A systematic literature review on Security in Blockchain technology-based applications

S. Senthil kumar
School of Arts and Science, AV Campus, VMRF, Chennai-603104, India
S. Rajaprakash
Department of Computer science and Engineering, AVIT, VMRF, Chennai-603104, India

Abstract:

The evolution of modern internet technologies necessitates data security. The essential development of modern internet technology is digital information. Blockchain technology is the backbone of a new sort of internet that allows digital information to be distributed yet not replicated. The backbone of a new type of internet was established by block chain technology, which allows all transactions to be stored in immutable records and spread over multiple participant nodes. The use cases for block chain technology are rapidly expanding, with the primary goal of enabling Authentication, data integrity, and secure data sharing. This study's goal is to give a comprehensive overview of the literature on the use of Block chain as a base technology for protecting both financial and non-financial applications. The goal is to aims to see if Blockchain technology can deliver the needed security solutions in a variety of applications. Previous research is evaluated for its benefits, problems, and solutions. Integrity, Availability, Authenticity, Accountability, and Reliability are terms that apply to information were among the topics covered in the poll. The study concludes that Blockchain technology has potential for both financial and non-financial industries because it can address the majority of security concerns. Future research should focus on putting the proposed solutions outlined in the security issues of Blockchain technology into practice.

Keywords: Blockchain, distributed, Authentication, data integrity

1. INTRODUCTION

Using an open distributed ledger, the blockchain built on cryptographic techniques that may record transactions and make them tamper-proof between one or more parties. The records are kept in blocks and connected by links. Using a peer-to-peer network called blockchain, the records are The blockchain is an open, distributed ledger that uses cryptographic methods to preserve transactions between two or more parties that cannot be altered in any way. Blockchain is a peer-to-peer technology that distributes data rather than storing it centrally. The information is shared among the many node participants. When Satoshi Nakamoto created Bitcoin as a currency in 2008, the blockchain idea became more well-known [2]. According to the author of [3], sophisticated countries like Japan have begun to commercialise bitcoins (blockchain kind). Additionally, it has an impact on global currency markets [4]. Blockchain is now much more valuable than just a decentralised cryptocurrency due to its special characteristics. It has grown into something more, and other blockchain platforms with public and private accessibility, including Ethereum [5] and Hyperledger Fabric [6] have also gained a lot of traction.

2. SECURITY CHALLENGES

In this section, we spoke about the findings drawn from the articles that were chosen and prepared using different security concerns. Table IV lists the papers that were chosen, the security issues they addressed, and the application domain.

Key Findings, Security Aspects, and Applications Area of Selected Papers are listed in Table IV.

Paper	Important qualitative and numerical data reported	Security Aspects	Area
[8]	JP Morgan Blockchain Banking Information Network	Integrity, privacy, and access control	Banking Sector
[9]	Supply chain systems by IBM	Access control, Privacy and integrity	Supply chain systems
[12]	Programming language Solidity reentrancy attack	Validity	Smart Contracts
[23]	Energy trading on a decentralized smart grid without the use of trusted third parties requires transaction security.	Privacy	Smart grids
[24]	Blockchain protects user privacy and offers a decentralized storage system for access control.	Privacy, Access Control	IoT
[26]	A blockchain-based architecture for secure and private transportation	Privacy	Smart Vehicles
[27]	Denial of Service attack in blockchain	eventual likelihood of having a lesson available	Generic
[28]	With the use of blockchain, many people can exchange resources in a public and decentralized setting while maintaining their privacy.	Privacy	Smart Communities
[29]	By leveraging blockchain, privacy is maintained while data is transferred between PSN nodes.	Privacy	Healthcare System
[30]	Determining IP address and Bitcoin address ownership links.	Anonymity	Bitcoin
[31]	a payment system that protects anonymity for grid networks.	Privacy	IoT
[31]	a payment system for vehicle-to-grid networks that protects privacy.	Privacy	IoT
[32]	On the blockchain, user information is displayed in order to increase transaction flow transparency.	Privacy not provided	Bit coin
[34]	Based on blockchain PKI	Privacy	Generic
[35]	A blockchain called Credit coin safeguards the anonymity of drivers in linked cars.	Privacy	Smart Vehicles
[36]	One option to increase the reliability of data is to use blockchain technology and data provenance systems.	Trust	IoT
[37]	To securely store data, employ certificate-less cryptography.	Privacy, Authentication	Large scale IoT
[38]	Blockchain-based decentralized token-based energy trading system.	Privacy	Energy Trading System
[39]	trial process to confirm data integrity	Data Integrity	Biomedical Research

