ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Survey on Blockchain and Cyber Security

[1]Kanderp Narayan Mishra
[1]Department Of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
[1]Kanderp.narayan@galgotiasuniversity.edu.in

Abstract: Blockchain has become the most often examined techniques to secure data storage and move through peer-to-peer, decentralized, trust less frameworks. Cyber security is assurance of networks and computer systems from the robbery of or harm to its electronic data, software, or hardware, just as from the misdirection or interruption of the services it provide. This look into distinguishes peer-investigated writing that tries to employ blockchain for the purposes of cyber security and introduces an efficient investigation of the most every now and again adopted the applications of blockchain security. Its discoveries depict that the IOT i.e. Internet of Things lends itself better to novel applications of blockchain, as do machine visualization and networks, web applications, secure stockpiling of PII i.e. Personally Identifiable Information, public key cryptography and certification themes. This auspicious efficient audit likewise reveals insight into future headings of research, practices and education in cyber security and the blockchain space, for example, blockchain to AI data security, sidechain security and blockchain in IOT security, and so on.

Keywords: Artificial Intelligence, Blockchain, Cyber Security, IOT, Data Security, Lifecycle Review (SLR).

INTRODUCTION

As a cryptographic dependent distributed ledger, the blockchain technology empowers confided transactions between untrusted members in network. Since the presentation of first Bitcoin blockchain, different blockchain frameworks, for example, Hyper ledger Fabric and Ethereum, have risen with private and public availability outside of the existing electronic voucher systems and fiat currencies. As of late, blockchain innovation has additionally been a subject of an expanding number of the scientific inquires, and has raised critical enthusiasm among developers, industry practitioners and researchers because of its one of a kind security and trust qualities. There is no uncertainty that the prominence of blockchain has expanded around the world. More than essentially getting mainstream, it has made an enduring sway on the world. Such as it has been financially received, affected world currency markets, encouraged the multiplication of unlawful dull web commercial centres[1].

It additionally has been a noteworthy factor influencing the multiplication of monetarily driven cyber-attacks, e.g. denial of service and ransomware against retailers and some other online associations. Actually, the usage and implementation of the blockchain have far outperformed its unique reason as the spine for first decentralized cryptocurrency of world[2]. The estimation of the trust less, decentralized ledger which conveys memorable changelessness has been perceived by other enterprises hoping to apply the centre ideas to the current business forms. The extraordinary properties of blockchain innovation make its application the alluring thought for some business regions, for example, banking, pharmaceutical, cyber security, logistics, and smart contracts.

This paper tries to concentrate on existing writing concerning the utilization of blockchain as the supporting innovation for the applications of cyber security, involving fields of business identified with security, accountability of data, privacy and integrity, just as its utilization in the securing networked gadgets, for example, IOT[3]. Its overall objective is to give a network driven inception to a superior investigation of cyber security and blockchain that investigates the interaction between two oftentimes examined fields. Toward this objective, it will basically look at studies and existing works on the blockchain cyber security also use its experiences to grow new bearings.

- *Prior Research:*

Explicitly corresponding to the use of blockchain to the issue of the cyber security, apparently, there seems, by all accounts, to be very constrained SLRs i.e. "Systematic Literature Reviews". The latest overview papers in the domain of cyber security and blockchain was performed by researcher. Right now, creators feature the issues and challenges related with the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

utilization of the security services in centralized architecture in different application spaces, and give a thorough audit of current blockchain-empowered strategies for these applications of security service in regions of confidentiality, access control, integrity affirmation in distributed networks, authentication, privacy and resource and data provenance[4].

Towards the finish of 2015, researcher led a SLR concerning the adaptability and utilization of blockchain explicitly comparable to IOT and some peer-to-peer gadgets. Strangely, it featured that blockchain could be utilized for information misuse identification without the requirement of a focal announcing mechanism. All the past investigations referenced above answer addresses identified with the more extensive utilization of blockchain innovation, however it doesn't inspect explicitly its utilization in improving solutions of cyber security[5].

