Security Issues in Blockchain based Applications

Neha Jain

Abstract*: Data security is the key to the development of modern internet technology. By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. It allows storage of all transactions into immutable records and every record distributed across many participant's nodes. As there is huge increase in the use cases for blockchain technology, nowadays, the primary issue is to enable secure data sharing, data integrity and authentication. The goal of this study paper is to provide a systematic literature survey exploring the use of blockchain as a base technology for securing financial as well as non-financial applications. The purpose is to identify the whether blockchain technology is capable to provide the desired security solutions in various application. The advantages, challenges and the solution provided by previous research is discussed. The survey was focused on various security issues like Confidentiality, Integrity, Availability, Authenticity, Accountability, and Reliability. The study shows that the Blockchain technology is prospective for financial and non-financial services since it can provide solutions for majority of security issues. Future research needs to provide the implementations of desired solutions discussed in security challenges of Blockchain technology.

Keywords : Blockchain, confidentiality, Integrity, Availability

I. INTRODUCTION

The blockchain is an open, distributed ledger which is based on cryptographically techniques that can record the transactions (which are tamper proof) between two or more parties and store it in blocks which are linked together. Blockchain is peer to peer based technique in which the software runs on the user's machine and no centralized system is required to be present between all users. The digital information is distributed across many participants in the nodes [1].The concept gained the popularity in 2008 when Satoshi Nakamoto invented Bitcoin as a currency [2]. Author in [3] has indicated that bitcoins (blockchain type) is been commercialized in developed nations like Japan.It has also influenced world currency markets [4]. The unique properties of blockchain have made it much more valuable than just a decentralized cryptocurrency. It has evolved into something greater and other blockchain system like Etherem [5] and Hyperledger Fabric [6] with public and private accessibility also become very popular. Netscribes has done market research on global blockchain technology and stated that the market is expected to grow at a CAGR (compound annual growth rate) of 42.8% (2018-2023) leading to global revenue of USD 19.9 Bn by 2023 [7].Asia-Pacific region is expected to adopt this technology at a faster rate owing to its wide adoption in China and India. Its value has been recognized by other financial or non-financial sectors such as banking [8], Supply chain and logistics [9][10], the pharmaceutical industry [11], smart contracts [12],[13] cyber security [14]. Use cases of blockchain for government services is listed in [15] along with the security benefits and challenges.

By looking at the popularity of blockchain and its capability of being adapted by several different types of application, it is important to identify what research currently exists specially in relation to the application of blockchain with security aspects. The goal of this study paper is to provide a systematic literature survey exploring the use of blockchain as a base technology for securing financial as well as non-financial applications. While designing a secured computer system, following goals must be achieved. These are: Confidentiality, Integrity and Availability. At the same time other factors like: Authenticity, Accountability, Reliability must be considered as well.

II. STUDY DESIGN

A. Prior Research

To the best of our knowledge there have been very limited systematic literature reviews in existence. We have refereed [16-21] as a basic framework to provide our survey. In 2016, authors conducted SLR on use case and application of blockchain in IOT systems [16].An SLR on general concept of blockchain technology is presented in [17]. An SLR shown in [18] presented the use of blockchain in service industry. In [19], author analyses advantages and limitations of blockchain with respect to four major security issues. A comprehensive review of current blockchain ways for security services in centralized design is provided in [20]. They highlighted state of art techniques that square measure presently wont to offer security services, their challenges and the way blockchain will resolve those challenges. In 2018, [21] Taylor et al. has bestowed systematic literature survey on world applications of blockchain with reference to cyber security.

Revised Manuscript Received on September28, 2019.
* Correspondence Author
Neha Jain, Asst. Professor SLRTCE Mumbai

B. Research Goals

The scope of this research is to provide analysis on existing studies, their findings and to provide a summary about the efforts taken by researcher into the field of security in blockchain applications (financial and non-financial). In this study paper, a systematic literature review has been conducted focusing on various security issues like Confidentiality, Integrity, Authentication and Authorization Availability for blockchain applications. To systematize the study, we have developed three research questions presented in Table- I.

Table- I: Research Question

RQ I	What research topics have been addressed in current research on blockchain?
RQ II	What are the various applications of blockchain where security is major focus?
RQ III	How blockchain is used to improve the security of the system?

