IoT Focus on Security Using Blockchain

Senesh Wijayarathne
Sri Lanka Institute of Information Technology

IoT Focus on Security Using Blockchain

Senesh N. Wijayarathne
Sri Lanka Institute of Information Technology (SLIIT), Malabe, Sri Lanka
seneshw@gmail.com

***Abstract* — In the area of information technology, cyber security plays a significant role. One of the biggest challenges in the present day is the privacy and security of the information we have. 'Cybercrimes' is the first thing that comes to mind whenever we think about cybersecurity. In order to prevent these cybercrimes, various governments and companies are taking many measures. One of the solutions that have come up for these cybercrimes is the usage of Blockchain. The introduction and implementation of the Industrial Internet of Things (IIoT) have started a worldwide insurgency. The volume and assortment of information that is gathered and prepared in businesses are consistently expanding because of the boundless acknowledgment of current advances such as the Internet of Things (IoT). With the exponential increment of IIoT-associated devices has also incremented the number of threats of security and privacy breaches. Disadvantages such as low processing power, limited capacity abilities, and poor productivity standards are often found on IoT devices. In this specific situation, blockchain innovation can assist with taking out the security weaknesses looked at by the IIoT frameworks and gives broad assurance from information robberies, cyberattacks, and information debasement. Blockchain, with its disseminated design, offers shared systems administration and empowers auditable and straightforward exchanges. This report explores the concept of the Internet of Things (IoT), focusing on security by the usage of Blockchain. We further explore the evolution of the IoT security and the evolution of Blockchain, the future development of the IoT devices with the security of Blockchain, under the topic of IoT focus on security using Blockchain.**

***Keywords* — Industrial Internet of Things, Internet of Things, Blockchain, Security, Cyber Security.**

I. Introduction

Mr. Brendan O'Brien, the Co-Founder of Aria Systems, once said, "**If you think that the internet has changed your life, think again. The IoT is about to change it all over again!**". So, what is this IoT Mr. Brendan O'Brien was talking about? The Internet of Things or IoT is the communication of millions of smart devices, sensors, objects, people, or animals provided with Unique Identifiers, also known as UIDs. The IoT system has the ability to emit data over webwork without connection to the Internet [1].

Industrial Internet of Things (IIoT), alternatively known as Industry 4.0 or 14.0, alludes to the expansion and utilization of the Internet of Things (IoT) in the industrial sector to create connected spaces. IIoT is utilized to incorporate different machines, frameworks, actuators, and devices utilizing sensors and IoT gateways so they can flawlessly gather, interact, and trade information with one another. With the utilization of numerous sensors, data is collected and transmitted to the cloud-based systems where those gathered data could be stored, processed, and examined [2].

Notwithstanding, the multitude of interconnected devices creates monstrous volumes of complex information that customary unified systems struggle to deal with. Security threats and vulnerabilities additionally will, in general, increment with the increment in the number of associated devices. Since increasingly more information is gathered, security turns into another worry as any penetrate can bargain secret information [2].

Blockchain, being an arrangement of connected records, assists with defeating a large portion of the constraints looked at by the IoT. Since Blockchain is impervious to alterations and changes with modern cryptography, it is considered incredibly secure. Ms. Julie Sweet, one of the American businesswoman's, once said, "**Blockchain is moving beyond cryptocurrency, and it is worth paying attention especially since successful prototypes show that blockchain, also known as a distributed ledger technology, will be transformative.**" So, what is this Blockchain Ms. Julie Sweet was talking about? A Blockchain is an immutable ledger that has been shared with facilitates for the process of tracking assets and recording transactions in a business network. An investment can be tangible or intangible. On a blockchain network, anything of value can be traded and tracked virtually to reduce risk and to cut costs for all involved [3]. Combined with the IoT vision, Blockchain conveys unrivaled arrangements that can enable and change current cycles.

In the second part of this paper, there is the evolution of the topic and related parts. In the third part of this paper, there is the future development part of the topic, and in the fourth part of this paper, there are the conclusions about the subject, and in the end, there are the references for the topic.

