Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 02, February-2020

A Systematic plan of Blockchain Technology on Security Key

G.Vasukidevi
R.M.K. College of Engineering and Technology

T.Sethukarasi
R.M.K. Engineering College

***Abstract*:- In recent decades, blockchain has (slowly) become one of the most frequently discussed methods for securing data storage and transfer through decentralized, trustless, peer-to-peer systems. This review provides a complete and detailed documentation of the present technological and literary state of the Blockchain technology within Information Systems research. This paper also identifies peer-reviewed literature that seeks to apply blockchain for cyber security purposes and presents a systematic analysis of the most commonly approved blockchain security applications. It reviews moreover categories the current findings into different concept categories to enable further research into the area. Finally, it is noted that the Blockchain technology in its present state still has way to go before the technology will reach a state considered sufficient for mainstream adoption.**

Keywords: Blockchain, security, survey, Cyber security, network

I. INTRODUCTION

Almost a period ago Satoshi Nakamoto, the unfamiliar person/group behind Bitcoin, termed how the blockchain technology, a distributed peer-to-peer linked-structure, could be used to resolve the difficult of maintaining the order of transactions and to avoid the double-spending problem [1]. Bitcoin orders transactions and groups them in a constrained-size structure called as blocks sharing the similar timestamp. The nodes of the network (miners) are accountable for connecting the blocks to each other in sequential order, with each block comprising the hash of the previous block to make a blockchain [2]. Therefore, the blockchain construction achieves to comprise a robust and auditable registry of all transactions.

To cope with this challenge, distributed storage platforms [3], [4], by networking a large number of commodity storage devices, have received much attention with handle the huge set of data because of it scalability. As those storage platforms continue to rise in popularity, devices that host data content could become high-value targets of cyberattacks. To mitigate the risk of data breaches, encryption has been marketed as a distinguishing feature recently [4], [5]. Despite the progress, those distributed encrypted storage services have yet to provide any content search functionality. As search is ubiquitous, how to enable encrypted keyword search as a natural demand for this trending paradigm remains to be fully explored.

Achieving the above goal confronts two challenges. First, previous designs for search over encrypted data (aka searchable encryption [6]–[8]) mostly consider a logically centralized server setting. They are not specifically designed to suit a fully distributed network of nodes. As we show later, straightforward approaches, such as replacing a central server with a group of nodes connected via a distributed hash table (DHT), provide the functionality, but do not necessarily achieve good enough communication and search efficiency.

Second and more importantly, as the network of nodes grows, it becomes more and more apparent that the robustness of the system should be ensured, especially without the governing authority [9], [10]. Unlike centralized designs, distributed nodes in an open network raise a much larger barrier to establish a trust to the clients. Firstly, some systems allow loosely regulated nodes for storage [4]. As such, these nodes may return partial or fake results to save their resource consumption [11]. Secondly, nodes already in the system are subject to attacks by outside adversaries [9], who may intentionally violate the integrity of search results, e.g., poisoning the results for fraud and scams. Last but not least, malicious nodes could further infiltrate the network as the network grows, disrupting the system and damaging its robustness [10]. Considering a growing network of distributed nodes, enabling encrypted search while ensuring system robustness can be even more challenging.

As a starting point, it appears that combining any known searchable symmetric encryption (SSE) schemes and existing distributed data partition algorithms could enable encrypted search in distributed nodes. Unfortunately, without careful consideration, such integration will introduce considerable communication cost and fall short of preserving client transparency. For example, if encrypted dictionary-based SSE schemes [8] are adopted with DHT, the matched file list for a keyword will possibly be partitioned to different nodes. And a search request will be forwarded to multiple different targeted nodes to fetch and assemble the result. The client might further be involved to track the location of the partitioned index for each keyword. All such overhead could diminish the benefit of distributed systems.

This paper is organized as follows: Section 2 presents the findings of the investigation of all the primary studies selected. Section 4 deliberates the Descriptive analysis for research objectives. Section 5 concludes the research and offers some suggestions for future research.

II. BLOCKCHAIN FINDING

In standard, a blockchain should be well thought-out as a distributed append-only time stamped data structure. Blockchains permit us to have a distributed peer-to-peer network where non-trusting associates can verifiably interrelate with each without the need for a trusted specialist [4]. To attain this one can think through blockchain as a set of interrelated mechanisms which offer exact features to the framework, as illustrated in Fig. 1. At the lower most level of this infrastructure, we have the signed transactions between peers. These transactions represent an contract between two members, which may contain the transfer of physical or digital assets, the completion of a task, etc. As a minimum of one member signs this transaction and it is distributed to its neighbors. Normally, any individual which links to the blockchain is called a node. Though, nodes that authenticate all the blockchain guidelines are called full nodes. These nodes collect the transactions into blocks and they are responsible to decide whether the transactions are legal, and should be kept in the blockchain, and which are not.

