INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN: 2455-0620 [Impact Factor: 6.719]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 8, Issue - 11, November - 2022 Publication Date: 15/11/2022

DOIs:10.2015/IJIRMF/202211002 --:-- Research Article

A Comprehensive study on the Protection of Transactional Information in Blockchain and Privacy Issues

Dr. R. NAVEEN KUMAR
Asst. Professor, Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore, India
Email: naveenkumarr@skacas.ac.in

Abstract*: Blockchain is gaining friction and is termed as one of the most ubiquitous topics nowadays. Even though critics question its technology, scalability, sustainability, and security have already changed many individuals' lifestyles in some areas due to its undue influence on industries and businesses. Permitting the features of blockchain technology to guarantee more dependable and convenient services, it's important to consider the security and privacy issues and challenges of being a creative technology. The continuum of blockchain applications ranges from financial, health care, automatic, risk management, internet of things to public and social services. More things to focus on utilizing the blockchain data structure in various applications. Besides, a wide survey on technical and applications perspectives has not been trained. In this, we are trying to survey blockchain Technology and its security.*

Keywords*: Blockchain, Securities, Consensus model, Hash function.*

1. INTRODUCTION:

Over several years, the internet has been seen as the initiation of numerous bottom-up, significant applications that solve the problems in obliging, and distributed techniques. Some of those public and non-profit systems have become widespread and well-known [1]. The most question which is ascending with amazing frequency is referred to bitcoin and additionally, the technology source behind it is called Blockchain. Blockchain has been digitized, decentralized, and public records of all bitcoin transactions. The transaction has been digitally signed with a public key and a private key. The blockchain can change the way the data is stored, shared, and achieved. The most powerful aspects of the technology are the barriers to tampering or deleting information that has been added to the chain. In theory, the blockchain should be more cost-efficient, secure, and quicker than other technologies in the use of corporates. It became a big deal when Cryptocurrencies have been a buzzword since Bitcoin launched in 2008[2][4]. However, the potential of the blockchain has taken off over the past years. There are many potential uses of the blockchain being explored, including Know Your Customer, Anti-Money Valeting, trade scrutiny, smart contracts, collateral management, settlement, and clearing, as well as the ability to capture the current ownership of high-value items. Smart contracts are a set of agreements that are encoded in programming software and automatically executed upon certain criteria being met. The obvious advantages of smart contracts include reduced contract execution costs, improved quality, and increased speed. Smart contracts can be stored on the blockchain

1.1 ELEMENTS OF BLOCKCHAIN TECHNOLOGY:

Consensus model: The consensus model helps to save the sanctity of data recorded on the blockchain. A protocol has 3 properties: **a) Safety:** a protocol should be safe and stable, which means all the nodes should give the same output that is valid with the protocol rules. **b)Liveness:** a protocol gives promise to all nonfaulty nodes to earn value. **c)Fault tolerance:** a protocol gives tolerance while giving recovery to a failure node participating in the protocol.

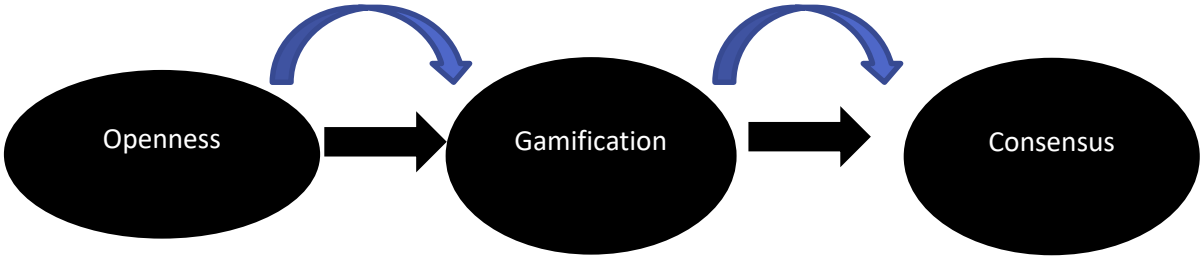

Fig 1: Elements of blockchain technology

2. STRUCTURE OF BLOCKCHAIN:

Blockchain technology is expected to greatly impact approximately all industries shortly. Accounts establishments are developing in ingenious ways to start testing and investing in this technology, making it extremely significant for everyone to understand the structure as well as the working algorithm of the blockchain technology. A blockchain is a growing list of records called blocks, which are secured using cryptography[3].

