International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

IoT Based Blockchain Methods for Data Association Technique for Secure Intelligent Contract

C. Sathish[1*], C. Yesubai Rubavathi[2]

Submitted: 25/05/2023 **Revised**: 17/07/2023 **Accepted**: 30/07/2023

Abstract: IoT data association based on blockchain smart contracts solves the problems of difficulty in confirming ownership of personal data, quantitative tracking of data assets and inability to efficiently complete value transfer in IoT systems. Transfer the right of control and control from the equipment manufacturer to the user to confirm the ownership of personal data; store the equipment status and data hash value in the blockchain through technologies such as full life cycle management and digital signatures to ensure the reliability of the data; use intelligent The contract construction goes to a third-party data trading platform to ensure the security of data sharing, and to easily complete data realization and data value transfer. The quantitative analysis results of attack possibility and attack success probability show that blockchain smart contract technology can provide defense against data Tampering, eliminating trust problems in data transactions. With the help of blockchain innovative contract technology, physical Internet data can be capitalized initially, and the data value transfer and sharing of Internet of Things devices can be promoted.

Keywords*: Blockchain; Smart Contract; Internet ofThings; Data Association; Data Confirmation*

1. Introduction

With the development of sensor-related technologies, hardware costs continue to decrease, and various IoT devices are becoming more and more popular. Therefore, IoT big data has extremely high potential value and is an important asset. Data assets are controllable, measurable, reliable, and reliability [1-2]. Controllability means that data assets have legal control and use rights, and measurability means that data assets have reliable measurement methods; reliability implies that data assets are traceable, falsifiable, and analyzable. Mobility refers to the possibility of data assets being converted into economic benefits. Equipment manufacturers mainly provide the IoT data storage solutions commonly used by users. Cloud storage service has the advantages of low price, convenient deployment, easy management, etc., but there are problems.

1) It is challenging to confirm personal data rights [3]. The data holder is usually the equipment manufacturer rather than the user. As a result, the user's request to consent, right to know, right to objection and other rights are deprived, and generally, only have the right to access data.

2) Data reliability is poor and unfalsifiable, and device manufacturers have absolute control over cloud storage databases and can tamper with user data or fabricate false data. As a result, it is difficult for relevant researchers and device manufacturers to maintain data trust relationships.

3) Data cannot be shared and cannot be monetized. Users can only use the service support provided by the device manufacturer and cannot share the data with other data collectors for a fee.

4) It is challenging to protect user privacy. There is usually a solid binding relationship between data and personal information use, and there is a risk of personal information leakage. The risk of privacy leakage seriously affects users' enthusiasm for data sharing and destroys the ability to monetize data assets.

Blockchain is a trustless, decentralized distributed ledger technology with transparency, reliability, tamper-proof, traceability, and high reliability. It is expected to solve extensive data management, trust, security, and key privacy issues [4]. Domestic and foreign scholars and related research institutions have researched applying blockchain technology to the Internet of Things and extensive data security. Author [5] to realize functions such as data privacy protection and data sharing, using blockchain technology and distributed hash table (distributed hash table, DHT) storage method to build a user data rights management system. Author [6] used smart contracts to make a distributed management system to manage each centralized electronic Medical database to promote data sharing among medical

[1]*Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering, Bodinayakanur, Tamil Nadu, India*
[2]*Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India*
Emails: [1]*sathishgcebodi@gmail.com,* [2]*yesubaicharles@gmail.com,* [3]*ayanlehassen@kdu.edu.et*
**Corresponding Author: C. Sathish[1] (sathishgcebodi@gmail.com)*