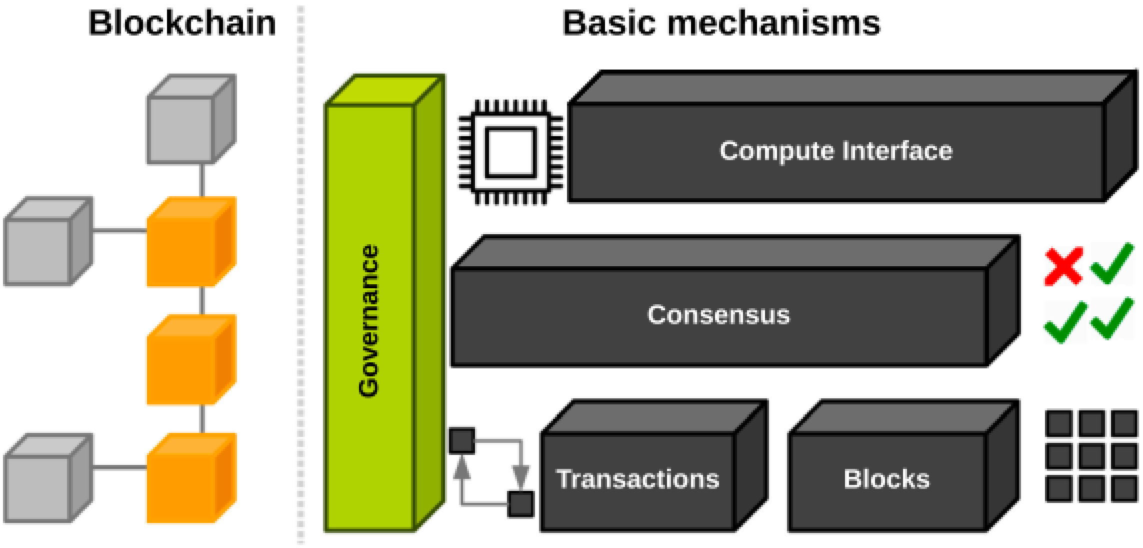

Fig 1. An outline of Block chain Architecture

A legal transaction means, for example, that Bob received one bitcoin from Alice. Though, Alice may have tried to transfer the same bitcoin, as it is a digital asset, to Carol. So, nodes must obey to an agreement on which transactions must be reserved in the blockchain to assure that there will be no unethical branches and divergences [12]. This is truly the goal of the second Consensus layer. Subject to the blockchain type, different Consensus mechanisms exist [13]. The most familiar is the Proof-of-work (PoW). PoW needs explaining a difficult computational process, like discovery hashes with exact patterns, e.g. a foremost number of zeroes [14], to confirm authentication and verifiability. In place of splitting blocks across correspondingly to the relative hash rates of miners (i.e., their mining power), Proof-of Stake (PoS) protocols split stake blocks correspondingly to the current wealth of miners [15]. In this way, the selection is fair-minded and avoids the wealthiest contributor from controlling the network. Numerous blockchains, such as Ethereum [16], are slowly shifting to PoS due to the important decrease in power consumption and better scalability. Further consensus methods include Byzantine Fault Tolerance (BFT) [17] and its variants [18].

A supplementary layer, the Compute Interface, permits blockchains to offer more functionality. Basically, a blockchain stores a state which contains e.g. of all the transactions that have been made by the consumers, thereby permitting the calculation of each user’s balance. But, for more improved applications we want to store complex states which are revised effectively using distributed computing, e.g. states that shift from one to another once specific criterion are met. This constraint has given rise to SCs which use nodes of the blockchain to perform the terms of an agreement.

Lastly, the Governance layer widens the blockchain architecture to cover the human communications taking place in the physical world. In fact, while blockchains procedures are well defined, they are also dominated by inputs from varied groups of people who join in new procedures, develop the blockchain procedures and patch the system. Whereas these parts are essential for the development of each blockchain, they establish off-chain social processes. So, blockchain governance acts on how these varied participant bands together to create, sustain, or alter the inputs that invent a blockchain.

