TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.02 (2024)
https://www.tejasjournals.com/

Beyond Cryptocurrency: Harnessing Blockchain for Cybersecurity

Dr. Shalini Lamba[a], Jatin Awasthi[b] and Vikas Yadav[c]

[a,b,c] Computer science, National Post Graduate College, Lucknow, India
[a]drshalinilamba@gmail.com, [b]anubhavjatin2907@gmail.com,
[c]thevikasyadav16@gmail.com

KEYWORD

Blockchain technology, Cybersecurity, Cryptocurrency, distributed ledger, Decentralization, Immutable records, Data integrity

ABSTRACT

This paper aims to explore the role of blockchain in strengthening cyber security. In an era where cyber threats are at its peak, the blockchain technology has come out as a promising method to strengthen the defenses of cyber security. This paper highlights the impact of blockchain technology on cyber security. The paper starts by explaining the basics of blockchain and will then discuss its various key features when integrated with cyber security such as secure data storage and processing, user confidentiality, decentralization and many more. But using blockchain also has some limits such as scalability issues, regulatory issues etc. which are also discussed in this paper. At last, the conclusion will summarize the benefits of integrating blockchain technology with cyber security and what the future holds.

1. Introduction

attacks, malware, data breaches, distributed denial of service (DDoS) attack have increased significantly in the recent years and pose a major threat to organizations, businesses, individuals and governments alike. Traditional methods often prove insufficient in tackling present-day cybersecurity threats. So to address today's dynamic cyber security challenges, there has been a search for new and enhanced methods where blockchain has emerged as an effective solution.

Blockchain technology was first introduced in 2008 by an unknown person or a group using the name Satoshi Nakamoto. In the views of IBM, blockchain is a decentralized distributed ledger technology that guarantees the security, transparency and immutability of transactions over the internet. The technology is termed as blockchain as every transaction in blockchain which can store various data types such as digital signature, metadata, description and many more.

2. How Does Blockchain Contribute to Cyber Security?

Blockchain uses a system i.e. decentralized distributed ledger system to register any transaction such as business transactions. It is a system that is spread out across many computers, organization, countries and can be accessed by more than one people around the world. The system gives each person on the network their own copy of ledger and in case of any change in one ledger, it is automatically updated in all the other copies of ledge which ensures that no single person or authority has control over the ledger and each person can view the information at the same time. Since all transaction are registered on every single network node, cybercriminals face difficulty in tampering the data. Also, every block of data in blockchain is linked together in a chain created over network where each block

Corresponding Author: Dr Shalini Lambaa, Computer science, National Post Graduate College, Lucknow, India
Email: drshalinilamba@gmail.com

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.02 (2024)
https://www.tejasjournals.com/

contains the hash code of previous block so even if the hacker tries to tamper the data within a block the hash code of the block gets changed which delinks the block from the chain.

2.1. Prevent from DDoS attack: A DDoS attack is when an attacker tries to overpower the network with requests resulting into server slowdown or shutdown and become inaccessible for users. However, due to being decentralized, blockchain have no single point of failure which help in neutralizing any chances of DDoS attacks.

2.2. Secure private messages: On a blockchain based messaging platform, using cryptographic algorithm, the message is encrypted into cipher text using a key which is unreadable. The encrypted message is then stored on blockchain which is later decrypted using a decryption key which is only available to receiver which makes it more difficult for attackers to use that information even if they are able to access the data.

2.3. Immutable record: Blockchain creates a chain of blocks where each block records a transaction and is hashed and linked with preceding block. So when a transaction is added to the blockchain it becomes almost impossible for attacker to alter the transaction as the entire chain gets tampered.

2.4. Protection from DNS: Peoplemight face limitations when trying to reach servers, networks, and websites during a DDoS (Distributed Denial of Service) assault, resulting in system interruptions. Hackers often view the Domain Name System (DNS) closely watched as an appealing target to tinker with website and IP addresses, potentially stirring up confusion. But, blockchain technology presents an answer to these weaknesses due to its spread out DNS entries, lessening the threat of such attacks. By getting rid of centralized shortcomings, blockchain bolsters safety in areas vulnerable to hacker actions, delivering practical distributed system remedies.

2.5. Smart contact security: These are sets of rules that are stored on blockchain. When certain conditions are met they trigger transactions which makes payment automated and convenient.

2.6. IoT: Blockchain protects IoT data using its constant record. It scrutinizes devices and halts any unwanted transactions. With unique codes, blockchain can identify each IoT gadget. All exchanges utilize digital signatures to confirm approval. This mechanism keeps data shielded from disruptions. Only gadgets that garner approval can join the network. It prevents harmful activities that could exploit IoT data.