The discussion based on above research question is presented in section IV.

C. Our Contribution

Our contribution in this research work is as follows:

- We have identified 37 papers related to blockchain and various security issues like confidentiality, integrity, availability etc. up until July, 2019. This list can be referred by other researchers to further their own work.
- We have done the analysis of the selected papers and highlighted the work done by the authors.

D. Research Methodology

By following the guidelines provided by Kitchenman and charters [22], we have planned, conducted and reported reviews to get an optimized SLR.

1. We have searched following keywords on platforms like IEEEXplore Digital Library, ScienceDirect, SpringerLink, ACM Digital Library and Google Scholar:
    1. ”blockchain” OR ”block-chain”
    2. ”blockchain” OR ”block-chain” OR ”distributed ledger”) AND ”security”
    3. ”blockchain” AND “Privacy” OR ”Confidentiality”
    4. “blockchain” AND ”Integrity” or “Data Integrity”
    5. “blockchain” AND ”Availability”

Table II is showing the total number of papers searched in different publishing houses mentioned.

2. We have set criteria for inclusion and exclusion as given in the Table III.

Table- II: Number of Paper Searched

Name of Publisher/ Keyword	IEEE Xplore Digital Library	Springer Link	ACM Digital Library	Science Direct
1.	2019	1393	632	1619
2.	1287	1201	370	1167
3.	677	723	260	739
4.	214	480	87	501
5.	73	350	45	1233

Table- III: Inclusion/Exlusion Criteria

Inclusion Criteria	Exclusion Criteria
Paper must be from peer reviewed journals or conferences	Non English language paper
It must be based on technical details	Grey Literature such as blogs
Relevance with the objective	Papers focusing on economic or legal impacts of blockchain

3. The interest of this study is to focus on papers on blockchain and security. So approximately 2000 papers were available. After removal of duplicates 1200 papers remaining. Applying inclusion and exclusion criteria on the papers, we get 250 papers. After studying every paper and reapplying the inclusion/exclusion criteria, we finally get 37 papers that are included in this SLR.

The next section provides the analysis of various security issues discussed in the selected papers.

III. RESULTS

In this section we report the results extracted from the selected papers, organized by various security issues. The list of selected papers, security issues addressed by them and the application area is shown in Table IV. Discussion on the results will follow in next section.

A. Confidentiality and Privacy

Confidentiality of data is to protect it from unauthorized access. It can be viewed as the privacy of data. One of the methods to provide confidentiality is through encryption. Privacy provides the users the ability to control who can access their data. There are number of research papers available which provide study related to this section. Our searching criteria were to select papers which provide confidentiality or privacy through blockchain. In blockchain user encrypts the data with own private key. A hash from user’s public key is identified which act as the ID indicator of the user. There is no connection of that hash with user identity. Hash function is one-way function, so generation of public key from hash is impossible. Hence, blockchain provides Privacy and anonymity of user. [23] is a paper based on proof of concept

for decentralized token-based energy trading system using blockchain. Multi-signatures and anonymous encrypted message streams are used to get privacy with blockchain technology. In [24], an IoT based environment uses a blockchain model for sharing data. Here, again blockchain provide a control to user to access the data they own on IoT devices. In this system, privacy of user is preserved by bockchain because it provides a decentralized storage for the access control. IoT data is generally owned by individuals or organizations, so access to that data will be beneficial for the world in some aspects but there is a drawback related to privacy if that data is shared. So, authors in [25] provided a multilevel security model to share the data. Another example of multi-level security was explained in [56] where IoT is divided into two parts: edge layers and the high level layers makes multi-level implementation of blockchain to simplify the deployment. Smart vehicles have risk of losing information like location tracking or remote hijacking. Privacy threats like this can be prevented through blockchain technology in smart vehicles [26]. So, authors proposed a blockchain based architecture to protect privacy of users. A whitepaper in ENISA in 2016 has presented the use of blockchain as a technological tool, which can be used byfinancial institutions to share information and transact easily with each other [27].

