Block Chain Security

Advance Cyber Security Research

By

Waleed Moqhem Almoqhem

University: Saudi Electronic University

College: Information Technology

Degree: Master of Cyber security

Date received: 7/7/2024

Date of acceptance: 5/8/2024

Abstract:

Pertaining to security, it is worth noting that although blockchain was primarily created to support cryptocurrencies, it now presents potential in increasing the security level in numerous industries. Due to its decentralized, transparence and, especially, non-tamable character, it provides a substantial value proposition in IoT, smart contracts, and IdV. This research therefore looks at how these domains can adopt the blockchain technology given certain security issues and with an objective of enhancing the systems' robustness.

The research investigates the use of blockchain technology in IoT device security, aiming to reduce single points of failure and enhance network robustness. It compares centralized security models and proposes lightweight consensus algorithms for energy-efficient blockchain protocols. The study also addresses energy consumption issues in data storage and transfer.

In conclusion, this study will seek to convince the world why blockchain technology has the potential of revolutionizing security in IoT, smart contracts and identity verification. Big strides are thus possible when one defines the challenges and the possible innovations necessary in enhancing cybersecurity.

Keywords: Block Chain Security, Cyber Security, Networking of Security

ملخص:

على الرغم من أن تقنية البلوك تشين تم إنشاؤها في المقام الأول لدعم العملات المشفرة، إلا أنها تقدم الآن إمكانات في زيادة مستوى الأمان في العديد من الصناعات. نظرًا لطبيعتها اللامركزية والشفافية، وخاصة عدم قابليتها للترويض، فإنها توفر قيمة كبيرة في إنترنت الأشياء والعقود الذكية وقيمة الهوية. لذلك، يبحث هذا البحث في كيفية اعتماد هذه المجالات لتقنية البلوك تشين نظرًا لقضايا أمنية معينة وبهدف تعزيز قوة الأنظمة.

يبحث البحث في استخدام تقنية البلوك تشين في أمان أجهزة إنترنت الأشياء، بهدف تقليل نقاط الفشل الفردية وتعزيز قوة الشبكة. ويقارن بين نماذج الأمان المركزية ويقترح خوارزميات إجماع خفيفة الوزن لبروتوكولات البلوك تشين الموفرة للطاقة. كما تتناول الدراسة قضايا استهلاك الطاقة في تخزين البيانات ونقلها.

وفي الختام، ستسعى هذه الدراسة إلى إقناع العالم لماذا تتمتع تقنية البلوك تشين بإمكانية إحداث ثورة في الأمن في إنترنت الأشياء والعقود الذكية والتحقق من الهوية. وبالتالي، تصبح الخطوات الكبيرة ممكنة عندما يحدد المرء التحديات والابتكارات المحتملة اللازمة لتعزيز الأمن السيبراني.

الكلمات المفتاحية: أمن سلسلة الكتل، الأمن السيبراني، شبكات الأمن.

Objective:

The foremost research aim in this regard is to propose and integrate blockchain frameworks to decentralize IoT networks' security system. This decentralization is meant to solve several essential issues of the traditional centralized IoT security models. The specific goals include:

Preventing Single Points of Failure:

In most of the conventional IoT structures, there is always that one critical point of attack that can breach the entire IoT network's security due to the imposed centralization norms. According to the results of the analysis, blockchain can share trust and control throughout the security structure and reduce or erase the chances of vulnerability from a solitary node.

Enhancing Resilience:

Hence, when the principle of decentralization is employed to the application in IoT networks by the application of blockchain technology it automatically enhances the networks resilience. Because of decentralization of the network, if one or some nodes are attacked by intruders or fail during their functioning, the rest of the nodes of the network can work safely. This makes the IoT devices to continue working and more secure even when the situations are a bit hard.

Reducing Vulnerabilities to Cyber-Attacks:

Centralized IoT security models are more vulnerable to the different categories of cyber threats such as the DDoS attacks on Linked IoT Data as well as data breaches of Linked IoT Data and unauthorized access. As a result, based on the decentralized and unchangeable structure of a blockchain, the research has the objective of minimizing these threats. They help in the major features of the blockchain whereby data integrity is preserved and incases of the attacker's flexibility is evident and security measures can be taken immediately.

