International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Survey Paper Volume-6, Issue-4, 2019 Regular Edition E-ISSN: 2349-7084

A Survey of Blockchain Technology Security

Ayushi Singh[1*], Gulafsha Shujaat[2], Isha Singh[3], Abhishek Tripathi[4], Divya Thakur[5]

[1]*Dept. Computer Science Engineering, Buddha Institute of Technology, Gorakhpur (U.P.), India*
[1]*Dept. Computer Science Engineering, Buddha Institute of Technology, Gorakhpur (U.P.), India*
[1]*Dept. Computer Science Engineering, Buddha Institute of Technology, Gorakhpur (U.P.), India*
[1]*Dept. Information Technology, Buddha Institute of Technology, Gorakhpur (U.P.), India*
[1]*Dept. Computer Science Engineering, Buddha Institute of Technology, Gorakhpur (U.P.), India*

e-mail: Ayushi Singh aayushissingh3003@gmail.com, Gulafsha Shujaat gulafsha1608@gmail.com, Isha Singh getisha5@gmail.com, Abhishek Tripathi a.tripathi1612@gmail.com,

**Corresponding Author: Ayushi Singh* aayushissingh3003@gmail.com,

Available online at: http://www.ijcert.org

Received: 08/04/2019, Revised: 16/04/2019, Accepted: 21/04/2019, Published: 30/04/2019

Abstract:- Bitcoin is a popular cryptocurrency that records all transactions in an allotted append-handiest public ledger referred to as a blockchain. The security of Bitcoin heavily relies on the motivation-suitable proof-of-work (PoW) founded dispensed consensus protocol, which is run with the aid of the community nodes known as miners. Because of its inception, blockchain technological know-how has proven promising application possibilities. The spectrum of blockchain functions stages from financial, healthcare, automobile, hazard administration, internet of matters (IoT) to public and social offerings. Several reports focal point on utilizing the blockchain information structure in various applications. These vulnerabilities result in the execution of different security threats to the ordinary functionality of Bitcoin. We then examine the feasibility and robustness of the brand new safety solutions. Moreover, we discuss the current anonymity concerns in Bitcoin and the privateness-related threats to Bitcoin customers together with the evaluation of the comprehensive privacy-keeping solutions.

Keywords: Blockchain, Bitcoin, Peer to Peer digital currency

1. Introduction

Since the beginning of Bitcoin in 2009, its fundamental technique, blockchain, has shown promising application prospects and attracted many attentions from academe and trade [1]. There is growing interest all told industrial zone to use blockchain technology for his or her functions (such as shielded obligation, money transactions, allocating health info, etc.) whereas it had been initially expanding to support cryptocurrencies like Bitcoin. It's price noting that Bitcoin is currently treated as stock in Wall Street and therefore the money market whereas its purpose and the real expense is, however, to go on, and its future isn't clear [2]. Bitcoin was evaluated because the prime acting currency in 2015 and therefore the best acting trade goods in 2016 and has over 300K confirmed transactions daily in could 2017. At constant time, the blockchain technology has been applied to several fields, together with medication, economics, Internet of things, code engineering so on [1].

The establishment of Turing-whole programming languages to regulate user to sensible contracts running on the blockchain marks the beginning of blockchain a pair of the era. With the localized agreement mechanism of the blockchain, good contracts permit reciprocally distrusted users to complete information exchange or dealings while not the necessity for any trusty third-party authority. Blockchain technology is getting used to shield sensitive records and to attest the identity of a user. Keyless Security Infrastructure (KSI) stores information hashes on blockchains and runs a algorithmic hashing rule for his or her verification. Public Key Infrastructure (PKI) [3].