A framework is proposed in [28] using blockchain for smart communities. In this various users share the resources among each other with the help of blockchain while presenting their privacy in an open and decentralized environment. Authors in [29] have implemented a PSN (pervasive Social Network) based healthcare system. In this privacy is preserved when the data is being shared between PSN nodes by using blockchain. In [30] authors proposed a novel approach to map bitcoin addresses directly to IP data analysing the anonymity. Authors in [31] provided a privacy preserving payment mechanism for V2G (Vehicle to Grid) networks. In this a registration and data maintenance process that is based on blockchain techniques, ensures the anonymity of the user payment data while enabling payment auditing by privileged users. There are some authors who claim that privacy of user is not maintained in bitcoin, an application of blockchain. In bitcoin the user details are exposed on the blockchain in order to provide transparency in the transaction flows [32]. They have specified that the existing systems do not provide privacy and hence all the transactions are exposed on blockchain revealing monetary details and user information. So, they presented a system called HAWK, which does not store the clear data on blockchain. HAWK compiler has private hawk module to provide privacy and protection. In [33] a comprehensive overview of existing blockchain technology is provided. The main focus is on the privacy and security of the IoT systems. Some challenges associated with the deployment of IoT and the blockchain for IoT is also explained. As the ledger of blockchain is immutable, the major challenge is to remove transactions from the ledger (if required) [27]. In a blockchain based PKI, a ledger of PKI events is published that is reliable as the majority of contributors are honest [34]. Creditcoin is chain proposed by authors in [35] which allows different users to generate the signatures and to send the announcements in a vehicular announcement network. In [36], using a proof-of-concept implementation based on Ethereum smart contracts, data provenance can be realised for a wide range of IoT use cases[37] eliminated cloud based IoT structure by implementing blockchain for storing and protecting large scale IoT data. They have also introduced certificate less cryptography to solve trust issues replacing trusted third party.

B. Data Integrity

Data Integrity is a security goal in which there should be no unauthorized change in data. That means whatever sender is sending must be received by the receiver. The Blockchain guarantees information integrity and hindrance of the unauthorized amendment of information by the utilization cryptography. These options square measure behind the adoption of the Blockchain technology in several applications In [38] authors used the immutable property of blockchain in which fake entries cannot be done in between the blocks. New data can only be entered only at the end of the chain. The authors used sharing of solar energy in a neighborhood using this approach. In [39], authors implemented a trial chain to validate data integrity in healthcare system using blockchain. In [40], while developing a solution for creation and preservation of digital records for a land registry, an analysis is provided by the author that blockchain technology maintains record integrity. A security framework for smart cities using Internet of Things is mentioned in [41] in which blockchain is used as a database layer. Similarly, in [42], author provided a framework based on blockchain to be used as service for data integrity for IoT data. This framework removed third party auditors who verify data integrity rather the IoT data consumes and owner performs the task. In [43], a reference integrity metric (RIM) of the IoT firmware is maintained for ensuring the integrity of the devices which uses blockchain. 51% attack and double spending attack were discussed in [44] and [45], which are threat to integrity in the system. In 51% attack, majority of nodes in the chain are dishonest, hence the chance to maintain integrity lesson eventually. Those nodes allow faster production of block, so the chain produced by them often considered as valid chain and promoting double spending attack onto it. In [46], As Splunk indexes data; it stores hashes of data on an immutable ledger. If the data is corrupted in the indexed record, then it will be mismatched from the distributed ledger. Splunk is DLT to prove that data hasn't tampered with.

Blockchain is capable of providing [47], tamper proofing, disaster recovery and privacy protection. For tamper proofing special chained data structure is used in blockchain. A time stamp is used to keep track of records. Data can be generated by any user and no centralized database is present instead data is stored at all user's side by constructing open source. Hence, maintaining disaster recovery.