Ensuring Data Integrity and Authentication:

This approach also guarantees the data 's integrity and authentication since certain details cannot be changed. Therefore, it can be stated that the application of the blockchain technology can contribute to the improvement of the reliability of the given information, as well as identification of the devices that are a part of IoT networks. It also incorporates the goal and process of developing mechanisms that use blockchain identification and validation of IoT, for the protection of devices that can access or transfer data. This approach shall help in avoiding any form of data damage such as corruption and forgery of the messages transmitted. This stress becomes a major problem especially when there is need to secure many IoT devices at once, this presents a problem in the centralization and scalability of IoT security models. This is because with the blockchain being distributed it has the ability to accommodate an increasing number of devices that interact and share data while not imploding the number of devices that come with security vulnerabilities or slowdowns in computations. Many IoT devices have limited processing power and also the energy limitation compared to traditional computers. The study aims at proposing security solutions for green block chain networks ideal for the IoT system of constrained resources. This can be done by creating light weight consensus algorithms and protocols which do not demand the use of high energy.

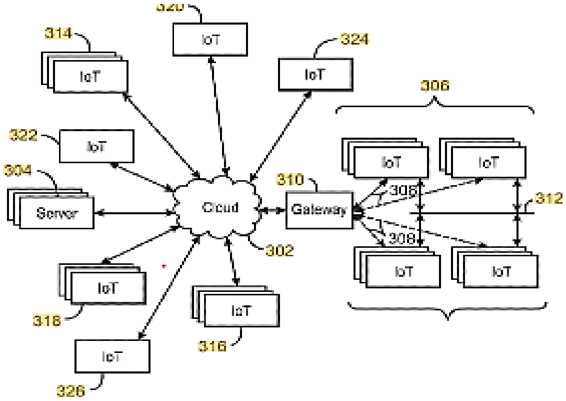
Background:

IoT is an umbrella term that addresses the connection of physical and virtual assets of everyday use to a computer network that allows objects to have sensors to acquire preset information from a system, and in return feed it back with data, commands, or other information on a preprogrammed schedule. As a result, when it comes to managing the IoT devices, the security risks are also rapidly increasing in proportion to the quantity of such devices. Conventional models of central security are slowly giving way to efficiency because of their dependence on a single point and problems with growth. The mentioned problems may be solved by utilizing the decentralized network based on blockchain technology.

Trusted communication environment in IOT networks:

(Google.com, 2017) A reliably communicative infrastructure consists of a primary entity that creates a group and a distributed journal and a secondary entity with communicative permissions. In the context of the Internet of Things (IoT), there is a trusted computation environment consisting of a block chain's chain history and a root-of-trust for chaining and root-of-trust for archives. This IoT network is composed of an IoT device having a communication system, an onboarding tool, a device discoverer, a trust builder, a shared domain creator, and a shared resource directory. Further, the IoT device at the network layer is equipped with communication system, PCE, policy database, PDE, PEP.

Figure 1



And peer monitor. Moreover, the IoT network also consists of an IoT device with the host environment and the trusted reliability engine which is targeted to perform the failover action in case of the host environment malfunction. Last but not the least; the IoT network comprises an IoT server having a secure r/measurer, trust anchor, authenticator, and key manager as well as key generator; this will be the heading of this part.

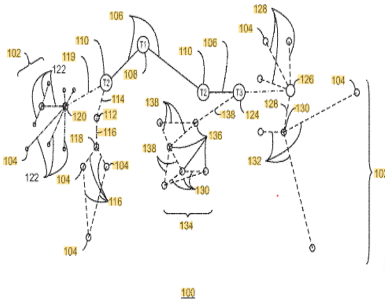


Figure 2

Literature review:

(ACM Other conferences, 2017) Security aspects in IoT and why there is need for iot security management This will take a new dimension as there are many ways of connecting technologies and the Internet of Things (IoT) will shift the focus on internet study. The following risks are realized with this increase in the coupling or conjunction of devices or things constituting an IoT. This is why, therefore, different scholars are of the opinion that IoT security issues are still rife and call for more persistent cyber-security threats with complexity increasing as they progress and require attention. The current literature on IoT security highlights several key issues: Some of the critical barriers with regards to RFID implementation include the following; there is an industry clarification issue, there is no standard to follow, interoperability, among others, the many security concerns. These are; identity and authentication, access control security protocols and networks, privacy and, trust and governance. If there were no governance in the IoT, it can lead to architectural, protocol, identity, responsibilities split in a disorderly manner. As the use of IoT devices advances the worry about in constantly rise hence the call for a security system that is strongly secure, large enough to support all classes of devices and at the same time flexible to support different technologies and platforms.

