Blockchain-based Efficient and Secure Peer-to-Peer Distributed IoT Network for Non-Trusting Device-to-Device Communication

Rajesh Kumar Sharma and Ravi Singh Pippal
Department of Computer Science & Engineering,
RKDF University, Bhopal, India
E-mail: rajeshsharma.ercs@gmail.com, ravesingh@gmail.com

Keywords: Security, blockchain, internet of things, avalanche effect, device-to-device communications, peer-to-peer communications

Received: April 5, 2021

The security and privacy issues in the Internet of Things (IoT) are a mandatory process and also a challenging task for researchers. Blockchain technology enhanced and motivated the recent security parameters, and it has been validating various technical sectors since its inception. In this paper, a peer-to-peer distributed IoT network is presented where non-trusting devices can interact with other devices without a trustworthy intermediary using the blockchain technique in automated verifiable mode. Major implementation issues for deploying blockchain in the IoT network are pointed out in this paper. The model presents a modern blockchain technique to surpass the traditional security system for efficient and secure IoT deployment under various conditions. Finally, to validate the signification of blockchain in the IoT network, the avalanche effect is calculated and compared with Triple-DES, AES, and Blowfish cryptographic algorithms for non-trusting device-to-device (D2D) communications and transactions. The result presents significant output changes in hash for the blockchain-IoT integrated model as compared to other cryptographic algorithms. Conclusively, blockchain in the IoT network can make a remarkable impact across various industrial and business applications.

Povzetek: Študija predstavlja varno bločno omrežje za IoT, ki omogoča komunikacijo brez zaupanja med napravami, s primerjavo z obstoječimi kriptografskimi algoritmi.

1 Introduction

The most auspicious technologies in this modern era are the Internet of Things (IoT) and the Blockchain. The perfect solution to incorporate decentralized security in IoT is blockchain technology for peer-to-peer communication, and the integration of these two technologies is certainly required in many applications and domains [1]. There are many possible blockchain applications for IoT cases, including the healthcare industry, supply chain management, public safety, personal data management, finance, education, insurance, notary services, smart homes, and cities [2, 3]. Blockchain is continuously blowing up modern IoT-based industries, and it is expected to motivate IoT onward. The distinguishing features, such as decentralized trust and security provided by blockchain, are crucial characteristics of IoT infrastructure [4]. Many researchers are innovatively working on IoT-blockchain collaboration in several ways due to the prevalence of both technologies and inventing extremely secure and robust systems to address the technical problems [5].

A blockchain framework stores information records in attached blocks, which are connected using a cryptographic algorithm [6]. Basically, it has a continuously extending database list in distributed form to maintain record information, where participating nodes in the blockchain validate new and existing records [7]. For establishing a trusted network between nodes, any central third-party authentication or participating node is not required in this decentralized blockchain network [8]. All the completed transactions and their information are always shared, distributed, and updated to each node in the blockchain network, so all the nodes have the exact same information record [9–11].

The most secure and transparent system than centralized transactions can be structured by the blockchain. It can efficiently record transactions and details between two parties using a distributed ledger in a permanent and verifiable way. Ultimately, privacy, security, anonymity, and transparency are the main goals of blockchain technology for all of its users.

Information about other physical conditions in the environment is acquired by Internet of Things (IoT) devices, and they communicate and transmit data with each other using inbuilt software systems. IoT devices generate a huge quantity of information and sensing data, but devices do not inevitably trust others at the time of transactions. Critical privacy issues can be raised because connected IoT devices transmit sensitive personal information and can disclose the preferences and behaviors of their users. When personal, sensitive data is utilized by any centralized or-

ganization, the privacy of IoT users is especially at risk due to the illegitimate usage of data. To solve this problem, blockchain technology can be beneficial in structuring privacy-preserving IoT systems. There are many technical benefits of blockchain, as presented in Figure 1. The foremost benefit is security, and other facilities such as open architecture, timestamped, smart contacts, distributed ledger technology, etc. are significant characteristics of blockchain technology.

