Future Of Security: Blockchain With Characteristics, Limitation And Various Possible Attacks

Rishav Kumar Mishra, Dr. Ritesh Rastogi, Rahul Kumar Gupta, Shashank Jain, Saurabh Gupta

Student, Associate Professor, Student, Student, Student

[1-5]Noida Institute of Engineering Technology (NIET) Greater Noida, India.

Abstract- As compared with the past the emerging of the internet is very wide. But providing security in IoT devices is still a big challenge and through blockchain, this problem can be solved. For the difficulties in sharing sensitive data among financial institutions, hidden dangers in data security, and high financial risk control costs, blockchain technology can be considered as a solution. Blockchain is a combination technology that takes part in innovative and well-built eyesight to all-inclusive explanation to IoT devices Securities. Blockchain provides security devices to IoT devices. The emerging of blockchain gradually increases in the future. In the upcoming time, it episodic revolution for safe connection that provides great change towards our working.

Keywords – Security, Blockchain, IoT, Digital signature, Secured hash value

1 Introduction

The money and protection area are essentially has been a seriously information-driven enterprise. Data distribution and operative storage in what way sensibly these data. Instead of this financial businesses holds a huge quantity of security-sensitive data if these data are leaked it will create harm to private welfares and national economic security. Thus, in private data sharing, it is difficult to stop this data to leak.

The introduction of the Internet of Things (IoT) and cloud computing gives a feasible specialized means to monetary information sharing. Monetary establishment transfers their business data to the cloud specialist co-op. At the point when different clients need to acquire the relating data, they just need to through a cloud check. Co-op. At the point when different clients need to acquire the relating data, they just need to through a cloud check. After the confirmation is passed, they can get information access privileges of information. That understanding the course of information sharing. In any case, information stockpiling dependent on distributed computing innovation has a specific deformity, that is, brought together the capacity of information. All delicate information will be spilled which will make gigantic misfortunes clients and monetary foundations even jeopardize public monetary security [1].

Blockchain is also known as Record-keeping technology. It is also used in another field such as providing security in IoT devices. It is a spread decentralized peer-to-peer hierarchy mechanism. The blockchain contains a hash pointer with a list of interlink blocks connected in a series. The data can be carried by each block that maintains the data and is not allowed to change by using cryptographic techniques. By implementing crypto technique blockchain stores full life cycle and program instruction transactions publicly. Thus the interaction in the olden days in blockchain cannot be changed or go down. When the entire data is changed instead by some data, data is modified. And due to this blockchain technology data is saved from the hacker.

According to Don and Alex Tapscott "Blockchain is an indestructible ledger containing various economic transactions that can be programmed to record not only all financial transactions but effectively everything of the value." Blockchain is incontestably original detection. The blockchain system formed the support of the modern internet. The block in the blockchain is the digital block of instruction. It can reserve instruction that differentiates them from other blocks [2].

1.1 Characteristics of blockchain

Blockchain technology has gained considerable praise because of the following characteristics-

- Decentralized- Blockchain does not grip only a group or unit.
- Secured- This technology uses cryptographic techniques for data transmission and data storage.
- Immutable- Blockchain is secure and there is no change happening in data.
- Traceable- If needed data can be hacked easily.
- Transparency- The data which is identified by the user is kept [3].

1.2 The building block of the blockchain

Figure 1 shows a blockchain that consists of n number of blocks. All blocks are linked with two other blocks that are previous block and the next block. Every block is made up of a block header, transaction counter, TX (Hashfunction).