Specific Industry Focus: Mining and Resources Industry of Western Australia

Sectors like Mining & Resource sector of Western Australia are already using technology and IoT incorporated. Yet they are also looking to acquire security solutions to level up in the market. The need for efficient security solutions of the sector highlights the necessity of envisaging proper IoT security paradigms.

Research Approach and Objectives

The research being done constitutes qualitative paradigms, documents, and live/real analytical cases concerning IoT cyber-security decisions in specific organizations. The end-user, therefore, has the intended addressees of the guidance geared toward being the actual developing of best-practice cross-party general guidance. This research is currently in its early stages; however, the goal of the research project is to specify and confirm the variables that will allow for the creation of a new design guide for the implementation of Information Technology (IT), Operational Technology (OT), and IoT ecosystems. This guide will also tackle the issues relevant to IoT security and would provide essential strategy for the large WA mining and resources firms and the energy and resources industries in general.

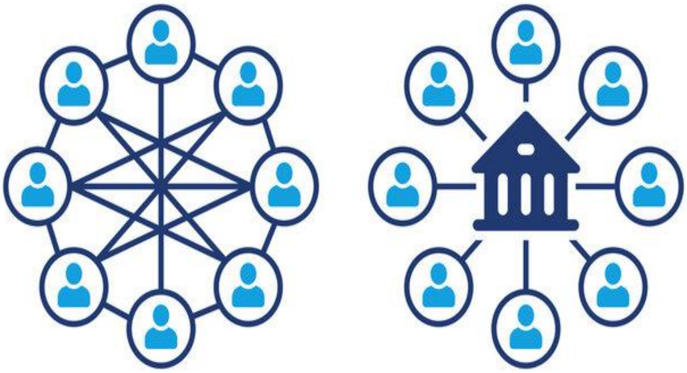
Solving these concerns calls for promoting blockchain solutions for IoT security decentralization to get rid of the SPOFs, increase system robustness, and decrease its susceptibility to cyber threats. Therefore, it can be stated that the proposed solutions based on blockchain technology can enhance the security of IoT networks due to the properties of decentralization, transparency, and non-tamper ability.

Centralized and decentralized security models represent two fundamentally different approaches to managing and securing data and systems:

Centralized Security Model:

(Nazanin Zahed Benisi, Aminian and Javadi, 2020) Control and Management: In the case centralized organisations security control and management is centralized at a single center or at most a few controlling organisations. Security central authority is a decision maker, a policy maker and an administrator of security of the whole system network.

Figure 3



Advantages:

- Simplicity: Hiring and firing is one area that becomes easy to implement when they are made central and issues to do with security, policies among others.
- Consistency: Section thirteen the author presents the understanding that polices and procedures can be standardized for the total of the network or system.
- Monitoring: Single point control and reporting could provide the right view on events and incidents that the security processes go through.

Disadvantages:

- Single Point of Failure: There is always the danger that should the centralized authority feel threatened then the whole system can indeed be at even a higher risk.
- Scalability: Centralized systems can pose problems once

more when the network or organisations is expanding because it is rather easy to do so.

- Dependency: There is high concentration of clients and participants of the system and all their functioning is dependent on the existence and stability of the central authority and there are few difficulties in such a system.

Decentralized Security Model:

Distribution of Control: Fictionalization of security control or management in Decentralized structures is not available and it is present at each of the nodes in the system. Each holds an amount of responsibility and authority for the safeguarding of the entity**. (Xi, 2020)**

Figure 4

Advantages:

- Resilience: Delegation eliminates the probability of having just one point of failure and malicious attacks because there is nothing to attack because there is control.
- Scalability: This architecture can be easier to scale as the nodes can be added into the network and they won’t much affect the general security architecture.
- Privacy: Distributed systems can hopefully improve the idea of privacy as lesser quantity of data can be present at any organization at one time.

