Mukta Patil.,2023,11:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Data Consistency, Transparency and Privacy in Blockchain

Mukta Patil,Udayan Gaikwad,Akash Bhagwat,Saniya Inamdar,Prof. Swati Jadhav
BRACT's Vishwakarma Institute of Technology
An Autonomous Institute affiliated with Savitribai Phule Pune University)
666, Upper Indiranagar, Bibwewadi,
Pune, Maharashtra, INDIA - 411 037
Office.vit@vitpune.edu, vit.edu

Abstract- Block chain has swept the world by a storm. It has completely revolutionized many domains by providing more reliable features than traditional systems. It incorporated trust and security within existing systems, reduced human load and enabled processing of a large amount of data quickly. Its most celebrated features are providing privacy for sensitive data, ensuring transparency between the involved parties and an assured consistency of data in transactions across the network. This paper analyzes the implementation of these features, their strengths and weaknesses, the challenges and finally provides a few solutions to overcome the highlighted gaps. The implementation of this can be viewed in our project, wherein we created our own crypto currency transaction website, incorporating the mentioned features.

Keywords- Blockchain, Cryptocurrency, Data Consistency, Data Privacy, Data Transparency, Ethereum

I.INTRODUCTION

Block chain is a peer-to-peer transaction ledger system that is decentralized, permanent, transparent, immutable, trusted, and supported by algorithmic trust and distributed consensus mechanisms. It allows for secure information sharing, authentication of parties, long-term preservation of digital records, and the verification and validation of digital transactions. It is well regarded for its security. Since it was a new and revolutionary idea, its acceptance has been slow, but has seen a staggering increase in the past decade. Many new technologies have sprung forth incorporating blockchain, and revolutionizing their industry or technology. Blockchain is, thus, justly crowned as a crucial catalyst for technological advances.

II.LITERATURE REVIEW

As the world prepares for a huge shift from Web 2.0 to Web 3.0 [1] decentralized applications i.e Blockchain-based applications will take the central stage. Even currently, many sectors and industries have started to realize and utilize the power of Blockchain for their benefit. A few of which are the Business sector, Health Sector, Banking Sector, Education Sector and many more. We can see the steps being taken in these directions by the following examples.

(i) Blockchain for Business [2]: Creation of permissioned blockchain for company-specific usage. Cryptocurrency transactions, facilitating faster payments without an intermediary [3].

(ii) Blockchain for Health Sector : A blockchain-based data sharing system, integrating the medical records and history of the patient and integrating the resources of various hospitals. This also helps to deter single-point attacks. [4]

(iii) Blockchain for Education Sector: Primarily dealing with digitalization and decentralization of educational certifications [5]

Various other novel and innovative applications of Block chain and its applications can be stated. However, the purpose of this paper is to analyze these and other such approaches for their fallacies.

III.ANALYSIS OF THE REVIEW

Usage of Blockchain based technology spans from the mentioned application and many more,ranging from the field of IOT to Logistics, to government applications. However, they all incorporate the following features

1. Security- Elimination of a single point of failure. Encryption of data.
2. Data Consistency-A peer-to-peer connected network, regularly updating the ledger across the network with approved transactions.
3. Data Transparency- Transaction across the network are updated into the ledger and visible to all network participants
4. Data Privacy- Abstraction of sensitive information with the help of a pair of keys and Secure Hashing algorithm.

These features allow Blockchains to be versatile and meet the various needs of numerous industries. Within the context of this paper, we will be focusing on Implementation of data privacy, consistency and transparency. We would look at the gaps within these domains and enlist a few solutions.

