A Comprehensive survey on Blockchain: Working, security analysis, privacy threats and potential applications

Sumit Soni
Department of Computer Science and Engineering
HMR Institute of technology and Management
Delhi, India
sumitv1998@gmail.com

Bharat Bhushan
Department of Computer Science and Engineering
Birla Institute of technology, Mesra
Ranchi, Jharkhand, India
bharat_bhushan1989@yahoo.com

Abstract—**Recently, Blockchain a decentralized as well as distributed public ledger technology in (P2P) peer-to-peer network, has received considerable attention. It applies a block structure (linked) used to store as well as verify data and also applies the trusted mechanism for synchronization of changes in data in order to possibly create a tamper-proof digital platform for sharing as well as storing data. Blockchain can also be used to diverse the interactive system of internet (e.g. supply chain system, Internet of things). The blockchain model of bitcoin has been used in wide range of services like from asset trading to transaction of real estate, from services of escrow to national income distribution system in some countries. In this paper we present a comprehensive survey on blockchain, working of blockchain, security analysis on blockchain, privacy threats for blockchain and potential applications of blockchain.**

Keywords— bitcoin, DoS attack, eclipse attack, Sybil, cryptocurrency.

I. INTRODUCTION

A blockchain technology is a database which is distributed and shared among as well as agreed upon P2P peer-to-peer network. It consists of sequence of blocks which is linked, holding the transaction that are time stamped secured by public-key cryptography and also verified by community of network. A blockchain, in other words, a series (time-stamped) of immutable data record that is managed by the cluster of computers [1, 2]. Each one of these data blocks are bounded as well as secured using the principle of cryptography. Furthermore, blockchain can be divided into two categories private and public blockchain. Private blockchains are restricted in terms of access rights which is very important to limit the number of users enter and their contribution to the network [3].

Two transactions are linked and added which each other in a block if these are verified. The transaction through timestamp and hash function is linked with previous blocks in the ledger [4]. These chains of blocks create blockchain. As soon as the generation of block is done, the participating users of the community of blockchain start the searching for the following blocks for solving the mathematical function and generates the genuine block of transaction which is encrypted for the purpose of adding it to ledger. It is known as mining in which all minors (customers) compete for generating the new block [5, 6]. Generation of authentic block as well as adding it to ledger by the primary minor is rewarded with the total sum of transactions' cost. Expenses are carried out to every transaction [7, 8]. Once the addition of singular block is done, the ledger is updated. If all the participating customers confirms the newly introduced block and all the transaction of this block is actual, then the block can be added as well as within the ledger it can stays permanently as a public document. Also, the block can be discarded if any warfare is determined. Since blockchain is immutable, if any malicious try to regulate the transactional contact, the repeated computations of PoW for the particular block as well as all the blocks can be done and it becomes tough to calculate which decrease the chances for the malicious to enter. In this paper we will discuss about the working of blockchain, security analysis, privacy threats and potential applications of blockchain [9, 10].

The remainder of the paper is organized as follows. Section II of the paper explains the working of blockchain and presents the differences between federated, public and private blockchain. Security analysis on blockchain is presented in section III. Section IV presents the privacy threats for blockchain followed by potential applications of blockchain explored in section V. Finally, the paper concludes in section VI with several open future research trends.

II. HOW BLOCKCHAIN WORK?

As earlier said, that the Integrity of transaction is maintained by distributed ledger and decentralization in blockchain. Let's talk about centralized architecture or classical ledger before discussing blockchain works. Ledgers were used for long time as means for governments and bankers to store land possession transactions and other activities like maintaining transaction record. Building and maintaining a trust relationship were major problem between certain transaction parties, government office or bank was used to accomplish required changes as central authority for defining who possess what and transactions contracts. Therefore, central authority is only able to distinguish between fake and genuine transactions.

The required trust is built by the ledger manager (government office or bank), since the access to information on the ledger is controlled by the centralized manager people who can buy and

978-1-7281-0283-2/19/$31.00 ©2019 IEEE

sell without worry. Totally centralized ledgers are an organization or third-party person which has complete control over transaction management and trusted by every user. Since for only ledger manager the contents are visible that's why ledgers are black boxed.