II. Evolution of the Topic

A. Evolution of the IoT

In the 1990s, the limitation of Internet connectivity was in its use due to the reason of low production of the network interrelationship. In that period, internet connectivity had begun to increase in enterprise and consumer markets. In the 2000s, the norm form for plenty of packages has become internet connectivity. These days, it is predicted as a part of abounding corporations, businesses, and purchaser consequence to provide admission to get information. However, monitoring through apps and interfaces through human interactions is more required for these devices, for these are still primarily things on the Internet.

Nearly 50 billion "**smart**" devices have been deployed in the world [4]. Still, predictions have said that there will be more than 75 billion connected devices by the year 2025 [5], and we will be able to experience life with trillion-node networks in our lifetime. The rapid proliferation of the IoT into diverse applications is changing the fundamental way in which the physical world is perceived and managed.

Internet-connected systems have been integrated by current machine-to-machine (M2M) manufacturers into alarm systems, high-value benefit tracking, and the like for more than a decade and a half years. Even though some M2M systems are based on production standard agreements, there has been a challenge to build these M2M systems. However, with the evolution of further powered processors and incorporated into the conclusion nodes, it is getting trouble-free to integrate with these M2M systems. Network Operations Center, also known as NOC, managers all the high-end business service layers that are typically tied into these systems. Things such as energy meters, music streaming and control systems, lighting control systems, pool systems, and thermostats with more devices have already been connected by consumers. IoT technology has evolved into a level that we could manage systems that have connectivity through a website from our own standard web browser or intelligent mobile phone application, which can act as a personal Network Operations Center (NOC) [6].

B. What Made Blockchain Enter to the Side of IoT

The current IoT ecosystem depends on the server/client paradigms, otherwise known as centralized, brokered communication models. All devices connected to cloud servers have the power of sports processing and storage, and all appliances are identified and authenticated.

While this model has integrated computer devices for decades and will continue to target small IoT networks as we see them in our day. However, it will not respond to the growing needs of the large IoT environment for the next few days.

Indeed, in time, the engineering and unprecedented economic challenges will be overcome, but cloud servers will remain an obstruction. That specific point of failure could disrupt the entire network. Moreover, machine-to-machine (M2M) communications have been complexed because of the diversity of ownership between cloud infrastructure and devices. There is no assurance that exceptional manufacturers' cloud offerings are interoperable and compatible, and there is no single platform that can connect all devices.

Most of the questions mentioned above can be resolved through a wide range of IoT communication methods. Adopting a standard peer-to-peer communication model to process billions of transactions between devices will drastically reduce the cost of installing and maintaining significant records and deploying computer and storage needs for all the billions of devices that make up IoT networks. [7]. However, planning peer communication will introduce its own unique situations, the main of which is the security problem. And as we all see, IoT security is far greater than protecting sensitive data. The proposed solution will maintain privacy and security on major IoT networks and provide specific transaction confirmation and consolidation to prevent corruption and looting.

As IoT structures are an increasing number of being entrusted with sensing and managing rather complicated ecosystems, questions about the safety and reliability of the information transmitted to and from the IoT devices are speedy becoming the first-rate situation. Two of the biggest questions in this IoT-based world are whether it is secure and how we can reduce the cost. In August 2015, a Jeep SUVs overall management was taken overusing the vehicle's CAN bus, and it was taken over by a crew of researchers. This was done by exploitation through a firmware update vulnerability [8]. A specific model of security cameras was exploited by a hacker that found a particular vulnerability in that camera model back in October 2016. Almost 300,000 Internet of Things (IoT) video recorders started to assault a couple of social network websites. It was able to take down Amazon, Netflix, Twitter, Spotify, and excessive-profile structures for almost a couple of hours [9]. These two attacks are just two examples out of many of what can happen to IoT devices with poor security.