[40]	here have been instances of attacks like Man in the Middle, Syn Flood, Sybil Attack, Timing Errors, Key Management, and Audit Server Attacks. Record integrity is ensured by blockchain technology.	Records authenticity and data integrity could be impacted..	Land Registry
[41]	The IoT architecture incorporates blockchain at every layer.	Data Integrity	Smart City
[42]	Using blockchain to ensure data integrity	Data Integrity	IoT
[43]	For the IoT firmware, a reference integrity metric (RIM) is kept for	Data Integrity	IoT
[44]	It is explained how to corrupt a blockchain using a 51 percent attack.	eventual opportunity to keep integrity lesson	Bitcoin
[45]	Double spending attack	chance to maintain integrity lesson eventually	Generic
[46]	Splunk, which uses blockchain to ensure data fidelity	Data Integrity	Banking
[47]	ProvChain will increase authenticity and privacy in the cloud environment.	Authentication, Privacy	Cloud
[48]	The use of a blockchain-based PKI in air traffic management enables a secure broadcast authorization connection with air traffic services.	Authentication	Air Traffic Management
[49]	Quantum attack	Authentication process may be affected	Generic
[50]	The system only accepts connections from authorized users.	Authorization	Generic
[51]	IP addresses were used to link the formation of identities in blockchain.	Accountability	Generic
[52]	a proof-of-concept architecture for a distributed access control system for the Internet of Things	Access Management	IoT
[53]	Using blockchain for trusted exchange of IOT data	Access Management, Integrity, Privacy	IoT
[54]	Blockchain is integrated into a personal data management platform as a trustless automatic access control manager.	Privacy, Access Control	Generic
[55]	Systems that mix edge computing with blockchain can offer dependable network access.	Access Control	Generic
[56]	a blockchain-based multi-layer network model that is secure	Identity Management, Authentication, Privacy	IoT
[58]	When Blockchain Meets Supply Chain: A Systematic Review of the Literature on Recent Advances and Future Applications	Handle a number of technical concerns connected to block chains, including performance, security, scalability, and interoperability.	Supply chain management

[59]	A new kind of blockchain for VANET's safe message exchange	Decreasing block generation time and increasing the vehicle network's capacity for growth.	Vehicular Ad-hoc Networks
[60]	A systematic literature review of blockchain cyber security	The surrounding cryptography and certification systems are safely managed by blockchain.	Cyber security
[61]	A systematic literature review of blockchain cyber security	Blockchain Network latency and power consumption to sustain the distributed network were frequently discussed in research on IoT security using blockchain applications.	Digital communications and networks

3. CONCLUSION

The study and development of blockchain technology are only beginning. Research on security and cryptographic systems has grown dramatically during the last few years. It will tremendously benefit both the financial and non-financial sectors. Shared data, security, and dependability will all be taken into account concurrently. The goal is to examine various blockchain applications in order to analyze the potential security advantages and difficulties of blockchain technology. We have developed and addressed three research questions to support our study in order to offer direction for future research. Finally, we can assert that the block chain’s distributed mechanism, password system, and protected hashing process present a completely new perspective for the development of Internet data security technology. Financial and non-financial applications already in use are, therefore, benefit from the security solutions offered by blockchain technology.

REFERENCES

[1] M. Pilkington, “Blockchain Technology: Principles and Applications,” in Research Handbook on Digital Transformations, 2016. [online] Available: https://ssrn.com/abstract=2662660

[2] Nakamoto, S., 2012. Bitcoin: A peer-to-peer electronic cash system, Oct, 2008.

[3] Bitcoin Could Be Accepted at 300,000 Japanese Stores in, 2017.