institutions. The above studies have discussed using blockchain to achieve data sharing and privacy protection, but they have not covered how to realize data capitalization. Author [7] proposed a new type of e-commerce model developed, which uses the blockchain to exchange IoT coins to trade with IoT devices to realize the transaction of intelligent devices and IoT data to third parties. Still, data reliability cannot be guaranteed, and the value transfer of personal data is limited. Nature IBM pointed out in the Internet of Things white paper [8] that "decentralized autonomous Internet of Things" can be realized by using blockchain technology to eliminate trust requirements facilitate transaction processing and device interaction, but does not mention how to reflect the value of device data. And realize the association of equipment data. This research proposes a method of IoT data association based on blockchain technology. Uploading data uniformly through the device signature transmission protocol provides a data value measurement method and saves the data in the user's local or decentralized database. , to confirm the rights of personal data; through the equipment life cycle management contract, provide IoT devices with whole life cycle event storage from the factory [9], provide falsification for device data, and enhance data reliability; through IoT data, The order contract provides data collection methods for value exchange for data demanders such as research institutions, and realizes the capitalization of equipment data.

2. Technical Basis

Blockchain technology has the typical characteristics of distributed peer-to-peer, chained data blocks, anti-forgery, anti-tampering, high transparency and high reliability [4], and solves the Byzantine general problem through distributed node verification and consensus mechanism [10], and a decentralized, trustworthy system can be built without trusting a single node [11]. Integrating the advantages of blockchain technology with the Internet of Things helps protect user rights, improve data reliability, promote data interoperability, achieve high efficiency and stability and Reliable IoT data association method.

Smart contracts are a series of state full on-chain codes deployed on the blockchain, with the characteristics of immutability, decentralization, and autonomy. The code and state information are stored on the blockchain, triggered by transaction events, and in all, it runs on the nodes. After all, nodes generate consensus results, the state information changes caused by the consensus results are recorded on the blockchain. The code and status of intelligent contracts are obtained through the blockchain, which can be copied and verifiable. The general characteristics of blockchain such as trustworthiness; the code runs on all nodes together, there is no central server, and it has the features of decentralization; the intelligent contract controls and manages the intellectual assets according to the pre-agreed trigger conditions and operating mechanism, and does not require any first The power of the three-party organization has the characteristics of autonomy. The use of smart contracts can eliminate third-party organizations such as intermediate platforms, transfer, and store and send ether and tokens and other valuables, manage assets on the chain, and realize programmable and automated assets Management systems [11-13].

Bitcoin is the earliest and most influential application of blockchain technology. The scripting language of the Bitcoin blockchain can realize intelligent contracts to a certain extent, but it lacks Turing completeness and cannot realize the method of IoT data association design. It is risky to build a new blockchain, especially when the initial total computation amount is small; attackers with the highest amount of malicious computation can freely generate branches and harmful data. The complete analysis of a stable blockchain the amount is extensive, it is difficult for attackers to create computational advantages in IoT-based e-healthcare [14-17], and the risk is relatively small. In case of IoT based e-healthcare system, patients are provided health services in smart manner. Internet of thing component such as sensor, controller and actuator works in coordination to provide healthcare services. Ethereum is the first Turing-complete blockchain intelligent contract platform [12]. The entire network has a huge computational load and many nodes. Strong network effect developers can freely define the ownership rules, transaction methods and state transition functions of smart contracts on the Ethereum blockchain to realize intelligent contracts that are more powerful than Bitcoin scripts. The Ethereum blockchain in this study is, For example, to design and implement a decentralized, trustless IoT data asset method.

3. Scheme Design and Implementation

The IoT data association solution generates a pair of public key and private critical addresses based on an elliptic curve digital signature algorithm (ECDSA) [15] for device manufacturers, users, devices and data collectors. It converts the public key. The address is used as the unique identifier for accessing the smart contract. The solution system consists of the device signature transmission protocol, the device life cycle management contract, and the IoT data order contract. The overall structure is shown in Figure 1. The device signature transmission protocol is responsible for receiving the data of the device, packaging the metadata into unit data with device signatures that can be shared; the device life

cycle management contract is responsible for recording the factory, binding and data generation of the device, and provides data falsification services for data collectors; IoT data order contract Responsible for receiving order applications from data collectors, and providing users with revenue extraction services after data assets are realized.