Due to similar vulnerabilities, security issues, and other issues that were mentioned above, billions of internet of things devices have raised concerns regarding the capability of security. These viable solutions could fill the security gaps and the bottleneck in cloud servers. Here the Blockchain enters IoT security, a transparent nascent technology that ensures reducing the risk of IoT devices being compromised by central authorities and increasing the robustness of IoT implementation. Blockchain, "released label, has emerged as one of the most popular in the technology business and elsewhere. Blockchain technology provides a way to record transactions on any visual basis. This is designed to be transparent, secure, surprisingly impenetrable against auditable, efficient, and outages; in particular, it includes the opportunity to disarrange and allow the latest business models [7]. In several respects, Blockchain can ensure the protection of IoT networks, forming a collection of consensuses on deviate community behaviors and quarantining any nodes acting irregularly.

C. Evolution of Blockchain

Since its first introduction in Bitcoin by Satoshi Nakamoto [10], Blockchain has been acknowledged as an obstreperous technology in various beyond health care, cryptocurrency, Internet of Things (IoT), energy, and logistics. When we compare Blockchain with conventional, centralized solutions, Blockchain has some significant advantages such as enhanced security, transparency, immutability, and fault tolerance. As blockchain technology keeps on evolving concerning the ways of how Blockchain is accessed, verified, and constructed, they have been classified into three main categories:

1. **Public Blockchain** – Anyone can participate in the public Blockchain, and it is worldwide accessible for everyone. It has a Trust Authority (TA) of 0, and the Speed of Consensus (SoC) is slow. Best for decentralized global scenarios [11].
2. **Consortium Blockchain** – A pre-selected node within the consortium controls this. It has a Trust Authority (TA) between 0 and 1. The Speed of Consensus (SoC) is slightly fast than Public Blockchain. Best for businesses among selected organizations [11].
3. **Private Blockchain** – Write an organization's control rights. It has a Trust Authority (TA) of 1, and the Speed of Consensus (SoC) is fast compared to Consortium Blockchain. Best for management and sharing information in an organization [11].

In the course of recent years, Blockchain has advanced past digital currency (Blockchain 1.0) into smart contracts (Blockchain 2.0) and numerous different associations that are enabled with high responsiveness and a significant degree of safety and trust (Blockchain 3.0). As the utilization of blockchain applications keeps on developing from Blockchain 1.0 to Blockchain 3.0, it turns out to be much harder for blockchain clients and engineers to acquire a superior comprehension of the security and protection spaces of blockchains [11].

As blockchains are as yet being conveyed and disseminated, exchanges and exchanges on blockchain frameworks are conceivable without focal worker confirmation. Subsequently, Blockchain can eventually lessen worker costs (counting the cost of proficiency and adequacy) and decrease the danger of execution on the worker you are focusing on. Changing subtleties on a blockchain network is a significant issue due to the manner in which squares are connected. All blockchain settings should be acclimated to alter the subtleties on any single court. Something else, all book squares would be supported by different establishments, and organizations would likewise be tried. Along these lines, any cuts in the association can be seen adequately [2].

Blockchain permits clients to expect an impressive degree of obscurity. Exchanges are recorded and checked, and their area is enlisted, yet the person's character is protected. Additionally, the client can make different characters to sidestep identification also. A particular level of obscurity is conceivable because of the circulated idea of blockchain networks, despite the fact that it is feasible to decide the personality of the client by noticing network traffic and the public blockchain framework.

Since all transactions made on blockchain networks are verified and recorded with a timestamp, customers can no doubt check and verify the integrity of past records by arriving at any location within a different framework. In the Bitcoin blockchain, each trade can be traced back to a previous transaction. It improves understanding of the information placed on the Blockchain and makes it less effective [2].

D. When Blockchain Meets with the IoT

Inside the numerous decagons, IoT has extraordinarily improved its openness and associated more gadgets and organizations to neighborhood working environments, transportation, and urban areas across the globe. Nonetheless, the ten-year-old Blockchain is set to change plans of action utilizing scrambled and conveyed records intended to make troublesome information and ongoing proof. As IoT and Blockchain cooperate, the last is relied upon to give a demonstrated and secure account mode for devices and cycles identified with the past. With Blockchain, everything gadgets can have strong cryptography, as well as protecting specific discussions with different gadgets and acquainting secrecy with IoT use situations where security is a significant concern. Adopters can follow contraptions and disseminate security refreshes, supporting the advancement of possible devices.