Disadvantages:

- Complexity: Security of multiple nodes and entities can be major an issue than that of few nodes and entities and for this reason require suitable coordination and consensus solutions.
- Consistency: The measures and policies that facilitate securing of nodes could be implemented with a lot of difficulty to arrive in all nodes.
- Trust: Normal Decentralized environment requires that the node should in some way be trusted and the trust sustained and such a feature is quite sensitive if poorly done.
- Blockchain in its essence is about a ledger which is not centralized and is dealing with the transactions on the network of the computers. Here's a review of its fundamentals and how it applies to IoT security:

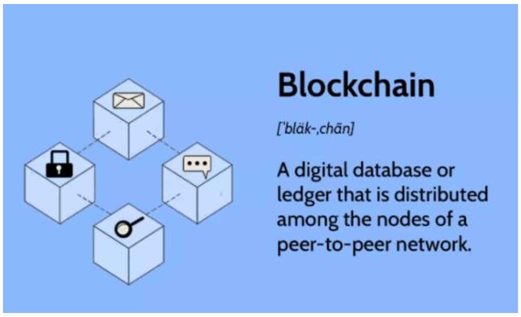
Fundamentals of Blockchain Technology:

Decentralization: Blockchain is distributed with nodes which are the computers that undertake the task of the validation of the transactions as well as storage. Each node contains the copy of the large database, which includes the chain of blocks; therefore, nobody controls anything.

Immutability: Changing or deleting records that one has input in the database that is situated in a blockchain environment is also very much challenging. This is done through the cryptography hash functions and consensus that aid in the validation of the data.

Security: First of all, they use the techniques of cryptography that contribute to the elimination of fraud and confirmation of the distinctiveness of actions. The financial transactions done within a specific network are regulated by the consensus of all the participants, so it is almost impossible to perpetrate fraud and change it.

Transparency: The record book is normally available to the public and transparent in regards to the transaction history based on the type of the transaction while, at the same time the record book allows anonymity of the users based on cryptographic means.



Blockchain

['bläk-,chān]

A digital database or ledger that is distributed among the nodes of a peer-to-peer network.

Smart Contracts: Consequently, smart contracts are computerized efficient means within block chain which is programmable contract which can perform a set of protocol on occurrence of specific conditions. This particular function assists in avoiding the use of middlemen and simplifying them.

Application of Blockchain in IoT Security:

Data Integrity: (Minhaj Ahmad Khan and Salah, 2018) Thus, it can be stated that in the context of IoT networks, blockchain may contribute to achieving the data credibility of various devices. Each and every single piece of data can be time-stamped, hashed, and saved to the blockchain to exclude the risk of alteration.

Authentication and Identity Management: In this case, Blockchain is used as an application of decentralized device identification apart from safely storing the identity information of the devices. On top and beyond that, it can itself be registered with identifiers inscribed on the blockchain such as minimizing spoofing or intrusion.

Secure Communication: Blockchain can assist the IoT devices to have a secure connection through encrypted transaction and have decentralized architectures. It can minimize risks that are likely to be associated with central and unified communication channels since they are easy to hack.

Supply Chain Transparency: Therefore, in the supply chain IoT applications, it validates goods tracking from the manufacturers, through transporters, distributors and reaches to the end use. Each operation starting from supply channel can be recorded on the blockchain so that emanating instances of fraud in the market can be prevented.

Decentralized Control and Consensus: Self-sufficiency of the IoT networks is evident since most IoT networks possess the ability of allowing many devices in the network to operate autonomously. In the case of Blockchain, there is an opportunity for attaining consensus for the agreement between the devices for the data transactions and actions without any imperative order of central regulation.

Auditing and Compliance: Particularly, the openness and untampered trait of the blockchain can enhance auditing with regard to the regulatory standards in the IoT implementations. Thus, auditors can check the accuracy of data and transactions in relation to the sending and receiving individuals without direct reference to centralizing bodies.

Importance of Blockchain in Achieving Product Traceability:

- Immutable Record Keeping: Reality is that block chain offers a signed transaction<|reserved_special_token_259|> and immutability of each record beginning from production up to distribution and quality assurance.
- Transparency and Accountability: It gives all the participants in the supply chain a clear view of the history of the product eliminating fraud in the chain.

- Efficiency: The usage of blockchain in the supply chain drastically minimises the time spent on data capture and its verification owing to the automated manner of tracing the products.
- Compliance: Helps in ensuring compliance with regulatory provisions by offering evidential documentation of the product’s source, processing and credibility.

