BLOCKCHAIN TECHNOLOGY ADOPTION IN E-COMMERCE PLATFORMS

Rezwanul Alam, Md. Aminul Islam*, Arifur Rahman Khan, Nushrat Jahan

Department of MIS
School of Business and Entrepreneurship
Independent University, Bangladesh (IUB)

Abstract

Internet expansion changed how people obtain services and how organizations operate. The Internet and related services are crucial for most people nowadays. E-commerce is a service and industry. E-commerce transfers a lot of sensitive data, including consumer and financial data. Such information attracts cybercriminals who want to break into the system and steal data. As e-commerce grows, so do cyberattacks, raising concerns about the security of e-commerce platform databases. Since data comprises customer, employee, and transaction information, organizations must safeguard it. The data leak will hurt the company's earnings and clients' faith in the platform. A blockchain database management system may alleviate this challenge, improve data security, and safeguard sensitive data. It solves the problem by inserting blockchain nodes into the database and inheriting distributed peer-to-peer data security.

Keywords: blockchain, e-commerce, and data security.

Introduction

Our everyday lives depend on the internet, and online service needs are developing rapidly. The digitized world has changed global e-commerce. For many network users, online business platforms offer ease and flexibility from multiple retailers (Balaji N, 2019). An example,

Online registration and transactions are similarly simple. As a result, cyberattacks are on the rise worldwide. Thus, insecure network architecture became the main threat to e-commerce platforms (Richard Apau et al., 2019). Customer trust and organizational data are essential to success in the development cycle. Data helps firms make informed decisions (L. Steve, 2019). Accordingly, only stakeholders and management teams should have access to data to protect businesses' and customers' privacy and loyalty.

* Corresponding author: Md. Aminul Islam, Email: islam@iub.edu.bd

Therefore, trustworthy techniques and technologies are needed to secure this asset against unauthorized access (P. Kale, 2019). E-commerce business platforms will use blockchain technology as their repository. Satoshi Nakamoto proposed Bitcoin and Blockchain in 2008 (Nakamoto, 2008). Decentralized and encrypted Bitcoin technology ensures data integrity and accountability. This level of security makes the technology appealing to many sectors. It provides a distributed database that unauthorized users cannot change by recording and encrypting data in back-linked blocks (Wang, 2020). Smart contracts become a significant feature of blockchain. They manage access rights for data nodes using self-enforcing agreements between two or more parties. The properties of blockchain technology enable its use in e-commerce platform databases. Money and contracts can be stored there (Alex and Don, 2020). Blockchain in e-commerce platforms may enhance supply chain management, multinational operations, data transparency, and transaction costs (Sharma, 2020; Saakian, 2020). Most significantly, it may make e-commerce platform consumers feel safe and trust the companies. Blockchain's unique structure increases database security and protects against cyberattacks. Blockchain-encrypted data structures are used for data verification and storage, while distributed nodes are used for data updates and creation. Hackers must disable all server nodes, which is a challenging task. To ensure the organization's data security, this research suggests a blockchain-based e-commerce database solution.

Problem background

Data breaches are becoming increasingly important for individuals and companies as they attempt to protect their privacy and security, given the expanding number of cyberattacks. Wertz (2019) found that data breaches surged at an unanticipated rate, from 36.6 million in 2016 to 197.6 million in 2017, setting a new peak of 446.5 million data exposure concerns. Data breaches affect both large and small firms because they are simpler to target and extort. The attackers threatened and demanded ransoms from firms using stolen data. Uber paid $100,00 to the hacker to destroy the stolen data and resolve the 2016 data breach (C. Kate, 2018).

Organizations' data breaches undermine consumer loyalty and public trust because customers value their data privacy, especially personal and transaction history. In March 2018, Under Armour's online shop database was accessed by unauthorized parties, exposing over 150 million customers'

usernames, emails, and encrypted passwords (Dennis Green, et al., 2019). Fortnite, which has 200 million users, also exposed players' personal account information and intercepted in-game conversations (Alon Boxiner et al., 2019). The story showed that cyberattacks on internet platforms are expanding quickly and must be handled and monitored to prevent organizational losses. E-commerce companies should use blockchain technology to secure sensitive data and decrease data breaches.