Tracking connected devices in the devices, authenticate users and network, maintaining data security, removing the single point of the misfire, building trust between IoT processes, and reducing cost by terminating intermediaries are just a few of the potential benefits that we have with Blockchain when it is in the IoT. The issue of oversight is expected to be addressed by merging Blockchain with the IoT. Since Blockchain eliminates intermediaries or go-betweens, it helps to reduce operational costs [12].

The Blockchain, when integrated with the IIoT space, expands the security features of the entire framework. Blockchain has incredible privacy and security features that are important to IIoT frameworks. It is distributed, repaired, durable, and secure and therefore helps IIoT frameworks to overcome their fundamental evils. Since blockchains include linked and distributed information squares, they are faster and more critical in the attack. Information can be placed in the center of focus; it is being distributed throughout the organization. In addition, blockchains also use robust encryption calculations and hashing techniques and are therefore more secure. Blockchain trading is obviously straightforward, and customer value can be tested manually. This prevents clients and malicious devices from entering and corrupting the blockchain network [2].

In IoT conditions, a massive piece of the writing is machine-to-machine (M2M) investment, with no human intercession. In such situations, setting up trust among the sharing machines is a critical test that IIoT really has not met widely. Blockchain improves certainty among contraptions by ensuring the believability of the gadgets, additionally offering expansive advanced confirmation. Such associations can, in like manner, proactively perceive [13].

Appropriated booking of data offering to a dispersed framework makes exchanges quicker. It makes it harder for the organization to close down as the disappointment of any single hub will irrelevantly affect the whole framework. Hash-based security, character testing, and provenance check are fundamental in recognizing incredible gadgets and limiting dangers.

By empowering enlistment and approval of devices to enlist against the framework, the blockchain-composed IIoT game plan can improve the general structure prosperity. Keen agreements likewise support customized execution of business reasoning. Without a central structure to attack, the threats of framework disappointment because of alleged assaults on the focal hub can be kept away from inside and out [14].

III. FUTURE DEVELOPMENT IN THE AREA

A. FUTURE DEVELOPMENT IN BLOCKCHAIN

Blockchain is often regarded as a world-changing technology and, in many ways, of course. However, it is not really the solution to the world's problems that most evangelizers do not believe in. Let us break down some of the issues with Blockchain that everyone should understand.

1. Blockchain has a natural cost

Blockchain relies on betting to provide its security, for example, ending a concurrence with a scattered association. This implies that to "illustrate" that the customer has consent to speak with the arrangement, complex estimations should be performed, which require a great deal of enrollment power. Clearly, this incorporates some huge issues [15].

2. Its complexity means that end users find it difficult to appreciate the benefits

Unless its potential for development is evident whenever one tries to understand encryption rates and is allocated a delay behind the Blockchain, a time limit should pass, and a good piece of reading, before "man in town" can see what makes blockchains perhaps be so helpful. Technology experts talk about replacing offices that middle-class men traditionally give to the financial management industry - such as cleaning installments and expecting to loot. In any case, taking everything into account, banks offer this assistance well enough, at an obviously minimal effort to the end client [15].

3. Blockchains can be moderate and lumbering

Essentially due to their intricacy and their coded, appropriated nature, blockchain trades can require a considerable time interval to gauge, decidedly stood out from "customary" portion structures, for instance, cash or charge cards. Bitcoin trades can require a couple of hours to finish up, which infers there are trademark issues in the likelihood that you will really need to use them to pay for some coffee in your mid-day break aside from if the shipper will take on a segment of danger [15].

These are a few of the issues that Blockchain specialists are working on, so it is safe to say that these issues and many more issues that are similar to these will be sorted out in the near future. With the upsurge of the old technology and with the help of new technology, these issues will be sorted out.