Present literary work classifies blockchain networks in several ways [19, 18, 20, 4, 21]. These classes are made according to the network’s management and authorizations as public, private and joined. In public blockchains (permission less) anybody can join as a new user or node miner. Also, all members can do operations such as transactions or agreements. In private blockchains; which along with the joined belong to the licensed blockchain category, generally, a whitelist of certified users is defined with specific features and authorizations over the network operations. Meanwhile the threat of Sybil attacks is almost insignificant there [22], private blockchain networks can prevent expensive PoW processes. In its place, a broad range of consensus procedures based on disincentives could be accepted. A joined blockchain is a hybrid combination of public and private blockchains [19, 18]. Even if it shares similar scalability and privacy protection level with private blockchain, their main dissimilarity is that a group of nodes, named leader nodes, is chosen instead of a single individual to authenticate the transaction procedures. This permits a slightly decentralized design where leader nodes can get permissions to other users.

Famous applications of public blockchains include Bitcoin, Ethereum, Litecoin and, at large, most crypto-currencies [1,7]. One such their main benefit is the lack of infrastructure costs: the network is self-maintained and capable of sustaining itself, extremely reducing management overheads. In private blockchains, the foremost applications are database management, auditing and, as a whole, performance demanding solutions [18]. Multichain [3] is a sample of an open platform for creating and organizing private blockchains. As a final point, joined blockchains are frequently used in the banking and industry sectors. This is the case of the Hyperledger project, which improves cross-industry permission-based blockchain structures. Newly, Ethereum has also delivered tools for creating joined blockchains. Other schemes,[23] are rather ambitious trying to deliver more capability. Further on blockchain classification, the interested reader may refer to [24] and [22].

III. DESCRIPTIVE ANALYSIS

Explicitly in relation to the application of blockchain to the issue of cyber security, to the best of our knowledge, there acts to be very narrow Systematic Literature Reviews (SLRs). One such the furthermost recent survey papers in the domain of blockchain and cyber security was implemented by [22]. In this paper, the authors point out the challenges and problems related with the use of security facilities in the centralized structure in various application domains, and present a complete review of present blockchain-enabled approaches for such security related service applications in areas of authentication, confidentiality, privacy, access control, data and resource beginning, and integrity guarantee in distributed networks. In our point of view, this paper provides a useful start to corresponding researchers who might be interested in blockchain-based network and service security. Other than it, a small number of reviews in relation to blockchain and its broader impact have also been published and we will deliberate them below to observe the changes between the topics selected by the authors and our research.

Research goals

The intention of this research is to examine existing studies and their outcomes and to summarize the works of research in blockchain applications for cyber security.

Findings

Every main research paper was read in full and applicable qualitative and quantitative data was mined and briefed in Table 1. All the main studies had an attention or theme in relation to how blockchain was handling with a particular issue. The aim of each paper is also documented below in Table 1. All paper's concentrate was further grouped into wider categories to permit for a simplified classification of the themes of the main studies. Some papers had a focus about virtual machines, networking and virtual network management was grouped together into the networks group. Studies that had an aim related to peer-to-peer sharing, encrypted data storage and searching were grouped into the category of data storage and sharing.

Key finding of primary studies

Guy Zyskind [25] in 2015 presented decentralized personal data management system. Data between users and applications can be protected and remain un-tampered by being kept and passed through a blockchain. Instead of proof-of-work, trusted nodes are satisfied instead by their level of intended trust allocated by the network by using personal data security application

B. Benshoof [26] in 2016 proposed D3NS Method technique, the security application DNS can be protected with blockchain using proposed “D3NS”. Proposal for backwards well-matched new DNS.

A. Ouaddah [27] in 2016 proposed the method named new framework for access control in IoT based on the blockchain technology. The security application is IoT and the Proof of concept pseudonymous procedure for safe communications between IoT devices using bit coin blockchain for case study.

M. Ali, et al [28] in 2016 implemented the new blockchain-based naming and storage system called Blockstack, they inference new project for unchallengeable naming and storing of data, called “BlockStack”. Recognition for already developed Namecoin blockchain not contributing security and reliability of bitcoin block chain and data storage as a security application

B. Qin [29] in 2017 used Distributed certificate scheme, referred to as Cecoin. The proposal for a distributed ledger of Public Key Infrastructure (PKI) to prevent potential failure of central repository of PKI's recognition for token. New token named Cecoin suggested and this scheme is certified types of security application named as Public Key Infrastructure.

L. Yue [30] in 2017 recommended Credible big data sharing model, inference the proposal for safely sharing big data and preventing interfering. Uses the ethereum blockchain in big data.