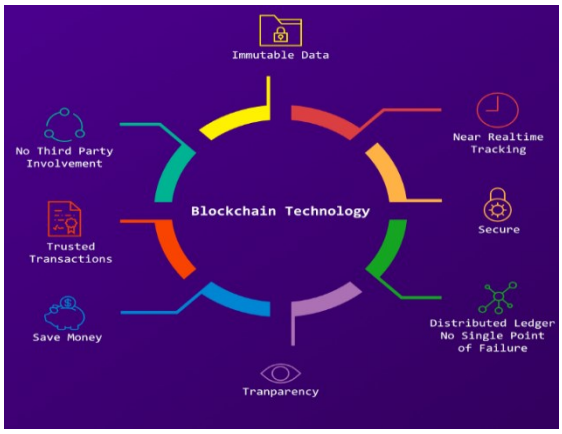

Fig 1: BlockChain Technology [4]

Any information manipulation may be noticed because the original hash is obtainable on different nodes coupled to the system, sanction native banks to travel on the far side uneven coding and caching keys [5] publicly. Blockchain technology is finding applications in a big selection of areas; each money and non-financial. Money establishments and banks now not recognize blockchain technology as a threat to ancient business models.

2. Analysis of Blockchain Technology

This segment introduces the most techniques used within the blockchain. We tend to 1st add the basic trust structure (i.e., the agreement mechanism) employed in the blockchain, so make a case for the synchronization method between nodes. After that, we tend to introduce the development phases of the blockchain.

2.1 Consensus Mechanism

Being a decentralized blockchain structure don't want a trusty third-party authority. Instead, to ensure the creditability and unity of the information and transactions, blockchain acquires the decentralized system. Within the actual blockchain systems, there is a unit four primary accord system [6]. PoW (Proof of Work), PoS (Proof of Stake), Other consensus mechanisms, such as PoB (Proof of Bandwidth) [7], PoET (Proof of Elapsed Time) [8], PoA (Proof of Authority) [9] and so on, are also used in some blockchain systems.

PoW mechanism uses the explanation of the puzzle to justify the believability of the info. The problem is typically a hard computationally however directly testable downside.

2.2. Block Propagation and Synchronization

In the blockchain, every full node reserve the knowledge of every block. The ingenuity to building trust and consensus for blockchain, the block spreading mechanisms may be divided into the following classes [10].

a. Advertisement-based propagation

This Transmission mechanism is originated from Bitcoin. Once node A receives the know-how of a block, A can send AN inv message (a message sort in Bitcoin) to its linked peers. Once node B obtain the inv message from A, it'll do as follows. If node B already has the understanding of this block, it's going to do not anything. If node B would not know, it will reply to node A.

b. Send headers propagation

This propagation mechanism is accomplice associated improvement to the advertisement-based propagation mechanism. Within the send headers propagation mechanism, node B can ship a send headers message (a message kind in Bitcoin) to node A. Once node A receives the facts of a block, it will send the block header information on to node B.

c. Unsolicited push propagation

In the automatic push mechanism, while one block is strip-mined, the miner can immediately broadcast the block to opportunity nodes. During this propagation mechanism, there may be no inv message and ship headers message

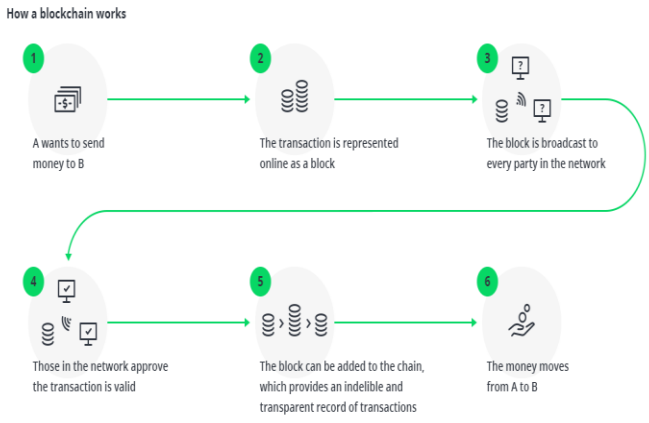

Fig 2: How blockchain work [4]