In terms of maintaining and storing transactions similar functions is provided by blockchain, but there is no requirement of third party. Transaction by ledger decentralization is verified by solving the central authority problem in which each participating user holds an original ledger copy within the blockchain ledger. Request for addition of transaction can be done by any participating user; however, the transaction is only added to the block and only in the blockchain network majority of users verifies it. For generating protected and fast ledger an automatic checking is done reliably for each user, that helps in making blocks and transaction significantly tamper-proof [11]. Difference between the three types of blockchain namely federated, private and public blockchain is presented in Table 1.

Table 1 Differences between federated, public and private blockchain.

Item	Federated	Public	Private
Speed	Lighter and faster	Slower	Lighter and faster
Immutability	Could be tampered	Nearly impossible to tamper	Could be tampered
Asset	Any Asset	Native Asset	Any Asset
Access	Read/write for multiple selected organizations	Read/write for anyone	Read/write for a single organization
Consensus process	Permissioned and known identities	Permissionless and anonymous	Permissioned and known identities
Security	Pre-approved participants and voting/multi-party consensus	Proof of work, proof of stake, and other consensus mechanisms	Pre-approved participants and voting/multi-party consensus
Network	Partially decentralized	Decentralized	Partially decentralized
Efficiency	Lighter and faster	Slower	Lighter and faster

A transaction is linked and added with other transactions in a block if it is verified. The transaction is linked in the ledger with previous blocks through hash function and timestamp. Blockchain is created by these chains of blocks. As soon as the block is generated, all participating users inside the blockchain community begin to search for the following block with the aid of seeking to solve the complicated mathematical function and generate a genuine encrypted block of transactions to add it to the ledger. This technique is referred to as mining, in which all customers (minors) compete to generate the new block. The primary minor to generate an authentic block and add it to the ledger is rewarded with the sum of costs for its transactions. Expenses are carried out to each transaction. Since blocks contain a huge quantity of transactions which are delivered time and again, minors could gather multiple fees.

The ledger held by using all participating customers inside the community is updated once a singular block is added. If the newly introduced block has been confirmed by means of all taking part customers and all its transactions are actual, the block could be added and stays permanently within the ledger as a public document. If a warfare is determined, the block can be discarded. Corrupting a classical ledger desires an assault at the third party (centralized supervisor). At the same time as the blockchain is Immutable, so if there is a malicious try to regulate the contact of any transaction, this can want repeated computations of PoW for the concerned block and all other blocks in a while. These calculations are very tough to perform unless most of the users inside the blockchain network are malicious. Also, the opportunity of having a fake ledger does no longer exist when you consider that all taking part users have their very own genuine replica of the ledger to evaluate with suggests the waft system of a standard economic transaction using the blockchain while a consumer A desires to send money to person B [12]. The flow starts while person A requests to add a block to the ledger which includes information regarding his financial transfer transaction. After growing the block, it broadcasted between all participating customers inside the blockchain network to verify it. While the new block is established by way of all participating customers in the community, the block can be introduced to the ledger and the transfer operation might be finished.

III. Security Analysis on Blockchain

Blockchain does not mandates peers to have a trust among them. Despite this, blockchain exhibits some vulnerabilities [13]. Some common security threats that blockchain has are elaborated in the section below.

- Attacks targeting consensus protocols: Such attacks can reconstruct the whole chain. A good example is the 51% attack happened in PoW Blockchains, e.g., Bitcoin [14]. Attackers who are having with them more than half of power of hashing can easily control blockchain and make it accept blocks which are illegitimate, by just solving problem of consensus faster and quicker than rest all peers who are present there. Recently, it has been proved that hash power which is enough to overpower the PoW is just 33% [15].
- Smart contracts vulnerability: Due to irreversibility and openness of Blockchain smart contracts are very susceptible. All bugs which are present are completely visible to all public and since it includes all public, it obviously includes adversaries as well [16].
- Distributed denial-of-service attack (DDoS): With the help of collaborative attack, the Blockchain resources are exhausted by the adversaries. In the year of 2016, instructions of EVM which were under-priced by adversaries were taken up by these

adversaries to reduce block processing [17, 18]. Large number of low balance accounts which were produced by adversaries led to a DDoS attack.

