Blockchain Technology in Cybersecurity Management

[1]Centre for Advanced and Smart Systems (CAST), University of Northampton, UK,
[2]University of Warwick Coventry UK,
Michael.OpokuAgyeman@northampotn.ac.uk

Abstract: Blockchain is a decentralised ledger used to secure digital currency, perform deals and transactions. A new transaction is validated when each member of network has access to the latest copy of the encrypted ledger. The features of blockchain are immutability, trackability, trustworthiness and decentralisation. This paper explores the concept, characteristics and the need for blockchain in cybersecurity management. Blockchain is based on cryptography to ensure trust in transactions. Blockchain technologies made a remarkable contribution in Cybersecurity.

Keywords: Blockchain, Cybersecurity, Cyberattacks, Cyberthreat.

1 Introduction

Over the years the emergence of cyber threats and the increased frequency of cyberattacks reinforced the need for cybersecurity initiatives. Solutions has been proposed to address cyber threats, one of such is blockchain technology. Blockchain is a technology that provides secure records validated by algorithms thereby encouraging trust on peer-to-peer networks [1]. Traditional security methods support preserving privacy and security however, their centralised nature with low computational capabilities makes them less efficient [2]. Blockchain technology has been adopted in many applications to strengthen security issues in a decentralised manner. It eliminates the need for password which is described as the weakest link in cybersecurity [3]. Blockchain is an emerging technology for cybersecurity, it has been the subject of many researches. Blockchain is a method for securing data through decentralized and peer to peer systems [4]. The use of blockchain has been applied to core business processes like banking [5], logistics [6], pharmaceutical industry [7], smart contracts [8] and most importantly cybersecurity.

Blockchain is an emerging technology for cybersecurity, it has been the subject of many researches in recent years. Blockchain is a distributed ledger that provides opportunity for data protection through decentralised identity. The ledger system makes information transparently available to members of the blockchain. It has gained traction in different application fields with focus on creating trust. Blockchain is used in cases where data requires trust without the need for third-party verification.

Blockchain use cases have emerged in areas such as healthcare. With patients data on blockchain, organisations can work together to improve care while patients privacy is protected [13]. In pharmaceutical industry, Blockchain can add traceability to drug supply thereby increasing the success rate of clinical trials. In a supply chain digitising paper based processes makes data shareable and trustworthy. It adds intelligence and automation to execute transactions [14]. In a loan process, consent for access to personal records is granted on the blockchain. Trust in the automated process for evaluating loan applications helps to drive closing faster and improve customer satisfaction [15]. Blockchain is a digital ledger that has the ability to be programmed to anything of value. The use of blockchain gained interest for its distinguished cybersecurity capabilities, resulting in many organisations becoming interested in using its security infrastructure to safeguard their information security systems [25]. With Blockchain, if an application needs to manage sensitive information it is solved by protecting a node, if the node is compromised, cybersecurity is threatened [16].

Blockchain technology has been applied in the use of Ethereum to advertise blacklisted internet protocols (IPs) that were suspected to be involved in Distributed Denial of service attacks (DDoS) [17]. Implementing security with blockchain is demonstrated in terms of confidentiality, integrity and availability. Blockchain technology offers a decentralized storage that can store data without the need of a single trusted party. Information is managed through a distributed ledger where nodes maintaining the ledger do not need to be mutually trusted, trust is distributed among all nodes. To add data to the ledger, a consensus is needed to be reached among all involved nodes. It possesses several features such as decentralization, immutability and validation [18].