In literature there are two main categories of blockchain are distinguished:

• *Permissionless Blockchain*
• *Permission Blockchain*

a. Permissionless Blockchain

Permission-less Blockchain is those wherever anybody will be a part of the network to be a champion while not getting any prior permission to perform such network tasks. Since anybody will be a part of, distinctive styles of incentive mechanisms are necessary so as for verifiers to participate. Its advantage that it will accommodate each anonymous and pseudo-anonymous actors [11]. Bitcoin and Ehtereum samples of permission-less blockchains. Risk in Permissionless blockchain [12].

b. Permissioned Blockchain

The other kind is that the supposed permissioned blockchain wherever special permission is required from associate degree authority to become a supporter within the system. Permissioned blockchains square measure meant to be purposeful, and might, therefore, be created to keep up compatibility with existing applications (financial or otherwise) [12]. A bonus of a permission blockchain is quantifiability. During a permissionless blockchain, the information is held on each pc within the network, and every one node verify all transactions. During a permission blockchain, solely a smaller range of preselected participants can get to operate. However, due to the lower range of participants, it's abundant easier for a gaggle of users to collaborate and alter the principles or revert transactions which is why solely trustworthy parties ought to be a permission to act as verifiers. Samples of permission blockchains embody Eris, Hyper ledger, and Ripple [13].

The dialing information is recorded and shared with the different computer systems in the blockchain community. The completed block is distributed out across the community, wherever it's appended to the chain. The key to blockchain's safety are some things known as a hash. A hash perform takes the knowledge in each block and uses it to shape the hash (a different string of characters). The HASH from one block is price-introduced to the records inside the next block, so as soon as succeeding block goes via the hash carry out the dealing info is recorded and shared with the alternative computers within the blockchain community. On the community, the document is mixed with alternative transactions right into a block –like a traditional online database. Every dealing is time-stamped.

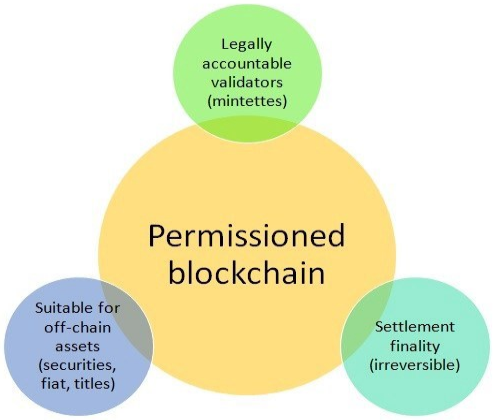

Fig 3: Permissioned Blockchain [14]

1. Risks to blockchain

Blockchain era can come to be the new engine of the boom in digital economy wherever we tend to place unit steadily victimization net to conduct virtual commerce and proportion our statistics and lifestyles events.

a. Private key security

When exploitation blockchain, the person's hidden secret's idea to be the identification and safety credentials, this is generated and maintained by the consumer rather than third-party organizations [15]. Once the private key of a people is lost, it will no longer be able to be recovered. If criminals take the personal key of consumers, the user's blockchain account can face the threat of being tampered with the aid of others.

b. Criminal activity

When victimization blockchain, the crucial personal concept to be the identity and security certification that is generated and maintained utilizing the user in preference to third-party businesses some frequent criminal activities with Bitcoin include

c. Ransomware:-

The cyberpunk frequently uses ransomware for coins coercion and use Bitcoin as a commercialism coinage. In July 2014, ransomware titled CTB-Locker escalation around the world via cloaking itself as mail attachments [16]. If the user clicks the connection, the ransomware can run in the legacy of the device and code concerning 114 forms of each record

d. Underground market:-

Bitcoin has usually used because of the foreign money within the underground marketplace. As an example,

an alternate path is AN anonymous, global online marketplace that operates as a Tor hidden service and makes use of Bitcoin as its trade forex [17].

e. Transaction privacy leakage

Since the customers' behaviors in the blockchain are traceable, the blockchain systems take measures to safeguard the dealings privacy of customers. Within the Bitcoin and Zcash, they use one-time accounts to keep the acquired cryptocurrency. Moreover, the user has to assign a personal key to each dealings [18]. During this method, the wrongdoer cannot infer whether or not an equal user receives the cryptocurrency in numerous transactions.