C. Availability

The DoS (Denial of Service attack in blockchain are discussed in [27] which affects the availability of the network. The miners can get affected as it can slower down

the processing time by sending a large number of the fake

Table- IV: Key Findings, Security Aspects and Application Area of Selected Papers

Paper	Key Qualitative and Quantitative data reported	Security Aspects	Area
[8]	Blockchain in Interbank Information Network by JP Morgan	privacy, Data integrity and access control	Banking Sector
[9]	Supply chain systems by IBM	privacy,data integrity and access control	Supply chain systems
[12]	Reentrancy attack if solidity programming language is used	Validity	Smart Contracts
[23]	Transaction security in decentralized smart grid energy trading without reliance on trusted third parties	Privacy	Smart grids
[24]	Privacy of user is preserved by bockchain because it provides a decentralized storage for the access control	Privacy, Access Control	IoT
[26]	A blockchain based architecture to provide privacy and security in smart Vehicles	Privacy	Smart Vehicles
[27]	DoS (Denial of Service attack in blockchain	chance of availability lesson eventually	Generic
[28]	Various users share the resources among each other with the help of blockchain while presenting their privacy in an open and decentralized environment	Privacy	Smart Communities
[29]	Privacy is preserved when the data is being shared between PSN nodes by using blockchain	Privacy	Healthcare System
[30]	Identifying ownershiprelationships between Bitcoin addresses and IP addresses.	Anonymity	Bitcoin
[31]	A privacy preserving payment mechanism for V2G (Vehicle to Grid) networks.	Privacy	IoT
[32]	User details are exposed on the blockchain in order to provide transparency in the transaction flows	Privacy not provided	Bitcoin
[34]	Blockchain based PKI	Privacy	Generic
[35]	Creditcoin: a blockchain to preserve privacy in smart vehicles	Privacy	Smart Vehicles
[36]	Data provenancesolutions together with blockchain technology areone way to make data more trustworthy.	Trust	IoT
[37]	To store data securely and use of certificate less cryptography	Privacy, Authentication	Large scale IoT
[38]	Decentralized token-based energy trading system using blockchain	Privacy	Energy Trading System
[39]	Trial chain to validate data integrity	Data Integrity	Biomedical Research
[40]	Various attack like Man in the middle, Syn flood, Sybil attack, Timing errors, key management, audit server attacks. Blockchain technology maintains record integrity	Data Integrity and records authenticity may be affected.	Land Registry
[41]	Blockchain is incorporated in each layer of IoT architecture	Data Integrity	Smart City
[42]	Blockchain to be used as service for data integrity	Data Integrity	IoT
[43]	A reference integrity metric (RIM) of the IoT firmware is maintained for ensuring the integrity of the devices	Data Integrity	IoT
[44]	51% attack is discussed to make a blockchain corrupt.	chance to maintain integrity lesson eventually	Bitcoin
[45]	Double spending attack	chance to maintain integrity lesson eventually	Generic
[46]	Data integrity using blockchain called Splunk	Data Integrity	Banking
[47]	ProvChain to provide enhanced privacy and authenticity in cloud environment	Authentication, Privacy	Cloud
[48]	The use of blockchain – based PKI implementation in air traffic management provides a secure broadcast authorization communication with air traffic services	Authentication	Air Traffic Management
[49]	Quantum attack	Authentication process may be affected	Generic
[50]	Only authorized users can connect to the system	Authorization	Generic
[51]	Used IP address to link the identity creation in blockchain.	Accountabilty	Generic
[52]	An architecture to provide distributed access control system for IOT using proof of concept	Access Management	IoT
[53]	Using blockchain for IOT data trusted exchange	Access Management, Integrity, Privacy	IoT
[54]	A personal data management platform is constructed where blockchain is used as an automated trust less access control manager	Privacy, Access Control	Generic
[55]	Integrated Blockchain and Edge computing Systems can enable reliable access and control of the network	Access Control	Generic
[56]	A secure multi-layer network model based on blockchain technology	Identity Management, Authentication, Privacy	IoT

transactions and keeping the miners busy in processing them restricting to confirm legitimate transactions. Also if the transaction fees for fake transaction is set higher than the legitimate one, miners will be influenced to process them leaving the required transactions.

D. Authentication, Authorization and Access Control

Authentication means confirming your own identity. [40] described various attack like Man in the middle, Syn flood, Sybil attack, Timing errors, key management, audit server attacks etc., where records authenticity may be affected. The use of blockchain – based PKI implementation in air traffic management provides a secure broadcast authorization and communication with air traffic services preserving privacy of aircrafts and enable only

authorized communication [48]. Blockchain is vulnerable to quantum attacks that can solve elliptic curve digital logarithm problem (ECDLP). This problem is used for authenticating the transactions in blockchain. Hence an anti-quantum transaction authentication approach is presented in blockchain [49].