B. FUTURE DEVELOPMENT IN THE IOT

The end result of IoT may be infinite. Advances to the modern web will be accelerated using an expanded organizational environment, including Artificial Intelligence (AI), as well as the ability to deploy, generate robots, coordinate, and protect multiple use cases on a large scale. The potential is to empower billions of gadgets all the time using the vast majority of logical information that can use a variety of business methods. As IoT organizations and segments continue to overcome this challenge, through the increased scope and AI, professional co-ops will enter the IT and web-based markets - opening up new revenue surges. [16].

Because of the boundless possibilities in the IoT system and the rapid growth of technology, we predict that in the upcoming future; More urban communities will become "**smart**." Cybercriminals will keep on utilizing IoT devices to work with DDoS assaults. Artificial Intelligence will keep on turning into something more significant. Routers will keep on getting safer and more intelligent. 5G

Networks will keep on energizing IoT development. Vehicles will get much more astute. 5G's appearance will likewise make the way for new protection and security concerns. IoT-based DDoS assaults will take with respect to more hazardous structures. Security and privacy concerns will drive enactment and administrative movement [17].

In the near future, IoT producers will zero in on building explicit industry arrangements and area parts instead of standard prerequisites. There is a developing requirement for specific use cases that help tackle detailed area explicit difficulties. For instance, distant IoT patient observing arrangements are pointed toward decreasing expenses and improving the nature of patient consideration. The worldwide patient consideration market is required to reach $ 1.8 billion by 2026, as indicated by Grand View Research [18].

Nonetheless, unique IoT alone, it offers a ton of chances when joined with different advancements like manufactured brainpower, important information, blockchain, AI, AR/VR, and distributed computing. Later on, there will be irrefutably more hybrid courses of action.

For example, the usage of Blockchain in IoT will help decentralize organizations and assure higher security data transmission between interconnected gadgets. Blockchain is presently the basic IoT pattern, and more worth tries to ascend out of the blending of these two progressions [18].

Future IoT advancement examples will help workplaces with getting the primary viability and proficiency out of their stuff and collecting parts. This will change over into massive financial motivators for adventures that get IoT. The headway of IoT will get further improvements mass personalization, virtual prototyping, network assurance, vehicle-to-everything (V2X) accessibility, and clinical consideration [19].

The new era of the Internet of Things is coming, and the new decade makes sure to get critical changes in the mechanical area and public administrations. Beginning with the way we gather and store information and finishing with the manner in which we drive our vehicles, IoT will reshape our lives on various levels. Organizations should adjust to these progressions and receive new innovations to remain applicable. That is actually why today is the best and ideal opportunity to plan for the difficulties of the following decade and the progressions it will, without a doubt, bring [19].

C. Future Developments When the IoT Meets Blockchain

As the web as it is currently just an organization of workers, there are various blockchains in presence. This is one of the boundaries to make a totally self-sufficient framework for the IoT. For example, at the present time, the entirety of the devices that speak with one another must be on an identical blockchain.

There is an answer for this issue a work in progress to permit any device to associate with any blockchain. It is a **Bitcoin wallet (BTC wallet)** called a Ledger Nano that would be installed in the machines to speak with different blockchains [20].

What is this Bitcoin wallet or BTC wallet? A Bitcoin wallet is an item program in which Bitcoins are taken care of. Truth be told, Bitcoins are not taken care of wherever. For every individual who has a balance in a Bitcoin wallet, there is a private key (secret number) identifying with the Bitcoin address of that wallet. Bitcoin wallets work with sending and getting Bitcoins and giving duty regarding Bitcoin harmony to the customer. The Bitcoin wallet comes in various designs. The four chief sorts are work territory, compact, web, and hardware. [21].

At this moment, versatility is the most significant impediment to the full incorporation of IoT into the Blockchain. This piece of innovation will empower it to scale unbounded. Not least of which, in light of the fact that the Blockchain that might be best for the present IoT could be diverse later on can, in any case, be carried out.
Now, blockchains are youthful and can make themselves obsolete rapidly. This can assist with developing alongside the Blockchain when it very well may be carried out for a great scope. One of the advantages of utilizing the Blockchain in numerous applications and not simply with the IoT is that there is a record of each exchange in route. These records cannot be changed by anyone whenever they are enrolled on the register. This makes it essentially hack-verification [20].