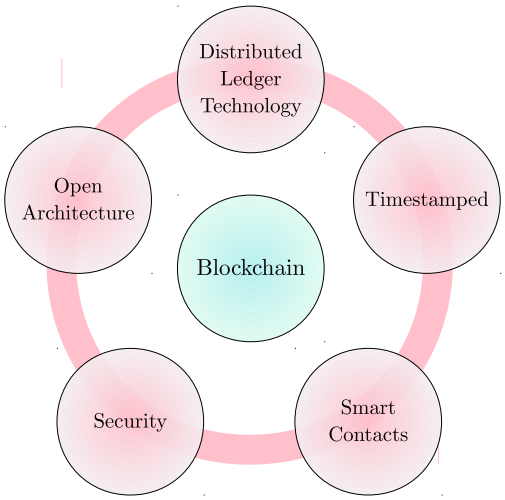

Figure 1: Technological Benefits of Blockchain

Since the blockchain is peer-to-peer (P2P) technology, it is tamper-proof, contains only trustworthy information, and is not dominated by any single centralized entity. The blockchain technology provides secure agreement-based peer-to-peer communications between devices in the IoT network. It also resolves other issues such as trust, privacy, scalability, time-stamping, single points of failure, and reliability challenges of the network for IoT devices. For the transmission of data between devices in a consistent, secured, and time-stamped manner, blockchain technology offers a trustworthy framework for the IoT network. In this infrastructure, IoT devices can take advantage of smart contracts to enable message conversations, which create trust agreements between devices. The characteristics of autonomous activities and intelligent applications for sensing devices can be enabled using these features. To construct a completely distributed, trustworthy blockchain-based digital infrastructure, IoT-based peer-to-peer transactions can be extended to a person-to-device or person-to-person platform. Currently, there are numerous blockchain-based solutions and applications; it has continuously been applied in various cases since its inception.

2 Blockchain technology

Blockchain is a distributed, trusted, shared, and public ledger of transactions that every user can analyze but a single user cannot control. Basically, it is a distributed database system that preserves the endlessly developing list of all transaction data and records in a cryptographically locked system from any tampering or violation. Since the Blockchain is a distributed system, the concept of a centralized master node is not required, and all the other connected nodes maintain a true copy of the database. An efficient, highly resistant, transparent, and secured digital interaction and transaction storage system is offered by blockchain technology. This system has the potential to enable new industrial and business models.

In blockchain technology, all transaction data and relay information are listed in the connected chain of blocks initiated and generated by anonymous users. It provides advantages such as speed, transparency of transactions, cost efficiency, and high security. Blockchain provides data immutability using cryptographic hashes, where data is stored linearly and the new block keeps a record of the hash value of the previous block. Each transaction is required to undergo validation before being appended to the blockchain by participants in the network. The noteworthy issues constituted by blockchain technology are related mainly to the following:

- Accuracy,
- Trust,
- Intermediaries,
- Decentralization,
- Transparency,
- Transaction freedom.
- Data privacy and security,

3 Beneficial aspect of blockchain-based IoT

The engrossment of blockchain-based IoT research is to gear up an efficient, secure, and trusted peer-to-peer distributed IoT network for communications among non-trusting devices. Blockchain technology offers many beneficial aspects for IoT [12]:

- The blockchain-based shared ledger is immutable and can hold records. Many characteristics of the IoT network, such as the type of device, sensing features, range, embedded software, malfunctions, status, hardware changes, and current position, enhance trust among devices and their data.
- Trust agreement between devices for any sensed and measured value of specific characteristics in the IoT network.
- The smart contracts allow the devices to interact autonomously and independently with other commercial systems and devices.

– Third-party validation, verification, or trust is not required, which provides cost reduction and high transaction speed.

– Easy and efficient recovery of data and information due to distributed ledger recording management during system failure.

The overall important advantage is the transfer of trust in a trustless infrastructure. This is especially applicable in the IoT network, where many types of IoT device manufacturers have a different standard of accuracy, range, and functional characteristics. In the network, if new devices are added, smart contracts can be used to interact and communicate with other IoT devices for transactions, repair services, or replacement. The other devices can assume the responsibilities in case any device malfunctions. It validates and increases the value of data generated by IoT devices.

4 Related work

This section presents existing works, efforts, and literature reviews based on blockchain-integrated IoT systems to target the issues of privacy and security.

Chen *et al.* [14] proposed a data integrity checking system on the Internet of Things (IoT) network using the stochastic blockchain technique. They investigated the potentiality of blockchain to protect data integrity and security in the Internet of Things networks. The conventional decentralized techniques face the issues of network congestion and single-point failure. To overcome these shortcomings, a stochastic-based blockchain method is proposed for verifying data integrity in the IoT network. The proposed method minimizes the quantity of cooperating IoT devices and relies on edge devices to produce the block, which reduces the computational and transmission time. The simulation outcomes present an enhanced success rate against large-area IoT networks with a low number of cooperating devices.