Problem statement

The company's staff and customers' data should always be secure. To secure consumer and corporate data, companies continuously work to protect it. E-commerce breaches can damage Brand reputation and income can be negatively impacted by online vandalism or criminal charges due to data misuse (L. Nick, 2018). Without database encryption and network security, cyberattacks are more likely; thus, the company's tools and technologies should focus on those areas (R. Sophie, 2018). Chuen (2020) suggested a third-party app for selling gadgets for premium credits.

Therefore, this research study advocates the use of blockchain technology in database systems due to its unique capabilities to secure data for e-commerce firms and prevent unauthorized access. Blockchain provides a secure framework that allows data to be accessed in blocks, each with a unique cryptographic signature. A single control point makes it simpler for attackers to steal and manipulate data, while blockchain's decentralized approach makes it more challenging. This technique can protect data integrity and confidentiality better than a central database system, which hackers may easily exploit (P. Santhosh, 2018). Blockchain increases trust and data security in online services, making it suitable for e-commerce business platforms. It also improves channel expansion, supply chain management, e-business transactions, and organizational performance.

This study evaluates and finds strategies to decrease data breaches on e-commerce platforms using blockchain technology.

Literature review:

To justify the solution, several studies were conducted. Internet use has boosted e-commerce and changed buying habits (Tam, C. et al., 2019). Customers may buy nearly anything online today. Online shoppers can

purchase products and services at any time and from anywhere. As internet businesses develop, so do fraudsters. E-commerce databases hold a lot of personal data, which might compromise a person's safety. For e-commerce company platforms, databases using blockchain technology are recommended.

Data breaches in E-commerce

Roberts (2019) mentioned that most companies underestimate the damages of data breaches and the issues they might lead to, as well as a lack of prevention. More than 90% of online business platforms are experiencing login attempts from hackers (Detrixhe, J., 2018). That means the data breach problem is becoming serious, and unauthorized entities are targeting e-commerce businesses.

Figure 1: Share of login attempts that are credential stuffing attacks (Detrixhe, J, 2018)

E-commerce companies should identify the issues and generate alternative solutions to them.

4.2. Enhance public trust in E-Commerce with Blockchain

Trust and loyalty are two of the most significant impacts of blockchain on the e-commerce industry. Rajesh Ramachandiran found that trust-related research focuses on blockchain's capacity to create rules and regulations without arbitrary control (2018). Applying a blockchain network to the company's database system helps build user confidence in the e-commerce platform. The company's blockchain and database system allow e-commerce platform providers, suppliers, and clients to examine their data, promoting data transparency. The final result is increased privacy and confidentiality for e-commerce platform customers, which boosts loyalty and confidence in the company.

4.3. Blockchain Performance

Another research by Mohammad Jabed Morshed Chowdhury (2018) noted that decentralization, which democratizes the system, makes blockchain solutions immutable (2018). Additionally, blockchain data uses public-key cryptography. Performance is one of blockchain's most significant drawbacks. The analysis found that blockchain transactions were delayed compared to traditional techniques. In 10 minutes, a well-designed database system can process thousands of transactions per second. The researcher stated that they are currently investigating algorithms that could process transactions in 10-20 seconds. This issue will be considered before installing blockchain in the e-commerce database.

4.4. Integrate blockchain technology with conventional storage.

Jian Chen et al. observed that blockchain's main drawbacks include the restricted storage space of each node or block, which makes massive data storage nearly impossible, and data redundancy (2019). The suggested system combines blockchain technology with traditional storage methods, which include separating data in the blockchain and storing it in a central database, to increase data storage efficiency. The proposed technique can solve the issue of insufficient blockchain storage and information redundancy.

4.5. Blockchain-based database

Muhammad Mazammal (2018) observed that blockchain data is challenging to modify and add. Additionally, the blockchain database system provides data-level disaster recovery backup and audit middleware. To improve the weaknesses of blockchain networks, CHAINSQL is proposed. The many-to-one design of a blockchain-based database system offers adequate data backup across multiple production nodes. This technique combines the flexibility, fast throughput, and large capacity of distributed databases with the security and audibility of blockchain databases. Moreover, this technology enhances data integrity and dependability in distributed database systems and blockchain databases, reducing issues with tamper resistance and latency. This strategy works for e-commerce company platforms because the data saved can be modified for permission access, and companies and clients can be assured of data protection. When creating the proposed system, it will be referenced. Saleh

(2020) observed that the web and decision support systems made it inexpensive.