- *Research Goals:*

The motivation behind this examination is to break down existing investigations and its discoveries and to abridge the endeavours of research in applications of blockchain for cyber security.

- *Contributions:*

This SLR is reciprocal to existing examination and gives the following commitments for all those having an enthusiasm for cyber security and blockchain to assist its work:

- It recognize 40 essential examinations identified with cyber security and blockchain up to mid-2018[6].
- It further select 32 essential investigations that meet criteria it set to the quality assessment.
- It lead a thorough audit of the information contained inside subset of 33 studies.
- It depict a meta-examination of the condition of play as to techniques wherein blockchain can be actualized to enhance security of existing also, rising cyber technologies.
- It make portrayals and produce rules to help further work right now[7].

RESEARCH METHODOLOGY

To accomplish the aim of responding to the exploration questions, it directed the SLR as per the direction published by researcher. It tried to travel through the arranging, reporting and conducting phases of the audit in emphases to take into account exhaustive assessment of SLR. Primary considers were featured through passing catchphrases for search office of a specific search engine or publication. The catchphrases were chosen to advance the rise of the research results that will help with noting the exploration questions. Studies for being remembered for this SLR must conduct exact discoveries and can be papers on contextual analyses, new specialized blockchain applications what's more, editorials on the improvement of existing security systems through blockchain joining[8]. It should be peer-inspected and composed in the English. There were sum of 744 examinations recognized from the underlying catchphrase look on the chose stages. This was decreased to 663 after expelling copy contemplates. In the wake of checking the investigations under the consideration/rejection criteria, the quantity of papers staying for perusing was 70. 70 papers were perused in full with incorporation/rejection criteria being re-applied, 34 papers remained. The evaluation of the nature of essential examinations was made agreeing to the direction set by researcher. This considered an appraisal of the pertinence of papers to the examination questions, with thought for any indications of research predisposition and the legitimacy of test data. All papers which had passed quality appraisal at that point had its information extracted to evaluate the culmination of information to test the precise account of data contained inside the papers. The process of data extraction was taken a stab at an underlying five examinations before being extended to incorporate the full arrangement of concentrates which have passed quality evaluation stage. The information from each investigation were extricated, arranged and afterward put away in a spreadsheet[9].Figure 2 is an outline indicating the quantity of essential examinations published every year. As it can be found in figure, there is the upward pattern in the utilization of blockchain in context of cyber security. It conceive that later on it will see a critical number of research considers with respect to the selection of blockchain in certifiable applications, as the quantity of the publication up to 2019 is just 50% of the entire number of the publications in 2018.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

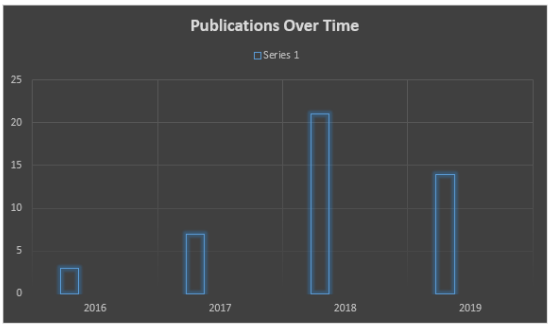

Fig. 1: Number of Primary Studies Published Over Time

FINDINGS

All the essential examinations had a concentration or subject according to how the blockchain was managing a specific issue. Each paper's centre was additionally assembled into more extensive classes to take into consideration a rearranged grouping of the topics of the essential investigations. Concentrates that had a centre concerning virtual machines, virtual network management and networking were gathered into the category of networks[10]. Concentrates that had a centre identified with distributed sharing, encoded information stockpiling and looking were gathered into the class of sharing and data storage. Figure 2 depicts the percentages of various subjects of the 30 essential contemplates which had made it pass the quality appraisal to be incorporated in the information investigation.