[4] S. Chen, C.Y.-H. Chen, W.K. Hrdle, T.M. Lee, B. Ong, Chapter 8 – Econometric Analysis of a Cryptocurrency Index for Portfolio Investment BT - Handbook of Blockchain, Digital Finance, and Inclusion, vol. 1, Academic Press, 2018, p. 175206.

[5] G. Wood, Ethereum: a Secure Decentralized Generalized Transaction Ledger Yellow Paper, Ethereum Project. Yellow Pap., 2014, p. 132.

[6] V. Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, Etherum, 2014 [Online]. Available: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[7] Global Blockchain Technology Market (2018-2023),Ntescribe (India) Pvt. Ltd., May 2018. ID: 4593797

[8] Martin Arnold, Five ways banks are using blockchain. OCTOBER 16,2017. [Online]. Available:

[9] https://www.ft.com/content/615b3bd8-97a9-11e7-a652-cde3f882dd7b

[10] Bernard Marr, How Blockchain Will Transform the Supply Chain and Logistics Industry , March 2018, [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchainwill-transform-the-supply-chain-and-logistics-industry/#359010b95fec

[11] Sunil K (2018) Value Creation through Blockchain Technology in Supply Chain Management. J Inform Tech Software Eng. 8: 1000248. doi: 10.4172/2165-7866.1000248

[12] K. Megget, Securing the supply chain, Pharma Times magazine - March2018.[Online]Available: http://www.pharmatimes.com/magazine/2018/march 2018/securing th e supply chain

[13] R.M. Parizi, Amritraj, A. Dehghantanha, Smart contract programming languages on blockchains: an empirical evaluation of usability and security, in: International Conference on Blockchain, Seattle, USA, 2018, pp. 75–91.

[14] Roger Aitken, Smart Contracts on the Blockchain: Can Businesses Reap the Benefits. [Online] Available:

[15] https://www.forbes.com/sites/rogeraitken/2017/11/21/smart-contracts-o n-the-blockchain-can-businesses-reap-the-benefits/#2be0ee110744

[16] Adewale Omoniyi, Convergence of Blockchain and Cybersecurity - IBM Government Industry Blog. December 2, 2017. Online Available:https://www.ibm.com/blogs/insights-on-business/government/convergence-blockchain-cybersecurity/

[17] A. Alketbi, Q. Nasir, M. A. Talib, Blockchain for Government Services- Use Cases, Security Benefits and Challenges, IEEE 2018. Pp 112 -119.

[18] M. Conoscenti, A. Vetr, J.C. De Martin, Blockchain for the internet of things: a systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, p. 16.

[19] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, where is current research on Blockchain technology? - a systematic review, PLoS One 11 (10) (2016) 127.

[20] S. Seebacher, R. Schritz, Blockchain technology as an enabler of service systems: a structured literature review, in: Exploring Services Science, 2017, p. 1223.

[21] F. Dai, Y. Shi, N. Meng, L. Wei, Z. Ye, From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security Issues, in the 4th International Conference on System and Informatics, 2017, pp. 975-979.

[22] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: a state-of-the-art survey, in: IEEE

[23] Communications Surveys & Tutorials, 2018, https://doi.org/10.1109/COMST.2018.2863956.

[24] P. J. Taylor, T. Dargahi , A. Dehghantanha , R. M. Parizi ,K. K. R. Choo, A systematic literature review of blockchain cyber security, in Digital Communication Network, ScienceDirect, Feb 2019.

[25] B. Kitchenham, S. Charters, Guidelines for Performing Systematic Literature Reviews in Software Engineering, in: Engineering, vol. 2, 2007, p. 1051.

[26] N. a. S. D. Aitzhan, "Security and Privacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and Anonymous Messaging Streams," IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, pp. 1-1, 12 October 2016.

[27] S. H. F. F. R. P. C. R. H. Hashemi, "World of Empowered IoT Users,"in First International Conference on Internet-of-Things Design and Implementation (IoTDI), Berlin, Germany, 2016.