IV. DATA CONSISTENCY IN BLOCKCHAIN

Block chain implements a distributed ledger across the network which maintains a history of approved transactions. Every participant can view the ledger and participate in the validation of transactions. The ledgers are immutable and possess a timekeeping mechanism for accurate recording of transactions. Further more, Consensus Algorithms are implemented to verify the transactions. Proof of work consensus requires providing a valid hash, generated after mining the block. Proof of stake algorithm enables validators to bet on discovery of blocks that can be added to the block chain and is an alternative to investing in expensive hardware. A shift has been seen from Proof of Work to Proof of Stake in the Ethereum Environment. Along with this, Blockchain also incorporates Encryption Consistency. This is based on the unique hashes of the blocks. The hashes have various properties such as:

1.Uniqueness: They are uniquely generated. No two data have the same hash.

2.Avalanche Effect- The hash value changes drastically with even the smallest change in the data.

3.Consistency- However, each data will always generate the same hash for the same hashing algorithm. This ensures the consistency of data, while strengthening its safety. A good hashing function has great randomization and minimal chances of hash collision. Other consistency attributes offered are auditability and verification of data, atomicity, durability as well as information integrity.

1.Challenges in the domain

The most obvious problems with the domain is that of consistency of data across various blockchains due to a lack of proper industry standards. This obstructs interoperability within Blockchains and deters construction of a collaborative environment. However, the major challenge is that of eventual consistency. It is achieved by using an order-executive architecture where the consensus mechanism first organizes the transactions and then sequentially executes them. It speeds up the confirmation process for a group of nodes. But it often results in performance failures in various blockchain. Additionally, the serial execution can make it slow and computationally expensive. It also compromises the security and transparency of a blockchain. The solution to these problems is discussed in Section VI.

V. DATA TRANSPARENCY IN BLOCKCHAIN

Data Transparency is a key feature of data quality. It ensures that valid and proper data is being utilized in important processes such as planning and decision making [8]. The transparency offered by Blockchain is unparalleled. Its smart contracts uphold the policies and queries of transparency. They also eliminate the need of an intermediary, thereby making the process more transparent and trustworthy. The ledgers are completely replicated among all peers as well and allow query transparency as well as auditability. Each participant can view the ledger and its recorded transactions. Data Transparency ensures that Blockchains are reliable. It eliminates the chances of tampering or duping. It helps ensure that no single entity has total control over the network.

1.Challenges

The major challenge in this domain is finding the right balance between Transparency and Privacy. Sharing data such that it does not infringe the privacy policies could be a tedious task.

Other problems that can be observed are:

1. Malicious Blockchain monitoring to map autonomous entities to real people or organizations.
2. Misusing validation for personal gain with the help of block-producing nodes. Since, they have the ability to choose which transactions and in what sequence to include in the upcoming blocks, as a result, they may increase their profits by keeping an eye on the transaction proposals that have not yet been included to a block (the mem-pool), choosing and ordering them in their favor, or even sandwiching them between their own transactions that are solely carried out for this purpose.
3. Excess transparency may even enable companies to monitor transactions of their competitors.

Section VI discusses the various practices that can be applied to reduce the severity of the problems. However, it is important to note that awareness of such problems and challenges is a crucial step in itself.

VI. DATA PRIVACY IN BLOCKCHAIN

Data privacy addresses how sensitive data, particularly personal data, should be handled. In order to ensure proper data management, data privacy regulations have been implemented that govern how personal data is gathered, processed, and kept. A key aspects of privacy with blockchains are:

1) Public and Private Keys: A special set of keys known as the public and private key is given to each user. They are connected cryptographically and consist of a random sequence of integers. Users cannot, theoretically speaking, infer another user's private key from that user's public key. Users are shielded from hackers by an additional degree of protection provided by this.

2) Digital Signature through Private Keys: Through digital signatures, private keys safeguard the user's security and identity. They provide an additional degree of identity identification and are used to access funds and personal wallets on the blockchain. When given access to the private key, individuals are required to provide a digital signature in order to send money to other users. Financial theft is prevented by this process.