Chengjun Cai [31] in 2017 planned Hardening Distributed and Encrypted Keyword Search; Blockchain based distribution of hashed search indices to permit for keyword searching of encrypted data. Integrity sustained by finding value deposit from a joining user and if they act maliciously, this deposit is shared to the rest of the nodes and use Encrypted Data
Storage & Searching as a security application.

S. Ram Basnet [32] in 2017 suggested Blockchain Security over SDN (BSS) which implicate Proposal for the use of blockchain to secure file sharing between nodes within a Software Defined Network (SDN). Using the ethereum platform in networking.

N. Bozic [33] in 2017 proposed Virtual Machine Orchestration Authentification (VMOA) method for Securing virtual machines in networked environments using private blockchain; IBM's Hyper ledger Fabric established adequate properties to permit for the researchers' proposals in the platforms of virtual machines.

L. Xu, L. Chen [34] in used 2017 Distributed ledger based access control system (DL-BAC), suggesting a Distributed Ledger Based Access Control (DL-BAC) for web applications. Distributed ledger denotes to a generic in Web Applications.

D. Fu, F. Liri [35] in 2017 projected Better encryption algorithm from NTT Service Evolution Laboratory approach. Using an MIT research data privacy idea to explore differences between blockchain proof-of-work and proof-of-credibility consensus approaches. Nodes are given a score to define their reliability dependent on number of connections to other trusted nodes in Data Privacy.

A. Moinet,[36] in 2017 implemented new decentralized and evaluative model is recommending their own blockchain for handling Public Key Infrastructure and mining is incentivized not through currency tokens but data payloads labeled approval, authentication, renew, blame, ban and revoke, which creates trust across nodes in Public Key Infrastructure

Yunhua He [37] in 2018 used Blockchain based truthful incentive mechanism is suggesting pricing approaches for blockchain based distributed peer to peer transactions. Blockchain ideas and incentivization based on bitcoin Peer to peer data sharing security application.

Minhaj AhmadKhan[38] in 2018 projected survey major security issues for IoT inference Significant review of IoT security and how blockchain could meet the difficulties of decreasing the existing security threats against such devices. Saying ethereum as a potential platform to permit for smart agreements to be established in endless ways in IoT.

Y. Gupta [39] in 2018 describes blockchain consensus model offers an application of blockchain in the form of safeguarding historic IoT connections and sessions and identifying malicious action. The proposed structure is that the blockchain protocol sits between the application and transports layers of the network. Developing token rewards similar to bitcoin but treating them as units of voting power in IoT as a security application.

IV. CONCLUSION

This survey has summarized available recent paper on how blockchain solutions can assist to cyber security issues. The primary keyword searches for this study and present media records highlight blockchain as a self-contained technology that carries with it an excessive array of feasible solutions for finance, logistics, healthcare and cyber security. This survey has aimed only on cyber security. Definitely, there are deserve applications for blockchain, though, a decentralized, trustless system cannot by itself resolve all issues one may reveal in the field of cyber security. Blockchain applications for cyber security have progressed and supported the existing works to improve security and to deter malicious users. This study highlights chances available for future research to be performed in areas of cyber security outside the domain of key management. As the World Wide Web moves towards a mass acceptance of https encryption and the end users are progressively using some methods of encryption for normal communication, there is an always increasing requirement to securely achieve the exisiting cryptography and key management schemes.

