EasyChair Preprint

№ 10179

Security, Privacy and Trust in Block Chain

Nikhil Rohidekar, Singam Reddy Suresh Reddy and
N Nassurudeen Ahamed

May 16, 2023

Security, Privacy and Trust in Block chain

Nikhil K Rohidekar
computer science and engineering
(of Affiliation)
Presidency University
Karnataka, India
nikhilrohid@gmail.com

Mr. N Nassurudeen Ahamed
Assistant Professor
Computer science and engineering
(of Affiliation)
Presidency University
Karnataka, India
nassurudeenahamed@presidencyuniversity.in

Singam Reddy Suresh Reddy
computer science and engineering
(of Affiliation)
Presidency University
Karnataka, India
singamreddysureshreddy203@gmail.com@gmail.com

***Abstract*— A distributed ledger is upheld by a network of nodes, with each node possessing an identical synchronized digital record. These nodes not only verify the data but also collaborate to achieve a mutual agreement on precise transactions.**

Some ledgers have been utilized for a significant period, and their usage has gained increased recognition, exploration, application, and advancement since the emergence of Bitcoin.

As Industry 4.0 continues to advance, distributed ledgers can now be employed across various industries where data is recorded and utilized for growth. While all blockchains are a form of distributed ledger, it should be noted that not every distributed ledger necessarily functions as a blockchain.

Although distributed ledger helps in more much accounts, security and accessibility, then it remains complex and more difficult to scale, DLT is not adaptable to strong regulation

This paper discusses how Security, privacy and trust are archived, function and play an important role in blockchain based distributed networks.

Key: -Blockchain - it is a decentralized & immutable method of storing transaction data in discrete sections (blocks) that are linked together.

Security in blockchain -security in blockchain is ensured using hashing algorithms such as SHA256 or keccak.

Distributed ledger - it is a digitally synchronized and distributed record of all transactions that happen within a network.

Distributed ledger technology It serves as a technological framework or infrastructure that enables simultaneous and authenticated access, as well as the continuous updating of records within a networked database.

Blockchain and DLT - Blockchain are created based on DLT which is a driving concept for its other business.

I. INTRODUCTION

Businesses and governments have been utilizing distributed computing for many decades, indicating that it is not a new concept to them.

During the 1990s, a significant development occurred where multiple computers and node users located in different places were able to collaborate on problem-solving and deliver the solutions to a central location.

Due to advancements in data science, computing hardware, and other technologies, these ledgers are becoming increasingly capable. Improved connectivity through intranet and internet protocols now enables the gathering, collection, analysis, and utilization of larger volumes of data. As the number of users with access to this data increases, ensuring security and verifying changes becomes crucial. Computer and data scientists have developed programs utilizing automation and data encryption techniques to validate database transactions or modifications, aiming to minimize the requirement for data auditing. Consensus mechanisms, which involve automated agreement on the validity of transactions, are employed to determine whether a transaction is a change made to the state of a database.[1].

Distributed ledgers have undergone significant development and now exist as scalable and programmable platforms, as demonstrated by Ethereum and IBM's Hyperledger Fabric. These platforms allow for the creation of solutions that effectively utilize databases or ledgers. Various functionalities, such as tokenizing physical assets and optimizing manufacturing and business processes, can now be securely stored on these distributed ledgers.[2]

I. How Blockchain Technology works

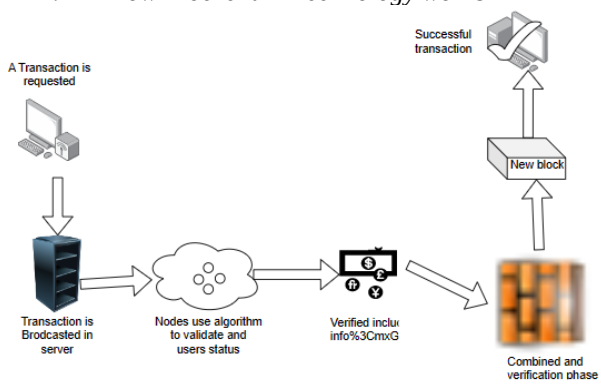

Fig. 1. This is a figure explains how Blockchain Technology Works

1Enabling a transaction: A fresh transaction is introduced into any blockchain network. All the necessary information to be

transmitted is encrypted twice using both public and private keys..