1.Blockchain Privacy Regulations

1. General Data Protection Regulation (GDPR)

This is one of the regulation policies that governs over blockchain. Typically presiding over organizations and businesses, it enforces that businesses must obtain consent from the users before processing their data. It also provides the users the right to correct their information or delete it. Organizations must also anonymize the data to protect data privacy and notify the users in case of a breach.

2. California Consumer Privacy Act

This act also promotes and reinforces similar rights like GDPR. It also allows the users to take legal action against a data controller business that fails to secure their information. The consumer also has a right to know all data that businesses collect about them and disallow them, if required. They can also know from where and for what purposes the data was collected. This act also reserves the customer's right to ask about entities with whom the company shared their data.

2.Challenges

Within this context, breach of personal data constitutes breach of privacy. Any data that can link the wallet and user violates the privacy of the user, undermining anonymity. Some of the challenges within this domain are:

1) Through browser cookies, the identity of the customer may be connected to his true identity. When a customer uses bitcoin as payment, the service provider can connect the customer's actual identity to the token history recorded on the blockchain.

2) Since the blockchain nodes interact with one another via a P2P overlay network over the Internet, it's possible that when users submit new transactions, their IP addresses will make them traceable over the network.

3) Blockchain wallets keep track of the blockchain keys on users' devices, either online or (offline). However, wallets are vulnerable to theft attempts in which the attacker might remove or steal the user's private keys.

Due to various viruses and trojans' potential to crash key recorders and obtain encryption keys, this issue also impacts encrypted wallets.

4) Public blockchains like Bitcoin allow anyone to join.Businesses employing such a blockchain to store user data will make it publicly accessible, in violation of privacy laws. Users' data should only be visible to parties with clear authorisation

5) Immutability of records in these blockchain networks is another impediment. Ethereum or Bitcoin would not let users to edit or even erase their data,

Though these are some severe discrepancies, Section VI provides various solutions and approaches that can be implemented to reduce their severity. Despite the fact that several businesses and other parties provide security solutions, it is up to the user, to both, be conscious of these problems and use these methods. The best way to be safe is through personal security.

V. Other Challenges within Blockchain

So far, we have discussed the various challenges within a blockchain system pertaining to only three key aspects of blockchain: data consistency, transparency, and privacy. However, we would like to extend the scope and discuss a few problems and challenges within blockchain over a broader spectrum.

This section discusses some of the general problems with the blockchain. The statistics mentioned in this section are from 2021.

- According to a Deloitte survey, the mortality rate for blockchain initiatives undertaken by corporations is over 85%, and when accounting for all blockchain projects on GitHub, it even rises to 92%.
- Additionally, major IT firms like IBM and Microsoft have declared a decrease in their blockchain involvement.
- In contemporary circumstances, it is not unexpected that large and complex IT projects have a high failure rate.
- And given the extent of blockchain hype around financial speculation in relation to cryptocurrencies and Decentralized Finances , an even larger failure rate may be anticipated.

But the observation of the unexpectedly delayed adoption of blockchain technology beyond conceptions and prototypes has already led to disappointment and a growing body of research on why blockchain technology has, to this point, fallen short of original, lofty expectations in the context of supply chains. The next section discusses some of the solutions that can be employed to overcome the enlisted challenges, pertaining to both the general and specific aspects of the blockchain.

VI. PROPOSED SOLUTIONS

There are a number of solutions that can be implemented to boost the data security, and privacy of data over the blockchain. Many of the enlisted solutions provide a combined advantage of upholding both the data privacy and transparency.
Some of solutions are enlisted as follows:

1) Use of permissioned Blockchains:
Among the two types of blockchain available, one's the public permissionless blockchain. It allows anyone to join the network. It provides excessive data visibility and low throughput. Additionally, its transaction costs are substantial and frequently unstable. Alternatively, a private blockchain can be formed using only the concerning parties. Private blockchains with permissions that limit read access and consensus participation offer greater information exposure control.

