Blockchain and IoT: Opportunities and Challenges

Viddi Mardiansyah[1], Sunjana[2]

Abstract*—Blockchain innovation has been changing the budgetary business and has made another crypto-economy in the most recent decade. The fundamental ideas, for example, decentralized trusting and distributing ledger is pledge for dispersed, and substantial scale IoT (Internet of Things) implementation. In any case, the utilizations of blockchain digital forms of money in this space are rare in light because of lack understanding and inborn design difficulties. In this paper, we depict the open doors for implementation utilizing blockchain and IoT and to inspect the difficulties engaged with architecting Blockchain-based IoT applications (Abstract)*

Keywords *— Blockchain; Internet of Things; Security*

I. Introduction

Satoshi Nakamoto established framework for blockchain innovation in 2008, by exhibiting an answer for decentralized trusting among obscure elements [1]. BitCoin, is the main decentralized digitize currency, affected budgetary establishments, and a wide-number of cryptographic forms of money step in to market place in the following years. Most of blockchain applications right now include advanced digital forms of money, where the clients trade fiscal incentive with one another through the decentralized system.

Empowering decentralized trust through an agreement convention or agreement protocol and disseminated stockpiling through a carefully designed record are the basic highlights of blockchain. Any application that includes various stakeholders can profit by these highlights since it empowers straightforward communications without requiring a confided in outsider. IoT implementation with regards to savvy urban communities and production network the board comprise of various partners, where the Blockchain technology can be utilized to reinforce the certainty among the included substances and associations.

In spite of the fact that the innovation has been around for very nearly ten years, its specialized underpinnings are made clearer just over the most recent couple years. From one viewpoint, engineers planning IoT implementation are completely mindful of the constraints and capacities of contemporary IoT stages and advances. Then again, Blockchain designers and devotees comprehend the down to earth subtleties of blockchain structures and their feasibility on various class of calculation and capacity stages. We see a hole between two networks, and it's fundamental to connect this hole, and to completely misuse the capacities of the blockchain innovation past cryptocurrency and the FinTech implementation.

This paper, will displays the guarantees of blockchain and Internet of Things and portrays the difficulties and restrictions of blockchain, by connecting the structural components of Internet of Things with the blockchain. Moreover, this paper

[1] *Informatics Department, Engineering Faculty*
Widyatama University
Bandung, Indonesia
viddi.mardiansyah@widyatama.ac.id

likewise examines the basic plan inquiries for application engineers who planning and actualizing implementation at the crossing point of blockchain and Internet of Things.

Segment 2 in this paper will gives an outline and the architecture of Internet of Things. The design components and blocks building of blockchain are exhibited in segment 3. Segment 4 in this paper will talks about the opportunity while applying blockchain for the Internet of Things. Segment 5 in this paper, portrays the opportunities inquiries and challenges. At the end, Segment 7 finishes up the conclusion of the paper.

II. Overview of IoT

IoT (Internet of Things) contains the “Things” that have exceptional characters and are associated with the Internet. The attention on IoT is in the arrangement, control and systems administration through the Internet of gadgets or "Things" that are generally not related with the web or internet, for instance a water siphon, utility meter, vehicle motor, and so forth. IoT is another insurgency in the capacities of the endpoints that are associated with the internet. The evolution of Internet of Things (IoT) is appeared on Figure 1.

Figure 1. Evolution of IoT

Application zones of IoT incorporate shopper, retail, medic, army, industry, automotive, ecological, agribusiness, smart city, production, supply chain, and some more. Internet of Things involves sensor, communication, computation, and activation functionality, and such functionality is circulated all through the system. Internet of Things design can comprehensively ordered on three layers as shown in below.