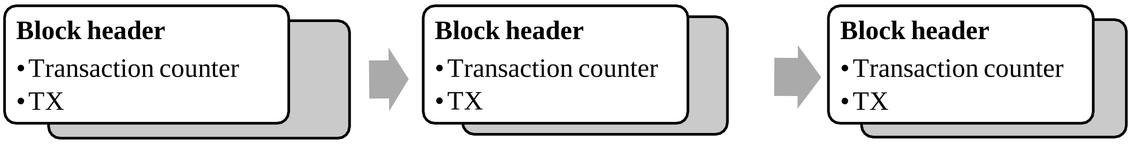

Figure 1 Block diagram of a blockchain

1.3 Structure of single blockchain

Figure 2 shows the structure of the block, which is divided into three parts are Block header, Transaction Counter, and n number of TX, Block header is also divided into six parts; block version, MTR hash, Timestamp, n-bits, Nonce, and PBH.

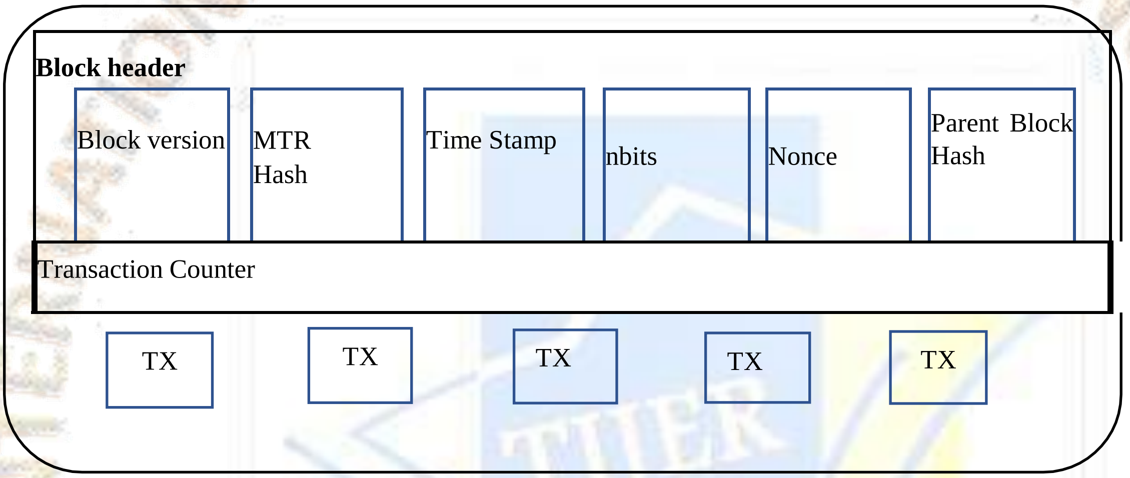

Figure 2 shows the structure of a single blockchain

2 Types of blockchain

There are mainly four types of blockchain as shown in figure 3.

- Public blockchain
- Private blockchain
- Consortium blockchain
- Hybrid blockchain