Facilitation of Product Inspection, Accounting Audits, and Information Exchange:

- Product Inspection: Paves way for tracking products thus helping stakeholders to physically or digitally confirm the conditions of products and quality requirements at a given time.
- Accounting Audits: They minimize the possibility of auditor having to rely on the management for audit trail since the system has a clear trail that the auditors can follow.
- Information Exchange Speed: Other ways that it enhances supply chain efficiency is by enhancing the flow of information throughout the supply chain thus increasing the speed at which participants are able to respond to disruptions.

Using RSA and ECC in Blockchain Security for IoT:

Encryption and Data Confidentiality:

RSA Encryption:

(Sonali Chandel et al., 2019) Data Encryption: Data encryption can be done with the help of RSA before it is transferred to the blockchain. This means that even when utilizing the structure of the blockchain, the information that is released to the public cannot be understood and can only be deciphered if the correct private key is used by those who have the right to access the data.

Private Key Storage: In IoT network, private key used in the RSA encryption can be kept in Hardware Security Module or secure element such that unauthorized access cannot be obtained.

ECC Encryption:

Efficient Data Encryption: ECC can be used for encrypting data following the fact that it is more efficient in the scenarios that involve the usage of smaller key sizes and is more preferable for the IoT devices that have limited computational capabilities. This ensures the data privacy, with no much computation complexity on IoT devices.

Authentication and Digital Signatures:

RSA Digital Signatures:

Transaction Verification: RSA digital signatures helps to sign blockchain transactions and at the same time, it is used to verify that a given transaction has not been altered in any way. This is important so as to ensure the correctness of the blockchain.

Device Authentication: As mentioned above, RSA can also be used to authorize the IoT devices that want to join the network and become the part of the block chain.

ECC Digital Signatures:

Efficient Signing: Digital signatures in ECC offer fairly like RSA but with less numbers of bits and speed of computation. This is very beneficial especially for IoT devices which have constrained resources.

Scalability: Specifically, ECC insures scalable authentication techniques that will be useful in IoT relying on vast numbers of devices.

Data Integrity and Immutability:

Blockchain Integration:

Tamper-Proof Records: RSA and ECC can be used for implementing digital signatures on the data entries in blockchain so that once data written, it cannot be tampered or deleted. This aspect is a characteristic of block chain, which, therefore, offers a secure track record of the collected IOT data.

Secure Communication Channels:

Hybrid Cryptography:

Combining RSA and ECC: This is possible mainly in the use of a combination of both RSA and ECC to enhance the appearance of communication channels between the IoT devices and the blockchain. For example, RSA may be used for key exchange while ECC is used for the actual encrypted communication and both the methods' strengths are incorporated.

Key Management:

Secure Key Distribution:

RSA Key Exchange: RSA can be implemented to securely transfer the keys anymore between the IoT devices and blockchain nodes; the data encryption keys that will be used for the process of encryption of the data will be transferred safely.

ECC Key Exchange: Using ECC, key exchange that may be suitable for devices having low processing capability is possible, thus making key management of the IoT network secure.

Resistance Against Attacks:

Brute-Force and Cryptographic Attacks:

RSA Security: Larger RSA key sizes also make it extremely improbable for the attackers to decipher the blockchain network hence securing it from brute force attacks.

ECC Security: The security is stronger than all its main competing algorithms with shorter keys as ECC is resistant to distinctive cryptographic attacks such as brute force and side-channel attacks.

Blockchain Malware and Their Background

- **Peer-to-Peer Network Attacks**

(Malik et al., 2019) Applicability of the blockchain increases the reliability and confidentiality of actions through decentralization of values and assets with the help of a consensus P2P system. However, several major attacks can target the network:

- **Distributed Denial-of-Service (DDoS) Attack:**

Floods the network with illegitimate requests such that they impair normal functioning of the network and deny genuine transactions a chance to go through.

Impact on IoT: Aims at IoT devices or blockchain nodes and has the capability to stop services in both cases as well as lose data or experience significant delays.

- **Sybil Attack:**

An entity creates multiple fake identity (nodes), so that it is diverting the actual consensus mechanism of the network.

Impact on IoT: Submerges the network with a multitude of dissimilar IoT devices by attempting to corrupt the network and the data that should be recorded on the blockchain.

- **Eclipse Attack:**

Covers up a node with rouge nodes which alters the information the node receives and cuts it off from other nodes in the network.