REFERENCES

[1] Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system
[2] Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., 2016. Blockchain technology: beyond bitcoin. Appl. Innovation 2, 6–10.
[3] J. C. Corbett, J. Dean, M. Epstein, A. Fikes, C. Frost, J. J. Furman, S. Ghemawat, A. Gubarev, C. Heiser, and P. Hochschild, “Spanner: Googles globally distributed database,” ACM TOCS, vol. 31, no. 3, p. 8, 2013.
[4] S. Wilkinson, T. Boshevski, J. Brandoff, V. Buterin, G. Hall, P. Gerbes, P. Hutchins, and C. Pollard, “Storj a peer-to-peer cloud storage network,” On line at: https://storj.io/storj.pdf, 2016.
[5] MORPHiS, “MORPHiS: a global encrypted distributed datastore,” On line at: https://morph.is/.
[6] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” Journal of Computer Security, vol. 19, no. 5, pp. 895–934, 2011.
[7] S. Kamara, C. Papamanthou, and T. Roeder, “Dynamic searchable symmetric encryption,” in Proc. of ACM CCS, 2012.
[8] D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.- C. Rosu, and M. Steiner, “Dynamic searchable encryption in very large databases: Data structures and implementation,” in Proc. of NDSS, 2014.
[9] G. Urdaneta, G. Pierre, and M. V. Steen, “A survey of dht security techniques,” ACM Computing Surveys, vol. 43, no. 2, p. 8, 2011.
[10] M. N. Al-Ameen and M. K. Wright, “Design and evaluation of persea, a sybil-resistant DHT,” in Proc. of ACM AsiaCCS, 2014.
[11] C. Cai, X. Yuan, and C. Wang, “Towards trustworthy and private keyword search in encrypted decentralized storage,” in Proc. of IEEE ICC, 2017.
[12] Vukolić, M., 2015. The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: International Workshop on Open Problems in Network Security. Springer, pp. 112–125.
[13] Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C., 2017. A review on consensus algorithm of blockchain. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)pp. 2567–2572.
[14] Antonopoulos, A.M., 2014. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O’Reilly Media Inc.
[15] Pilkington, M., 2016. Blockchain technology: principles and applications. Res. Handbook Digital Transformations 225.
[16] Dannen, C., 2017. Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. Apress.
[17] Castro, M., Liskov, B., 2002. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst. (TOCS) 20 (4), 398–461.
[18] Zheng, Z., Xie, S., Dai, H.-N., Wang, H., 2016. Blockchain challenges and opportunities: a survey. Work Pap.
[19] Buterin, V., 2015. On public and private blockchains, Ethereum Blog 7.
[20] Eris Industries, 2016. Explainer — Smart Contracts, https://docs.erisindustries.com/explainers/smart_contracts/.
[21] Kravchenko, P., 2016. Ok, I need a blockchain, but which one? https://medium.com/@pavelkravchenko/ok-i-need-a-blockchain-but-which-one-ca75c1e2100.
[22] Swanson, T., 2015. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, https://allquantor.at/blockchainbib/pdf/swanson2015consensus.pdf.
[23] Cardano, 2018. https://www.cardano.org.
[24] Walport, M., 2016. Distributed ledger technology: beyond block chain.
[25] G. Zyskind, A.S. Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015.
[26] B. Benshoof, A. Rosen, A.G. Bourgeois, R.W. Harrison, Distributed decentralized domain name service, in: Proc. - 2016 IEEE 30th Int. Parallel Distrib. Process. Symp. IPDPS 2016, 2016, p. 12791287.

[27] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, FairAccess: a new blockchain-based access control framework for the Internet of Things, Secur. Commun. Networks 9 (18) (2016) 59435964.

[28] M. Ali, et al., Blockstack: A global naming and storage system secured by blockchains, in: USENIX Annu. Tech. Conf., 2016, p. 181194

[29] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, W. Shi, Cecoin: A decentralized PKI mitigating MitM attacks, Futur. Gener. Comput. Syst. (2017).

[30] L. Yue, H. Junqin, Q. Shengzhi, W. Ruijin, Big data model of security sharing based on blockchain, in: 2017 3rd Int. Conf. Big Data Comput. Commun., 2017, p. 117121.

[31] C. Cai, X. Yuan, C. Wang, Hardening distributed and encrypted keyword search via blockchain, in: 2017 IEEE Symp. Privacy-Aware Comput., 2017, p. 119128.

[32] S. Ram Basnet, S. Shakya, BSS: Blockchain Security over Software Defined Network, Ieee Iccca, 2017, p. 720725.

[33] N. Bozic, G. Pujolle, S. Secci, Securing virtual machine orchestration with blockchains, in: 2017 1st Cyber Secur. Netw. Conf., 2017, p. 18.

[34] L. Xu, L. Chen, N. Shah, Z. Gao, Y. Lu, W. Shi, DL-BAC: Distributed ledger based access control for web applications, in: Proc. 26th Int. Conf. World Wide Web Companion, 2017, p. 14451450.

[35] D. Fu, F. Liri, Blockchain-based trusted computing in social network, in: 2016 2nd IEEE Int. Conf. Comput. Commun. ICCC 2016 - Proc., 2017, p. 1922

[36] A. Moinet, B. Darties, J.-L. Baril, Blockchain based trust & authentication for decentralized sensor networks, 2017, p. 12.

[37] Y. He, H. Li, X. Cheng, Y.A.N. Liu, C. Yang, L. Sun, A blockchain based truthful incentive mechanism for distributed P2P, IEEE Access xx (2018) no. c

[38] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Futur. Gener. Comput. Syst. 82 (2018) 395411.

[39] Y. Gupta, R. Shorey, D. Kulkarni, J. Tew, The applicability of blockchain in the Internet of Things, in: 2018 10th Int. Conf. Commun. Syst. Networks, 2018, p. 561564.