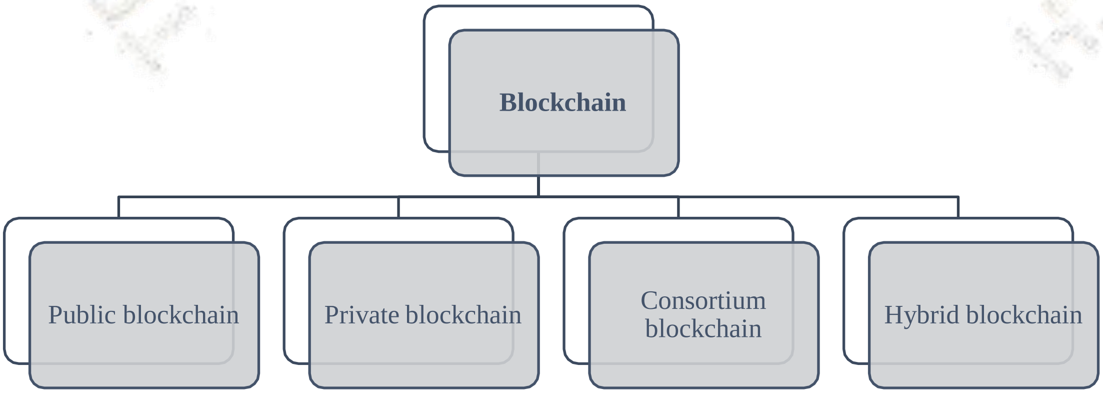

Figure 3 Types of blockchain

- **Public blockchain-** It is also called no access restriction, anyone can send a transaction and become authored. In this type of blockchain cryptography like bitcoin originated and helped to popularize distributed ledger technology. Public blockchains are permissionless, permit anybody to join, are decentralized. Public blockchain permits all hubs of the blockchain to have equivalent privileges to get to the blockchain, make new squares of information, and approve squares of information. Until this point, public blockchains are utilized for trading and mining digital money. You might have known about famous public blockchains the hubs" mine" for digital money by making blocks for the exchanges mentioned on the organization by tackling cryptographic conditions. As a trade-off for this difficult work, the excavator hubs acquire a limited quantity of digital currency. The excavators go about as new period bank employees that plan exchange and get (or "mine") a charge for their endeavors [4-6].
- **Private blockchain-** It is also called restricted blockchain, the user is selected by the network administrator. It is also called a managed blockchain. This type of network is considered as a middle- group for organizations that want blockchain technology. Private blockchain, which may likewise be alluded to as overseen blockchain, is permissioned blockchain constrained by a solitary association. In a private blockchain, the focal authority figures out who can be a hub. The focal authority additionally does not allow every hub with equivalent freedoms to perform capacities. Private blockchains are just somewhat decentralized because the community to this blockchain is limited. A few instances of private blockchain are the business-to-business virtual cash trade network Ripple and Hyperledger, an umbrella venture of open-source blockchain applications. Both private and public blockchain have a disadvantage

– public blockchain will in general have longer approval times for new information than private blockchain, and private blockchain is more defenseless against misrepresentation and troublemakers. To address these downsides, consortium, and crossover blockchain was created [4-6].

- **Consortium blockchain-** It is a semi-decentralized blockchain, for the implementation of harmony protocol, the supervisor of consortium restricts users' learning right as they can see, fit, and allow only a fixed set of dependable intersections. A consortium blockchain is a permissioned blockchain represented by a gathering of associations, as opposed to one substance, as on account of the private blockchain. Consortium blockchain, along these lines, appreciates more decentralized than private blockchains, bringing about more significant levels of safety. Notwithstanding, setting up a consortium can be a laden interaction as it requires collaboration between various associations, which presents strategic difficulties just as possible antitrust danger (which we will analyze in an impending article). Further, a few individuals from supply chains might not have the required innovation nor the framework to carry out blockchain devices, and those that do may conclude the forthright expenses are too steep a cost to pay to digitize their information and associate with different individuals from the inventory network. A well- known arrangement of consortium blockchain answers for the monetary administration's industry and past has been created by the venture programming firm R3. In the production network area, cargo smart has fostered the Global Shipping Business Network Consortium, a not-for-benefit blockchain consortium that plans to digitalize the delivery business and permit sea industry administrators to work all more cooperatively.
- **Hybrid blockchain-** Hybrid blockchain will be a blockchain that is constrained by a solitary association, however with a degree of oversight performed by the public blockchain, which is needed to play out specific exchange approvals. An illustration of a crossover blockchain is IBM Food Trust, which was created to further develop effectiveness all through the entire food production network. [4-6]. Summarization of section 2 is shown in table 1.

