Available online at: http://www.ijmtst.com/vol5issue01.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 05, Issue No: 01, January 2019

A Survey on Improving Security of Wireless Sensor Network using Block Chain

Komal Shinde[1] | Dr. S. V. Todkari[2]

[1,2]Computer Engineering, JSPM's JSCOE, Hadapsar, Maharashtra, India

To Cite this Article

Komal Shinde, Dr. S. V. Todkari, "A Survey on Improving Security of Wireless Sensor Network using Block Chain", *International Journal for Modern Trends in Science and Technology*, Vol. 05, Issue 01,January 2019, pp.-28-31.

Article Info

Received on 28-Dec-2018, Revised on 18-Jan-2019, Accepted on 24-Jan-2019.

ABSTRACT

Wireless sensor network is widely used in the word due to the need of drastically changing world. People want life to make easy as possible as. But we need to take care of cons of any new emerging technology. This paper discusses challenges in WSN, security concerns in WSN and pros of block chain to solve the issues involved in security. Block chain is widely used and accepted technique to improve the security in data and network. Basically, crypto currencies in the world uses block chain to make their currency secure.

Keywords: *WSN, Block chain, Crypto currency*

I. Introduction

The fast development in WSN, hardware and remote correspondence advancements have added to remarkable propels in our general public. This has brought about an expansion in the number of reasonable electronic gadgets for some territories, a decrease in their generation costs and a change in outlook from this present reality into the computerized world. Hence, the manner by which we collaborate with one another and with nature has changed, utilizing current innovation to pick up a superior comprehension of the world.

Block chain is the component that enables exchanges to be checked by a gathering of temperamental performing artists. It gives a circulated, unchanging, straightforward, secure and auditable record. The block chain can be counseled transparently and completely, enabling access to all exchanges that have happened since the primary exchange of the framework, also, can be checked and examined by any substance whenever. The block chain convention structures data in a chain of squares, where each square store a lot of Bit coin exchanges performed at a given time. Squares are connected together by a reference to the past square, shaping a chain. To help and work with the block chain, arrange peers need to give, the accompanying usefulness: steering, stockpiling, wallet administrations and mining [6].

Block chain has additionally given an innovation where the idea of brilliant contract can be emerged. When all is said in done terms, a shrewd contract alludes to the PC conventions or projects that permit a contract to be naturally executed / implemented considering a lot of predefined conditions. For instance, shrewd contracts characterize the application rationale that will be executed at whatever point an exchange happens in the trading of cryptographic money. In shrewd contracts, capacities and conditions can be characterized past the trade of cryptographic forms of money, for example, the approval of advantages in a certain scope of exchanges with non-money related components, which makes it an ideal segment to extend block chain innovation to other zones. Ethereal [6] was one of the pioneer block chains to incorporate savvy contracts. Today shrewd contracts have been incorporated in the greater part of existing block chain usage, for example, Hyper ledger [7], a block chain intended for organizations that permits parts to be conveyed by the necessities of clients (brilliant contracts, administrations or discussions among others) with the help of huge organizations, for example, IBM, JP Morgan, Intel and BBVA.

II. Literature Survey

E. Androulaki et al. [2] proposed a Texture which is a particular and extensible open-source framework for sending what's more, working permission block chains and one of the Hyper ledger ventures facilitated by the Linux Foundation (www.hyperledger.org).Texture is the first genuinely extensible block chain framework for running disseminated applications. It bolsters particular agreement conventions, which enables the framework to be custom fitted to specific use cases and trust models. Texture is likewise the first block chain framework that runs circulated applications written in standard, universally useful programming dialects, without fundamental reliance on a local digital money. This stands in sharp differentiation to existing block chain stages that require "brilliant contracts" to be written in area explicit dialects or depend on a digital currency. Texture figures it out the permission display utilizing a compact idea of participation, which might be coordinated with industry-standard character the executives. To help such adaptability, Fabric presents an altogether novel block chain plan and patches up the way block chains adapt to non determinism, asset depletion, and execution assaults.

This paper [3] depicts Fabric, its design, the basis behind different plan choices, its most unmistakable usage viewpoints, and in addition it's disseminated application programming model. We further assess Fabric by executing and benchmarking a Bit coin-enlivened computerized money. We demonstrate that Fabric accomplishes end-to-end throughput of in excess of 3500 exchanges for every second in certain well known arrangement setups, with sub-second dormancy, scaling admirably to more than 100 friends.

Z. Zhen et al. [4] discussed various advantages of Block chain, for example, decentralization, persistency, obscurity and audit ability. There is a wide range of block chain applications extending from cryptographic money, monetary administrations, hazard the board, web of things (IoT) to open and social administrations. Despite the fact that a number of studies centre on utilizing the block chain innovation in different application angles, there is no complete review on the block chain innovation in both innovative and application points of view. To fill this hole, we lead a thorough study on the block chain innovation. Specifically, this paper gives the block chain scientific categorization, presents regular block chain agreement calculations, surveys block chain applications and examines specialized difficulties and in addition ongoing advances in handling the difficulties. In addition, this paper likewise calls attention to the future bearings in the block chain innovation.

X. Li et al. [5] discussed the block chain innovation which has indicated promising application prospects. From the underlying digital money to the present brilliant contract, block chain has been connected to numerous fields. In spite of the fact that there are a few investigations on the security and protection issues of block chain, there comes up short on an orderly examination on the security of block chain frameworks. In this paper, we lead a deliberate report on the security dangers to block chain and overview the comparing genuine assaults by looking at mainstream block chain frameworks. We additionally survey the security improvement answers for block chain, which could be utilized in the advancement of different block chain frameworks, and recommend some future bearings to mix investigate endeavors into this region.