2. Transaction Verification: The transaction is sent to a network of peer-to-peer computers that are geographically dispersed worldwide.
Creation of New Blocks: Within the blockchain network, various types of nodes verify transactions at different times. Once the transactions are validated and added to a block, they are stored in a memory pool. The verified transactions at a specific node collectively form a memory pool in the blockchain.[3]

4. Consensus Algorithms: The node responsible for creating a specific block will incorporate the block into the blockchain network, ensuring its permanence.
Examples – pow, pos, poet

5. Incorporating Blocks into the Blockchain: Once a newly created block obtains its hash value and undergoes authentication, it becomes ready for inclusion in the blockchain. Each block within the blockchain contains a hash value that corresponds to the previous block, establishing cryptographic linkage between the blocks. Subsequently, the new block is added to the blockchain.[4]

6. Transaction Finalized: Upon the addition of the new block to the blockchain, a transaction is considered fully completed, and the specifics of this transaction are permanently stored within the blockchain.[4]

II. LITERATURE REVIEW

DLT (Distributed Ledger Technology) is a specific platform that leverages ledgers stored on individual or interconnected devices within a network to guarantee the accuracy and security of data. Blockchains, which have emerged from distributed ledgers, aim to tackle the increasing concerns surrounding the involvement of numerous third parties in various transactions.

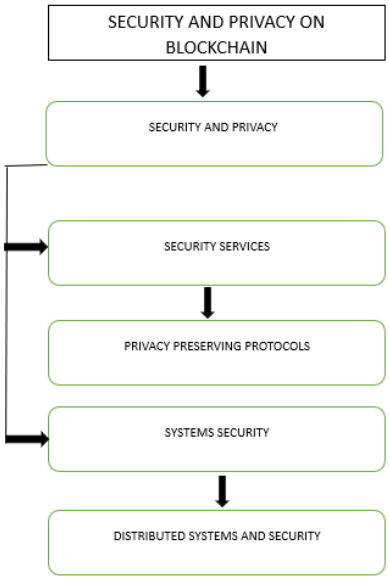

Fig. 2. This is a figure explains Security and Privacy and Blockchain

One of the primary features of blockchain technology is its inherent security. Blockchain networks employ sophisticated cryptographic algorithms to safeguard transactions and data stored within the network.

In addition, blockchain technology can be utilized to enhance privacy for images, thereby bolstering privacy within the system.

Furthermore, the use of blockchain technology instills trust in image-based applications by providing an immutable record of images, ensuring they cannot be tampered with. This enhances overall trust in the system..[5]

III. HOW SECURITY TRUST AND PRIVACY ARE ENSURED IN A DISTRIBUTED LEDGER USING BLOCKCHAIN AND ITS WORKING

DLT (Distributed Ledger Technology) ensures the security of data through cryptographic measures, preventing unauthorized tampering. Access to this data is granted using public or private keys and digital signatures. Once information is added to the ledger, it becomes an immutable and unchangeable database.

Consensus mechanisms are implemented to enforce network rules and govern the ledger within the blockchain-based ledgers. As these ledgers are decentralized, private, and encrypted, they are less susceptible to cybercrime. The distributed nature of the network, with multiple copies stored across the network, makes it extremely challenging for a successful attack. Moreover, peer-to-peer sharing and synchronized updates contribute to faster, cost-effective, and efficient processes.

In a DLT network, each node stores a copy of the digital ledger, and the synchronization ensures that any alterations or tampering of data are recorded by all nodes. Blockchains are constructed based on blocks, each containing an encrypted hash digest value, making them tamper-proof..[6]

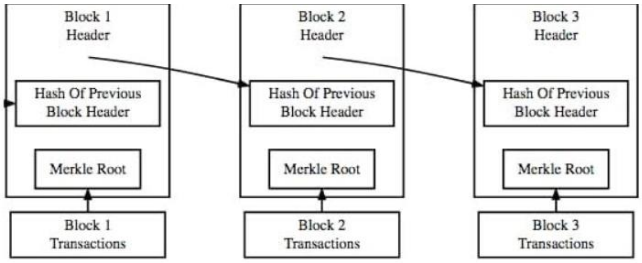

Fig. 3. . A Simplified Version of the Blockchain

A block consists of multiple transactions, each associated with a block number and a hash value. The individual transactions are hashed and their hashes are recursively merged and hashed until a single hash, known as the Merkle root, is obtained. This process utilizes the Merkle tree function, discovered by Ralph Merkle.