Haseeb *et al.* [13] presented "RTS: a robust and trusted scheme for IoT-based mobile wireless mesh networks" for increasing network coverage with the reliability of the system. Their proposed model for IoT-based mesh networks is presented in Figure 2. In this model, RSA-based cryptography is applied to communication links between gateways and clients of the mesh network with existing malicious devices. The existing data routing method works for static mesh devices and monitors transmission links, which can create a deficient effect on the performance of the network and increase the chance of packet drop ratio. Their proposed infrastructure constitutes a mesh network of mobile clients to perform better network exposure in data transmission lines, considering factors for packet drop reduction and a high ratio of data delivery. This model overcomes the communication cost by using the flooding of distance vector routing over periodic time intervals by mobile mesh clients. Their simulation outcomes present high data reliability as well as a low computational operating expense in different topological networks.

For edge-based devices in the Internet of Things (IoT) network, Pyoung *et al.* [15] proposed "LiTiChain, a blockchain with finite-lifetime blocks". The LiTiChain handles the difficulty of traditional blockchain as it continuously grows into an information block list. The outdated block of information should be promptly eliminated so that an extended blockchain list can be stored at the end node. To eliminate the information block consistently, a tree-structured end-time ordering graph (EOG) was introduced to arrange block lists according to their endings, and it also maintained the chain connectivity of the blocks.

Mazzei *et al.* [16] designed and implemented secure industrial devices using blockchain-based interfacing techniques. Their proposed system allows interaction devices to be made available to the public as a secure blockchain service. The proposed system can also be easily modified as an independent blockchain-equipped tracking system. The system acts as a connection between blockchain-based security and the industrial Internet of Things, which enable the tokenization of industrial devices.

Lei *et al.* [17] proposed "Groupchain", an original double-chain structure-based scalable public blockchain system for fog computing in IoT. To address the problem of increased transaction throughput generated by the serialized leader election process, they proposed a double-chain structured-based IoT security system using blockchain. The experimental results of the implemented "Groupchain" prototype present the scalability and transaction efficiency of "Groupchain".

Muthavhine *et al.* [18] studied concerning cryptographic algorithms applied, especially in the security of the Internet of Things. They collected existing cryptographic methods applied to several IoT devices for encryption and authentication, analyzed the Avalanche effects of cryptographic algorithms for each device, and improved their speed using mathematical methods.

Novo [19] addressed the extensibility problem of accessing, arranging, and managing a large number of secure IoT devices because conventional centralized control to access the system is unable to handle increasing loads effectively. This research introduced a novel access handling control that reduces the management problems of plenty of constrained devices in the Internet of Things network. The proposed technique is a completely decentralized blockchain-based method.

For autonomous cooperative intrusion detection in the devices of large Internet of Things networks, Mirsky *et al.* [20] introduced a blockchain-based security solution. In the IoT network, an agent system is configured for detection of any software exploitation on the devices, which provides regular control for intrusion detection. Any kind of manual activity or update is not required to generate a malware signature in this proposed framework.

Due to the deficient management of the Internet of Things network and devices, particularly the arrangement

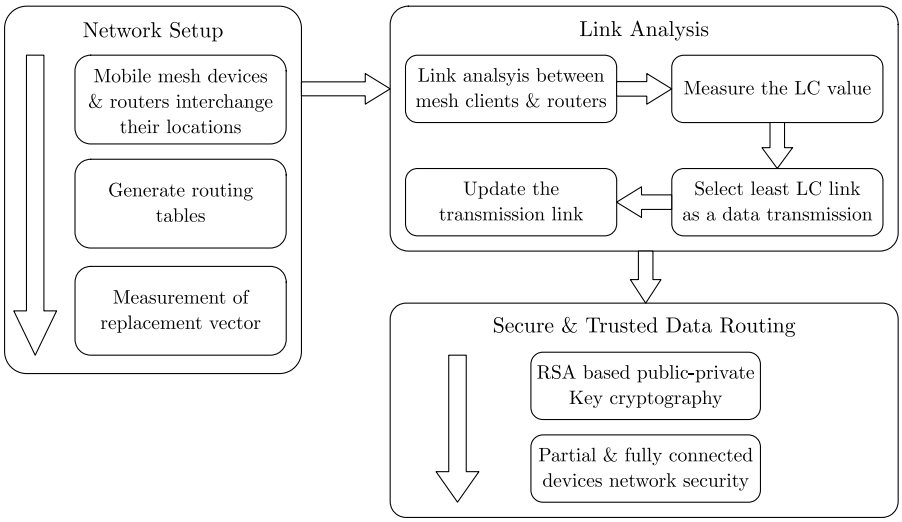

Figure 2: Trusted and Robust Model for IoT-based Mesh Network [13]