Table 1 Difference between all the types of blockchain

Public blockchain [4-6]	**Private blockchain [4-6]**	**Consortium blockchain [4-6]**	**Hybrid blockchain [4-6]**
Permissionless in nature	Permissioned in nature	Permissioned in nature	Permissionless / permissioned in nature
Advantage is trust	The advantage is its execution	The advantage is its security	The advantage is its scalability
Drawback is security	Drawback is trust	Drawback is transparency	Drawback is upgrading
Used in cryptocurrency	Used in supply chain	Used in banking	Used in real estate

3 Security in blockchain

In today's time, nothing is safe like diplomacies, atmosphere, network, capital, provider, server, etc. All the things which provide communication have to be given priority of its generalization and then it can whole component. These are some reason that is responsible for good security to the system when we use blockchain-

Blockchain is decentralized- Blockchain breaks every single this into small pieces and represents them to the complete network at the position of inserting them to cloud server or hold back them into sole place. It is a cardinal project of broadcast that does not present a middle command position. Due to blockchain, if any nodes get hacked by an attacker by any excuse there is no leakage of data. Figure 4 shows the hiring process, first of all by using hash function hash value is generated for data than by the help of user's private key SHV is obtained by converting hash value. At the end receiver's side receive data and SHV. And thus, this whole process is said to be data is digitally signed [7].

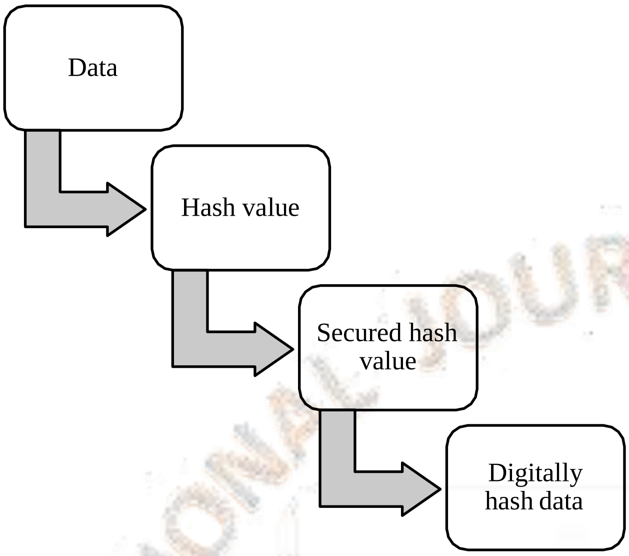

Figure 4 Decentralized process

Blockchain offers encryption, validation, and verification- By using blockchain technology, data is encrypted not changed and it is unarguable that is all data in the blockchain is fully converted and digitally signed. Figure 5 shows the verification process when the receiver received digitally signed data then entered data get split into data and SHV. With the help of the hash, the function receiver calculates the hash value of received data. And by using a public key hash value is obtained that is sent by the receiver. In the end, both hash value (a hash value that is calculated by hash function and public key) is compared if both hashes are valued is same then we can say that receiver receive secure and real data [8].

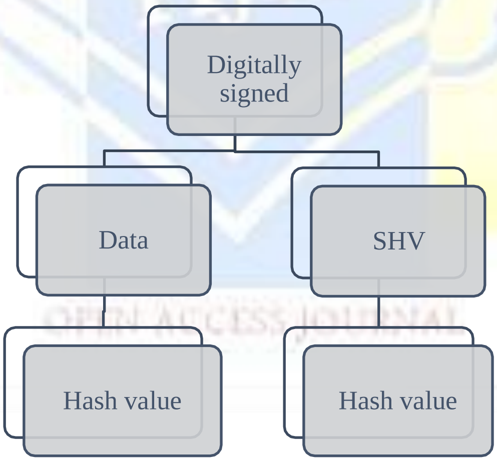

Figure 5 Encryption, verification, and validation process

4 Application of blockchain

Blockchain is mainly used to secure IoT devices. While blockchain technology is combined into multiple areas, such as Cryptocurrencies, Smart contracts, Financial services video games, etc. The allocated economy, Supremacy, supply chain auditing, Estimate markets, Anti-money laundering, and KYC, Data management, Stock trading. Some other applications are stated as below-

- **Money Transfer and Payment Processing-** We are using blockchain technology to transfer money from one person to another with this technology accelerates to transfer of funds. Almost all transactions are use blockchain to settle money within a second while the bank takes 24 hours.
- **Supply Chains Monitoring-** Monitoring supply chains are easy to be applied by blockchain technology. Enterprises and even customers are enabled blockchain to observe in what way products achieve from a quality-control when products are realized by origin to the retailer.