3.1 Device Signature Transfer Protocol

The device signature transfer protocol (DSTP) can unify data, transfer data ownership to users, and realize the controllability and measurability of data assets. To ensure data reliability, when the device transmits data, It is necessary to add a $DSTP_{header}$containing the device signature and basic information of the data to the data. This study takes the mobile client's acquisition of data ownership as an example to illustrate the characteristics of DSTP.

1) Data is transmitted through 2 communication channels. To avoid sending data to the device manufacturer when the device is directly connected to the Internet, the machine uses Bluetooth or the TCP protocol in the local area network to connect to the mobile client.

2) The data is stored using compound ($DSTP_{header}$, data) two-tuple. The $DSTP_{header}$ in the two-tuple is the $DSTP_{header}$ generated by the device; data is the data provided by the device, which can be either json format data supplied by the device or word Data in throttling format. DSTP requires equipment manufacturers to publish the data parsing method on the public network so that other organizations can parse the data.

3) The device needs to provide a digital signature for the data to ensure reliability of the data. The data storage capacity of the device itself is limited, and there are two main data transmission methods when transmitting complete data packets: one-time complete transmission (such as medical equipment) and continuous transmission (e.g. treadmill or power bike). DSTP requires devices with different data transmission methods to provide digital signatures in different ways. The SHA-256 algorithm [16] is used for hashing. The hash value is signed with the device's private key. The signature and basic data information are packaged into a $DSTP_{header}$. The metadata is transmitted to the mobile client together. When the device uses the continuous transmission mode, only the hash value of the basic information of the data needs to be signed, the metadata is continuously transmitted, and the $DSTP_{header}$ is regularly sent to the mobile client. Sort and package the metadata and $DSTP_{header}$ generated within a period into data packets. After collecting the data packets, the mobile client constructs a Merkle tree [17] and saves the Merkle tree in the $DSTP_{header}$of each data packet pass-through.

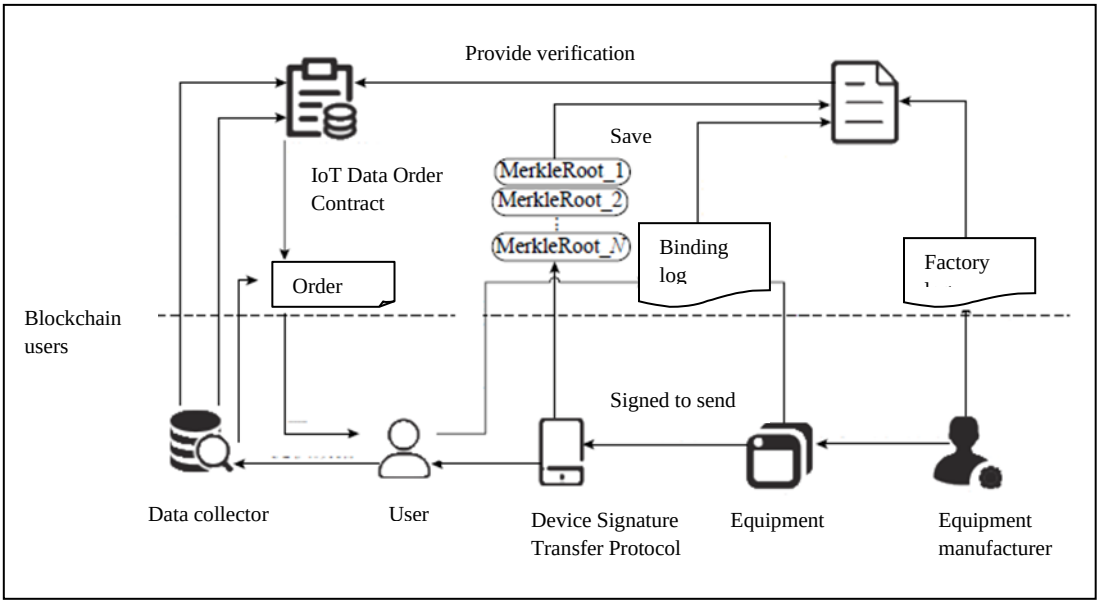


Fig 1: Overall architecture of IoT data association system

Protocol 3 in Section 3.2 saves the root node (MerkleRoot) of the Merkle tree in the device life cycle management contract. The expression is:

$$\omega = \mu \frac{(COST_{Save} + \delta COST_{transaction})}{pkgPrice};\ \mu > 1 \quad (1)$$

In the formula: is the cost of saving the root node of the Merkle tree into the device life cycle management contract; is the cost of submitting the receipt when the data collector is used to trading the IoT data order contract; is the value of a single data package; and δ are coefficients, which are dynamically set according to different data and order details.

3.2 Equipment Lifecycle Management Contract

The device life-cycle management contract (DLMC) requires device manufacturers, users and devices to complete protocols such as delivery and binding through the public key address and provide authenticity for the data according to the data stored in the intelligent contract Verification ensure the reliability of data assets. After the compound (qk^n_{add},qk^e_{add}) device leaves the factory, the device manufacturer generates a pair of public and private keys for the device and saves it in the machine next, call the intelligent contract interface to protect the binary team in the smart contract generate a factory log with the device address as the index. As shown in Protocol 1, m is the device manufacturer, you are the user, and e is the device. The map is the mapping search operation using the public key address, qksig is the digital signature operation, qkadd is public key address, even leave is the generated factory log, and indexed means that the attribute is used as an index to search the catalogue.

Protocol 1 Leave Factory

1. Procedure Leave Factory(n; contract;d)
2. m executes:
3. generate a keyPair ⟶
4. $qk^n_{sig}\ (qk^n_{add},qk^e_{add}) \rightarrow contract$
5. contract executes：
6. if map (qk^n_{add},qk^e_{add}) =ϕ then
7. add compound
8. end if
9. returnevent$_{leave}$ ($qk^e_{add}, (indexed)qk^e_{add}$)
10. end procedure

The user sends the random number nonce and the user's public key address generated by the smart contract to the device. The device uses the device's private key to sign the user's public key address and random number nonce. After the smart contract verifies the device signature, it changes the binding state. Two-tuple compound generates a critical log (event$_{bind}$) with the device address as the index, as shown in Protocol 2. It should be noted that when the device is a shared device in public places such as gyms and hospitals, the relationship between the user and the device is frequently changed and does not need to be Binding is carried out. Therefore, reliability is guaranteed by the device signed transmission protocol.

Protocol 2 User Bind to the Device

1. Procedure BindDevice(u, contract, e)
2. u executes :
3. qk^e_{add} ⟶ e
4. e execute :
5. compound $(qk^n_{add},qk^e_{add}) \rightarrow contract$
6. contract executes：
7. if map $(qk^n_{add},qk^e_{add}) \neq \phi$ then
8. generate a nonce→ $contract$ e
9. end if
10. e executes :
11. $qk^n_{add}(qk^e_{add}, \text{nonce}) \rightarrow contract$
12. contract executes：
13. change compound (qk^n_{add}, qk^e_{add})
14. return$event_{bind}(qk^n_{add}, (indexed), qk^e_{add})$
15. end procedure

After the user obtains a certain amount of data, he takes out the hash value of the last data, and the current hash number from the smart contract hashes the two and the root node of the Merkle tree of the current packet list (qkg) and obtains the current hash value. The value is stored in the smart contract. The smart contract will save the hash value and blockchain timestamp, as shown in Protocol 3, is the user public key corresponding to the device public key in the device binding log, and is the data packet the root node of the Merkle tree of the list. According to the hash number in the data packet, the hash value of the current data packet (hash$_{qkg}$) and the last hash value (hashlast$_{qkg}$) can be obtained from the smart contract to verify whether the current data packet has been tampered with.