and installation method, observable exploitation in the IoT network environment can be detected. To provide a solution to this problem, Yohan *et al.* [21] proposed the "Firmware-Over-the-Blockchain (FOTB) Framework, a secure and efficient blockchain-based firmware update structure between manufacturers of IoT devices and network-deployed devices. In this proposed framework, a peer-to-peer verification technique through a blockchain-based mechanism is applied for the security of firmware distribution activities, which also ensures the integrity of the system in a distributed IoT network.

Li *et al.* [22] designed "Blockchain-based Distributed IoT Data Transaction (BDDT)" a novel data architecture for the IoT network that offers a framework for data producers and users and provides a solution for reliability problems and usage of data facilities offered by the central storage of IoT. The problems of secure data circulation and transaction in IoT network, BDDT system efficiently resolve these problems.

Liu *et al.* [23] combined blockchain technology in the "Attributed-Based Access Control (ABAC) Model", which carries the benefits of blockchain-based decentralized technology for access control demands into the Internet of Things and solves the problem of conventional access control techniques. The ABAC model provides a device authentication system, implements the management policy of ABAC, and verifies device security access using the smart application. A Hyperledger Fabric-based opensource access control system "Fabric-IoT" is developed and applied in the network. The final steps involved in this model are network deployment using blockchain, installation of chaincodes, and invoking smart contracts.

Rathee *et al.* [24] proposed a blockchain technology-based secure hybrid "Industrial Internet of Things (IIoT)" framework. In this framework, the activities of employees are collected and stored by blockchain-based industrial IoT devices to maintain the security, transparency, and tracing of all work by producing the hash of each record for IoT devices. The proposed secure framework expressively minimizes the loss ratio of the product and falsification problems in network devices.

Chatterjee *et al.* [25] developed a lightweight authentication network protocol for secure key swapping, text messaging, and supporting the hierarchically architectural framework of the IoT network. To protect against adversarial active and passive threats, the Physically Unclonable Function (PUF) [26] cryptography method is used. The limitations of previous PUF-based security methods can be eliminated using their proposed protocol, which is strong against many threats.

Wang *et al.* [27] proposed a hierarchically structured storage system for storing the blockchain in a cloud network, and it maintains newly added blocks in the blockchain network. They presented a blockchain-integrated Internet of Things architecture to protect and maintain blocks and transactions produced in IoT networks. The blockchain and cloud connection as a software interface is designed to build block synchronization for storage in the cloud.

For the security of supply chain management applications, Malik *et al.* [28] proposed a blockchain-based "Trust Management Framework (TrustChain)" to solve the issues related to the quality trust of commodities and the entity of logging data. Basically, the "TrustChain" framework utilizes blockchain technology to monitor all interactions. The agent- and asset-based reputation model is also provided by this framework; it reaches efficiency and automation through smart contracts with the reputations provided to the same participant for the particular product.

Biswas *et al.* [29] designed and implemented a novel "lightweight block cipher named LRBC" to constrict Internet of Things resources. By integrating Feistel and substitution-permutation networks (SPN), the proposed structure has been implemented, which takes advantage of

both techniques. To resist linear and differential attacks, LRBS produces a high quantity of extinct S-boxes. Guruprakash and Koppu [30] carried out an empirical investigation to showcase that the "Edwards curve digital signature algorithm (EdDSA)" can serve as a performance-enhancing alternative to the "elliptic curve digital signature algorithm (ECDSA)" in the context of Blockchain and IoT. Tanweer Alam [31] introduced "IBchain", an IoT and blockchain-integrated system that can be used for secure communications in a smart city network.

Various state-of-the-art methods for securing the IoT network have been provided in the literature, with their advantages and limitations. Many researchers addressed blockchain-based solutions in their unique and specific proposed methods. However, these studies lack validation and comparative analysis with other applicable modern cryptographic algorithms. To address this research gap, a comparative analysis of blockchain with modern cryptographic techniques is provided in this research, using the Avalanche effect as a parameter to observe the significant changes in the hash value.