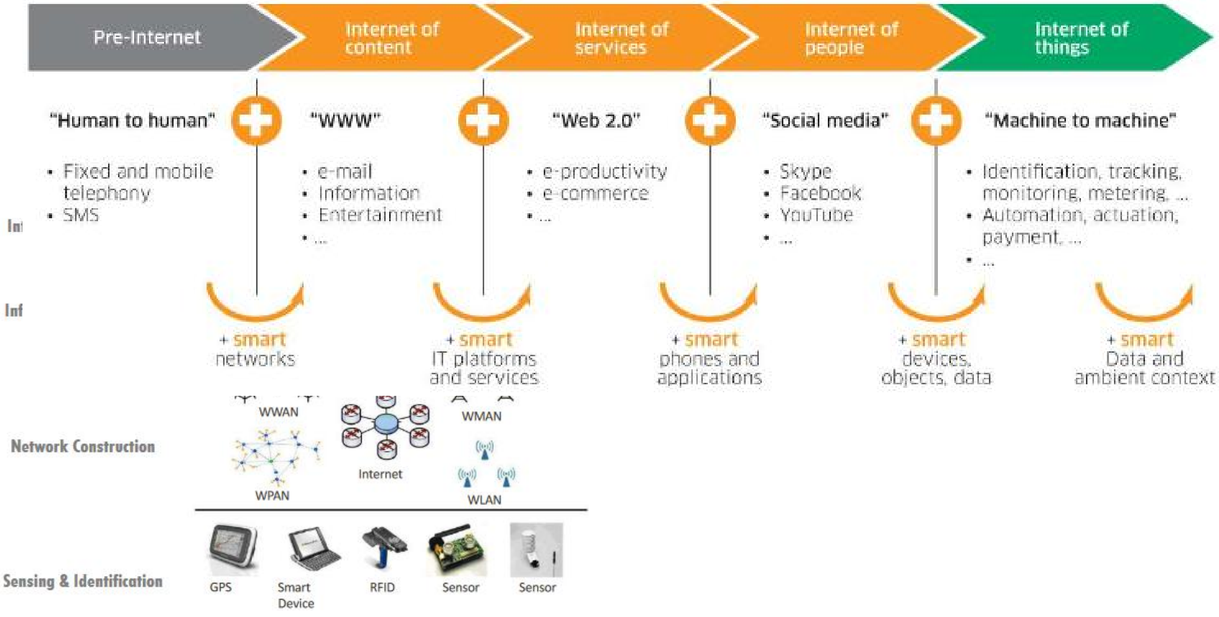

Figure 2. IoT Architecture

Integrated Application: The Integrated Application layer is an application that can seamlessly integrated into many project. For example, the smart transportation environment will integrated with all the traffic light and provide priority lines for an ambulance on their way to the nearest hospital.

Information Processing: The Information Processing layer is responsible to process the data that came from the sensor to be processed further more. For example in water level indicator, when the sensor indicating the high voltage, it will processed as information that the water level already reach the maximum capacity, so it will open the valve to maintain the water level on the secure level.

Network Construction: The Network Construction layer is in charge of gathering sensor information from the gadgets. This layer comprises of a system door for dealing with inbound and outbound interchanges between the sensor and the gadget. Likewise, the information from various sensor gadgets are prepared in this layer to fulfill the ongoing needs of the IoT application.

Sensing & Identification: The Sensing and Identification involves sensors, low-power installed stages, remote correspondence advancements, and savvy gadget. Low-power inserted IoT stages go about as a center for sensors and at least one remote communication technologies. IoT stages are regularly sent in testing and difficult to-achieve situations. Along these lines, it's the basic to keep the gadgets running longer while using on battery. This layer is the most asset compelled layer in Internet of Things architecture.

The above architecture of IoT implementation have been generally utilized in different organizations, yet the combination of blockchain into such a design stays testing as talked about in Segment 5. The outline of blockchain and its center structure blocks are introduced in the following area.

III. Overview of Blockchain

The framework for blockchain innovation is established by Satoshi Nakamoto in 2008, by exhibiting an answer for decentralized trust among obscure elements [1]. Blockchain fills in as a permanent information which permits the exchanges happen in a decentralized ways. Blockchain-based implementation are jumping up, covering various fields including budgetary administrations, notoriety framework and Internet of Things (IoT) particularly in security in IoT.

Blockchain is an arrangement of blocks, which is holds a total rundown of exchange informations like regular open ledger [2]. Figure 3 below is delineates a case of the blockchain. With the past block hashing contained in the blocks header, a block only have a single parent block. It is the same significant that uncle block (offspring of block predecessors) hashes would likewise be put away in the ethereum blockchain [3]. The principal blocks of the blockchain is called beginning block where there is no parent block. We at that point clarify the internals of blockchain in subtleties.