3. Benefits Of Integrating Blockchain with Cyber Security

3.1. Data transparency and traceability: Every transaction on blockchain can be viewed by any participant over the network and since each transaction in the blockchain is linked, the participants can easily track the history of data.

3.2. Zero chance of failure: Since blockchain is a decentralized technology, even if a single node fails, the overall blockchain system is not affected and the system continues to function normally.

3.3. Safe data transfer: Blockchain offers the use of Public key infrastructure (PKI) which authenticates user and data during transfer with the help of unique cryptographic keys. PKI also encrypts the data which can only be decrypted the intended receiver’s private key

3.4. User confidentiality: Public key cryptography is plays a major role in this sector. When to participant in blockchain interact with each other, addresses are used to represent them instead of their original identity which are retrieved from cryptographic keys.

4. Security Challenges and Issues of Using Blockchain

Although blockchain has emerges as a very optimal solution for tackling cyber threats, it’s not invincible. Implementation of Blockchain comes with following problem and challenges.

4.1. Scalability and Adaptability: There is a fixed limit to the number of transaction that can be processed per second so blockchain system may face difficulty to handle a large number of transaction.

4.2. High cost: Implementing blockchain requires a large storage capability and computing power that leads to a much higher cost compared to traditional applications.

4.3. 51% attack: Blockchain systems using Proof of Work face “51% attack” issue. When a group controls the majority of mining power, they gain significant influence. If they acquire more than 51% of the power, they can interfere with transactions. Actions like responding coins or causing disruption in the network becomes feasible. Such actions could damage the system's trust and safety.

4.4. Theft of keys: Attackers uses methods such as phishing to demand access credential from a participant. If the attackers succeed in fooling the key owner, they can harm the owner and blockchain system.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.03, I.02 (2024)
https://www.tejasjournals.com/

4.5. Insufficient encryption: Although encryption makes data transfer secure, it’s not impossible for attacker to decrypt data if the strength of encryption is too low or weak keys are used.

5. Future Scope

The future of blockchain in cybersecurity holds vast possibilities. Possible exploration includes scalability solutions for constraints, privacy-focused tech for delicate data, and standards for combining various systems. The joining of blockchain with AI and IoT gives new possibilities for defense. Nonetheless, it's important to adapt governmental regulations for wider usage and to stay legal. As a whole, sustained team effort and creativity will push forward strong blockchain cybersecurity fixes for a safe digital network.

6. Conclusion

Blockchain provides fresh paths to enhance cybersecurity. Its unique layout, cryptography, and stable logs defend information. It's tough for hackers to breach. However, blockchain faces some hurdles. It has trouble with expanding, privacy, and rules. To make full use of blockchain for cybersecurity, we require answers. Collaboration between areas is critical. Additional study pushes forward blockchain cybersecurity. Blockchain shields critical systems from current cyber dangers. In various industries, its relevance multiplies. It paves the way for a safe digital future.

References

[1] Swan, Melanie. Blockchain: Blueprint for a new economy. " O'Reilly
[2] Iansiti, Marco, and Karim R. Lakhani. "The truth about blockchain." Harvard Business Review 95.1 (2017): pp. 118-127
[3] . Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied Innovation 2.6-10 (2016)
[4] Cachin C. Architecture of the hyperledger blockchain fabric. InWorkshop on distributed cryptocurrencies and consensus ledgers 2016.
[5] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2019.
[6] Gao Y, Nobuhara H. A proof of stake sharding protocol for scalable blockchains. Proceedings of the Asia-Pacific Advanced Network. 2017.
[7] . Li, Wenting, et al. "Securing proof-of-stake blockchain protocols." Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, Cham, 2017.
[8] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2019.
[10] . Sharma PK, Moon SY, Park JH. Block-VN: A distributed blockchain based vehicular network architecture in smart City. JIPS. 2017.
[11] "How Blockchain Can Fight Fraud Based on Know-Your-Customer Data", Nasdaq.com, 2019
[12] Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS in the IoT: Mirai and other botnets. Computer. 2017.
[13] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services, 2018,
[14] Gao Y, Nobuhara H. A proof of stake sharding protocol for scalable blockchains. Proceedings of the Asia-Pacific Advanced Network. 2017.
[15] "How Blockchain Can Fight Fraud Based on Know-Your-Customer Data", Nasdaq.com, 2019.