Authorization is process of verifying what a user (who is already authenticated) have access to. Only authorized users can connect to the system in an application based on blockchain through public Wifi networks as shown in [50]. In this the communication between devices is encrypted using blockchain methodology where encryption key will be P2P network address. To maintain the accountability, authors in [51] used IP address to link the identity creation in blockchain. But the problem is with price of IPV4 addresses which makes this process costly. Though, it ensures that the user has only one identity.
In [52], author has presented an architecture for IoT where access control information is stored and distributed using a blockchain technology. The second generation blockchain is having feature of access control mechanism where user have to specify their details in order to get the data or access the data which makes it different from cloud based systems where users have to keep their data on cloud or website having no control on who is accessing their data [53]. In [54], a personal database management platform is constructed where blockchain is used as an automated trust less access control manager. Instead of storing the data directly in the ledger, data is encrypted and pointer to that encrypted data is stored in the ledger. This will provide the confidentiality as well as access control. By incorporating blockchain into edge computing network, system can provide reliable access and control of the network [55]. A framework is proposed in [56] to provide secure key management within heterogeneous network. The blockchain concept is implemented to provide the distribution of key in vehicular communication system. Blockchain technology does not guarantee or improve data quality [57]. The data must be provided by the source should be of good quality. Once it is into chain then the accuracy of data is guaranteed by blockchain. A credit-based payment scheme is proposed to support fast and frequent energy trading using blockchain. It is proved in the paper that the blockchain is able to provide security features like integrity [38].

IV. DISCUSSION

RQI: What research topics have been addressed in current research on blockchain?

When we have searched through the keyword:"blockchain", we have found approximately 2000 papers in which its challenges, issues, limitations and use-cases presented. Papers on applications of blockchain in bitcoin, IoT, smart contracts, Botnet, P2P broadcast etc. have been identified. Majority of papers are focusing on security and privacy issues. It has been observed that issues like computational power, throughput, scalability, latency has got lesser attention as compared to security issues. One of the reasons behind this could be because the concept of blockchain is still very new. The required size or number of block in current scenario is acceptable but in future when number of users would increases drastically or size of block will increase then these issues must be taken care of. It has been observed that a very small portion of research is done in the combination of AI and blockchain. AI can be a better support to improve the security in B2B blockchain applications. As of now by analyzing the number of research work done in the field of privacy and confidentiality, one can conclude the role of blockchain is very important to get the same.

RQII: What are the various applications of blockchain where security is major focus?

The main objective of this research is to focus on security issues addressed through blockchain. Originally Bitcoins was the main application of blockchain and security issues related to it was major concern. But this study shows that blockchain technology is not limited to application in crypto currencies. Instead, we have noted that use cases like IoT, finance and healthcare are most popular. More than half of the published papers are addressing the security issues with applications concerned with IoT. The reason of such interest could be because of the use of IoT in everyday life increasing the security concerns related to that. Blockchain is integrated with Edge Computing is also a recent topic where new security issues like lost transactions in off chain require attention. A practical example that is proving that the need of secure communication in financial sector (Interbank Information Network) where blockchain is used by JP Morgan and in non-financial system like IBM's supply chain systems, security is the biggest concern.

RQIII: How blockchain is used to improve the security of the system?

It has been observed that there are plenty of applications available in the market that is focused on security as shown in the selected papers. Blockchain is solving the security aspects in financial and non-financial application. The benefits of using blockchain are mentioned below:

- Blockchain provides encryption and hashing to store the Blockchain provides encryption and hashing to store the records which cannot be changed or tampered.
- Blockchain use signature of transactions so denial later is not possible
- The new transaction is only added into blockchain if it is verified by majority of nodes making difficult to put the fake data in chain.
- Blockchain are decentralized systems and does not require additional trusted third parties to control the system.
- Blockchain uses Elliptic curve cryptography which is difficult to break.

Some security issues identified from papers while using blockchain:

- In bitcoins, user details are exposed on the blockchain in order to provide transparency in the transaction flows.