DISCUSSION

The underlying watchword look through depict that there are the significant number of papers identified with blockchain. The innovations of blockchain and genuinely disseminated decentralized frameworks have just been produced for a long time and are obviously still in its early stages. A sizeable segment of the chose essential examinations are test proposition or ideas for answers for the present issues, and it has minimal quantitative information and hardly any viable applications. A portion of the more viable security arrangements offered in the staying essential examinations show creative methods for tackling a wide scope of issues concerning mutability, authentication of users and data security. The arrangements frequently rely upon a critical change to that framework's foundation, for instance, an adjustment in the reliance or network architecture on a specific blockchain or stage over a solitary, centralized server. Because of the worker associated with moving or changing a current framework, it is hard for a portion of the pragmatic ideas to be execute in a trial situation for a specific time allotment to decide the viability of the application of blockchain over traditional security[11].

The scientists utilized built up stages, for example, Bitcoin and Ethereum for a couple of various reasons. Ethereum considers truly customisable programming of shrewd agreements and applications of blockchain in language Solidity, that isn't excessively far expelled from Python and JavaScript and in that capacity makes it appealing to developers. The present mechanisms of proof-of-work receiving Bitcoin or Ethereum for accomplishing agreement can prove up being detrimental for lightweight lOT frameworks, as it has to utilize asset concentrated procedures and networking for hash squares of the transactions for a point where it accomplish a foreordained degree of difficulty. The robustness, trust less and strength intrigue of a blockchain originate from its democratic framework. Furthermore, because of this, the essential examinations when all is said in done have demonstrated an acknowledgment that the utilization of existing blockchains is a need[12].

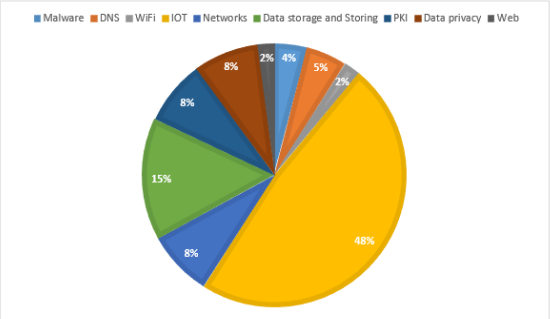

Fig. 2: Chart of Themes of Primary Studies

FUTURE RESEARCH DIRECTIONS

In light of the aftereffects of this review and its observations, it present the accompanying exploration bearings of blockchain for the cyber security which worth further examination:

- *Blockchain to IOT Security:*

In IOT networks, security has been guaranteed as a squeezing need of the business and has gotten most extreme need for enforcement and improvement, in spite of recent research depicts the way that pretty much every article on the blockchain digital security in the writing calls attention to that security of the IOT frameworks could be rejuvenated on the off chance that

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

it is bolstered with blockchain innovation. However, little is known furthermore, talked about elements identified with choices about and possibility to receive this innovation, and where and how it tends to be efficiently put into utilization to cure recent IOT security dangers/risks in an unmistakable setting, taking into consideration the creative mind and afterward production of the future vectors right now explicit space[13]. Along these lines, it is significant for the future research to build up a few quantifiable rules and instruments that can assist fill this clear in the writing.

- *Blockchain to AI Data Security:*

In current computing environment, information is caught from different sources and transmitted between gadgets through networks. AI i.e. Artificial Intelligence and its subordinates have been utilized as incredible assets to break down and process the caught information to accomplish compelling reasoning in tending to security issues. Despite the fact that AI is amazing and can be locked in with the distributed computing, the deceptive investigation would be produced when undermined or untrustworthy information is purposefully or unexpectedly coordinated by a malevolent outsider in light of antagonistic data sources. Blockchain as a famous ledger innovation can possibly be utilized in various regions of cyber space. Blockchain endeavours to diminish financial fraud and transaction risks, attributable to its qualities, for example, verifiability, immutability and decentralization for guaranteeing the reliability, integrity and authenticity of data. Future look into heading could be the investigation of the blockchain for security of the AI information in M2M and B2B environments[14].

- *Sidechain Security:*

The sidechain innovation has most currently developed as a different chain appended to the principle chain, in corresponding with transactions, to reduce the difficulties (for the most part performance) identified with fundamental blockchains. Sooner rather than later, it imagine distributed multi-blockchain system, in which diverse principle chains what's more, sidechains work to team up with one another in different situations.