Protocol 3 Save Data Hash

1. Procedure SaveHash(v; contract)
2. v executes :
3. generate a MerkleRoot$_{Pkg}$
4. $qk^v_{sign}(qk^n_{add},qk^e_{add}) \rightarrow contract$
5. contract executes：
6. if map $(qk^n_{add},qk^e_{add}) = compound.qk^v_{sign}$ $=qk^v_{sign}$ then
7. (hash$_{lastqkg,\ Indexed}$) → u

8. end if
9. v executes :
10. SHA-256($hash_{lastPkg}$; Index; $MerkleRoot_{Pkg}$)→ hashPkg
11. $hash_{Pkg}$→ Contract
12. return Index
13. end procedure

After recycling and destroying the equipment, the equipment manufacturer is recommended to visit.A smart contract that sets the device state to be invalid and uses the device's private the critical address generates a destruction log for the index.

3.3 IoT Data Order Contract

The device signature transfer protocol can transfer data ownership, provide a unified data format, and realize the controllability and measurability of data assets [26]. The device life cycle management contract offers an endorsement for data reliability through the entire life cycle certification of the storage device after it leaves the factory. Based on the first two, this method can realize the Internet of Things data order contract (IoTDOC) and provide the monetization for the data [24].

As shown in Figure 2, the data collector generates a pair of Ethereum public and private keys and uses this public key address to register on the IoT-DOC; when the data collector needs the data generated by a particular device, on the IoT-DOC Publish an order message. As shown in Figure 2, the address of the IoT data order contract and the amount of the deposited deposit are shown. As shown in Figure 3, after the user obtains the device, first generate a pair of Ethereum public and private keys; then bind with the device; the user checks the order that can be submitted with the device he owns and sends a data packet to the address provided by the order. Because the data is large, it is generally not transmitted through the smart contract but uploaded through the HTTP protocol.

The data collector creates a set of Ethereum public and private keys and registers on the IoT-DOC using this public key address. When the data collector wants the data produced by a certain device, they utilise the IoT-DOC. Publish a message with an order, as seen in Figure 2. Figure 3 displays the location of the IoT data order contract as well as the deposit amount. The user examines the order that may be submitted with the device he possesses and transmits a data packet to the address supplied by the order after first creating a pair of Ethereum public and private keys and binding with the device. Due to its size, data is typically uploaded over the HTTP protocol rather being transferred via the smart contract.

As shown in Figure 4, when the device leaves the factory, the device developer will register the device in the smart contract to generate the factory log; when the user binds the device, the binding record will be developed in the smart contract; after the data, collector obtains the data, according to the factory log Verify the data source with the binding log, verify the reliability of the data according to the data DSTP header and the DLMC contract, after confirming the data reliability, send a receipt to the IoT-DOC contract to confirm receipt of the data. Only when the data collector sends a ticket to the contract after that, the agreement will transfer the data deposit to the user account. At this time, the contract will generate a submission log indexed by the device address, and the log information is shown in Figure 4. As shown in Figure 3, the user is receiving after the log prompts, it is learned that the data collector has fulfilled the contract and completed the transaction [25]. The following data transmission transaction can be performed.

The IoT data association method uses the mist wallet to imitate the order submission process and uses the web3.js library and web3j library provided by Ethereum to access smart contracts. The web3.js library is a JavaScript library used primarily after the server receives data and completes data verification. , submit the receipt of received data to the blockchain. The web3j library is a Java library, mainly used to access intelligent contracts on Android devices [27].