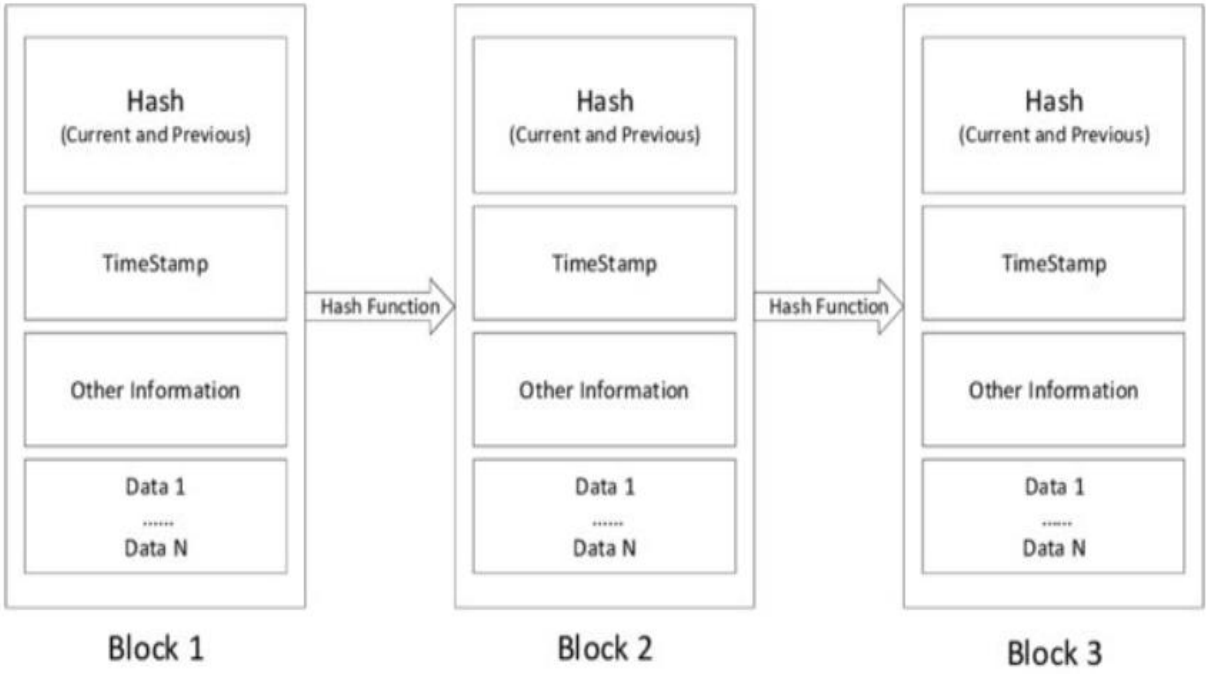

Fig 1.1 Structure of blockchain data

The structure of blockchain data is efficient and the adjoining list of transaction blocks can be maintained in a modest database or the form of flat files. **Data:** It could be used in a peer-to-peer file system such as IPFS, in distributed databases such as Apache Cassandra, in cloud file storage such as storj, Ethereum swarm, Asia, etc. **Hash:** A hash function is the one that takes an input of any length and generates the output with a unique fixed length. If a single value in the input is modified, the output is extremely different. Hash functions are used ubiquitously in blockchain technology. **Timestamp:** Timestamping is a method used to track the creation or modification time of a document securely[4].

3 . SECURITY OF BLOCKCHAINS:

Security in blockchain can be defined as the protection of transaction information and data in a block (whatever form of data) against internal and peripheral, malevolent, and unintentional threats. Typically, this protection involves the detection of threats, prevention of threats, and an appropriate response to threats using security policies, tools, and IT services. Some ideas and principles in security are listed as **Defense in penetration:** It is a plan of action that uses numerous corrective measures to prevent the data.