5 IoT management in blockchain

The management of IoT devices in blockchain technique offers essential information to the significant structured layer and works on the controllable components of the systems. Figure 3 illustrates the structured layer of blockchain-based IoT management. The four major components of

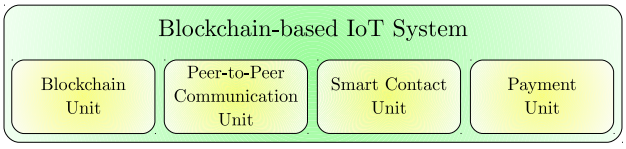

Figure 3: IoT Management in Blockchain

this structured layer are represented as:

- **Blockchain Unit:** It manages useful information and blockchain activities. All kinds of ledger data and information are used by this part. It contains three sub-units:
  1. Blockchain of things,
  2. Microservice for blockchain,
  3. Smart contracts.

  The microservice index contains information about smart contracts.

- **Peer-to-peer Communication Unit:** Data communication, exchange, and transfer are facilitated by this component with the help of peer-to-peer network technology. The management process related to the blockchain of things is also controlled by this component.

- **Smart Contract Unit:** The function and process required for smart contracts defined by the system are provided by this component. The blockchain unit is responsible for storing smart contract codes and information. The smart contracts are capable of processing the mechanism of the system.

- **Payment Unit:** All the payment processes and transactions are supported by this unit in cooperation with the structured function layer and other components of the IoT device management layer. The wallet information of the user and IoT devices is also managed by this unit.

6 Proposed method

In cryptographic analysis, the avalanche effect is basically a mathematical function applied to the encryption technique, and it is evaluated as the most preferable attribute of the encryption algorithm. The avalanche effect presents a considerable change in the ciphertext if a few changes are made in either the plaintext or key. This basic property is known as the avalanche effect in cryptography. Generally, it measures the quantity of effect on the ciphertext concerning minor alterations made to the key or the plaintext.

The method is to consider fixed-length inputs to the hash function f. Otherwise, it is problematic what probability distribution it wants to impose on the input set $\{0,1\}^*$ which is the collection of all finite input strings. In practice, hash functions do have an upper limit on the input string, but that's astronomical, in terms of testing all input strings. The simple explanation of the Avalanche Effect is that "A small change in the plaintext (or key) should create a significant change in the ciphertext". Concerning these characteristics, "Data encryption standard (DES)" has been proven to be significantly strong.

So, let's assume the hash function has a security parameter of k bits. This corresponds to the function acting like a random function with outputs of length $n = 2k$ bits.

The testing would generate numerous random values from a uniform distribution on $\{0,1\}^m$, thus treating the hash function as a random function $f : \{0,1\}^m \to \{0,1\}^n$. Let this random set of inputs be denoted by X. Now define

$$a_{ij} = \#\{x \in X : [f(x \oplus e_i)]_j \neq [f(x)]_j\} \tag{1}$$

for $1 \leq i \leq n, 1 \leq j \leq m$, where e_i is the vector with a one in the i^{th} position and zeroes everywhere, and $[u]_j$ denotes the j^{th} component of vector u. a_{ij} counts the number of inputs from X that differ in the j^{th} output bit when the i^{th} input bit is flipped.

It can now be defined as a degree of strict avalanche criterion, $D_{\text{SAC}}(f)$ as

$$D_{\text{SAC}}(f) := 1 - \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{\| \frac{2a_{ij}}{\#X} - 1 \|}{nm} \tag{2}$$