[28] W. Ejaz and A. Anpalagan, Internet of Things for Smart Cities, SpringerBriefs in Electrical and Computer Engineering, oct 2018. https://doi.org/10.1007/978-3-319-95037-2_5

[29] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, BlockChain: A Distributed Solution to Automotive Security and Privacy, IEEE

[30] Communications Magazine • December 2017,

[31] 10.1109/MCOM.2017.1700879

[32] Hon, W. K. Palfreyman, J. and Tegart, M, A White paper on Distributed Ledger Technology & CybersecurityImproving information security in the financial sector by European Union Agency for Network and

[33] Information Security (ENISA), 2016.978-92-9204-200-4, 10.2824/80997.

[34] P. R. J. a. L. K. Kianmajd, "Privacy-Preserving Coordination for Smart Communities," in IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), San Francisco, CA, USA, 2016.

[35] J. X. N. a. H. X. Zhang, "A Secure System for Pervasive Social Network-Based Healthcare," Special Section on Trust Management in Pervasive Social Networking (TruPSN), 29 December 2016.

[36] P. K. D. a. M. P. Koshy, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," in International Conference on Financial Cryptography and Data Security. FC 2014: Financial Cryptography and Data Security, Christ Church, Barbados, 2014.

[37] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, “A Blockchain-Based Privacy-Preserving Payment Mechanism for

[38] Vehicle-to-Grid Networks, IEEE network,2018, Digital Object Identifier: 10.1109/MNET.2018.1700269.

[39] A. M. A. S. E. W. Z. P. C. Kosba, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in In Proceedings of the 2016 IEEE Symposium on Security and Privacy, SP '16, 2016.

[40] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE 6th International Congress on Big Data, pp 557-564.

[41] L. Axon, M. Goldsmith, PB-PKI: A Privacy-aware Blockchain-based PKI in proceedings of the 14th International Joint Conference on e-Business and Telecommunications, Vol 4, pp 311-318, 2017.

[42] L. Li et al., CreditCoin:A privacy –preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles, IEEE Transactions on Intelligent Transportation Systems, 2018 DOI: 10.1109/TITS.2017.2777990.

[43] Marten Sigwart, Michael Borkowski, Marco Peise, Stefan Schulte, and Stefan Tai. 2019. Blockchain-based Data Provenance for the Internet of Things. In Proceedings of 9th International Conference on the Internet of

[44] Things (IOT'19). ACM, New York, NY, USA, 8 pages.

[45] https://doi.org/10.1145/nnnnnnn.nnnnnnn

[46] R. Li, T. Song, B. Mei, H. Li, X. Cheng, L. Sun, Blockchain for Large Scale Internet of Things: Data Storage and Protection, IEEE Transaction on services computing, 2018.

[47] Z. Li,J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, IEEE Transactions on Industrial Informatics, 2017.

[48] H. Dai, H Patrick Young, "TrialChain: A Blockchain-Based Platform to Validate Data Integrity in Large, Biomedical Research Studies ", published in ArXiv 2018.

[49] V. L. Lemieux, "Trusting records: is Blockchain technology the answer?" Records Management Journal, vol. 26, no. 2, pp. 110-139, 2016.

[50] K. a. M. V. Biswas, "Securing Smart Cities Using

[51] BlockchainTechnology,"in IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems, Sydney, NSW, Australia, 2016.

[52] X. L. Y. S. C. X. X. a. L. Z. B. Liu, "Blockchain based Data Integrity Service Framework for IoT data," in IEEE 24th International Conference on Web Services, 2017.

[53] J. L. K.-K. C. M. Banerjee, "A blockchain future to Internet of Thingssecurity: A position paper," in Digital Communications and Networks, 2017.

[54] J. J. Xu, "Are blockchains immune to all malicious attacks?" Xu Financial Innovation, 2016.

[55] C. R. C. Pinzon, "Double-spend Attack Models with Time Advantange for Bitcoin," Electronic Notes in Theoretical Computer Science (ENTCS), vol. 329, no. C, pp. 79-103, December 2016.

[56] N. Mckervey, Advanced Data Integrity with Blockchain. Online:

[57] https://www.splunk.com/blog/2018/09/24/the-newest-data-attack.html

[58] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. credNjilla,ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability, 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp 468-477.

[59] R. J. Reismann, Air traffic Management Blockchain Infrastructure for Security, Authentication and Privacy, by NASA Ames Research Center in AIAA SciTech Forum, 7-11 Jan 2019. DOI: 10.2514/6.2019-2203.