- If majority of nodes are dishonest then chances of getting a false transactions is more (51% attack).
- Blockchain only guarantees pseudonymity.
- As the ledger of blockchain is immutable, the major challenge is to remove transactions from the ledger (if required).
- Denial of Service attack can slow miners to perform computing on authorized transactions.
- Attacks like Man in the middle, Syn flood, Sybil attack, Timing errors, key management, audit server attacks etc. may affect the reliability and authenticity in the system.
- Blockchain are prone to quantum attack hence affecting authentication process.

V. FUTURE RESEARCH DIRECTIONS

Researchers are requested to identify more issues related to security in blockchain based applications as there exist many issues without a proper solution. Though there is a rapid increase in the research in this area, it still requires more study. There are several solutions to various issues have been presented in various papers, but many of them are just a brief idea which requires further evaluation.

Majority of papers are pointing out that IoT system's security should be improved if it is supported by blockchain technology but the actual implementation and its analysis is yet to be done. Hence, it is important for future research to develop such application. Blockchain can be used with artificial intelligence to provide a better security in B2B or M2M environment. Sidechains or off chains can be the next level of blockchain technology. Sidechains are the separate chains attached to the main chain. This can improve the performance of a blockchain system. Security aspects in sidechain can be the topic for research.

VI. CONCLUSION

Blockchain is still prevailing at its early stage of its research and development. There is an increase in research in the domain of security and Cryptography in last 4 years. It is going to a great help for the financial and Non-Financial sectors. It will pay heed to the issues of reliability, security and shared knowledge at the same time.

The objective of this SLR was to explore various blockchain applications and included literature review to identify the possible security benefits and challenges of Blockchain technology.To support our study, we have prepared three research questions and answered them to provide direction for future research. At the end of this SLR we are able to conclude that the distributed mechanism, password mechanism and secured hashed mechanism of the blockchain present a completely new perspective forthe development of Internet data security technology. Thus, the Blockchain technology can provide security solutions to existing financial and non-financial applications.

ACKNOWLEDGMENT

I would like to thank Dr. R. R. Sedamkar, Academic Dean in Thakur College of Engineering and Technology, Mumbai, for his guidance and constant support in conducting this review.

REFERENCES

1. M. Pilkington, "Blockchain Technology: Principles and Applications," in Research Handbook on Digital Transformations, 2016. [online] Available: https://ssrn.com/abstract=2662660
2. Nakamoto, S., 2012. Bitcoin: A peer-to-peer electronic cash system, Oct, 2008.
3. Bitcoin Could Be Accepted at 300,000 Japanese Stores in, 2017.
4. S. Chen, C.Y.-H. Chen, W.K. Hrdle, T.M. Lee, B. Ong, Chapter 8 – Econometric Analysis of a Cryptocurrency Index for Portfolio Investment BT - Handbook of Blockchain, Digital Finance, and Inclusion, vol. 1, Academic Press, 2018, p. 175206.
5. G. Wood, Ethereum: a Secure Decentralized Generalized Transaction Ledger Yellow Paper, Ethereum Project. Yellow Pap., 2014, p. 132.
6. V. Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, Etherum, 2014 [Online]. Available: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
7. Global Blockchain Technology Market (2018-2023), Ntescribe (India) Pvt. Ltd., May 2018. ID: 4593797
8. Martin Arnold, Five ways banks are using blockchain. OCTOBER 16,2017. [Online]. Available: https://www.ft.com/content/615b3bd8-97a9-11e7-a652-cde3f882dd7b
9. Bernard Marr, How Blockchain Will Transform the Supply Chain and Logistics Industry , March 2018, [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/#359010b95fec
10. Sunil K (2018) Value Creation through Blockchain Technology in Supply Chain Management. J Inform Tech Softw Eng 8: 1000248. doi: 10.4172/2165-7866.1000248
11. K. Megget, Securing the supply chain, PharmaTimes magazine - March2018.[Online]Available: http://www.pharmatimes.com/magazine/2018/march_2018/securing_the_supply_chain
12. R.M. Parizi, Amritraj, A. Dehghantanha, Smart contract programming languages on blockchains: an empirical evaluation of usability and security, in: International Confernce on Blockchain, Seattle, USA, 2018, pp. 75–91.
13. Roger Aitken,Smart Contracts on the Blockchain: Can Businesses Reap the Benefits. [Online] Available: https://www.forbes.com/sites/rogeraitken/2017/11/21/smart-contracts-on-the-blockchain-can-businesses-reap-the-benefits/#2be0ee110744
14. Adewale Omoniyi, Convergence of Blockchain and Cybersecurity - IBM Government Industry Blog.December 2, 2017. Online Available :https://www.ibm.com/blogs/insights-on-business/government/convergence-blockchain-cybersecurity/
15. A. Alketbi, Q. Nasir, M. A. Talib, Blockchain for Government Services-Use Cases, Security Benefits and Challenges, IEEE 2018. Pp 112 -119.
16. M. Conoscenti, A. Vetr, J.C. De Martin, Blockchain for the internet of things: a systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, p. 16.
17. J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on Blockchain technology? - a systematic review, PLoS One 11 (10) (2016) 127.
18. S. Seebacher, R. Schritz, Blockchain technology as an enabler of service systems: a structured literature review, in: Exploring Services Science, 2017, p. 1223.
19. F. Dai, Y. Shi, N. Meng, L. Wei, Z. Ye, From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security Issues, in the 4th International Conference on System and Informatics, 2017, pp. 975-979.
20. T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: a state of the art survey, in: IEEE Communications Surveys & Tutorials, 2018,