Kaspars Zīle and Renāte Strazdiņa [6] give an obscure outline of as of now existing block chain use cases in the data innovation industry. Separate use cases have been inspected in effectively existing logical papers, Master Theses, industry white papers and online journals of industry specialists. The paper likewise contains a depiction of block chain fundamental mechanical angles and working standards, which permits making the evaluation of the displayed use cases. For each utilization case separate organizations or associations are included that are applying or testing the given arrangement. Due to explore constraints the paper ought not to be considered a thorough block chain use case portrayal. The paper additionally gives short presentation into a possibility examination of explicit block chain use case. The creators portray the essential strides of potential thought assessment concerning block chain primary angles. It comprehends the need for advancement of a nifty gritty block chain possibility display.

Kosba et al. [7] proposed brilliant contract frameworks over decentralized digital currencies enable commonly incredulous gatherings to execute securely without confided in outsiders. In case of legally binding ruptures or prematurely ends, the decentralized block chain guarantees that legit parties get similar remuneration. Existing frameworks, nonetheless, need value-based security. All exchanges, counting stream of cash among aliases sum executed, are uncovered on the block chain.

III. CHALLENGES IN WSN

Confidentiality: It is the act of protecting the secret information from unauthorized users or entities.

Integrity: This is the term that ensures that the messages in the network are unaltered through malicious nodes.

Data Origin Authentication: This authenticates the source of message.

Entity Authentication: This authenticates the user / node / base - station is indeed the entity that it claims to be.

Access control: This takes care of restricting access to resources only to those privileged users or entities.

Availability: This makes sure that the desired services are available as and when required.

Forward secrecy: This makes sure that the node does not decrypt any future secret messages even after it leaves the network.

Backward secrecy: This considers preventing a joining node to decrypt the previously transmitted secret message.

Survivability: This ensures that a certain level of service is provided at the case of failures or attacks.

Freshness: This is to ensure that the data is recent and no adversary can replay old messages.

Scalability: This feature is to support addition of great number of nodes in the network.

Efficiency: This is to maintain the efficiency of processing, storage and communication limitations on sensor nodes.

IV. ADVANTAGES OF BLOCK CHAIN

1. Transparency

One of the prime reasons block chain is fascinating to organizations is that this innovation is quite often open source. That implies different clients or engineers have the chance to adjust it as they see fit. In any case, what's most vital about it being open source is that it makes modifying logged information inside a block chain unimaginably troublesome. All things considered, if there are endless eyes on the system, somebody is most likely going to see that logged information has been changed. This makes block chain an especially secure innovation.

2. Reduced transaction cost

Block chain enables distributed and business-to-business exchanges to be finished without the requirement for an outsider, which is frequently a bank. Since there's no agent inclusion fixing to block chain exchanges, it implies they can really diminish expenses to the client or organizations over time.

3. Faster transaction settlements

It is normal for exchanges to take days to totally settle. This is because of conventions in bank exchanging programming, and in addition the way that budgetary foundations are just open amid typical business hours, five days seven days. You additionally have money related foundations situated in different time zones far and wide, which can postpone preparing times. Nearly, block chain innovation is working 24 hours every day, seven days seven days, which means block chain-based exchanges process extensively more rapidly.

4. Decentralization

Another focal reason block chain is so energizing is its absence of a focal information center point. Rather than running a monstrous server farm and confirming exchanges through that center, block chain really enables singular exchanges to have their own evidence of legitimacy and the approval to uphold those limitations. With data on a specific block chain piecemealed all through the world on individual servers, it guarantees that if this data fell into undesirable hands (e.g., a digital *criminal), just* a little measure of information, and not the whole system, would be imperiled.

5. Client controlled systems

In cryptographic money financial specialists are will in general be truly empowered by the control part of block chain. As opposed to hosting a third gathering run the show, clients and designers are the ones who get the opportunity to give orders. For example, a powerlessness to achieve a 80% agreement on an overhaul attached to bit coin's block chain is the thing that required a fork into two separate monetary forms (bit coin and bit coin money) over four months back. Having a state runs far with financial specialists and engineers.

V. Conclusion

This paper discussed the various issues concerned in wireless sensor network. The main concern in wireless sensor network is a security. As data is transferred over network, there are changes of tampering with data or data stolen is possible. To avoid this various algorithms are used but still there are chances to happen misuse of this data. Block chain is one of the best technique to make your data secure. Due to popularity of block chain technique, it is widely used in crypto currency all over the world.

References

[1] Attilio Fiandrotti, Rossano Gaeta, Marco Grangetto, Securing Network CodingArchitectures against Pollution Attacks withBand Codes,IEEE Transactions oninformation forensics and security, July 2018.

[2] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro,D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: A distributed operating system for permissioned blockchains, 2018, arXiv preprint arXiv:1801.10228.

[3] A.M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media, Inc., 2014.

[4] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. (2017).

[5] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. (2017) (in press).

[6] Kaspars Zīle, Renāte Strazdiņa, Blockchain Use Cases and Their Feasibility, ISSN 2255-8691 (online),ISSN 2255-8683 (print),May 2018, vol. 23, no. 1, pp. 12–20,doi: 10.2478/acss-2018-0002,https://www.degruyter.com/view/j/acss

[7] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: the blockchain model of cryptography and privacy-preserving smart contracts, in: Security and Privacy (SP), 2016 IEEE Symposium on, San Jose, CA, USA, IEEE, 2016, pp. 839–85.