[60] W. Yin, Q. Wen, W. Lin, H. Zhang, Z. Jin, An Anti-quantum Transaction Authentication Approach in Blockchain.IEEE Access Vol 14, August 2015.

[61] T. a. I. H. Sanda, "Proposal of New Authentication Method in Wi-FiAccess Using Bitcoin 2.0," in 5th Global Conference on Consumer Electronics, Kyoto, Japan, 2016.

[62] R. O. G. Dennis, "Rep on the block: A next generation reputation system based on the blockchain," in 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 2015.

[63] O. Novo, Blockchain Meets IoT:an Architechture for Scalable Access Management in IoT, IEEE journal of Internet of Things, Vol.14, No.8, March 2018.

[64] Z. Huang, X. Su,Y. Zhang, C. Shi, L. Xie, A Decentralized Solution for IoT Data Trusted Exchange Based on Blockchain, published in 3rd IEEE International Conference on Computer and Communications, pp-1180-1184,2017.

[65] G. N. O. P. A. Zyskind, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in Security and Privacy Workshops (SPW), 2015 IEEE, San Jose, CA, USA, 2015.

[66] R. Yang, F. R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated Blockchain an Edge Computing Systems: A survey, Some Reseacrh Issues and Challenges, in IEEE Communication Surveys and Tutorials, Volume 21, issue 2, secondquarter 2019, pp 1508-1532.

[67] C. Li, L. J. Zhang, A blockchain based New secure Multi-Layer Network Model for Internet of Things, 2017 IEEE International Congress on Internet of Things (ICIOT), pp 33-41.

[68] E. Piscini,D. Dalton, L. Kehoe , Blockchain and cyber security, De loitte EMEA Grid Blockchain Lab,2018. Available:

[69] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gra-Changingthegameoncyberrisk.pdf.

[70] "SHUCHIH E. CHANG AND YICHIAN CHEN" When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications, IEEE journal, Vol.8, March 2020

[71] Rakesh Shrestha a, Rojeena Bajracharya b , Anish P. Shrestha c , Seung Yeob Nam b,*: A new type of blockchain for secure message exchange in VANET, Digital Communications and Networks 6 (2020) 177–186.

[72] Paul J. Taylor a, Tooska Dargahi a, Ali Dehghantanha b , Reza M. Parizi c , Kim-Kwang Raymond Choo d,: A systematic literature review of blockchain cyber security, Digital Communications and Networks · February 2019.

[73] Martin Westerkamp, Friedhelm Victor, Axel Küpper: Tracing manufacturing processes using blockchain-based token compositions. Digital communications and networks Volume 6, issue2, MAY 2020.

[74] Chavan, Amrita B., and K. Rajeswari. "The design and developement of decentralized digilocker using blockchain." *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)* 9 (2019): 29-36.

[75] Miraz, Mahadi Hasan, et al. "The Innovation of blockchain transparency & traceability in logistic food chain." *International Journal of Mechanical and Production Engineering Research and Development (IJMPERD)* 10.3 (2020): 9155-9170.

[76] Miraz, Mahadi Hasan, et al. "Factors Affecting Consumers Intention to Use Blockchain-Based Services (BBS) in the Hotel Industry." *International Journal of Mechanical and Production Engineering Research and Development (IJMPERD)* 10.3 (2020): 8891-8902.

[77] Ravi, Srivel, Arokiaraj David, and Mohammed Imaduddin. "Controlling & calibrating vehicle-related issues using RFID technology." *International Journal of Mechanical and Production Engineering Research and Development* 8.2 (2018): 1125-1132.

[78] Bangar, Ashwini, and Swapnil Shinde. "Study and comparison of cryptographic methods for cloud security." *Int J Comput Sci Eng Inf Technol Res* 4.2 (2014): 205-213.

[79] Wadhwani, Priyanka, Akanksha Gaur, and Vipin Jain. "Cryptanalytic JH and Blake Hash Function for Authentication and Proposed Work Over Blake-512 on C Language." *International Journal of Computer Science Engineering and Information Technology Research* 4 (2014): 187-198.