- Fraud in Programming: The frauds inside programming codes can be exploited by attackers to take out properties of Blockchain, like the piracy attack which took place in 2018 [19, 20].
- Private Key leakage: Attackers can take control of an account by stealing its private key and this can be readily done by attacks on network or by capturing the nodes which are physical [21, 22].
- Eclipse attacks: They are the attacks taking place in P2P networks. In these attacks adversaries stops the legitimate nodes from making a connection to honest peers. It was reported some time ago that Ethereum was also exposed to attacks of eclipse.

Double spending: In this transaction receivers are misguided with the conflicting transactions by the adversaries, like spending in Bitcoin the coin which is same.

IV. Privacy Threats for Blockchain

The transaction of blockchain generally contains the previous transaction ID, trade values, signature and timestamp of its sender, participants' addresses. It is possible for someone to trace the transaction flow for extracting users' physical identities by data mining. This is called De-anonymization. Several attacks are described in this section:

A. DoS Attacks

A (Denial of service) DOS attack is a type of cyber-attack where a network resource or machine is made unavailable to the clients by disrupting the host connected services by a malicious attacker. Using anonymity networks for example TOR, is one of the IP addresses hiding approach in P2P network. However, Biryukov et al. [23] pointed out that TOR node may be disconnected by a DoS attack form blockchain network.

B. Transaction Fingerprinting

Transaction's user-related features is another type of threat to anonymity. Six attributes that characterize several aspects of the behavior of transaction is summarized by Androulaki et al. [24]. If Extra consideration is done on these attributes, it may lead to increase the chances to de-anonymize the individual user. In their paper an experiment is conducted where the Bitcoin is used as daily transaction currency by university students and the researchers could be able to find the 40% of users' profile by utilizing transaction fingerprint-based cluster analysis.

C. Sybil Attacks

Sybil attack is type of cyber-attack in which the reputation system of P2P network is subverted from the creation of very large number of pseudonymous identities and using them to gain influence which is disadvantageous. It is analyzed by Bissias et al. [25] that decentralized anonymity protocols could be blocked or broken which will increases the chances for getting users' real identities.

D. AS-level deployment analysis

Not only personally identifiable information but also extraction of statistical distributions occurs by the means of transaction information flows especially to the public network. Crawling the network of bitcoin with the help of recursively connecting to their clients, collecting and requesting their list of IP addresses of other peers. Hence one can easily obtain the concrete information on structure size and bitcoin's core network distribution.

V. Potential Application of Blockchain

Many opportunities for saving time, cost and also increased any kind of online transactions security are offered by blockchain. In this part several major applications of this technology in healthcare sector, financial sector and scientific research areas will be discussed.

A. Implementation of Blockchain in Healthcare

Due to realization of blockchain technology, the benefits for the healthcare sector are started which make many opportunities to arise in such important sector. Some new models for sharing and managing the medical records are being emerged using the ability of blockchain to provide security and trust while cutting time, resources and cost required by the traditional infrastructure of health management. As a result of this, some system like (APCD) All-Player Claim Database and (HIE) Health Information Exchange became useless [26]. For example, Gaurdtime (Cyber-security firm) and the Estonia government in 2007 has come together to replace APCD as well as HIE systems. To apply the (KSI) Keyless Signature Infrastructure of blockchain in order to verify and authenticate medical public data integrity is the mail goal of this partnership [26]. Digital health innovator like Netcetera (Switzerland), Healthbank (Switzerland) and Noser (Germany) have already started an initiative for sharing personal medical data securely by investing in as well as making use or applying the blockchain technology.

B. Implementation of Blockchain in Banking

Because of many factors like the inefficiencies which are caused by third party organization, logistic processing time, streamlining cumbersome and risky as well as costly correspondent networks [27]. Major Banks like Goldman Sachs and JP Morgan created a partnership for investing in blockchain technology as well as developing it to fulfil their needs, expectation and standard. An estimation by Santander Bank has been done which tells that Blockchain has the enough potential to save banks $20bn by eliminating the centralized trust agencies. The checking check creditworthiness process is also facilitated by blockchain which results in increasing transparency and reducing friction. Similarly, the ability of blockchain to decrease the settlement time which is required in post-trade settling and clearing part of financial exchanges [28].