CONCLUSION

This exploration has distinguished accessible current research on how the blockchain arrangements can add to the cyber security issues. The underlying watchword scans for this exploration and recent media reports feature blockchain as an independent innovation that carries with it an extreme exhibit of potential answers for logistics, healthcare security, cyber security and finance. This examination has concentrated exclusively on the cyber security. Without a doubt, there are commendable applications for blockchain, in any case, a trust less, decentralized framework can't without anyone else's input take care of all issues one may reveal in the cyber security field.

Applications of Blockchain to cyber security have developed and reinforced the current endeavours to upgrade security and to prevent noxious actors. This examination features openings accessible for future research for being led in cyber security areas outside the domain of the IOT. As Internet moves towards the mass selection of the https encryption also the end clients are progressively utilizing a few types of encryption for regular communication, there is a consistently expanding need to safely deal with the encompassing certification and cryptography schemes.

REFERENCES

[1] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Futur. Gener. Comput. Syst.*, 2017.

[2] I. C. Lin and T. C. Liao, “A survey of blockchain security issues and challenges,” *Int. J. Netw. Secur.*, 2017.

[3] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, “A systematic literature review of blockchain cyber security,” *Digital Communications and Networks*. 2019.

[4] S. Singh and N. Singh, “Blockchain: Future of financial and cyber security,” in *Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics, IC3I 2016*, 2016.

[5] A. L. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” *IEEE Commun. Surv. Tutorials*, 2016.

[6] W. Wang and Z. Lu, “Cyber security in the Smart Grid: Survey and challenges,” *Computer Networks*. 2013.

[7] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-Physical Systems Security - A Survey,” *IEEE Internet Things J.*, 2017.

[8] M. Conti, K. E. Sandeep, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surv. Tutorials*, 2018.

[9] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, 2018.

[10] M. Banerjee, J. Lee, and K. K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digit. Commun. Networks*, 2018.

[11] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Computer Communications*. 2019.

[12] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors (Switzerland)*. 2018.

[13] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*. 2018.

[14] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks," *IEEE Trans. Smart Grid*, 2019.

[15] Gagandeep Singh Narula, Dr. Vishal Jain, Dr. S. V. A. V. Prasad, "Use of Ontology to Secure the Cloud: A Case Study", International Journal of Innovative Research and Advanced Studies (IJIRAS), Vol. 3 No. 8, July 2016, page no. 148 to 151 having ISSN No. 2394-4404.

[16] Gagandeep Singh Narula, Ritika Wason, Vishal Jain and Anupam Baliyan, "Ontology Mapping and Merging Aspects in Semantic Web", International Robotics & Automation Journal, having ISSN No. 2574-8092, Vol. 4, No. 1, January, 2018, page no. 01 to 05 .

[17] Gagandeep Singh Narula, Usha Yadav, Neelam Duhan and Vishal Jain, "Evolution of FOAF and SIOC in Semantic Web: A Survey", CSI-2015; 50th Golden Jubilee Annual Convention on "Digital Life", held on 02nd to 05th December, 2015 at New Delhi, published by the Springer under Big Data Analytics, Advances in Intelligent Systems and Computing having ISBN 978-981-10-6619-1 page no. 253 to 263

[18] S. Balamurugan, K. Amarnath, J.Saravanan and S. Sangeeth Kumar, "Scheduling IoT on to the Cloud : A New Algorithm", European Journal of Applied Sciences 9 (5): 249-257, 2017.

[19] S.Balamurugan et.al., "Smart Healthcare: A New Paradigm", European Journal of Applied Sciences 9 (4), 212-218, 2017

[20] S.Balamurugan ,R.Madhukanth , V.M.Prabhakaran and Dr.R.GokulKruba Shanker, "Internet of Health: Applying IoT and Big Data to Manage Healthcare Systems," International Research Journal of Engineering and Technology (IRJET), Volume 3 issue 10, pp.732-735,e-ISSN: 2395 - 0056, p-ISSN: 2395-0072, 2016