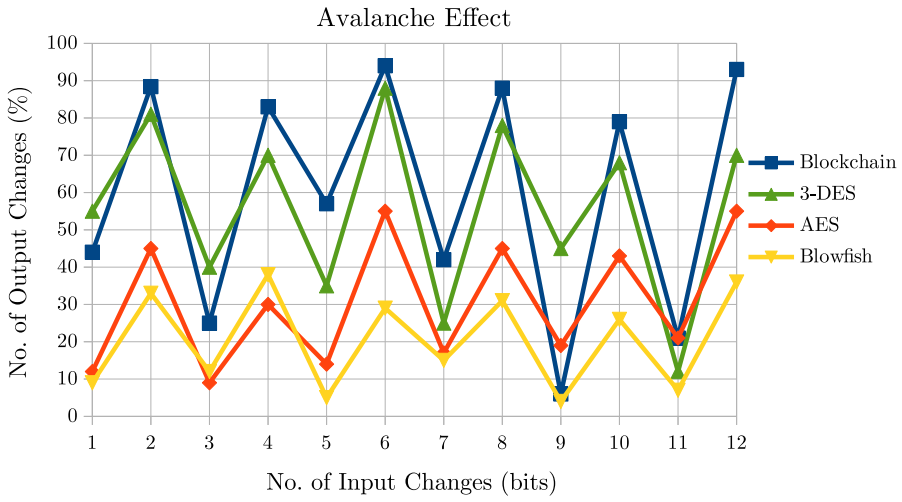

Figure 4: Avalanche Effect on Cryptographic Algorithms

with the expectation that $D_{\mathrm{SAC}}(f)$ should be approximately 1, i.e., the sum of the absolute differences. A modification in a single bit of plaintext or key generates a significant modification in many bits at the ciphertext outcome; this is well known as the Avalanche effect.

$$\text{Avalanche Effect} = \frac{N_c}{N_{p|k}} \tag{3}$$

where, N_c is the number of bit changes in ciphertext and hash, whereas $N_{p|k}$ is the number of bit changes in plaintext or key in the IoT-generated data. The Avalanche effect hash function is presented in Figure 5.

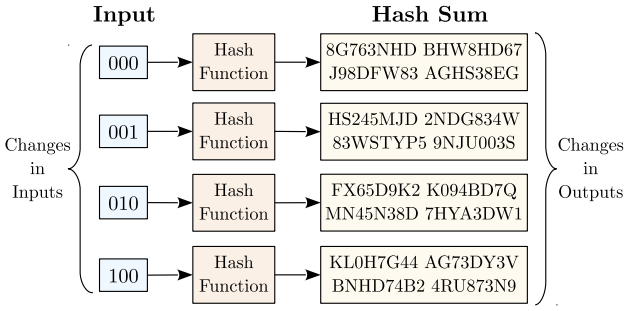

Figure 5: Avalanche Effect Hash Function

7 Result analysis

After a successful simulation, the test result shows the outcome of the Avalanche effect. Similar and uniformly small changes were made to the input value of plaintext or key (IoT-generated data), and the hash functions generated a hash sum as the output. For testing purposes, three cryptographic encryption methods are considered "Triple Data Encryption Standard (3-DES), Advanced Encryption Standard (AES), and Blowfish", along with the blockchain method. A desirable attribute of any encryption technique is that some minor modification in either plaintext generated from IoT devices or the key must generate a considerable difference in the ciphertext output and its associated hash value. The simulation result is presented in Figure 4. The Avalanche effect as a significant change in hash value is presented in the Table 1, which shows the percentage of output changes in hash with respect to the number of input bits changes for Blowfish, AES, 3-DES, and Blockchain. Table 1 is basically a numeric representation of the simulation result (Figure 4).The quantity of changes in the percentage of hash output depends on the cryptographic algorithms and the changes in the number of input bits. Table 1 definitely shows that the blockchain presents high percentages of variations in hash output as compared to other cryptographic methods, as 1–2 bits changes in input affect 9%–33% changes in a hash using Blowfish, 12%–45% for AES, 55%–81% for 3-DES, and 44%–88.4% for Blockchain. Similarly, when changing 11–12 bits in input, the percentage of changes in hash output for Blowfish is 7%–36%, for AES it is 21%–55%, for 3-DES it is 12%–70%, and for Blockchain it is 21%–93% as the highest changes. The blockchain percentage may not vary uniformly with the increment in the number of inputs because the avalanche effect is basically a ratio of the number of bit changes in ciphertext or hash to the number of bit changes in plaintext or key. The significance of the result is considered based on the maximum percentage of variation in the hash for the blockchain. The result shows the high avalanche effect of blockchain as compared to Triple-DES, AES, and Blowfish. Significantly, the maximum changes in the bits of ciphertext can be observed in the blockchain method as compared to other cryptographic techniques. A blockchain-based IoT network is more secure for non-trusting device-to-device communications and transactions.

Our objective is to present a method for efficient and trustworthy P2P communications and transactions in a blockchain-based distributed IoT network for non-trusting D2D communication without a centralized 3rd party.