- **Retail Programs Based on Loyalty Rewards-** On loyalty rewards transferred it is also done by blockchain. A blockchain helps design a token-based system that rewards customers and stores all data. It is also reduced paper and card-based programs. [9].
- **Digital IDs-** The identity issue is a challenge expressed by more than one billion people in the world. The alternative to this is looking at Microsoft. Currently, this is used by millions of people for authenticator applications for designing digital IDs. Digital identities are controlled and managed in thisway.
- **Sharing of data-** Cryptographic money IOTA has presented a beta form of its Data Marketplace in November, clarifying that the blockchain could be utilized as a commercial center to share or sell information that is unused. Since most endeavor information goes unused, blockchain could go about as a go-between to store and move this information to improve a mass of enterprises.
- **Protection of Royalty and Copyright-** Copyright and eminence laws on music and other substance have developed claggy in a world that has developing web access. Blockchain can be applied to expand those copyright for computerized content downloads which will guarantee that the maker of the substance being bought gets their genuine offer.
- **Digital voting-** Blockchain gives the capacity to cast a ballot carefully, and it is straightforward enough that many controllers would have the option to check whether something was modified on the organization. It coordinates the simplicity of computerized casting a ballot with the changeless (i.e., constant nature) of blockchain to make the most of the vote truly.
- **Transfer of Real Estate, Land, and Auto Title-** One of the preeminent objectives of blockchain is to remove the paper from the situation since paper trails are frequently a course for disarray. In case individuals are purchasing or selling land, a house, or a vehicle, they should move or get a title. Rather than working this on paper, blockchain helps in putting away titles on its organization, empowering for a straightforward perspective on this exchange, just as displaying a completely clear image of lawful proprietorship.
- **Food Safety-** One more entrancing utilization of blockchain innovation empowers the following food from its starting point to the plate. Since blockchain information is unchangeable, one can follow the vehicle of food items from their starting point to the general store.
- **Unchanged Data Backup** - Blockchain innovation is the best way of support up information. Even though distributed storage frameworks are made to be a go-to hotspot for information protection, they are powerless to the programmer, or even foundation issues. Utilizing blockchain as a reinforcement hotspot for cloud server farms or any information could settle this issue [10].

5 Drawback of blockchain

Blockchain is modern technology, but we have not all proper solutions yet, but blockchain provides security to data in the data world security. If blockchain is not always a solution. The potential use cases for safety that are positively worth observing. In these modern days, nothing is impossible to total hack but blockchain technology provides security that has come nearly to Holy Grail status so far. So, this is all stirring, it is important to remember the potential problems and drawbacks of blockchain

- Attack 51%- The hash value is calculated of the same block at a particular time by an attacker, then blockchain breaks with itself into two blockchains, one is real one is fake.
- Double-spending- The working and outcome of double-spending and attacker 51% are similar but double-spending happens when a user spends money yet again.
- Cracking of the cryptographic- For the security of data blockchain use cartography technique, but these days with the help of this attack cryptographic technique may be hacked.
- Denial of service (DoS) attack- In a Denial of services (Dos) attack, a huge quantity of garbage packets are used by the attacker to create a network conflict of Ad hoc network in the blockchain. Communication with others is rejected because a busy node can prevent by the malicious node that is why the availability of the network is affected.
- Sybil attack- In a Sybil attack, a blockchain is hijacked in the network and then claims multiple characteristics by sybil attack. It affects the remaining security goal and accessibility of the network.
- WannaCry ransomware/Crypto-worm attack- Microsoft Windows operating system is used to the hacked blockchain. The attacker encrypted its malware content and make valid content and bitcoin cryptocurrency is used by the attacker for demanding money [11].
- Petya attack- Microsoft windows as an operating system are always targeted by the attacker to hack. The purpose of the attacker is to infect the leading boot archive after encryption of the hard drive file system.
- Distributed denial of service- In this attack working of blockchain is blocked by the attacker and also denies the financial services or resources Bicton is used by an attacker to achieve the malicious activity.
- Time jacking- Timestamp of blockchain is performed by the attackers to improve time counting of a node is used the phony blockchain or encouragement to use them.
- Delay attack /Jellyfish attack/Guaranteed Time Slot (GTS) attack/ Timing attack-In this attack, an attacker are used needlessly delay to send data packets and prevent blockchain from working on the devices