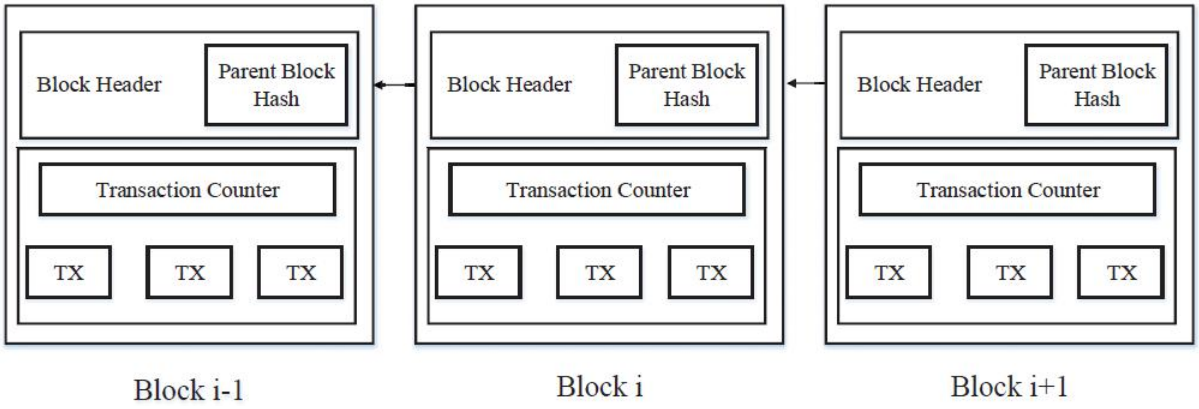

Figure 3. An Example of Blockchain

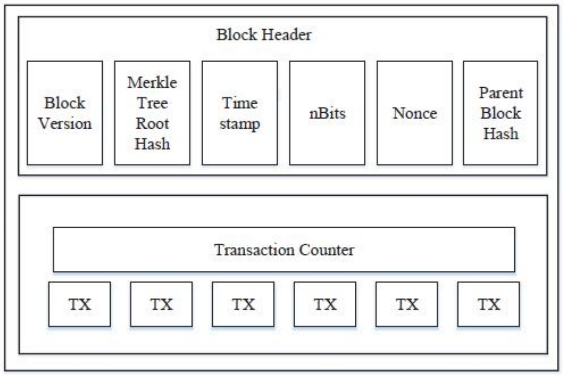

Figure 4. Block Structure

The three key aspects of blockchain technologies that will discuss in this section is:

1. **Cryptographic Digital Signature:** The open key or public key cryptography is utilized in blockchain to produce a mark for Blockchain exchanges. Clients complete exchanges by making a computerized mark utilizing their keys private. Beneficiaries of blockchain organize check the exchange utilizing the open key private of sender to guarantee, that the exchange is for sure marked by the sender. The source and/or the end device sign the exchanges, while they make an exchange.
2. **Distributed Ledger:** Blockchain utilize a dispersed stockpiling to record the exchanges. Fundamentally, every one of the stages in the system store either the whole exchanges or a subset of exchanges. Every one of the hubs in the system go to an agreement (utilizing an agreement algorithm) before it entered the exchanges into ledger. And because of it, this component will makes the blockchain adequately changeless.
3. **Consensus/Agreement Algorithm:** The blockchain doesn't depend on concentrated servers for their confirmation and approval of exchanges. Rather, blockchain utilizes a shared model and every one of the choices inside the system are made by the taking an interest individuals through a agreement protocol.

In blockchain, how to achieve accord among the deceitful hubs are a change of the Byzantine Generals (BG) problems, which was brought up in [4]. In the BG issue, a gathering of officers who direction a bit of Byzantine armed force circle the city. A few commanders want to assault while different officers want to withdraw. Be that as it may, the assault would fizzle if just piece of the officers assault the city. In this way, they need to achieve a consent to assault or withdraw. Step by step instructions to achieve an agreement in circulated condition is a test. It is additionally a test for blockchain as it arrange is circulated. In blockchain, there are no center hub that can guarantees records on circulated hubs are all is the same. A few protocols are expected to guarantee ledger in various hubs are steady.

IV. Opportunities

The center structure block of blockchain, for example, public key cryptography, disseminated ledger, and agreement algorithm are very pledge while implementing Internet of Things. We will portray the opportunity for applying blockchain implementation to the Internet of Things in this area.

a. **Privacy/secrecy:** Used of transaction in the blockchain utilize the computerized character produced utilizing open/public key cryptography and hashing method algorithm implementation. Internet of Things implementation with touchy data, can use these system to conceal genuine character in the system

b. **Monetary trade of information and figure:** Monetary trade of information and figure: IoT implementation in the region of savvy urban areas use sensors in blend with publicly supporting to convey advanced administrations to the city populace. Money related prizes might be fundamental to include the network individuals in brilliant city applications and to use the edge assets, for example, calculation influence, stockpiling, and transmission capacity. Blockchain can likewise be utilized to set up a financial framework to issue key to the network individuals for their cooperation.