Moreover, the IoT on the Blockchain will consider a considerably more smoothed out measure from the producer to the beneficiary and everything in route. One way that the old framework was indeed downright terrible was managing documentation in convenient manners. Since everyone approaches each record and a secure and straightforward approach to sign them, this is a lot quicker.

At the point when the IoT winds up smoothed out on the Blockchain, it will likewise bring along different businesses like production network coordination and protection since every one of the three of these enterprises is dependent on one another.

These businesses are, as of now, utilizing the Blockchain and can, without further ado, access the others when blockchains can speak with one another [20].

Despite the fact that there are numerous benefits of receiving Blockchain for IoT security, the innovation is a long way from excellent. Being an innovation empowering influence for Bitcoin, Blockchain manages its work competently in the cryptographic money domain: ensuring touchy monetary information while moving cash starting with one individual then onto the next. Be that as it may, IoT suggests power over an organization of devices, where complex security must be set up [22].

One of the significant barriers while in transit to selection is perplexingly connected to one of the proposed benefits of Blockchain: each activity on the organization must be endorsed by other organization members for it to go live. For instance, if there should arise an occurrence of an absolute security penetration through one of the associated gadgets, denying admittance to that gadget would essentially diminish the adverse consequence of spreading the malware. On a grander scale, with a considerable number of 'things' associated with a vast organization, it tends to be hard to get permission from most of the substances [22].

There is no simple method to address this test. However, a custom blockchain stage can be an answer. Blockchain engineers need to guarantee that undermined gadgets could be in a flash disposed of from the organization without the requirement for an ordinary blockchain agreement.

Associations ought to thoroughly research their protection prerequisites and pick an appropriate blockchain type or solicitation for the improvement of a custom one until instant arrangements show up on the mass market [22].

IV. CONCLUSION

In conclusion, technology will develop unimaginably in the near future. Comparing to the 1980s, 1990s, and 2000s, the technology we have today is improved in ways we did not expect. Technological evolvement is only limited to human imagination. With the advanced technology we have today, and with the advanced technology that we will soon have, the evolvement of the IoT technology is limitless. The IoT has evolved to a certain level that we believe that we can get everything done. No! If we just talked about the IoT, there is still a lot we could develop and improve. We still only have scratched the surface of connecting the IoT with Artificial Intelligence (AI). Just imagine the possibilities there could be if we could combine the IoT with Artificial Intelligence. When technology evolves, there should be proper security measures to keep this technology safe. Without it being used in an unnecessary manner and without letting attackers, hackers get access to this technology. Blockchain is already taken the central part when it comes to digital security. With the rise of the IoT, security should be improved, and Blockchain will improve in ways that hackers could not imagine. The future is uncertain, but the development of the IoT and Blockchain is a matter of time.

We are living in a world that everything is becoming accessible from the internet, and most of the things are done by machines and robots. There is a considerable risk for this advancement as well, and technology advancement is done by programming. Programs could be hacked; programmers could mistakenly or literally give malicious code for the system to act in a certain way that it should not operate. The IoT with AI could malfunction and do things that those systems were not programmed to do. With the advancement of blockchain digital security, hackers would do learn with time how to manipulate those digital security systems. We all talk about the positive side of the advancement, but the negative side is much greater. Most of the people in our world believe that the movie “Terminator” is just a horror and action movie, but it is a science fiction movie as well. If we do not take responsibility for our own actions regarding the IoT, Blockchain, and AI, we could just by mistake or literally enter malicious code into machines, systems, or robots.

V. REFERENCES

1] A. S. Gillis, "IoT Agenda," February 2020. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. [Accessed 30 April 2021].

2] Z. Mahmood, Ed., The Internet of Things in the Industrial Sector Security and Device Connectivity, Smart Environments, and Industry 4.0, 1 ed., Springer, Cham, 2019, p. 326.

3] IBM," IBM, [Online]. Available: https://www.ibm.com/topics/what-is-blockchain. [Accessed 30 April 2021].