https://doi.org/10.1109/COMST.2018.2863956.

21. P. J. Taylor , T. Dargahi , A. Dehghantanha , R. M. Parizi ,K. K. R. Choo, A systematic literature review of blockchain cyber security, in Digital Communication Network, ScienceDirect, Feb 2019.
22. B. Kitchenham, S. Charters, Guidelines for Performing Systematic Literature Reviews in Software Engineering, in: Engineering, vol. 2, 2007, p. 1051.
23. N. a. S. D. Aitzhan, "Security and Privacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and Anonymous Messaging Streams," IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, pp. 1-1, 12 October 2016.
24. S. H. F. F. R. P. C. R. H. Hashemi, "World of Empowered IoT Users,"in First International Conference on Internet-of-Things Design and Implementation (IoTDI), Berlin, Germany, 2016.
25. W. Ejaz and A. Anpalagan, Internet of Things for Smart Cities, SpringerBriefs in Electrical and Computer Engineering, oct 2018. https://doi.org/10.1007/978-3-319-95037-2_5
26. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, BlockChain: A Distributed Solution to Automotive Security and Privacy, IEEE Communications Magazine • December 2017, 10.1109/MCOM.2017.1700879
27. Hon, W. K. Palfreyman, J. and Tegart, M , A White paper on Distributed Ledger Technology & CybersecurityImproving information security in the financial sector by European Union Agency for Network and Information Security (ENISA), 2016.978-92-9204-200-4, 10.2824/80997.
28. P. R. J. a. L. K. Kianmajd, "Privacy-Preserving Coordination for Smart Communities," in IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), San Francisco, CA, USA, 2016.
29. J. X. N. a. H. X. Zhang, "A Secure System For Pervasive Social Network-Based Healthcare," Special Section on Trust Management in Pervasive Social Networking (TruPSN), 29 December 2016.
30. P. K. D. a. M. P. Koshy, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," in International Conference on Financial Cryptography and Data Security . FC 2014: Financial Cryptography and Data Security, Christ Church, Barbados, 2014.
31. F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks, IEEE network,2018, Digital Object Identifier: 10.1109/MNET.2018.1700269.
32. A. M. A. S. E. W. Z. P. C. Kosba, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in In Proceedings of the 2016 IEEE Symposium on Security and Privacy, SP '16, 2016.
33. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE 6th International Congress on Big Data, pp 557-564.
34. L. Axon, M. Goldsmith, PB-PKI: A Privacy-aware Blockchain-based PKI in proceedings of the 14th International Joint Conference on e-Buisness and Telecommunications, Vol 4, pp 311-318, 2017.
35. L. Li et al., CreditCoin:A privacy –preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles, IEEE Transactions on Intelligent Transportation Systems, 2018 DOI: 10.1109/TITS.2017.2777990.
36. Marten Sigwart, Michael Borkowski, Marco Peise, Stefan Schulte, and Stefan Tai. 2019. Blockchain-based Data Provenance for the Internet of Things. In Proceedings of 9th International Conference on the Internet of Things (IOT'19). ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn
37. R. Li, T. Song, B. Mei, H. Li, X. Cheng, L. Sun, Blockchain For Large Scale Internet of Things: Data Storage and Protection, IEEE Transaction on services computing, 2018.
38. Z. Li,J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, IEEE Transactions on Industrial Informatics, 2017.