4.6 Enhance Data Security using Blockchain

Another study by Alex. R. Mathew demonstrated that standard data management systems are vulnerable to cyberattacks (2019). The research addresses the centralized nature of current data management systems, such as using a single, independent security system, which is vulnerable to DDoS (Distributed Denial of Service) attacks. In these attacks, hackers take down a single security system and steal personal data. Due to its peer-to-peer and distributed nature, blockchain technology might improve security systems and secure data storage, according to the research. The report recommends blockchain due to its robust architecture, as the existing data management method has a single point of failure. Only two parties may read and alter data, so if information leaks, third parties cannot use it. Alex. R. Mathew reports that security researchers have found that blockchain technology might address security gaps beyond current security methods (2019). Private keys and wallets improve blockchain data security. Paper and hardware wallets are suggested to safeguard blockchain databases (Alam Khan et al., 2020).

4.7 Database System Metadata Segregation

Devanshu Trivedi et al. (2016) found that database metadata contains information about the data. According to a study, database columns will be split by sensitivity level, and referential integrity will be established at runtime to isolate metadata and enhance database security. When one table

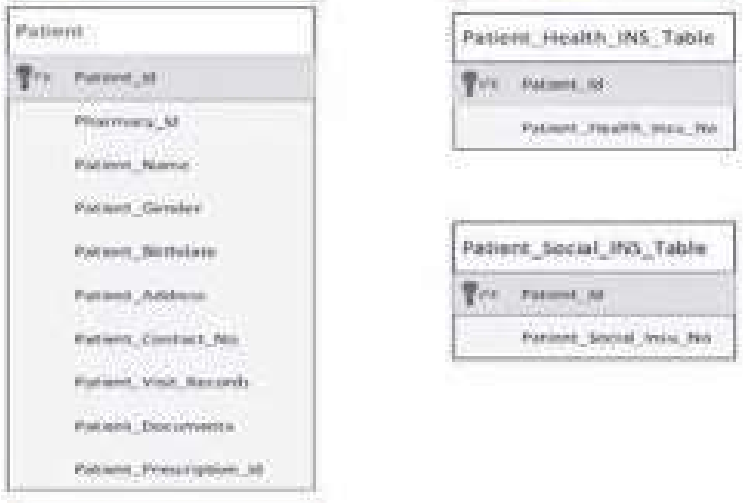

Figure 2: Segregated tables in a database system (Trivedi et.al, 2016)

is suspected of being hacked, referential integrity restrictions will separate the metadata. Thus, attackers cannot join database objects or move data from other tables.

This strategy is effective for preventing illegal access, but the varying levels of sensitivity and relationships between data tables will make data recovery after segregation challenging. The e-commerce database system includes various types of data and uses, such as transaction information, customer data, and competitive data, making it unsuitable for implementation. Since servers are located in different locations, implementing this strategy in e-business network design is difficult and expensive. The fundamental principle of metadata segregation can guide the development of systems.

Significance of the Work

Company operations and data management system administration are enabled by queries in the database (Vincetabora, 2018). A central control point allows administrator control. It is reliable for large-scale data storage and efficient for business platform data transactions. The central control point becomes a system weakness and is easily exploited. However, some studies recommend blockchain and outline its advantages over traditional database systems. Studies show that blockchain technology's decentralization, non-tamperability, and programmability help overcome security issues, particularly in protecting personal data in conventional database systems. E-commerce platforms benefit from blockchain technology's data privacy and security. Blockchain's drawbacks also need to be examined. E-commerce platforms will face hurdles from unstable blockchain technology, data scalability, and immutability.

Thus, a blockchain-based database is better for the business than a traditional database. Data may be updated and modified on blockchain network nodes by the organization. It can encrypt data and prevent illegal access. All data is in blocks linked by a hash value. A change in data affects succeeding blocks. While data storage and backup are efficient and scalable, data is always available to support business operations. The combination system can enable secure e-commerce platforms by modifying restrictions on blockchain and database systems. This system is ideal for e-commerce businesses that need data protection, scalability, flexibility, and stability. Data breaches can be prevented simultaneously.

System overview - simulator

The study examines the feasibility of integrating blockchain technology into the databases of e-commerce platforms. Data protection is its fundamental purpose. This technology is suited for business database systems to regulate and secure data.

Public, private, and consortium blockchains existed (Chen, Lv, and Song, 2019). Decentralized public blockchains are open to everyone without agency control. They are transparent and trusted by users. Bitcoin is a public blockchain. Blockchain represents the platform, while cryptocurrency represents the application functioning on it. However, a private blockchain is an environment that only the corporation can access. Consortium blockchains mix public and private blockchains and are used in multi-user ecosystems.