- Vulnerabilities in contact source code- In vulnerabilities in contract source code, a hacker creates a duplicates agreement and then deals with the object as a real deal to gain function on the victim.
- Immutable defects- we know in blockchain, blocks are unchangeable, that is fixed cannot be modified or changed. When an intelligent contract has problems in its document so it is very tough to restore it, hence attacker gain ambiguity here and achieved to secure fork [12]
- Cryptocurrency lost in transfer- In cryptocurrency lost in transfer attack data comes from the evil origin, the bitcoin goes in the block have not known any owner or contract.
- Bugs in access control- In the bugs in the access control attack function contract get hacked by the attacker when a bug is present in bitcoin.
- Alternative history attack- In an alternative attack, the attacker sends the transaction to the vendor and mines a temporary part with extra transactions respectively. Due to this attack vendors endure money loss they will send transactions after n acceptance.
- Selfish mining/ block withholding- By Selfish mining attack, the mined blocks are kept for a particular time to prevent it from spreading into the network, and then many mined blocks are free from the attacker at that time to create floods and to disconnect of authentic- working mined blocks.
- Fork after withholding attack – In Fork after withholding attack, a clone miner carries a victorious block and anyplace remove it too or maybe open it after earlier to set up a branch, transmit and incidents.
- Race attack- In a race attack, two times transaction happens that is created by the attacker. The first transaction is received by the user that is sent by the attacker and then the user sends this payment based on that transaction as they(user/victim) do not about the attack. And other different contracts including fail messages are forwarded to the network and requested to do the entire procedure again [13].
- Short-address attack – Short-address attack generally happen on EVM because somewhere EVM allow/accept wrong, duplicate, or fake address and this attack make a connection via an illegal addressing
- Flawed key generation- As the name signifies, this attack is accomplished to hack the private key. If users do not update the content of keys correctly and carefully then this type of attack happened.
- Attack on the cold block- Attack on cold block kept private key used in cryptographic technique and the apps which are interconnected via internet provide.
- Attack on the cold block- Attacks on the cold block are happening on blockchain to obtain all probable keys, hash function, resources, workshop, important PINs, improvement seeds, and important data subjects.
- Eclipse attack- In an eclipse attack, the attacker has authority on a big set of IP addresses as well as a circulated botnet, and when the sufferer reopens its blockchain then all the connections refresh, and then data goes to the attacker directly as the attacker is under control IP addresses.
- Phishing - In this attack, the attacker smartly influences the customer to perform illegal content to steal important data as well as records.
- Dictionary attack- In a dictionary attack, by using the hit and trial method attacker hacks the password, user id, hash, digital signature, etc per to play malevolent action. Attackers use names, middle name, last name, date of birth for hacking passwords. [14].

6 Conclusion

In this paper, we label around the information of Blockchain, its features, characteristics, the basic structure of Blockchain and Assembly of Blocks and nature of blockchain. We have also deliberated that blockchain is very significant for security purposes, it is the first choice where we believe around securely data broadcast in air. Blockchain is regionalized so the security in blockchain increase the trust, after proper confirmation and authentication encryption is done, it is virtually impossible to hack, and its nature. And then we discuss the application of blockchain. But as we distinguish that nothing is secure in air communication, so we also keep an eye on the boundaries of the blockchain, and finally, we discover some likely bouts that damage the system, data and influences as well. The paper offers an inclusive study in the achievement of attacks in blockchain, proposed by various researchers. In the end, it achieves that the use of blockchain is truly a very significant feature, so creation is protected is the main apprehension. This paper attempts to improve understanding of the relevant matter of the blockchain and allows us to suggest a new and better key to deal with those attacks.