Table 1: Avalanche Effect on Cryptographic Algorithm

No. of Input Bits Changes	Output Changes (%)			
	Blowfish	AES	3-DES	Blockchain
1–2	9%–33%	12%–45%	55%–81%	44%–88.4%
3–4	12%–38%	9%–30%	40%–70%	25%–83%
5–6	5%–29%	14%–55%	35%–88%	57%–94%
7–8	15%–31%	17%–45%	25%–78%	42%–88%
9–10	4%–26%	19%–43%	45%–68%	6%–79%
11–12	7%–36%	21%–55%	12%–70%	21%–93%

Changes made by intruders in IoT-generated data can be validated using the Avalanche effect, and blockchain-based integrity can be provided by using the proposed model.

8 Conclusion and future work

This research presents a significant peer-to-peer distributed IoT network based on blockchain technology for secure and efficient non-trusting device-to-device communication and transaction. Manipulating and integrating the IoT network with blockchain modeled a secure system successfully. The model presents a modern blockchain technique to surpass the traditional security system for efficient and secure IoT deployment under various conditions. Finally, to validate the signification of blockchain in the IoT network of non-trusting device-to-device communication, the avalanche effect is calculated and compared with Triple-DES, AES, and Blowfish cryptographic algorithms using IoT-generated data. The result presents significant output changes in hash for the blockchain IoT integrated model as compared to other cryptographic algorithms. Using the Avalanche effect calculation, the hash function with the encryption technique of blockchain can significantly provide strength to the IoT network, as proven by the security level validation.

The proposed work can be applied to applications based on intrusion detection techniques. This work can be extended by comparing blockchain with other hybrid cryptographic methods. In the future, using the Avalanche effect, the validation assessment can be done in the fog/edge computing model as well as on a cloud server. The avalanche effect assessment is an engrossing process to notice the IoT-generated data processing techniques of blockchain that can be enhanced for validity checking in other applications such as banking, financial, business, and industrial transactions.

References

[1] P. Cui, U. Guin, A. Skjellum, and D. Umphress, "Blockchain in iot: Current trends, challenges, and future roadmap," *Journal of Hardware and Systems Security*, vol. 3, no. 4, pp. 338–364, Dec 2019. doi: https://doi.org/10.1007/s41635-019-00079-5

[2] P. Rathee, *Introduction to Blockchain and IoT*. Singapore: Springer Singapore, 2020, pp. 1–14. doi: https://doi.org/10.1007/978-981-13-8775-3_1

[3] V. Gatteschi, F. Lamberti, and C. Demartini, *Blockchain Technology Use Cases*. Singapore: Springer Singapore, 2020, pp. 91–114. doi: https://doi.org/10.1007/978-981-13-8775-3_4

[4] C. Davila and J. Tarnow, *The Blockchain in IoT*. Cham: Springer International Publishing, 2019, pp. 269–296. doi: https://doi.org/10.1007/978-3-319-99516-8_10

[5] M. H. Miraz, *Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies*. Singapore: Springer Singapore, 2020, pp. 141–159. doi: https://doi.org/10.1007/978-981-13-8775-3_7

[6] G. Pulkkis, J. Karlsson, and M. Westerlund, *Blockchain-Based Security Solutions for IoT Systems*. John Wiley & Sons, Ltd, 2018, ch. 9, pp. 255–274. doi: https://doi.org/10.1002/9781119456735.ch9

[7] A. Erdem, S. Ö. Yildirim, and P. Angin, *Blockchain for Ensuring Security, Privacy, and Trust in IoT Environments: The State of the Art*. Cham: Springer International Publishing, 2019, pp. 97–122. doi: https://doi.org/10.1007/978-3-030-18075-1_6

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *https://www.bitcoin.org*, 03 2009.

[9] S. Van Hijfte, *Blockchain Platforms: A Look at the Underbelly of Distributed Platforms*. Morgan & Claypool, 2020. doi: https://doi.org/10.2200/S01022ED1V01Y202006CSL011

[10] S. S. Shetty, C. A. Kamhoua, and L. L. Njilla, *Blockchain for Distributed Systems Security*. Wiley-IEEE Press, 2019, pp. 205–232. doi: https://doi.org/10.1002/9781119519621.ch10

[11] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. O'Reilly Media, 2015.