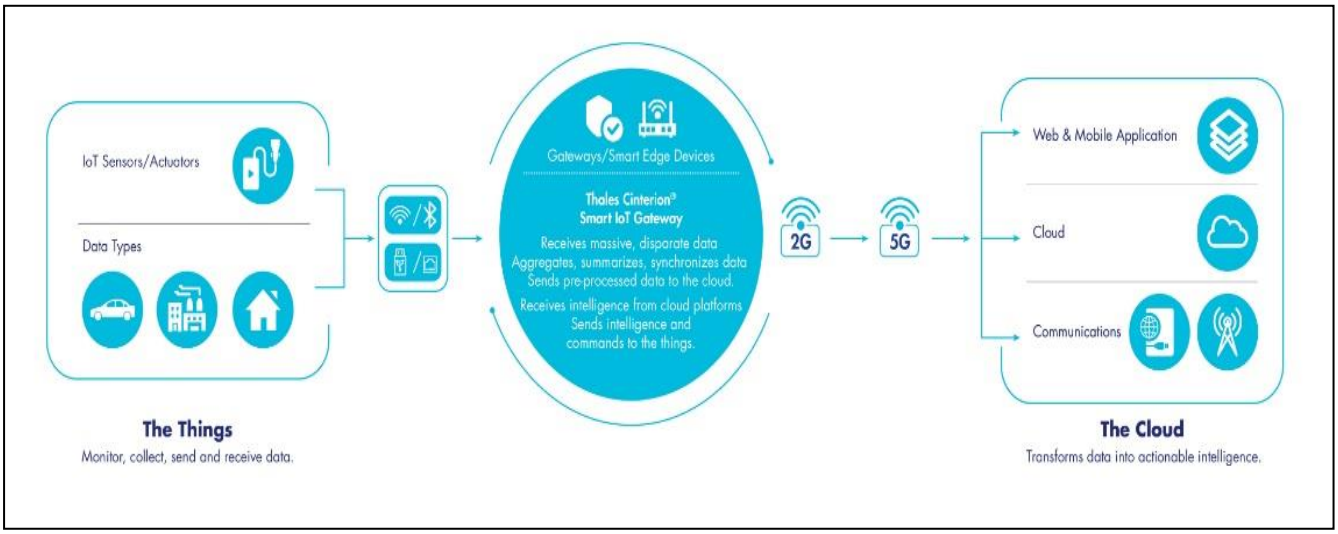


Fig 2: IoT data order contract operation process

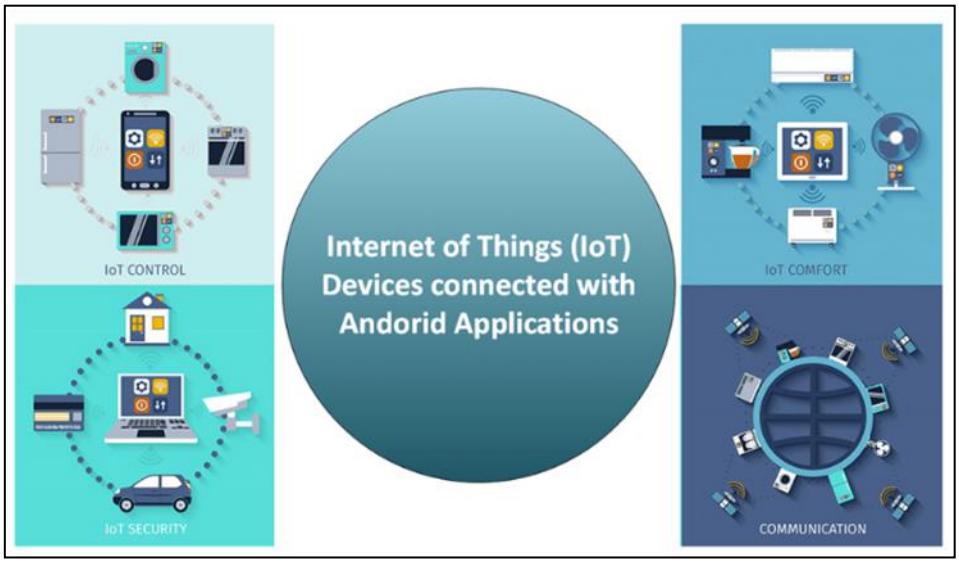


Fig 3: User mobile client implementation of IoT data assetization method

The data collection order can be terminated as soon as possible, the remaining deposit can be recovered, and the public-private key pair can be replaced [28-30]. The device's private key is stored in the device hardware, and a read protection mechanism can be added to the hardware to prevent the private key from being stolen.