2 Private Transactions
Private transactions are a characteristic feature of well-known permissioned blockchains like Quorum and Hyperledger Fabric, which help mitigate the downsides of overly open systems. Only a small number of nodes—specified at the smart contract or transaction level—carry out the execution based on the original data in these private transactions. These nodes can access the original data via a peer-to-peer messaging layer or read it from the blockchain and decrypt it.

3.Self-governing identities for individuals:
One of the main benefits of blockchains is the immutability of identity-related data, which may be given via digital signatures from third parties. It also involves using a distributed ledger to replace some ecosystem-related services that certificate authorities have previously offered which contain

information that is intended for public consumption. This idea was mostly inspired by the digital wallets that gained popularity thanks to blockchains, and is now frequently associated with blockchains.

4. Self governing identities for organizations

Digital IDs are easily accessible to businesses, enabling efficient cross-organizational identification and, as a result, allowed bilateral data interchange. Better master data and dynamic data exchange between firms may be made possible by this. Such systems provide access control for bilateral (non-blockchain based) operational data exchange that satisfies data sovereignty requirements by allowing businesses to precisely control the permissions of other organizations.

How self-governing identities preserve privacy

Digital IDs are easily accessible to businesses, enabling efficient cross-organizational identification and, as a result, allowed bilateral data interchange. Better master data and dynamic data exchange between firms may be made possible by this. Such systems provide access control for bilateral (non-blockchain based) operational data exchange that satisfies data sovereignty requirements by allowing businesses to precisely control the permissions of other organizations.

5) Using the "Zero-Knowledge Proof" technique to store only the proof of users' data on the blockchain and not the data itself. Within this system, only the proof of users' data on the blockchain. The actual user data must be kept in a different database using this method. Such distributed databases allow modification and deletion of users' data, therefore, data controllers can meet this key condition of the privacy regulations. You must still demonstrate the validity of the users' data, the accuracy with which your company gathered it, and the absence of any tampering. You must keep the blockchain updated with evidence of the veracity of the user data for this. You can accomplish this thanks to zero-knowledge proofs. With this method, the information in question may be kept elsewhere, but you just keep the documentation of its veracity.

VII. IMPLEMENTATION

To experience working of the Blockchain, we simulated our own Ethereum Transaction website, complete with MetaMask Connectivity. It is important to note that the system was tested in a developmental environment, with Ethereum borrowed from faucets like Goerli. Within this project, creating an account over the website is mandatory for usage. This ensure Data Consistency across various devices. Data Transparency is implemented by presenting a log recording the transaction, with their timestamps, a message if attached. And more importantly, Data Privacy is implemented with abstraction of public key within records as well. Data Security is also strengthened with the use of third party application such as Metamask. Github link for the project is as follows: https://github.com/MuktaPatil/ETH_Wallet.git

VIII.CONCLUSION

This paper presents a detailed study of the blockchain, with respect to some of its key features. As a revolutionizing technology, we study what kinds of challenges are encountered within the various aspects of blockchain. We see a lot of light being shed on the positive impacts of the blockchain, while most people are unaware of the fallacies and loopholes within the internal working of the system. Though blockchain still provides some revolutionary features, it is important to keep in mind that this technology is still in its infancy. Even its strongest features have room for improvement. Within this paper, we have discussed six such methods that are currently being researched and up for experimentation. Many of these are being employed in various fields and applications. However, a widespread implementation is yet to be achieved.

IX. FUTURE SCOPE

Blockchain has a distinctively decentralized nature, making it the perfect instrument for a strong cybersecurity architecture. the primary field in which blockchain is already advancing. The importance of cybersecurity is increasing every day, especially in light of recent cyberthreats and assaults on major corporations. For instance, a number of well-known companies, such as Apple and Sony, had their data compromised.

When it comes to security data, blockchain might be a hidden rescuer for both large and small businesses. Although the technology has been thriving in many areas, it appears that cybersecurity is where it shines the brightest so far.