[12] G. Fiorentino, C. Occhipinti, A. Corsi, E. Moro, J. Davies, and A. Duke, *Blockchain: Enabling Trust on the Internet of Things*. John Wiley & Sons, Ltd, 2020, ch. 11, pp. 141–157. doi: https://doi.org/10.1002/9781119545293.ch11

[13] K. Haseeb, I. Ud Din, A. Almogren, N. Islam, and A. Altameem, "Rts: A robust and trusted scheme for iot-based mobile wireless mesh networks," *IEEE Access*, vol. 8, pp. 68 379–68 390, 2020. doi: https://doi.org/10.1109/ACCESS.2020.2985851

[14] Y. Chen, L. Wang, and S. Wang, "Stochastic blockchain for iot data integrity," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 373–384, 2020. doi: https://doi.org/10.1109/TNSE.2018.2887236

[15] C. K. Pyoung and S. J. Baek, "Blockchain of finite-lifetime blocks with applications to edge-based iot," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2102–2116, 2020. doi: https://doi.org/10.1109/JIOT.2019.2959599

[16] D. Mazzei, G. Baldi, G. Fantoni, G. Montelisciani, A. Pitasi, L. Ricci, and L. Rizzello, "A blockchain tokenizer for industrial iot trustless applications," *Future Generation Computer Systems*, vol. 105, pp. 432–445, 2020. doi: https://doi.org/10.1016/j.future.2019.12.020

[17] K. Lei, M. Du, J. Huang, and T. Jin, "Groupchain: Towards a scalable public blockchain in fog computing of iot services computing," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 252–262, 2020. doi: https://doi.org/10.1109/TSC.2019.2949801

[18] K. D. Muthavhine and M. Sumbwanyambe, "An analysis and a comparative study of cryptographic algorithms used on the internet of things (iot) based on avalanche effect," in *2018 International Conference on Information and Communications Technology (ICOIACT)*, 2018, pp. 114–119. doi: https://doi.org/10.1109/ICOIACT.2018.8350759

[19] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018. doi: https://doi.org/10.1109/JIOT.2018.2812239

[20] Y. Mirsky, T. Golomb, and Y. Elovici, "Lightweight collaborative anomaly detection for the iot using blockchain," *Journal of Parallel and Distributed Computing*, vol. 145, pp. 75–97, 2020. doi: https://doi.org/10.1016/j.jpdc.2020.06.008

[21] A. Yohan and N.-W. Lo, "Fotb: a secure blockchain-based firmware update framework for iot environment," *International Journal of Information Security*, vol. 19, no. 3, pp. 257–278, Jun 2020. doi: https://doi.org/10.1007/s10207-019-00467-6

[22] H. Li, L. Pei, D. Liao, X. Wang, D. Xu, and J. Sun, "Bddt: use blockchain to facilitate iot data transactions," *Cluster Computing*, May 2020. doi: https://doi.org/10.1007/s10586-020-03119-w

[23] H. Liu, D. Han, and D. Li, "Fabric-iot: A blockchain-based access control system in iot," *IEEE Access*, vol. 8, 2020. doi: https://doi.org/10.1109/ACCESS.2020.2968492

[24] G. Rathee, A. Sharma, R. Kumar, and R. Iqbal, "A secure communicating things network framework for industrial iot using blockchain technology," *Ad Hoc Networks*, vol. 94, p. 101933, 2019. doi: https://doi.org/10.1016/j.adhoc.2019.101933

[25] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A puf-based secure communication protocol for iot," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 3, Apr. 2017. doi: https://doi.org/10.1145/3005715

[26] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002. doi: https://doi.org/10.1126/science.1074376

[27] G. Wang, Z. Shi, M. Nixon, and S. Han, "Chainsplitter: Towards blockchain-based industrial iot architecture for supporting hierarchical storage," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 166–175. doi: https://doi.org/10.1109/Blockchain.2019.00030

[28] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trustchain: Trust management in blockchain and iot supported supply chains," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 184–193. doi: https://doi.org/10.1109/Blockchain.2019.00032

[29] A. Biswas, A. Majumdar, S. Nath, A. Dutta, and K. L. Baishnab, "Lrbc: a lightweight block cipher design for resource constrained iot devices," *Journal of Ambient Intelligence and Humanized Computing*, Jan 2020. doi: https://doi.org/10.1007/s12652-020-01694-9

[30] J. Guruprakash and S. Koppu, "An empirical study to demonstrate that eddsa can be used as a performance improvement alternative to ECDSA in blockchain and iot," *Informatica (Slovenia)*, vol. 46, no. 2, pp. 277–290.

[31] T. Alam, "Ibchain: Internet of things and blockchain integration approach for secure communication in smart cities," *Informatica (Slovenia)*, vol. 45, no. 3, pp. 477–486.