4. Analysis of Attack Methods

4.1 Stealing the private key

Stealing the private key means that the attacker obtains the user's private key, the device manufacturer, the data collector, and the device and forges the identities of the four the possibility of taking the private key is relatively slight. If the private key is stolen, the user can transfer the existing assets as soon as possible and replace the public-private key pair to avoid losses; the device manufacturer needs to publish the private critical theft statement to prevent the new factory log from being regarded as Legal; data collectors can terminate the data collection order as soon as possible, recover the remaining deposit, and replace the public-private key pair. The device's private key is stored in the device hardware, and a read protection mechanism can be added to the hardware to prevent the private key from being stolen [31].

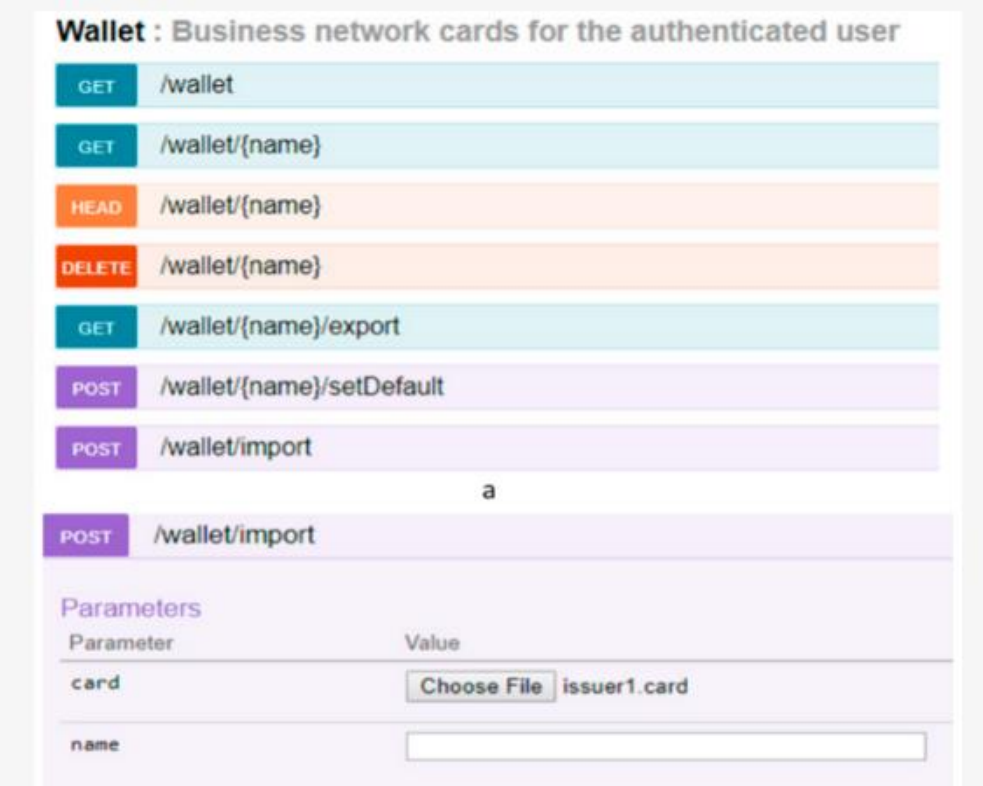


Fig 4 Device life cycle log and transaction log generated by intelligent contract