2. Security enhancements

In this section, we tend to summarize security enhancements to blockchain systems, which may be utilized in the event of the blockchain system

4.1. SmartPool

The guide miner conducts hashing computation supported the duties and returns the finished stocks to the smart pool purchaser. Once the quantity of the completed stocks reaches to a certain amount, they're going to be devoted to smart pool contract this is deployed in Ethereum. The poor smart contract can confirm the shares and supply rewards to the customer [19]. Compared with the standard P2P pool, SmartPool system has the following advantages:

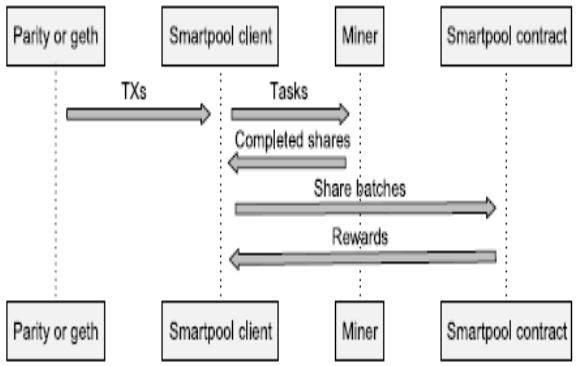

Fig 4: Overview of SmartPool's execution process [5].

Decentralized:

The core of the SmartPool is enforced in the form of a realistic settlement this is deployed inside the blockchain. Miners must be forced to preliminary hook up with Ethereum to mine through the shopper [20]. Mining pool will accept Ethereum's agreement mechanism to run. During this approach, it ensures the decentralization nature of pool miners.

Efficiency:

Miners will send the completed stocks to the smart pool take delivery of batches. Moreover, miners entirely must be forced to carry a part of the shares to be established, no longer all stocks. Hence, SmartPool is additional low-cost than the P2P pool [21].

Secure:

SmartPool clout a unique business enterprise, which may prevent the assailant from republishing stocks in many batches. Moreover, the verification methodology of Smart Pool will guarantee that honest miners can advantage expected rewards even there exist malicious miners inside the pool [5]

4.2. Quantitative framework

There exist trade-offs among blockchain's overall performance, and protection recommend a quantitative framework; this is leveraged to investigate PoW-based blockchain's execution overall performance and security provisions. Through the simulator's evaluation, it's going to benefit performance data of the target blockchain, in addition, to block propagation instances, block sizes, network delays, stale block rate, throughput, etc. [22]. The old block refers to a neighborhood that's properly-mined but now not written to most people chain. The turnout is that the range of transactions that the blockchain will deal with inline per second.

4.3. Hawk

Privacy leakage might be a critical risk to the blockchain. Within the generation of blockchain 2.0, now not solely transactions but conjointly agreement-related material are public, like contract's bytecode, appeal to parameters, and many others. Hawk, an exact framework for growing privateness-preserving properly agreements. Leverage Hawk, developers will write precise personal contracts, and it's not vital for them to use several code secret writing or obfuscation techniques.