Impact on IoT: Infects individual IoT devices to prevent them from reporting correct data to the blockchain and to stop receiving updates.

- **Routing Attack:**

Contains processes that corrupt the routing information of the network, routing all the data to the malicious nodes and sometimes denying confirmation of the transactions.

Impact on IoT: Intercepts the information from IoT devices altering them thus feeding wrong information to the user and making the devices open to hackers' attacks.

- **Liveness Attack:**

Slows down the time taken to confirm a transaction by having three processes; preparation, denial of the transaction and delay by the use of block chain. This attack benefits from creating a secret chain, letting only the fake ones go through, and decreasing the chain's growth frequency.

Impact on IoT: Schedules important IoT data transactions and hence cause problems such as data synchronization and operational problems.

- **Smart Contract-Based Attacks**

Smart contracts are self-executing digital agreements for the performance of transaction and operations in blockchain environment consisting of IoT system. However, they can be vulnerable to several attacks:

- **DAO Attack:**

Attacks smart contracts and especially find ways around reentrancy to steal money. In Jun 2016, unknown hackers stole $60M of Ether cryptocurrency from the digital decentralized autonomous organization known as The DAO.

Impact on IoT: Targeted smart contracts are likely to be jeopardized to steal resources or interrupt services and hence, all the IoT-network.

- **Wallet-Based Attacks**

Wallets are necessary tools for storing all private keys which are required for a transaction. Attacks on wallets can have severe consequences:

Private Key Security Attack:

Focuses on the private keys with an intention of stealing money or relevant information. With Key-Coded items, when a private key is lost or stolen tracking and retrieving the stolen items is a herculean task.

Impact on IoT: In the case of IoT, failure in private-key security means hostile parties get control of the devices, an area that poses major security threats.

- **Transaction Privacy Leakage:**

Pass secrets like cryptographic keys or a transaction that one had to perform on behalf of his/her organization. Historically the operations of bitcoin wallets commonly performed have been known to be vulnerable.

Impact on IoT: With regards to the privacy, it becomes clear that leaking information of IoT devices will imply privacy violations, unauthorized access, and changes of data in these devices.

- **Other Blockchain Attacks**

Double Spending Attacks:

Happens when the same particular digital token is completed multiple times and this is based on the blockchain consensus algorithm.

Impact on IoT: IoT data transactions rely on the accuracy, and in some cases, on the confidentiality of the transaction; double spending affects the efficiency of both.

- **51% Vulnerability Attack:**

A rival with over 50% of the network's computational ability can tamper with the block chain, reverse transactions and prevent new ones.

Impact on IoT: A 51% attack results in compromising the rightful integrity of IoT data where an attacker is in a position to manipulate or delete crucial data as they wish.

- **Selfish Mining Attack:**

Thus, selfish miners do not reveal discovered blocks to form their own chain, gaining an advantage and over the top computation of honest miners.

Impact on IoT: Selfish mining makes IoT data processing slower and the security and efficiency of the network is compromised.

- **BGP Hijacking Attack:**

intvallls Border Gateway Protocol messages to intercept and redirect traffic of the blockchain network to slow the propagation of the blocks. Impact on IoT:

Can block IoT device signals, jeopardising data integrity and causing logistical complications. Balance Attack: Description: Validity of subgroups of miners ensures there is time when an attacker executes transaction in one subset and mines blocks in another to gain chain superiority. Impact on IoT: Causes integration problems and transaction slower availability in IoT based networks, the gains overall network dependability.

Blockchain Security Issues

(Singh, A. S. M. Sanwar Hosen and Yoon, 2021) Transaction Malleability: It is necessary to understand that during the contracted transactions, not all the information included in the hashed transaction is covered by the agreement hence a node can change a transaction in the network in a way that the hash is not valid. They provided a definition to transaction malleability in which they stated that it occurs when transactions are anonymously altering and resent, and this causes the transaction legal entity to fail in confirming the initial transaction.

Network Security: An eclipse attack takes place when an adversary captures some pieces of net- work communication and splits the network to introduce a higher synchronization delay ,an ex- ample is the simple form of the DoS attack to gain advantage on selfish mining and double- spending. In eclipse attacks, an attacker chooses one or multiple pieces of information and withholds it from one or more users, perhaps by not forwarding the blocks to the node.