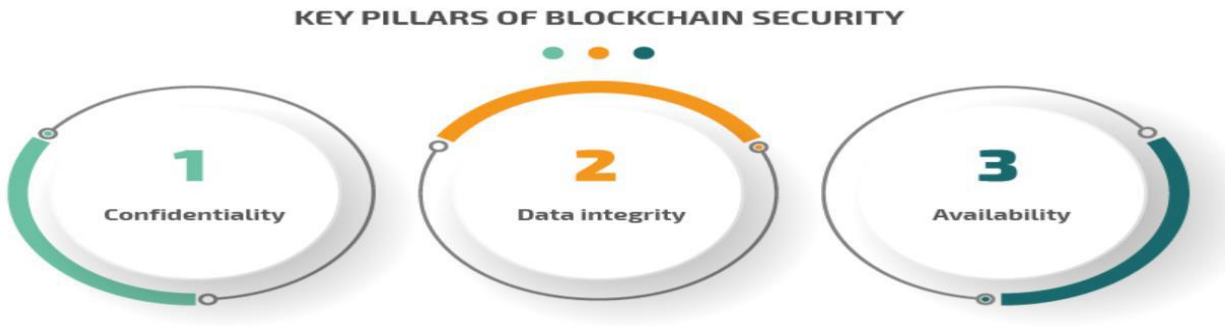

Fig:2 Security in blockchain

It follows the principle that protecting data in different layers is more efficient as opposed to a single security layer. **Minimum privilege:** In this strategy, access to data is reduced to the lowest level possible to reinforce an elevated level of security. **Manage vulnerabilities:** In this master plan, we check for exposures and manage them by identifying, authenticating, modifying, and patching. **Manage risks:** In this, we process the risks in an environment by identifying, assessing, and controlling risks. **Manage patches:** In this, we patch the flawed part like code, application, operating system, firmware, etc. by acquiring, testing, and installing patches[5].

4. PRIVACY OF BLOCKCHAINS:

Privacy is the competence of a single person or a group to concealed themselves or data, therefore, expressing themselves thesaurus. Privacy in blockchain means being able to perform transactions without leaking identification information. At the same time, privacy allows a user to remain compliant by discerningly revealing themselves without showcasing their activity to the entire network. The goal of intensifying privacy in blockchains is to make it extremely difficult for other users to copy or use other users' crypto profiles. An unfathomable volume of variations can be perceived when applying blockchain technology[6].

Some common characteristics are particularly significant and are summarized as follows: **a) Stored data sorting:** The privacy perspective in blockchain varies for personal and organizational data. Although privacy rules are pertinent for personal data, more stringent privacy rules apply to sensitive and organizational data. **b) Storage distribution:** The nodes in the network that stores complete copies of the blockchain are called full nodes. The full nodes in combination with the append-only characteristic of blockchain lead to data redundancy. This redundancy of data supports two key features of blockchain technology including transparency and verifiability. The compatibility of the application with data minimization decides the level of transparency and verifiability of that network for an application. **c) Append-only:** It is impossible to alter the data of previous blocks in the blockchain undetected. The append-only feature of blockchain in certain cases does not curtail the right to correction of users, especially if data is recorded incorrectly. Special attention needs to be provided while assigning rights to data subjects in blockchain technology[7].

5. BLOCKCHAIN IN MOBILE APPLICATIONS:

The first client successfully solving the puzzle to validate a transaction using any of the consensus techniques a reward is specified. This is called a speed game amid miners and the puzzle cannot be handled using mobile devices. To attain mobile blockchain processing we can use the computing concept.