Moreover, the economic transaction's records won't be expressly held in blockchain. Once programmers broaden Hawk contract, the settlement might be divided into 2 parts: personal component, and public component [23]. The intimate knowledge and monetary operate connected codes will be written into the personal portion, and codes that don't involve personal data will be written into the general public portion

5. Conclusion

The blockchain could be very appraised and supported for its suburbanized infrastructure and peer-to-peer nature. However, many varieties of analysis regarding the blockchain are secure by using Bitcoin. However, blockchain can be applied to a spread of the field's way on the same distance side Bitcoin. Blockchain has proven its capability for remodeling the regular alternate with its essential characteristics: decentralization, tenacity, anonymity, and auditability in the course of this paper, we generally tend to specialize inside the protection issues with blockchain technology. By finding out the favored blockchain systems (e.g., Ethereum, Bitcoin, Monero, and many others.), we tend to behavior a regular exam of the safety risks to the blockchain. For every danger or vulnerability, we tend to analyze its causes and attainable consequence. Moreover, we generally tend to survey the vital attacks at the blockchain structures and analyze the vulnerabilities exploited in these attacks. Finally, we tend to summarize blockchain security improvements and endorse several destiny guidelines all through this space.

REFERENCES

[1] A. Ferrag, M. Derdour and. M. Mukherjee, "Blockchain technologies for the internet of things: research," *IEEE,* 2018.

[2] . B. Carminati, . L. Bahri and . E. Ferrari, "Decentralized privacy preserving services for online social networks," *Online Soc Netw media,* 2018.

[3] Z. Zheng , . S. Xie and H.-N. Dai, "Blockchain challenges and opportunities: a survey," *Int. J. Web and Grid Services,* vol. 14, 2018.

[4] Unocoin, "What Factors Are Influencing Blockchain Technology," 2018.

[5] X. Li, P. Jiang, Q. Wen and X. Luo, "A survey on the security of blockchain systems," *Future Generation Computer Systems,* 2017.

[6] Z. Zheng, S. Xie and H. Wang, "Blockchain challenges and opportunities: A Survey," *Internat. J. Web Grid Serv.,* 2016.

[7] M. Ghosh, M. Richardson and B. Ford, "A TORPATH TO TORCOIN, PROOF-OF-BANDWIDTH ALTCOINS FOR COMPENSATING RELAYS".

[8] Intel, "Proof of elapsed time (poet)," 2017.

[9] P. Technologies, "Proof of Authority Chains," 2017.

[10] A. Gervais, G. Karame and V. Glykantzis, "On the security and performance of proof of work blockchains,," *SIGSAC Conference on Computer and Communications Security,* 2016.

[11] W. J. Gordo and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," *Computational and Structural Biotechnology Journal,* 2018.

[12] M. Hölbl, A. Kamišali´ and L. N. Zlatolas, "A Systematic Review of the Use of Blockchain," *Symmetry 2018,* 2018.

[13] P. Novotny, D. N. Dillenberger and R. Vaculin, "Permissioned Blockchain Technologies for".

[14] K. Yilmaz, "Comparison of Permissioned Blockchains," Coinmonks.

[15] H. Mayer, "ECDSA Security in Bitcoin and Ethereum: a Research," 2016.

[16] S. Alliance, "Know your ransomware: Ctb-locker," 2017.

[17] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous," *The 22nd International Conference on World wide,* 2017.

[18] A. Miller, M. Möser, K. Lee and A. Narayanan, "An empirical analysis of linkability in the monero blockchain," *ArXiv preprint,* 2017.

[19] E. community, "Official Go implementation of the Ethereum protocol," 2017.

[20] B. Bodó, J. P. Quintais and D. Gervais, "Blockchain and smart contracts: the missing link in copyright licensing," *International Journal of Law and Information Technology,* vol. 26, no. 4, 2018.

[21] Z. Zheng, S. Xie and H.-N. Dai, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *IEEE International Congress on Big Data,* 2017.

[22] M. Bartoletti, T. Cimoli and L. Pompianu, "Blockchain for social good: a quantitative analysis," *Goodtechs,* 2018.

[23] A. Kosba, C. Papamanthou and . A. Miller, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *IEEE Symposium on Security and Privacy,* 2016.