The Merkle root is stored in the block header, and each block can contain the hash value of the previous block's header. This linking of blocks forms a chain, indicating that modifying a transaction would require altering the entire block and all subsequent blocks, as the values within each block would change..[2]

IV. ENCRYPTION AND DECRYPTION

Encryption involves transforming a regular message, known as plaintext, into a secure and unreadable form called ciphertext.

Decryption, on the other hand, is the process of converting the ciphertext back into its original plaintext form.
The main distinction between encryption and decryption lies in the fact that encryption involves converting a message into an unintelligible form that cannot be deciphered unless decrypted correctly, while decryption is the recovery of the original message from the encrypted data. [12]

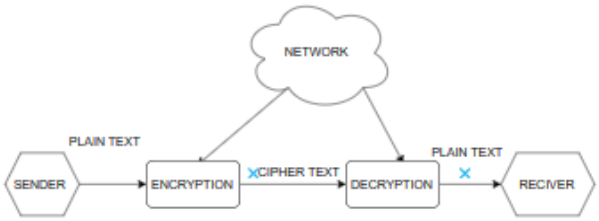

Figure 4 illustrates the transformation of plain text into cipher text, as well as the reversal of this process where cipher text is converted back into plain text.

V. THE NEW TECHNOLOGY OF TRUST -BLOCKCHAIN

A newly developed platform for commercial interactions has emerged, thanks to blockchain technology, offering a combination of usability, affordability, and high security. This technology establishes a fresh foundation of trust for commercial transactions on the blockchain, which has the potential to simplify and accelerate economic growth in line with everyday needs.

Trust forms the cornerstone of every business, serving as the bedrock for success and nurturing our business networks. We also rely on intermediaries to foster our relationships, necessitating our confidence in their ability to facilitate business. Banks play a crucial role in verifying transactional parties and ensuring accurate monetary exchanges. Lawyers are involved to safeguard against product duplication. However, employing these intermediaries is challenging, expensive, and time-consuming. Furthermore, in the era of hackers, such reliance on intermediaries also presents security concerns.

VI. Public and private blockchain

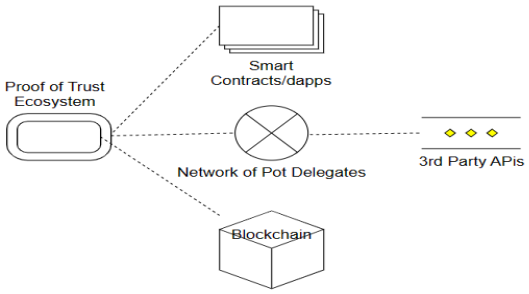

Fig. 4. Trust in Blockchain diagram representation

Public blockchain networks offer inclusivity, allowing anyone to participate while maintaining private anonymity. These networks rely on internet-connected computers to achieve consensus and validate transactions. Bitcoin, a widely recognized public blockchain, utilizes "bitcoin mining" as its consensus mechanism. In this process, computers on the Bitcoin network, referred to as miners, exert computational effort to solve complex cryptographic puzzles in order to generate proof of work (PoW) and proof of stake (PoS) to validate transactions. Such networks have limited identity and access control, except for a few public keys.[1],[14]

VII. ENCRYPTION AND DECRYPTION

Public Blockchain Private Blockchain

Fig. 5. Picture to represent Public and Private Blockchain

Private blockchains exclusively allow known organizations to join and participate, requiring verified identities to verify membership and permissions. These organizations form a select, members-only business network. Transactions are then validated by authorized users. Only members with specific access and privileges have the ability to maintain the accurate digital transaction ledger. This type of network places greater emphasis on identity and access control compared to public blockchains.[3]