c. **Record exchanges information and review:** The information from Internet of Things implementation are carry away through framework possessed by different associations. Supply chain observing spotlights on following and checking resources all through the production network process. Customary production network observing frameworks depend on a concentrated design, wherein every one of the information from resources are put away in a center of database. Utilizing blockchain for chronicle the information in a decentralized record expands the trust, while moving resources (genuine or computerized) through framework possessed by different and various partners.

d. **Smart Contract:** The idea of Smart Contracts was presented by Nick Szabo [5] as an option in contrast to the customary paper based contracts. The brilliant contract is a computerized contract installed into the framework, which will gets executed by the time when the conditions announced and the understanding are meet. Brilliant contracts referee exchanges self-rulingly while trading resources between gatherings or managing non-confided in individuals in a blockchain arrange. IoT implementation, for instance, can utilize brilliant contracts while transporting sensor information through frameworks claimed by various partners and selling information delivered by the sensors.

V. Challenges

We currently talk about the difficulties that emerge in applying blockchain in the IoT.

1. **Resource imperatives:** Most of the IoT stages are extremely restricted assets for calculation, correspondence, and capacity, while blockchain is request an unnecessary assets for calculation, correspondence, and capacity. Low power IoT have only under 10 KB of memory information retrieval and only have memory program under 100 KB [6], while a Blockchain hub require more memory up to GBs [7]. Likewise, the calculation prerequisites of agreement algorithm, for example, Proof-of-Work are well-past the capacities of low power, is the asset obliged in IoT.
2. **Security limitations:** Blockchain pursues a decentralized architecture, wherein every one of the gadgets in the system organize and participate with one another through pre-characterized conventions. Along these lines, the gadgets remain associated with the blockchain organize for taking an interest in the agreement procedure. This constantly associated highlight makes IoT gadgets conceivably increasingly powerless to security assaults. Yet additionally wound up one of answer for keep the aggressor, in light of the fact that each blockchain are organize one another, on the off chance that one of them are suspect to be contaminated, at that point the other will affirming it.
3. **Bandwidth prerequisites:** As mention previously that Platforms in the Blockchain requires memory in GBs, it is need to interface with different stages in the system to take an interest in the agreement procedure. Because of the decentralized idea of the consensus procedure, stages in the system trade data the blockchain is to approve exchange and to make a new block. IoT gadgets working at end of gadget layer, and have extreme transmission capacity limitations,

which additionally implies the modern blockchain arrangements are not appropriate for end gadgets. The adequate transmission capacity may have by the edge device and the server, yet note that the data transmission necessity of blockchain may surpass the transfer speed prerequisite by itself, in any event with most blockchain conventions.

4. **Access Permission:** Blockchain advances can be comprehensively characterized into two classifications, which is public/open and permissioned. Public/open blockchains, for example, Bitcoin and Ethereum enable everybody to turn into a piece of the system with no approval. Everybody wishing to take an interest in the open blockchain can basically download and introduce the vital systems. Permissioned blockchains, then again, comprises of approved individuals to the system. This sort of model might be appropriate for IoT implementation including different referred to associations as the system comprises of approved individuals, which open up opportunities for quick, higher-throughput agreement conventions.
5. **Latency requests:** IoT implementation regularly comprise of an accumulation of information makers and information customers, and now and again, the information purchasers respond an occasion and will perform some activation. The blockchain presentation in this setting may diminish the responsive, if the information customer might be require to hang tight for finishing of the agreement procedure right before responding to occasion.
6. **Transaction Fees:** Most of the open blockchain usually charge expense for an exchanges, and will be use it to compensating the hubs engaged with agreement process. Internet of Thing gadgets can't store every information to such a blockchain since putting away the information to a blockchain causes an exchange expense. In the event that somebody want to put the information from Internet of Things gadgets on a blockchain implementation, that might should be collected to decrease the exchange expenses, yet for this situation it is vital to ensure that the accumulation procedure does not sift through fundamental data. On the other hand, where the design of where the information itself is migrated from the blockchain and just hash qualities or the key to exchange records are put away on it for confirmation and original destination might be favored.

VI. Related Work

Writing joining blockchain and Internet of Things might contribute the security and the protection arrangements. Kshetri [8] approves the uses of blockchain in order to verifying the IoT. Tomer. contribute CIoTA [9] to distinguish oddities in Internet of Things implementation. CIoTA applied the ideas of block chain and mix with the (EMM) Extensible Markov Model to distinguish noxious exercises. Dorri. [10] present that the holes in modern securities and protection strategies, and contribute with the LSB, a very light weight and adaptable blockchain for Internet of Things securities and privacy. LSB's light weight conventions decrease the data transfer capacity and calculation fees. Pietro. [11] Examine the correspondence overhead of the blockchain implementation to synchronize conventions for the Internet of Things and feature the up and down link transfer speed requests. PlaTIBART [12] trying the system to oversee and convey the blockchain systems for transactive Internet of Things implementation. Hossein. [10] Presents a circulated information stockpiling system for Internet of Things implementation utilizing the blockchain. [13] Guarantees that the Internet of Things information proprietorship remains with the partners. These papers address a portion of the difficulties in depicted in segment 5, in any case, the building subtleties and execution suggestions are not plainly tended to, particularly for asset compelled IoT stages.