Using blockchain technology for identity management links digital identity to a device IP address. Digital identities are secured using the principle of public and private key cryptography. A generated digital identity presents the verified identifier in the form of a QR-code or a digital certificate. Blockchain technology encourages secure communication thereby increasing trust when carrying out a transaction [19]. It utilizes peer-to-peer networks and distributed systems which include registers to store transactions. Blockchain security protects transactions against internal, malevolent and unintentional threats [20]. The core concept and unique property of Blockchain technology makes it attractive for business and cybersecurity. Protecting information through a decentralised technology tend to be more secure as it undergoes verification processes. When using blockchain the threshold of data veracity is higher [21]. Blockchain is an evolving technology that is finding traction in several areas such as banking [22], logistics [23], pharmaceutical industry [24], defence of IoT devices [32] and cybersecurity. It is a decentralized database that generates a digital log of trusted transactions that create reliability and reduce risk when a business is entered with an unfamiliar party. It can be shared across a public or private network that provides transparent and verifiable cybersecurity system. With blockchain, documentation of transactions can be verified by participating users in the Blockchain network [19]. Items can be tracked in a supply chain for traceability across companies using Blockchain. The operating process is similar to an IT process in a large organisation where compliance inspection and certificate issuing is performed. The supplier and receiver must trust the information along the supply route, this is an ideal Blockchain scenario. While using Blockchain and there is an attempt to incorporate unregistered software, it will be flagged [25]. The security qualities of blockchain are cryptography, software-mediated consensus, public and private keys, contracts and identity controls. This qualities offer integrity and data protection by verifying and authenticating transaction records and maintaining traceability and privacy [26]. The emerging trend of blockchain could enable decentralized applications without intermediaries, this could serve as a foundation for internet security.

2 Related Research on Blockchain in Cybersecurity Management

This study focused on existing approaches of Blockchain to provide cybersecurity. Blockchain was initially conceived as a financial protocol in the form of bitcoin. In view of its security capabilities researchers began to focus on blockchain to address privacy and security issues. Blockchain integrates several components such as a distributed data storage, consensus mechanisms and encryption algorithms. It separates data randomly and distributes them across an entire network of computers [27]. Features of blockchain technology include trustworthiness, trackability and immutability. According to Bansal et al's [28] survey on Blockchain for cybersecurity in the field of IoT, Blockchain can authenticate users by creating a decentralised system to provide interaction among users. By using blockchain technology security, reliability and transparency is provided to users through optimization and revolutionisation which is present in blockchain technology.

According to Vance et al. [29] Blockchain solutions provide protection against persuasive phishing and social engineering using digital identities to enable safer IoT devices to prevent DDoS attacks. Alotaibi [30] explored cybersecurity relating to IoT and utilized end to end traceability, data privacy, anonymity, identity management, authentication, confidentiality, data integrity and availability. Initiatives like GUITAR and REMOWARE allow IoT devices to be updated in real-time. Blockchain supports a variety of functions, it can be installed in a smart home to enhance cybersecurity [11].

Alkadi et al. [32] discussed intrusion detection, Blockchain and data centralization in the cloud. Centralizing data in the cloud offers capabilities to protect consumer privacy. They proposed Blockchain implementation in information trust management in the cloud as the volume of information stored on the cloud is over-whelming, it cannot be processed by conventional methods alone. Lack of trust between IoT devices is solved by a decentralized Ethereum Blockchain that enables the survey of information from the Industrial Internet of Things to the cloud Fan et al. [12]. Wang et al. [13] reviewed a study on Blockchain for IoT and proposed a distributed and decentralized approach that promises IoT security.

Mittal et al. [22] explored cybersecurity enhancement through Blockchain training via a serious game approach and proposed an adaptive sandbox game which educates the players on the importance of Blockchain. Their approach provided skill advancement and a greater learning outcome which can be adopted by a large work force. Serrano et al. [37] presented a blockchain random neural network for cybersecurity and proposed a method that enables a decentralised authentication method. Their validation result proved that adding blockchain random neural network provides user access control algorithm with increased cybersecurity resilience

3 The use of Blockchain to improve Cybersecurity

Blockchain is a ledger technology with potential blockchain based characteristics such as decentralization and immutability that ensures authenticity, verifiability, reliability and integrity of data. When credibility of data can be ensured, trust worthy outcomes can be produced. This section gives a brief view on use cases of blockchain in data protection, privacy and security.