REFERENCES

[1] J. Hendler, "Web 3.0 Emerging," in Computer, vol. 42, no. 1, pp. 111-113, Jan. 2009, doi: 10.1109/MC.2009.30.

[2] Grover, P., Kar, A.K., Vigneswara Ilavarasan, P. (2018). Blockchain for Businesses: A Systematic Literature Review. In: , *et al*. Challenges and Opportunities in the Digital Era. I3E 2018. Lecture Notes in Computer Science(), vol 11195. Springer, Cham. https://doi.org/10.1007/978-3-030-02131-3_29

[3] Brühl, V., 2017. Bitcoins, Blockchain und Distributed Ledgers. Wirtschaftsdienst, 97(2), pp.135-142.

[4] Chen, C.-M., Deng, X., Kumar, S., Kumari, S., & Islam, S. H. (2021). Blockchain-based medical data sharing schedule guaranteeing security of individual entities. Journal of Ambient Intelligence and Humanized Computing. doi:10.1007/s12652-021-03448-7

[5] Steiu, M.-F. (2020). Blockchain in education: Opportunities, applications, and challenges. First Monday, 25(9).

[6] Kanga, D.B., Azzouazi, M., El Ghoumrari, M.Y. and Daif, A., 2020. Management and Monitoring of Blockchain Systems. Procedia Computer Science, 177, pp.605-612.

[7] Marijan, D. and Lal, C., 2022. Blockchain verification and validation: Techniques, challenges, and research directions. *Computer Science Review*, *45*, p.100492..

[8] Elisa Bertino, Ahish Kundu, and Zehra Sura. 2019. Data Transparency with Blockchain and AI Ethics. J. Data and Information Quality 11, 4, Article 16 (August 2019), 8 pages.

[9]Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." 2015 IEEE Security and Privacy Workshops. IEEE, 2015.

[10] Sedlmeir, J., Lautenschlager, J., Fridgen, G. et al. The transparency challenge of blockchain in organizations. Electron Markets 32, 1779–1794 (2022). https://doi.org/10.1007/s12525-022-00536-0

[11] Hellani, Houssein, et al. "On blockchain integration with supply chain: Overview on data transparency." Logistics 5.3 (2021): 46.

[12] Bernabe, J.B., Canovas, J.L., Hernandez-Ramos, J.L., Moreno, R.T. and Skarmeta, A., 2019. "Privacy-preserving solutions for blockchain: Review and challenges". IEEE Access, 7, pp.164908-164940.

[13] Zyskind, G. and Nathan, O., 2015, May. "Decentralizing privacy: Using blockchain to protect personal data". In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.

[14] Wang, H., Ma, S., Dai, H.N., Imran, M. and Wang, T., 2020. "Blockchain-based data privacy management with nudge theory in open banking". Future Generation Computer Systems, 110, pp.812-823.

[15] Arora, D., Gautham, S., Gupta, H. and Bhushan, B., 2019, October. " Blockchain-based security solutions to preserve data privacy and integrity." In 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 468-472). IEEE.

[16] I.-C. Lin, T.-C. Liao, " A survey of blockchain security issues and challenges" , Int. J.Netw. Secur. 19 (5) (2017) 653–659.

[17] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, " Blockchain challenges and opportunities: a survey" , Int. J. Web Grid Serv. 14 (4) (2018) 352–375.

[18] D. Bayer, S. Haber, W.S. Stornetta," Improving the efficiency and reliability of digital time-stamping" , in: R. Capocelli, A. De Santis, U. Vaccaro (Eds.), Sequences II, Springer, New York, NY, USA, 1993.

[20] A. Groetsema, A. Groetsema, N. Sahdev, N. Salami, R. Schwentker, F. Cioanca Blockchain for Business: an Introduction to Hyperledger Technologies" , The Linu Foundation, 2019.

[21] P. Vasin, BlackCoin's Proof-of-Stake Protocol v2. in-pos-protocol-v2-whitepaper.pdf. Accessed March 21, 2021.