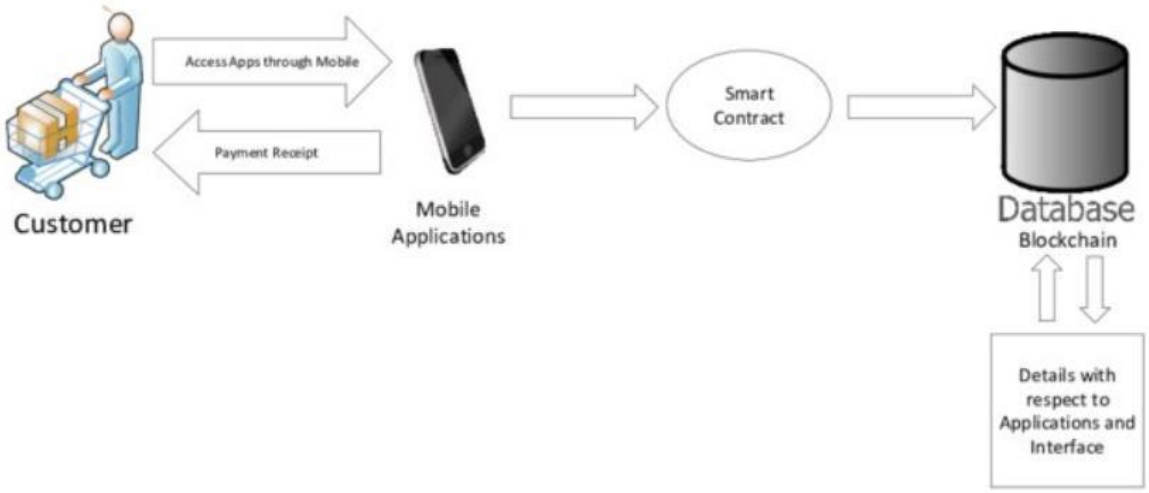

Fig:2.1 **Mobile applications**

The current cyber defense seems to be faltering and incremental enhancements fall short of the growing cyber threat. Blockchain technology overturns the cybersecurity paradigm due to its trustless, transparent, and fault-tolerant thereby reducing the probability of data compromise.

The application of blockchain technology in national defense Since Blockchain uses a Keyless Security Infrastructure (KSI) to store all the data in form of a cryptographic hash and run a hashing algorithm for verification, any manipulations to the data can be instantly identified in real-time as the original hash object is always available on other blocks in the chain, ensure and securing the maximum protection of the mobile app infrastructure[8].

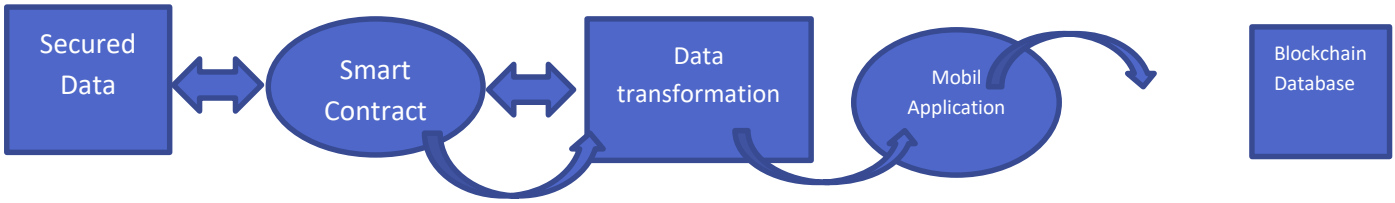

Fig : 2.2 The working of Mobile application using Blockchain.

The core elements in the working of blockchain, like secure hashing, backlinked data structure, and consensus mechanism, play a significant role in attributing the security factor of blockchains. Blockchain can be used in defense applications by acting the operational or support roles as follows: Cyber defense, Supply chain management, and Resilient Communications.

5.1 CHALLENGES AND OPPORTUNITIES :

Blockchain technology faces a few good times as well as a dare. Although significant, the challenges can be overcome with the maturity and enhancement of technology in the future. This will lead to a plethora of future opportunities for blockchain to be implemented and accepted. The challenges and opportunities would be discussed in detail in this section. **Selfish mining:** Selfish mining is another challenge faced by blockchains. A block is susceptible to cheating if a small portion of hashing power is used. In selfish mining, the miners keep the mined blocks without broadcasting to the network and create a private branch that gets broadcast only after certain requirements are met. In this case, honest miners waste a lot of time and resources while the private chain is mined by selfish miners[9].

Personally identifiable information: Personal Identifiable Information (PII) is any information that can be used to extricate an individual's identity. **Security:** It is a challenge in open networks. Confidentiality is low in distributed systems that imitate information over its network. Probity is the specialism of blockchains although there exist many challenges. Blockchains are high in terms of comprehensibility due to wide replication compared to write availability. **Opportunities:** Opportunities can be stated as a chance to integrate blockchain technology in existing applications to improve efficiency and usage use as well as to promote this technology in future applications. Some of the future opportunities are listed in more detail as follows. **Strategic alignment and governance:** Active management of connections between enterprise progressions and administrative priorities that aims to facilitate operative actions for

business performance improvement can be referred to as strategic alignment. The analysis includes the evaluation of different processes on how they can be improved with the usage of blockchain technology. The risks of these strategies analogous to the lock-in effects might also need to be analyzed[10].