References

[1] Malik A, Gautam S, Abidin S and Bhushan B (2019) Blockchain Technology-Future Of IoT: Including Structure, Limitations And Various Possible Attacks, 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 2019, pp. 1100-1104, doi: 10.1109/ICICICT46008.2019.8993144.

[2] Gautam, S., Malik, A., Singh, N., & Kumar, S. (2019). Recent Advances and Countermeasures Against Various Attacks in IoT Environment. 2019 2nd International Conference on Signal Processing and Communication (ICSPC). https://doi.org/10.1109/icspc46172.2019.8976527

[3] Frauenthaler P, Sigwart M, Spanring C, Sober M and Schulte S, (2020) "ETH Relay: A Cost-efficient Relay for Ethereum-based Blockchains," 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 204-213, doi: 10.1109/Blockchain50366.2020.00032.

[4] Salman T, Jain R and Gupta L, "A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains," (2019) IEEE International Conference on Blockchain (Blockchain), (2019), pp. 520-527, doi: 10.1109/Blockchain.2019.00078.

[5] Moschou et al K., "Performance Evaluation of different Hyperledger Sawtooth transaction processors for Blockchain log storage with varying workloads," (2020) IEEE International Conference on Blockchain (Blockchain), 2020, pp. 476-481, doi: 10.1109/Blockchain50366.2020.00069.

[6] Kim et al J., "Anomaly Detection based on Traffic Monitoring for Secure Blockchain Networking," (2021) IEEE International Conference on Blockchain and Cryptocurrency (ICBC), (2021), pp. 1-9, doi: 10.1109/ICBC51069.2021.9461119..

[7] Malik Ayasha, Steganography: Step Towards Security and Privacy of Confidential Data in Insecure Medium by Using LSB and Cover Media (December 12, 2020). SSRN Electronic Journal, doi:10.2139/ssrn.3747579.

[8] Mounnan O, Mouatasim A, Manad O, Outchakoucht A, Es-samaali H and Boubchir L, "A Novel Approach Based on Blockchain to Enhance Security with Dynamic Policy Updating,"(2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2020), pp.1-6, doi: 10.1109/IOTSMS52051.2020.9340164.

[9] Sönmeztürk O, Ayav T and Erten Y.M, "Loyalty Program using Blockchain," (2020) IEEE International Conference on Blockchain (Blockchain), (2020), pp. 509-516, doi: 10.1109/Blockchain50366.2020.00074.

[10] Zhang et al. Y, "Deployment of backup core switch in scalable distributed data center networks," (2014) 13th International Conference on Optical Communications and Networks (ICOCN), 2014, pp. 1-4, doi: 10.1109/ICOCN.2014.6987082.

[11] Chuquilla A, Guarda T and Ninahualpa Quiña G, "Ransomware - WannaCry Security is everyone's," (2019) 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019, pp. 1-4, doi: 10.23919/CISTI.2019.8760749.

[12] Chen J, Xia X, Lo D, Grundy J, Luo X and Chen T, "DEFECTCHECKER: Automated Smart Contract Defect Detection by Analyzing EVM Bytecode," in IEEE Transactions on Software Engineering, doi: 10.1109/TSE.2021.3054928.

[13] Cai et al. Y, "Resource Race Attacks on Android," (2020) IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER), (2020), pp. 47-58, doi: 10.1109/SANER48275.2020.9054863.

[14] Nam J, Paik J, Kang H, Kim U.M and Won D, "An off-line dictionary attack on a simple three-party key exchange protocol," in IEEE Communications Letters, vol. 13, no. 3, pp. 205-207, March (2009), doi: 10.1109/LCOMM.2009.081609.