- Data Storage and sharing- Blockchain ensures that data stored in the cloud is resistant to unauthorized change. It utilizes public and private ledger to protect data from tampering, the hash list allows data to be securely stored. Blockchain ensures that exchanged data is verified as being the same from dispatch to receipt [38].
- Network security-Blockchain authenticates and store data in a decentralized and robust manner. Blockchain uses public and private architecture for point to point communication between nodes in the network to make blockchain appropriate to address network security issues [29].
- Navigation of the world wide web-Blockchain is used to improve the validity of the wireless internet access points thereby monitoring the access control on the local ledger. It ensures the validity of World Wide Web by navigating to correct web pages through accurate DNS records and communicate with others through secure encrypted methods [4].
- Intrusion detection- Blockchain can be used to detect malicious behaviour in a network environment [39].
- Securing transactions-Blockchain is used to secure electronic transactions particularly sensitive data. Blockchain utilises encryption and hashing to store immutable records [20

4 Conclusion

In conclusion, Blockchain improves data storage by creating a decentralized network that uses client-side encryption such that data owners will have traceable control of their data. The innovative features of Blockchain make it ideal for today's cybersecurity needs, it can be used to prevent identity theft by verification through a decentralized identity system. Blockchain technology can be used to prevent data breaches, identity theft and cyberattacks by improving cyber defense through consensus mechanisms. Blockchain technology can be used in companies to authenticate users without password thereby eliminating human intervention and preventing potential stacks vectors. Blockchain is gaining traction in data assurance thereby implementing trustworthy and secure data infrastructures. Although blockchain provide advantages in cybersecurity, it also comes with disadvantages such high energy consumption required to keep a ledger and ensure transparency. The initial capital cost is high. Blockchain secures IoT through reliable authentication and data transfer. For a start, businesses could go for a private Blockchain that can serve as a platform for technology.

References

1. G.R. Carrara, L.M. Burle, D.S. Medeiros, de Albuquerque, C.V.N. and D.M. Mattos, 2020. Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. *Annals of Telecommunications*, *75*(3), pp.163-174.
2. R. Zhang, R. Xue, and L. Liu, 2019. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, *52*(3), pp.1-34.
3. N. Kshetri, 2017. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications policy*, *41*(10), pp.1027-1038.
4. P.J. Taylor, T. Dargahi, A. Dehghantanha, R.M. Parizi, and K.K.R.v, 2020. A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), pp.147-156.
5. H. Hassani, X. Huang, and E. Silva, 2018. Banking with blockchain-ed big data. *Journal of Management Analytics*, *5*(4), pp.256-275.
6. E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, 2019. Blockchain technology implementation in logistics. *Sustainability*, *11*(4), p.1185.
7. I. Haq, and O.M. Esuka, 2018. Blockchain technology in pharmaceutical industry to prevent counterfeit drugs. *International Journal of Computer Applications*, *180*(25), pp.8-12.
8. L.W. Cong, and Z. He,, 2019. Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*(5), pp.1754-1797.

9. P.T. Duy, D.T.T. Hien, and V.H. Pham,, 2020. A survey on Blockchain-based applications for reforming data protection, privacy and security. *arXiv preprint arXiv:2009.00530*.
10. D. Yaga, P. Mell, N. and K. Scarfone, 2019. Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.
11. T. R. Vance and A. Vance, "Cybersecurity in the blockchain era: A survey on examining critical infrastructure protection with blockchain-based technology," in *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*. IEEE, 2019, pp. 107–112.
12. K. Fan, Z. Bao, M. Liu, A. V. Vasilakos, and W. Shi, "Dredas: Decen- tralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial iot," *Future Generation Computer Systems*, vol. 110, pp. 665–674, 2020.
13. Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the iot and industrial iot: A review," *Internet of Things*, vol. 10, p. 100081, 2020.
14. C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: a systematic review," in *Healthcare*, vol. 7, no. 2. Multi- disciplinary Digital Publishing Institute, 2019, p. 56.
15. P. Sylim, F. Liu, A. Marcelo, P. Fontelo *et al.*, "Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention," *JMIR research protocols*, vol. 7, no. 9, p. e10163, 2018.
16. P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE access*, vol. 7, pp. 17 578–17 598, 2019.
17. M. Moniruzzaman, S. Khezr, A. Yassine, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," *Computers & Electrical Engineering*, vol. 83, p. 106585, 2020.
18. R. Vishwakarma and A. K. Jain, "A survey of ddos attacking techniques and defence mechanisms in the iot network," *Telecommunication systems*, vol. 73, no. 1, pp. 3–25, 2020.
19. W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and con-sensus in modern business processes," *Journal of Industrial Information Integration*, vol. 13, pp. 32–39, 2019
20. .R. Stephen and A. Alex, "A review on blockchain security," in *IOP Conference Series: Materials Science and Engineering*, vol. 396, no. 1. IOP Publishing, 2018, p. 012030.
21. J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain secu- rity: A survey of techniques and research directions," *IEEE Transactions on Services Computing*, 2020.
22. A. Mittal, M. Gupta, M. Chaturvedi, S. R. Chansarkar, and S. Gupta, "Cybersecurity enhancement through blockchain training (cebt)–a seri- ous game approach," *International Journal of Information Management Data Insights*, vol. 1, no. 1, p. 100001, 2021.
23. R. Arjun and K. Suprabha, "Innovation and challenges of blockchain in banking: A scientometric view." *International Journal of Interactive Multimedia & Artificial Intelligence*, vol. 6, no. 3, 2020.
24. E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, "Blockchain technol- ogy implementation in logistics," *Sustainability*, vol. 11, no. 4, p. 1185, 2019.