The second use of this technology is to tackle problems about the ledger duplication since all financial institutions have to maintain their own registers. The cost of ledgers' reconciliation process especially for large banks is very high, and also the traditional process which is used to tackle is performed by using unsecured and primitive tools which makes it risky, hence we need of blockchain technology which gives more security as well as decreases the delays which are caused by these fragmented architectures [29].

C. Implementation of blockchain in Scientific Research

Trust in the field of scientific research is very important factor for the outcomes' credibility especially in important fields like medical sciences. Although this factor suffers trust issues which are caused by data manipulations like data cleansing, selective results publication and outcome switching. Carsile in 2014 has proved in studies that blockchain technology offer a low cost, method which are independently verifiable to confirm and audit the result reliability of scientific studies with the help of blockchain-timestamped protocols. Carsile's study also shows how blockchain provide immutable record of existence, ownership and integrity a particular medical trial protocol [30].

D. Application of Blockchain in Various Industries

- Proof services: The ability of blockchain to store very detailed level value (ownership, membership, identity, etc….) helps the government for providing citizen related services like death and birth certificates, property tiles and business licenses.
- Decentralized autonomous systems/services: This can be most prominent or important role of blockchain about establishing mechanism of trust between the computer and human. This is called (DAO) Decentralized Autonomous Organization and it autonomously hire agents for performing specialized task on internet. However, creating self-governing and self-organizing DAO is not an easy task but once it implemented properly, it will have major impact on different industrial sectors like healthcare, cloud storage and transportation.
- Cryptocurrency: Generally used to transfer value and payments, this application of blockchain technology works by allowing several different parties for transaction among each other without third party intermediaries, in trusted manner.

VI. Conclusion and future scope

The enhanced technological advances such as rise of societal challenges, internet-enabled global world and increased competition for limited resources have accelerated the transition to a data driven world. In such an ecosystem, blockchain offers trusted information platform to IoT for non-collaboratively defying organizational structures. IoT makes people's day to day life easy and provides convenience by making comprehensive decisions as well as exchanging data. However, this simultaneously brings privacy and security concerns. In this article, we explain the working of blockchain and presents the differences between federated, public and private blockchain. Moreover, the security analysis on blockchain is presented. We also present the privacy threats for blockchain followed by potential applications of blockchain. In this paper we present the working of blockchain along with the differences between federated, public and private blockchain. Moreover, the paper presents the security analysis of the blockchain along with the privacy threats for blockchain followed by potential applications of blockchain. A few more solutions beyond privacy and security issues based on blockchain are explored as well.

Despite the promising future of blockchain technologies, a careful analysis of this brings forth several challenges that might disrupt its deployment and further development. Introduction of novel methods is needed in order to enhance these decentralized approaches in business processes. Moreover, there is a need for creation of a comprehensive trust framework that is capable of fulfilling all the requirements related to the blockchain usage. Also, the designed blockchain architecture must be capable of considering the decentralized requirements of the company that use it. Recently in order to form a distributed ledger, several alternatives to blockchain have been proposed. The proposed GHOST protocol modifies the blockchain using a tree structure in the main ledger. Investigation of such DAG-based solutions to privacy and security issues in IoT can be interesting and of great importance.

References

[1] Ma, Z., Huang, W., Bi, W., Gao, H., & Wang, Z. (2018). A master-slave blockchain paradigm and application in digital rights management. *China Communications,15*(8), 174-188. doi:10.1109/cc.2018.8438282

[2] Shahzad, B., & Crowcroft, J. (2019). Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access,7*, 24477-24488. doi:10.1109/access.2019.2895670

[3] Dinh, T. T., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering,30*(7), 1366-1385. doi:10.1109/tkde.2017.2781227.

[4] Fan, K., Ren, Y., Wang, Y., Li, H., & Yang, Y. (2018). Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. *IET Communications,12*(5), 527-532. doi:10.1049/iet-com.2017.0619.

[5] She, W., Liu, Q., Tian, Z., Chen, J., Wang, B., & Liu, W. (2019). Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks. *IEEE Access,7*, 38947-38956. doi:10.1109/access.2019.2902811.

[6] Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2019). Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys & Tutorials,21*(1), 858-880. doi:10.1109/comst.2018.2863956.

[7] Lu, H., Huang, K., Azimi, M., & Guo, L. (2019). Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks. *IEEE Access,7*, 41426-41444. doi:10.1109/access.2019.2907695.