4] R. J. W. G. B. W. &. J. D. Hany F. Atlam, "SpringerLink," Mobile Networks and Applications, 28 January 2019. [Online]. Available: https://link.springer.com/article/10.1007/s11036-019-01214-w. [Accessed 25 April 2021].

5] SIMON IoT," SIMON IoT, 20 November 2020. [Online]. Available: https://www.simoniot.com/history-of-iot/. [Accessed 25 April 2021].

6] J. Chase, "Texas Instruments," September 2013. [Online]. Available: https://www.ti.com/lit/ml/swrb028/swrb028.pdf?ts=1619211479778&ref_url=https%253A%252F%252Fwww.google.com%252F. [Accessed 03 May 2021].

7] B. Ahmed, "Open Mind BBVA," 24 October 2016. [Online]. Available: https://www.bbvaopenmind.com/en/technology/digital-world/securing-the-internet-of-things-iot-with-blockchain/. [Accessed 27 April 2021].

8] H. Fairhead, "I Programmer," 16 August 2015. [Online]. Available: https://www.i-programmer.info/news/149-security/8892-how-the-jeep-was-hacked.html. [Accessed 25 April 2021].

9] N. Wolf, "The Guardian," The Guardian, 26 October 2016. [Online]. Available: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet. [Accessed 25 April 2021].

10] Z. B. a. G. Kay, "INSIDER," INSIDER, 26 February 2021. [Online]. Available: https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12. [Accessed 26 April 2021].

11] R. X. a. L. L. Rui Zhang, "ACM Digital Library," July 2019. [Online]. Available: https://dl.acm.org/doi/fullHtml/10.1145/3316481. [Accessed 26 April 2021].

12] Trend Micro," Trend Micro Incorporated, 17 May 2018. [Online]. Available: https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/blockchain-the-missing-link-between-security-and-the-iot#:~:text=With%20blockchain%2C%20each%20device%20will,privacy%20is%20of%20utmost%20concern.. [Accessed 27 April 2021].

13] V. P. a. P. Brody, "Device democracy: Saving the future of the Internet of Things," IBM, 2014.

14] J. EF, "A survey of how to use blockchain to secure Internet of Things and the stalker," vol. 2018, p. 28, 08 April 2018.

15] B. Marr, "The 5 Big Problems With Blockchain Everyone Should Be Aware Of," [Online]. Available: https://www.bernardmarr.com/default.asp?contentID=1354. [Accessed 07 May 2021].

16] Ericsson," [Online]. Available: https://www.ericsson.com/en/future-technologies/future-iot#:~:text=The%20future%20of%20IoT%20has,diverse%20use%20cases%20at%20hyperscale.. [Accessed 06 May 2021].

17] S. Symanovich, "The future of IoT: 10 predictions about the Internet of Things," 28 August 2019. [Online]. Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html. [Accessed 06 May 2021].

18] S. Khvoynitskaya, "The history and future of the internet of things," 25 November 2019. [Online]. Available: https://www.itransition.com/blog/iot-history. [Accessed 07 May 2021].

19] O. Martynova, "The Future of IoT: Innovations to Expect in the New Decade," Intellias - Intelligent Software Engineering, 06 November 2020. [Online]. Available: https://www.intellias.com/the-future-of-iot/. [Accessed 07 May 2021].

20] Manufacturing Business Technology," 24 March 2021. [Online]. Available: https://www.mbtmag.com/best-practices/article/21342740/the-future-of-the-internet-of-things-with-blockchain. [Accessed 06 April 2021].

21] J. Frankenfield, "Bitcoin Wallet," 30 June 2020. [Online]. Available: https://www.investopedia.com/terms/b/bitcoin-wallet.asp. [Accessed 06 April 2021].

22] S. Khvoynitskaya, "Blockchain for IoT security – a perfect match," itransition, 16 April 2020. [Online]. Available: https://www.itransition.com/blog/blockchain-iot-security. [Accessed 07 May 2021].

23] CISCO," CISCO, [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-it-security.html. [Accessed 02 May 2021].