6. CONCLUSION :

Blockchain technology is exceedingly recognized and appraised due to its decentralized infrastructure and peer-to-peer nature. These characteristics have the potential to support a plethora of requirements in different areas and applications. In this paper, we propose a comprehensive survey by initially discussing the structure of blockchains and their major components and characteristics. Then we endeavor to highlight the security and privacy issues faced by blockchain technology in the different areas of its usage. Finally, future applications, opportunities, and challenges of blockchain technology are summarized. With the rapidity of its growth and development, we believe that blockchains will soon become a very common and well-known phenomenon. Blockchain can be compared to the Internet a few decades ago to a certain extent. Since the core of blockchains is secure and supportive, gradually many major applications that require security and non-repudiation will move on to this technology.

REFERENCES :

1. C. Ai, M. Han, J. Wang and M. Yan, An efficient social event invitation framework based on historical data of smart devices, in 2016 IEEE International Conferences on Social Computing and Networking (Social Com), IEEE, 2016, 229–236. doi: 10.1109/BDCloud-SocialCom-SustainCom.2016.44.CrossRef Google Scholar.
2. Dr. R. Naveen Kumar "The Future Impact of Blockchain Technology using Decentralization Networks" (IJARESM), ISSN: 2455-6211 Volume 8, Issue 9, September-2020, Impact Factor: 4.597.
3. Archana Prashanth Joshi, Meng Han∗ and Yan Wang Kenne saw "A Survey On Security And Privacy Issues Of blockchain Technology State University, Marietta, GA30060, USA.
4. N. Barnas, Blockchains in national defense: Trustworthy systems in a trustless world, Blue Horizons Fellowship, Air University, Maxwell Air Force Base, Alabama. Google Scholar
5. Z. Cai, Z. He, X. Guan, and Y. Li, Collective data-sanitization for preventing sensitive information inference attacks in social networks, IEEE Transactions on Dependable and Secure Computing, (2016), 1-1. doi: 10.1109/TDSC.2016.2613521.CrossRef Google Scholar.
6. N. Capurso, T. Song, W. Cheng, J. Yu, and X. Cheng, An android-based mechanism for energy-efficient localization depending on indoor/outdoor context, IEEE Internet of Things Journal, 4 (2017), 299-307. doi: 10.1109/JIOT.2016.2553100.CrossRef Google Scholar.
7. F. Chen, P. Deng, J. Wan, D. Zhang, A. V. Vasilakos and X. Rong, Data mining for the internet of things: Literature review and challenges International Journal of Distributed Sensor Networks, 11 (2015), 431047. doi: 10.1155/2015/431047.CrossRef Google Scholar
8. A. Dorri, S. S. Kanhere and R. Jurdak, Blockchain in the internet of things: challenges and solutions, arXiv preprint, arXiv: 1608.05187. Google Scholar
9. Dr. R. Naveen Kumar "The Persistence of Blockchain Technology using Digital Signature and Hash Functions" (IJARESM), ISSN: 2455-6211 Volume 8, Issue 11, November-2020, Impact Factor: 7.429.
10. M. Han, Z. Duan and Y. Li, Privacy issues for transportation cyber-physical systems, in Secure and Trustworthy Transportation Cyber-Physical Systems, Springer, Singapore, 2017, 67–86. DOI: 10.1007/978-981-10-3892-1_4.CrossRef Google Scholar.
11. M. Han, J. Li, Z. Cai, and Q. Han, Privacy reserved influence maximization in GPS-enabled cyber-physical and online social networks, in 2016 IEEE International Conferences on Social Computing and Networking (Social Com), IEEE, 2016, 284–292. DOI: 10.1109/BDCloud-SocialCom-SustainCom.2016.51.CrossRef Google Scholar.
12. M. Han, M. Yan, J. Li, S. Ji, and Y. Li, Generating uncertain networks based on historical network snapshots, in International Computing and Combinatorics Conference, Springer, Berlin, Heidelberg, 2013, 747–758. DOI: 10.1007/978-3-642-38768-5_68.CrossRef Google Scholar.
13. M. Han, M. Yan, J. Li, S. Ji and Y. Li, Neighborhood-based uncertainty generation in social networks, Journal of Combinatorial Optimization, 28 (2014), 561-576. DOI: 10.1007/s10878-013-9684-y.CrossRef math-review Google Scholar.