[8] Shahzad, B., & Crowcroft, J. (2019). Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access,7*, 24477-24488. doi:10.1109/access.2019.2895670.

[9] Fernandez-Carames, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. IEEE *Access,6*, 32979-33001. doi:10.1109/access.2018.2842685.

[10] Naser, F. (2018). Review : The Potential Use Of Blockchain Technology In Railway Applications : An Introduction Of A Mobility And Speech

Recognition Prototype. *2018 IEEE International Conference on Big Data (Big Data)*. doi:10.1109/bigdata.2018.8622234.

[11] A. Dorri, S. S. Kanhere, and J. Raja. "Blockchain in Internet of Things: Challenges and Solutions," arXiv preprint arXiv:1608.05187, 2016.

[12] Y. Li et al., "Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems," IEEE Trans. Dependable and Secure Computing, 2016. DOI: 10.1109/ TDSC.2017.2662216.

[13] M. Conti, C. Lal, S. Ruj, et al., "A survey on security and privacy issues of bitcoin", arXiv preprint arXiv:1706.00916.

[14] Y. Zhang and J. Wen, "The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things," Peer-to-Peer Networking and Applications, vol. 10, no. 4, 2017, pp. 983–94.

[15] I. Eyal, E. G. Sirer, Majority is not enough: "Bitcoin mining is vulnerable", 2014 Proc. Int. Conf. Financial Cryptography Data Secur. (FC '14), Springer, pp. 436–454.

[16] N. Atzei, M. Bartoletti, T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)", in: Proc. 6th Int. Conf. Principles Secur. Trust, 2017, pp. 164–186.

[17] M. Vasek, M. Thornton, T. Moore, "Empirical analysis of denial-of-service attacks in the bitcoin ecosystem", 2014 Proc. Int. Conf. Financial Cryptography Data Secur. (FC '14), Springer, pp. 57–71.

[18] Ozyilmaz, K. R., & Yurdakul, A. (2019). Designing a Blockchain-Based IoT With Ethereum, Swarm, and LoRa: The Software Solution to Create High Availability With Minimal Security Risks. *IEEE Consumer Electronics Magazine,8*(2), 28-34. doi:10.1109/mce.2018.2880806

[19] S. S. Team, "Billions of Tokens Theft Case cause by ETH Ecological Defects", March, 2018.

[20] X. Wang, X. Zha, G. Yu, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, K. Zheng, "Attack and defence of ethereum remote apis", 2018 Proc. IEEE Globecom Workshops (GC Wkshps'18), 2018.

[21] S. Verb¨ucheln, "How perfect offline wallets can still leak bitcoin private keys", arXiv preprint arXiv:1501.0044.

[22] M. Smache, N. E. Mrabet, J. J. Gilquijano, A. Tria, E. Riou, C. Gregory, "Modeling a node capture attack in a secure wireless sensor networks", 2016 Proc IEEE 3rd World Forum on Internet of Things (WF-IoT'16), 2016, pp. 188–193.

[23] Biryukov and I. Pustogarov, "Bitcoin over tor isn't a good idea," in Security and Privacy (SP), 2015 IEEE Symposium on, pp. 122–134, IEEE, 2015.

[24] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in International Conference on Financial Cryptography and Data Security, pp. 34–51,Springer, 2013.

[25] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybilresistant mixing for bitcoin," in The Workshop on Privacy in the Electronic Society, pp. 149–158, 2014.

[26] Nichol PB 2016, Blockchain applications for healthcare. http://www.cio.com/article/3042603/innovation/blockchain applications-for-healthcare.html. Accessed 12 Oct 2016.

[27] Umeh, J. (2016). Blockchain Double Bubble or Double Trouble? *Itnow,58*(1), 58-61. doi:10.1093/itnow/bww026

[28] M. Andrychowicz et al., "Fair Twoparty Computations Via Bitcoin Deposits," Proc. Int'l. Conf. Financial Cryptography and Data Security, Springer, 2014, pp. 105–21.

[29] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive Block Chain Protocols," Proc. Int'l. Conf. Financial Cryptography and Data Security, Springer, 2015, pp. 528–47.

[30] Z. Guan et al., "Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smart Grid," IEEE Internet of Things J., vol. 4, no. 6, Dec. 2017, pp. 1934– 44.