39. H. Dai, H Patrick Young, "TrialChain: A Blockchain-Based Platform to Validate Data Integrity in Large, Biomedical Research Studies ", published in ArXiv 2018.
40. V. L. Lemieux, "Trusting records: is Blockchain technology the answer?," Records Management Journal, vol. 26, no. 2, pp. 110-139, 2016.
41. K. a. M. V. Biswas, "Securing Smart Cities Using BlockchainTechnology," in IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems, Sydney, NSW, Australia, 2016.
42. X. L. Y. S. C. X. X. a. L. Z. B. Liu, "Blockchain based Data Integrity Service Framework for IoT data," in IEEE 24th International Conference on Web Services, 2017 .
43. J. L. K.-K. C. M. Banerjee, "A blockchain future to Internet of Thingssecurity: A position paper," in Digital Communications and Networks, 2017.
44. J. J. Xu, "Are blockchains immune to all malicious attacks?," Xu Financial Innovation , 2016.
45. C. R. C. Pinzon, "Double-spend Attack Models with Time Advantange for Bitcoin," Electronic Notes in Theoretical Computer Science (ENTCS), vol. 329, no. C, pp. 79-103, December 2016.
46. N. Mckervey, Advanced Data Integrity with Blockchain. Online: https://www.splunk.com/blog/2018/09/24/the-newest-data-attack.html
47. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. credNjilla,ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability, 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp 468-477.
48. R. J. Reismann, Air traffic Management Blockchain Infrastructure for Security, Authentication and Privacy, by NASA Ames Research Center in AIAA SciTech Forum, 7-11 Jan 2019. DOI: 10.2514/6.2019-2203.
49. W. Yin, Q. Wen, W. Lin, H. Zhang, Z. Jin, An Anti-quantum Transaction Authentication Approach in Blockchain.IEEE Access Vol 14, August 2015.
50. T. a. I. H. Sanda, "Proposal of New Authentication Method in Wi-FiAccess Using Bitcoin 2.0," in 5th Global Conference on Consumer Electronics, Kyoto, Japan, 2016.
51. R. O. G. Dennis, "Rep on the block : A next generation reputation system based on the blockchain," in 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 2015.
52. O. Novo, Blockchain Meets IoT:an Architechture for Scalable Access Management in IoT, IEEE journal of Internet of Things, Vol.14, No.8, March 2018.
53. Z. Huang, X. Su,Y. Zhang, C. Shi, L. Xie, A Decentralized Solution for IoT Data Trusted Exchange Based on Blockchain, published in 3rd IEEE International Conference on Computer and Communications, pp-1180-1184,2017.
54. G. N. O. P. A. Zyskind, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in Security and Privacy Workshops (SPW), 2015 IEEE, San Jose, CA, USA, 2015.
55. R. Yang, F. R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated Blockchain an Edge Computing Systems: A survey, Some Reseacrh Issues and Challenges, in IEEE Communication Surveys and Tutorials, Volume 21, issue 2, secondquarter 2019, pp 1508-1532.
56. C. Li, L. J. Zhang, A blockchain based New secure Multi-Layer Network Model for Internet of Things, 2017 IEEE International Congress on Internet of Things (ICIOT), pp 33-41.
57. E. Piscini ,D. Dalton, L. Kehoe , Blockchain and cyber security, De loitte EMEA Grid Blockchain Lab,2018. Available: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gra-Changingthegameoncyberrisk.pdf.

AUTHORS PROFILE

Neha Jain is a research Scholar from Mumbai University, India. She is currently working as Assistant Professor in SLRTCE having 15 years of teaching experience. Her research interest is in Blockchain and security. She has published 15 papers in the security field.