Privacy: Security is also an issue especially when it comes to the issue of privacy in Blockchain since any one node can gain access to data from another node and, all the recorded transactions are visible to anyone who accesses the blockchain [67]. Different advices have been proposed regarding this problem and they are all hypothetical and don't encompass all problems for they can only be applied to certain cases. Because of the extensive number of data transfers, the communicating parties that engage the important data in the network may be vulnerable to some adversaries through the MitM attack and the DoS/DDoS attack. There are many privacy issues that IoT creates such as data privacy and tracking for phones and cars. Moreover, voice recognition is being incorporated to enable the devices to listen to the ongoing flow of discussion to passively push the data to cloud for analytics.

Redundancy: Stated simply, costly replication to remove the arbitration that enables every node of the network to retain a record of every transaction. However, it was economically as well as legally absurd to have duplicate brokering; banks are not prepared to facilitate any transactions with any particular bank or to compensate for other's transactions. The kind of replication that only generates costs cannot be justified by any conceivable benefits

Regulatory Compliance: Thus it is possible to see that blockchains are permanent no matter the law, and government authorities do not alter their work processes upon encountering blockchains. Blockchain adoption done in the sphere of law and finance in non-Bitcoin currencies causes some legal issues but the regulation of infrastructure is relatively close to the regulation of blockchains. they highlighted the major legal concerns which are putting a strain on block chain and the innovation distributed structure that has been adopted in both the Europe and United States.

Criminal Activity: Introduced by the Bitcoin digital currency, third-party trading services offer an opportunity to buy or sell almost any type of product. These processes are anonymous, and enabling control over the users and applying legitimate punish BDSs becomes nearly impossible. The daily use of Bitcoin in criminality involves ransomware, black markets, and money laundering. Some of the underground markets that are involved in the online sale of illicit goods and services trade as Tor hidden services but use the Bitcoin exchange currency, which means that the availability of blockchains is still unpredictable due to the mentioned criminal activities. The available item categories are as follows: Tent Event, Furniture Rental, Tents and Canopy, Lighting/Special Effects/Haze, Roaming Rotating Rabbit/Table Top Carousel, Tabletop Rental, Dance Floor/Specialty Dance Floor/Main Stage, Chairs and Reception Seating, Audio/Visual/Televisions, and Stages/Platforms/Platforms Accessories.

<u>Mitigation and solution for Attacks:</u>

Liveness Attack

(Sengupta, Sushmita Ruj and Sipra Das Bit, 2020) The liveness attack aims to delay the confirmation of transactions by proceeding through three stages: preparation which is one of the attacker strategies, transaction denial which is a strategy employed by the attacker, and last is the blockchain delay which is also a strategy used by the attacker. To combat this, the Conflux consensus protocol incorporates two block generation strategies: where approval needed it was done through one email while the other was for monitoring of progression. The combination of these two aspects is achieved by using an adaptive weight mechanism, so Conflux retains decentralization, scalability, high transaction throughput, and fast confirmation times.

Double Spending Attacks

This is the action that takes place in which the same digital token is used for more than one purchase, based on the non-secure properties of the digital cash system. For this purpose, the MSP framework known as Multistage Secure Pool has been established. This framework includes four stages: These are the detection, confirmation and forwarding as well as broadcasting procedures to enhance the availability of confirmation of the transaction and to curb the occurrence of double spending. Furthermore, several solutions can be suggested to fix the principal drawbacks of this type of attack and increase the level of transaction protection.

51% Vulnerability Attack

A 51% attack is an instance when an entity gains control over more than half of the networks' hashing power hence has the ability to assail the blockchain. To manage this risk, defensive mining has been crafted and a finality arbitration system that severely restricted the reorganization of the chain. Such measures help to strengthen the network's protection even when the has rate is not very high hence reducing such attacks.

Private Key Security Attack

Wallets consist of public and private keys where private ones are essential when it comes to withdrawing the funds or proving the operations. A suitable infrastructure that can be implemented to act against key security attacks is the public key infrastructure that is used to authenticate entities in the blockchain. It also uses group key management to secure the communication and network, plus the integrity and confidentiality of the network.

Transaction Privacy Leakage

Security is important to the transactions since the behavior of users in blockchains is openly transparent. To cope with the privacy leakage, some secure transaction methodologies are proposed. These are the homomorphic cryptosystems, ring signatures and others because they increase the security of transaction in the network.