Instead of a public blockchain or consortium blockchain, which the public may randomly access, the system will use a private blockchain. That is because outsiders should not access an organization's sensitive data. Since data should only be gathered and utilized for business objectives, the organization must prioritize data protection. The private blockchain ensures data access and regulation. While identical to the public blockchain, corporate participants needed separate permissions to view, write, execute, or store data (Mary Thibodeau, 2019). Additionally, private blockchains are faster than public blockchains, which speeds up data transactions on organizational nodes in private networks.

Figure 3: The architecture of the proposed database system

It also allows organizations to scale data storage easily to meet their needs.

At the lowest level, consensus includes numerous peer-to-peer machines agreeing on the current data. The choice is definitive, and data is committed when all machines agree. Blockchain's basic consensus mechanism will power the suggested system. The approach guarantees fault tolerance by requiring all nodes to apply committed data and calculate the same data if the state is decided. Even if only 2 of 5 servers are running, a client will see the state machine as fully functional and dependable. Blockchain technology is fully utilized here, as all state machine nodes are connected to create the blockchain, which determines which data is saved. Storage layers are above consensus layers. All nodes must agree before data can be added to the database. To query data, materialized views and key values are stored. Clients access data via the primary keys and tables. Finally, the suggested system would use PromQL to organize and query data.

Conclusion

This report concludes that e-commerce company platforms must integrate blockchain technology into their database systems to prevent data leaks. This strategy is superior to utilizing a regular database system, which is vulnerable to hackers, or blockchain technology, which is inefficient for commercial processes. Online retail businesses can use the suggested system's efficient and dependable repository. Further research on blockchain technology should address its limitations, notably the cost. A further in-depth examination should alleviate the need for highly competent technical teams to maintain the system, which presents another challenge for businesses.

References

Alam Khan, F., Asif, M., Ahmad, A., Alharbi, M. and Aljuaid, H., 2020. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society*, 55, p.102018.

Alex, T. and Don, T., 2020. *How Blockchain Is Changing Finance*. [online] Capital.report. Available at: <https://capital.report/Resources/Whitepapers/8e8d2fd2-9bef-40d5-9ff6- a2fed8ab1f09_finance_topic2_source2.pdf>

Apau, R., Koranteng, F. and Gyamfi, S., 2019. Cyber-Crime and its Effects

on E-Commerce Technologies. *Journal of Information*, 5(1), pp.39-59.

Chen, J., Lv, Z. and Song, H., 2019. Design of personnel big data management system based on blockchain. *Future Generation Computer Systems*, 101, pp.1122-1129.

Chong, J., 2020. *Alternatives To Blockchain*. [online] Medium. Available at:

<https://medium.com/@jimmysong/alternatives-to-blockchain-9f858c0a1f2d> [Accessed 14 April 2020].

Detrixhe, J., 2020. *Share Of Login Attempts That Are Credential Stuffing Attacks*. [online] Atlas. Available at: <https://theatlas.com/charts/H1M7IK2Q7> [Accessed 28 April 2020].

Drolet, M., 2020. *4 Reasons Blockchain Could Improve Data Security*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3279006/4-reasons-blockchain-could- improve-data-security.html> [Accessed 11 April 2020].

Green, D., Hanbury, M. and Cain, A., 2020. *If You Bought Anything From These 19 Companies Recently, Your Data May Have Been Stolen*. [online] Business Insider Malaysia. Available at:

<https://www.businessinsider.my/data-breaches-retailers-consumer-companies-2019- 1?r=US&IR=T> [Accessed 12 April 2020].

Ha, M., Kwon, S., Lee, Y., Shim, Y. and Kim, J., 2019. Where WTS meets WTB: A Blockchain- based Marketplace for Digital Me to trade users' private data. *Pervasive and Mobile Computing*, 59, p.101078.

hackernoon. 2020. *Databases And Blockchains, The Difference Is In Their Purpose And Design*. [online] Available at: <https://hackernoon.com/databases-and-blockchains-the-difference-is-in- their-purpose-and-design-56ba6335778b>

Koteska, Bojana & Karafiloski, Elena & Mishev, Anastas. (2017). Blockchain Implementation Quality Challenges: A Literature Review.