25. I. Haq and O. M. Esuka, “Blockchain technology in pharmaceutical industry to prevent counterfeit drugs,” *International Journal of Computer Applications*, vol. 180, no. 25, pp. 8–12, 2018.
26. M. Gimenez-Aguilar, J. M. de Fuentes, L. Gonzalez-Manzano, and D.Arroyo, “Achieving cybersecurity in blockchain-based systems: A survey,” *Future Generation Computer Systems*, 2021.
27. Le, D.N. and Khan, A.A. eds., 2022. *Evolving Software Processes: Trends and Future Directions*. John Wiley & Sons.
28. R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, “Integrated blockchain and edge computing systems: A survey, some research issues and chal- lenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.
29. P. Bansal, R. Panchal, S. Bassi, and A. Kumar, “Blockchain for cyberse- curity: A comprehensive survey,” in *2020 IEEE 9th International Con- ference on Communication Systems and Network Technologies (CSNT)*. IEEE, 2020, pp. 260–265.
30. T. R. Vance and A. Vance, “Cybersecurity in the blockchain era: A surveyon examining critical infrastructure protection with blockchain-based technology,” in *2019 IEEE International Scientific-Practical ConferenceProblems of Infocommunications, Science and Technology (PIC S&T)*. IEEE, 2019, pp. 107–112.
31. B. Alotaibi, “Utilizing blockchain to overcome cyber security concerns inthe internet of things: A review,” *IEEE Sensors Journal*, vol. 19, no. 23, pp. 10 953–10 971, 2019.
32. O. Alkadi, N. Moustafa, and B. Turnbull, “A review of intrusion detection and blockchain applications in the cloud: Approaches, challenges and solutions,” *IEEE Access*, vol. 8, pp. 104 893–104 917, 2020.
33. K. Fan, Z. Bao, M. Liu, A. V. Vasilakos, and W. Shi, “Dredas: Decen- tralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial iot,” *Future Generation Computer Systems*, vol. 110, pp. 665–674, 2020.
34. Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, “Blockchain for the iot and industrial iot: A review,” *Internet of Things*, vol. 10, p. 100081, 2020.
35. K. M. Giannoutakis, G. Spathoulas, C. K. Filelis-Papadopoulos, A. Collen, M. Anagnostopoulos, K. Votis, and N. A. Nijdam, “A blockchain solution for enhancing cybersecurity defence of iot,” in *2020 IEEE Intern ational Conference on Blockchain (Blockchain)*. IEEE, 2020, pp. 490–495.
36. R. Graf and R. King, “Neural network and blockchain based technique for cyber threat intelligence and situational awareness,” in *2018 10th International Conference on Cyber Conflict (CyCon)*. IEEE, 2018, pp. 409–426.
37. W. Serrano, “The blockchain random neural network for cybersecure iot and 5g infrastructure in smart cities,” *Journal of Network and Computer Applications*, vol. 175, p. 102909, 2021.
38. Q. Feng, He, D., Zeadally, S., Khan, M.K. and N. Kumar, 2019. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, *126*, pp.45-58.
39. W. Li, S. Tug, W. Meng, and Y. Wang,, 2019. Designing collaborative blockchained signature-based intrusion detection in IoT environments. *Future Generation Computer Systems*, *96*, pp.481-489.