ACKNOWLEDGMENT

The utilization and applications of blockchain technology have expanded far beyond its initial purpose of facilitating Bitcoin transactions and generation. Its inherent properties such as security, privacy, traceability, and reliable data and time-stamping have led to its adoption in various domains beyond the original scope. Blockchain, in its different forms, is now employed to secure diverse types of transactions, ranging from person-to-person communications to machine-to-person interactions. With the rise of the Internet of Things (IoT) on a global scale, the adoption of blockchain technology appears to be particularly secure. The decentralized applications (dApps) built on top of the existing global internet infrastructure offer appealing features like data redundancy, privacy, and increased survivability. Therefore, the invention of blockchain can be seen as a crucial and much-needed addition to the internet, addressing the long-standing issues of security and trust. It is worth noting that blockchain technology is still in the process of maturing, and it is anticipated that it will continue to witness widespread implementation and advancement globally for the next five years and beyond..[16]

FUTURE OF BLOCKCHAIN WITH TRUST

Blockchain technology is currently positioned at the Peak at Inflated Expectation, and some experts predict that it will take about five to ten years to reach a plateau. However, there are indications that the technology is heading downhill towards the Trough of Disillusionment. This shift is primarily due to the widespread adoption of blockchain in various applications beyond cryptocurrency. Blockchain shows significant potential in empowering citizens, particularly in developing countries, and it is extensively utilized in electronic governance applications for identity management, asset ownership transfer of valuable commodities like gold, silver, and diamonds, healthcare, and other commercial sectors. Furthermore, blockchain technology can greatly benefit national political decisions, providing a strong foundation for inclusive financial systems and overall development. [1]

REFERENCES

[1] 1. State of blockchain q1 2016: Blockchain funding overtakes bitcoin 2016 [online] Available: http://www.coindesk.com/state-of-blockchain-q1-2016/.

[2] S. Nakamoto Bitcoin: A peer-to-peer electronic cash system 2008 [online] Available: https://bitcoin.org/bitcoin.pdf.

[3] G. W. Peters E. Panayi and A. Chapelle Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective 2015 [online] Available: http://dx.doi.org/10.2139/ssrn.2646618.

[4] G. Foroglou and A.-L. Tsilidou Further applications of the blockchain 2015.

[5] A. Kosba A. Miller E. Shi Z. Wen and C. Papamanthou "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts" Proceedings of IEEE Symposium on Security and Privacy (SP) pp. 839-858 2016.

[6] B. W. Akins J. L. Chapman and J. M. Gordon A whole new world: Income tax considerations of the bitcoin economy 2013 [online] Available: https://ssrn.com/abstract=2394738.

[7] Y. Zhang and J. Wen "An iot electric business model based on the protocol of bitcoin" Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN) pp. 184-191 2015.

[8] M. Sharples and J. Domingue "The blockchain and kudos: A distributed system for educational record reputation and reward" Proceedings of 11 th European Conference on Technology Enhanced Learning (EC-TEL 2015) pp. 490-496 2015.

[9] C. Noyes Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning 2016.

[10] I. Eyal and E. G. Sirer "Majority is not enough: Bitcoin mining is vulnerable" Proceedings of International Conference on Financial Cryptography and Data Security pp. 436-454 2014.

[11] A. Biryukov D. Khovratovich and I. Pustogarov "Deanonymisation of clients in bitcoin p2p network" Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security pp. 15-29 2014.

[12] F. Tschorsch and B. Scheuermann "Bitcoin and beyond: A technical survey on decentralized digital currencies" IEEE Communications Surveys Tutorials vol. 18 no. 3 pp. 2084-2123 2016.

[13] Tech. Rep. 2015 [online] Available: http://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf.

[14] D. Lee Kuo Chuen and Ed. Handbook of Digital Crrency Elsevier 2015.

[15] V. Buterin "A next-generation smart contract and decentralized application platform" white paper 2014.

[16] D. Johnson A. Menezes and S. Vanstone "The elliptic curve digital signature algorithm (ecdsa)" International Journal of Information Security vol. 1 no. 1 pp. 36-63 2001.