Selfish Mining Attack

It is a strategy of some miners to solve other blocks and keep them secret to establish their own special chain and be favored. In order to address this, there are mechanisms such as the honest mining practices together with a notation of truth states for blocks in the course of forks. Self-confirmation heights also allocated to transactions so that the genuine miners can possess their deserving rewards and the wasted computations do not occur.

DAO Attack

The core problem with the DOS is that it lacks central control and therefore is relatively easy to attack. As a result of attacks, efforts have been made to counteract them using resource-intensive tools that were developed through experiments. They help to ensure that smart contracts and DAOs run safely within the network, thereby protecting the users.

BGP Hijacking Attack

BGP is significant to the Internet and can severely impact blockchain networks when it gets hijacked. For this purpose, a solution has to be designed based on blockchain technology in which smart contracts are assigned to monitor the resources distribution. Overall, this scheme is seen as being a ready-made security means for BGP in the blockchain environment since the routing information will be safeguarded from changes by unauthorized individuals.

Sybil Attack

Sybil attacks are specific for instance, when a number of fake accounts are created with the aim to control the network. To avoid such attacks, schemes have been put forward that would allow the system to watch node's activity and identify such behaviors as nodes forwarding blocks for a given user over and over. In this way, the network will be able to avoid any violations and, therefore, prevent Sybil attacks.

Conclusion:

Thus, the research proves the impact of blockchain in improving cybersecurity in different domains, especially in connected devices, contracts, and identity management. Crypto solutions based on blockchain prevents vulnerability of a single point of failing, enhances networking of security and decreasing of risks of cyber-attacks through decentralizing security frameworks. Therefore, the results of the present study support that lightweight consensus algorithms and energy efficient protocols should be designed to cope with the issues of IoT systems with limited capabilities. Besides, the work establishes definitive requirements for adequate regulation and advanced approaches toward various types of cyber threats, such as liveness attacks, double-spending, 51% vulnerability attacks, private keys leakage, and transaction privacy leakage. As more work and research are committed to the development of blockchain, there is a great potential for the enhancement of IoT networks' security, data authenticity, and the exemplary foundation on which the future of digital security will be built upon.

Reference

- Google.com. (2017). *US11290324B2 - Blockchains for securing IoT devices - Google Patents*. [online] Available at: https://patents.google.com/patent/US11290324B2/en
- ACM Other conferences. (2017). *IoT security | Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*. [online] Available at: https://dl.acm.org/doi/abs/10.1145/3018896.3018933
- Liu, Z. and Li, Z. (2019). A blockchain-based framework of cross-border e-commerce supply chain. *International Journal of Information Management*, 52, p.102059. doi:https://doi.org/10.1016/j.ijinfomgt.2019.102059.
- Singh, S., A. S. M. Sanwar Hosen and Yoon, B. (2021). Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. *IEEE access*, [online] 9, pp.13938–13959. doi:https://doi.org/10.1109/access.2021.3051602.
- Sengupta, J., Sushmita Ruj and Sipra Das Bit (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *Journal of network and computer applications*, [online] 149, pp.102481–102481. doi:https://doi.org/10.1016/j.jnca.2019.102481.
- Malik, A., Gautam, S., Shafiqul Abidin and Bhushan, B. (2019). Blockchain Technology-Future Of IoT: Including Structure, Limitations And Various Possible Attacks. [online] doi:https://doi.org/10.1109/icicict46008.2019.8993144.
- Sonali Chandel, Cao, W., Sun, Z., Yang, J., Zhang, B. and Ni, T.-Y. (2019). A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption. *Lecture notes in networks and systems*, [online] pp.988–1003. doi:https://doi.org/10.1007/978-3-030-12385-7_67.
- Minhaj Ahmad Khan and Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, [online] 82, pp.395–411. doi:https://doi.org/10.1016/j.future.2017.11.022.
- Nazanin Zahed Benisi, Aminian, M. and Javadi, B. (2020). Blockchain-based decentralized storage networks: A survey. *Journal of network and computer applications*, [online] 162, pp.102656–102656. doi:https://doi.org/10.1016/j.jnca.2020.102656.
- Xi, Z. (2020). The comparison of decentralized and centralized structure of network communication in different application fields. [online] doi:https://doi.org/10.2991/msie-19.2020.10.