Lansiti, M. and R. Lakhani, K., 2020. *The Truth About Blockchain*. [online] Harvard Business Review. Available at: <https://hbr.org/2017/01/the-truth-about-blockchain>

Medium. 2020. *How Blockchain Technology Works*. [online]

Available at: <https://medium.com/@ipspecialist/how-blockchain-technology-works-e6109c033034>

Metelin, S., 2020. *The Role Of Blockchain In Data Security*. [online] Infosecurity Magazine. Available at: <https://www.infosecurity-magazine.com/opinions/role-blockchain-data- security/>

Muzammal, M., Qu, Q. and Nasrulin, B., 2019. Renovating blockchain with distributed databases: An open source system. *Future Generation Computer Systems*, 90, pp.105-117.

Nathan, S., Govindarajan, C., Saraf, A., Sethi, M. and Jayachandran, P., 2019. Blockchain meets database. *Proceedings of the VLDB Endowment*, 12(11), pp.1539-1552.

O'Neal, S., 2020. *Blockchain Interoperability, Explained*. [online] Cointelegraph. Available at: <https://cointelegraph.com/explained/blockchain-interoperability-explained>

Paik, Hye-young & Xu, Xiwei & Bandara, Dilum & Lee, Sung & Lo, Sin Kuang. (2019). Analysis of Data Management in Blockchain-based Systems: From Architecture to Governance.

IEEE Access. PP. 1-1. 10.1109/

Palavesh, S., 2020. *Here's How You Can Secure Your Data With Blockchain*. [online] Entrepreneur. Available at: <https://www.entrepreneur.com/article/318477>

Panoho, K., 2020. *Council Post: The Age Of Analytics And The Importance Of Data Quality*. [online] Forbes. Available at: <https://www.forbes.com/sites/forbesagencycouncil/2019/10/01/the-age-of-analytics-and-the-importance-of-data-quality/#527fa32a5c3c>

R.Mathew, A., 2019. Cyber Security through Blockchain Technology. *International Journal of Engineering and Advanced Technology*, 9(1), pp.3821-3824.

Ramachandiran, Rajesh. (2018). Using Blockchain Technology To Improve Trust In eCommerce Reviews. 10.13140/RG.2.2.29324.00646.

Roussev, V., 2009. Hashing and Data Fingerprinting in Digital Forensics. *IEEE Security & Privacy Magazine*, 7(2), pp.49-55.

Saleh Hadidi, Maen Al-Rashdan, Mamoun Hadidi, 2020. Impact Web On Decision Support Systems On The Organizations. Journal of Critical Reviews, 7(3):2020.

Saakian, H., 2020. *How Blockchain Has Helped The Business Of E-Commerce - Asia Blockchain Review - Gateway To Blockchain In Asia*. [online] Asia Blockchain Review - Gateway to Blockchain in Asia. Available at: <https://www.asiablockchainreview.com/how-blockchain- has-helped-the-business-of-e-commerce/>

Sharma, T., 2020. *Top 10 Blockchain Solutions For E-Commerce*. [online] Blockchain- council.org. Available at: <https://www.blockchain-council.org/blockchain/top-10-blockchain- solutions-for-e-commerce/>

Suciu, P., 2020. *The Biggest Cybercrime Threats Of 2019*. [online] Ecommercetimes.com. Available at: https://www.ecommercetimes.com/story/85782.html

SZ Chuen, Al-Rashdan M, Al-Maatouk Q: Cloud Data Processing Network Via Online Game Users. Journal of Critical Reviews 2019, 7(3):2020. https://doi.org/10.31838/jcr.07.03.17

Trivedi, D., Zavarsky, P. and Butakov, S., 2016. Enhancing Relational Database Security by MetadataSegregation. *Procedia Computer Science*, 94, pp.453-458.Underwood, S., 2018. Blockchain Beyond Bitcoin. Blockchain Beyond Bitcoin, 59(11).

Wen M., Yu S., Li J., Li H., Lu K. (2016) Big Data Storage Security. In: Yu S., Guo S. (eds) Big Data Concepts, Theories, and Applications. Springer, Cham Wertz, J., 2019. While Data Breaches Accelerate, It's Critical That E-Commerce Businesses Stay Safe. [online] Forbes. Available at: <https://www.forbes.com/sites/jiawertz/2019/09/19/while-data-breaches- accelerate-its-critical-that-e-commerce-businesses-stay-safe/#12fe312d4f5c>