. Blockchain e sistemas distribuídos: conceitos básicos e implicações, 2024. URL https://arxiv.org/abs/2403.14854.

Hanjie Wu, Qian Yao, Zhenguang Liu, Butian Huang, Yuan Zhuang, Huayun Tang, and Erwu Liu. Blockchain for finance: A survey, 2024. URL https://arxiv.org/abs/2402.17219.

Ronghua Xu and Yu Chen. Fed-ddm: A federated ledgers based framework for hierarchical decentralized data marketplaces, 2021. URL https://arxiv.org/abs/2104.05583.

Lide Xue, Wei Yang, and Wei Li. A scale-out decentralized blockchain ledger system for web3.0, 2023. URL https://arxiv.org/abs/2312.00281.

Shakila Zaman, Muhammad R. A. Khandaker, Risala T. Khan, Faisal Tariq, and Kai-Kit Wong. Thinking out of the blocks: Holochain for distributed security in iot healthcare, 2021. URL https://arxiv.org/abs/2103.01322.

Marwan Zeggari, Renaud Lambiotte, Aydin Abadi, Louise Axon, and Mohamad Kassab. An efficient and decentralized blockchain-based commercial alternative (full version), 2022. URL https://arxiv.org/abs/2210.08372.

Ruipeng Zhang, Chen Xu, and Mengjun Xie. Secure decentralized iot service platform using consortium blockchain, 2022. URL https://arxiv.org/abs/2209.12145.

Xiongfei Zhao and Yain-Whar Si. Challenges of blockchain adoption in financial services in china's greater bay area, 2023. URL https://arxiv.org/abs/2312.15573.