The opportunity and challenge while applying the blockchain for the IoT are introduced in literature above. Huckle. [14] talk about the utilizations of blockchain while adapting Internet of Things implementation, yet their work still doesn't depict the difficulties. Seyoung. [15] shows how the blockchain is can utilized for putting away the sensor information utilizing shrewd contracts. Canoscenti et al. [16] audits the utilization instances of the blockchain and features the open issues in honesty, obscurity, and flexibility while putting away IoT information in a decentralized system. The creators of [11] dissect the correspondence overhead of blockchain synchronization for the IoT. Not at all like [15] and [16], our work focus around engineering difficulties and execution suggestions when utilizing blockchain for IoT for information stockpiling, adaptation, security, and protection.

VII. Conclusion

The blockchain has officially had a critical effect in the digital currency implementation or cryptocurrency implementation. The crucial structure block - conveyed ledger, agreement components, and open key crypto graph of the blockchain is pledge for Internet of Things monitoring. We have talked about the design of Internet of Things implementation and will mapped the utilitarian block of the blockchain to uncover the engineering difficulties associated with applying blockchain in Internet of Things. Next, we have displayed opportunities while applying blockchain implementation in Internet of Things.

At the end, we finished up with the difficulties which should be routed to completely abuse the advantages of blockchain in the IoT domain particularly in security. Notwithstanding the difficulties, blockchain are exceptionally encouraging for settling security, protection, and trust issues in multi application situations.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer to peer electronic cash system”, 2008.

[2] D. Lee Kuo Chuen, Ed., “Handbook of Digital Currency”, 1st ed., Elsevier, 2015. [Online]:http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170

[3] V. Buterin, “A next-generation smart contract and decentralized application platform”, *white paper*, 2014.

[4] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem”, *ACM Transactions on Programming Languages and Systems (TOPLAS)*, Vol. 4 - No. 3, Page 382–401, 1982.

[5] N. Szabo, “Smart contracts”, unpublished manuscript, 1994.

[6] C. Bormann, A. Keranen, and M. Ersue, “Terminology for constrained-node networks”, RFC Editor, RFC 7228, May 2014. [Online]: http://www.rfc-editor.org/rfc/rfc7228.txt

[7] Running a full node. 2018. [Online]: https://bitcoin.org/en/full-node#minimum-requirements/

[8] N. Kshetri, “Can blockchain strengthen the internet of things?”, IT Professional, Vol. 19 - No. 4, Page 68–72, 2017.

[9] T. Golomb, Y. Mirsky, and Y. Elovici, “CIoTA: Collaborative IoT Anomaly Detection via Blockchain”, ArXiv E-Prints, March. 2018.

[10] Dorri, R. Jurdak, S. S. Kanhere, and P. Gauravaram, “LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy”, ArXiv E-Prints, December. 2017.

[11] Pietro Danzi, A. Ellersgaard Kalor, C. Stefanovic, and P. Popovski, “Analysis of the Communication Traffic for Blockchain Synchronization of IoT Devices”, ArXiv E-Prints, November. 2017.

[12] M. A. Walker, A. Dubey, A. Laszka, and D. C. Schmidt, “PlaTIBART: a Platform for Transactive IoT Blockchain Applications with Repeatable Testing”, ArXiv E-Prints, September. 2017.

[13] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards Blockchain-based Auditable Storage and Sharing of IoT Data”, ArXiv E-Prints, May 2017.

[14] S. Huckle, M. White, R. Bhattacharya, and N. Beloff, “Internet of things, blockchain and shared economy applications”, Procedia Computer Science, Vol. 98, Page 461 – 466, 2016 [Online]: http://www.sciencedirect.com/science/article/pii/S1877050916322190

[15] S. Huh, S. Cho, and S. Kim, “Managing Internet of Things Devices Using Blockchain Platform”, 19th International Conference on Advanced Communication Technology (ICACT), Page 464–467. 2017

[16] M. Conoscenti, A. Vetr, and J. C. D. Martin, “Blockchain for the internet of things: A systematic literature review”, IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), November 2016, Page 1–6.