4.2 Forged signatures

Attackers forge signatures by revealing the signer's private key and other methods and use the forged signatures to gain benefits. When the ECDSA personal key bits are 160, 224, and 256 bits, respectively, use a computer with 1 million instructions per second to crack and crack. The times are 1012, 1024, and 1028 a, respectively. This shows that breaking the 256-bit ECDSA private key requires tremendous computation [18]. Even using a professional machine that calculates the logarithm of the elliptic curve with a cost of 10 million US dollars will take a month. It takes time to calculate the discrete logarithm of the elliptic curve, whose prime order is 2120 [15]. The excellent order of the elliptic curve algorithm used in this blockchain network signature algorithm is slightly less than 2256, and it is almost impossible to calculate by hardware.

4.3 Data tampering

After tampering with the data, the attacker modifies the data hash value stored on the blockchain according to the tampering result of the data, hoping to pass the data reliability verification of the data collector with false data.

Blockchain technology uses a proof-of-work (PoW) consensus mechanism to ensure data consistency for secure intelligent contract. Every valid block needs to add a random value so that the block hash value has a certain number of prefixes of 0. As the number of prefixes 0 increases, miners' difficulty finding random deals increases exponentially, and the CPU power spent to find random values is called workload. The block that finds the random value first will be added to the blockchain and become the latest Blocks. The chain with the most blocks contains the most considerable workload, called the main chain. The number of prefixes 0 increases with the increase of the entire network's computing power, ensuring that the speed of finding random values is a predetermined average [19]. Standard blockchain attacks include double-spend attacks [20] and selfish mining attacks. When an attacker's node computing power exceeds 50% of the entire network's computing power, a double-spend attack can be implemented, tampering with recent blocks and controlling future partnerships. Block; when the attacker’s computing power is greater than 25% of the entire network’s computing power; a selfish mining attack can be achieved, with a high probability of obtaining new block rewards and destroying the fairness of mining [33].

The main threat faced by this system is not double-spending attacks and selfish mining attacks but the tampering of block data. Assuming that the attacker tries to tamper with the data of the hth block before the latest block, the attacker must modify the block hash value and recalculate the hash value of all subsequent blocks. Assuming that the current computing power of honest nodes in the entire network is p hash value calculations

per second, the block hash value under the current calculation difficulty contains g prefixes of binary 0. Attack The attacker is the newly added computing power, and the size of the computing power is q hash value calculations per second [32]. Because the attacker mainly calculates the past blocks and does not affect the generation speed of new blocks, the analysis of the new block hash value the difficulty will not increase. To simplify the calculation, assuming that no new nodes participate, an honest node obtains a new block per second, and the likelihood of an attacker getting a new block is. Therefore, the initial height difference between the attacker and the honest node is set to the height difference of i seconds. The possibility of changing the height difference per second is divided into 3 cases [34].

Event X1: The attacker does not generate a block. The honest node generates a block, plus 1, probability $Q_1 = \frac{q}{2^g}(1-\frac{r}{2^g})$

Event X2: The attacker generates a block,) the honest node does not create a partnership, minus 1, probability $Q_2 = \frac{q}{2^g}(1-\frac{q}{2^g})$

Event X3: When both generate blocks or neither generate blocks, unchanged, probability $Q_3 = 1- Q_1-Q_2$.

The probability distribution of the change in height difference zi+1 per second follows a multinomial distribution:

$$a_{i+1} = \begin{cases} a_i + 1, (Q_1 = \frac{q}{2^g}(1-\frac{r}{2^g}) \\ a_i - 1, (Q_2 = \frac{q}{2^g}(1-\frac{r}{2^g}) \\ a_i, (Q3 = 1 - Q1 - Q2) \end{cases} \quad (2)$$

When = – 1, the attacker successfully catches up with the honest node, can publish the blockchain, and the data tampers successfully. Within seconds, there will be a second high change event, which is set as the number of occurrences of X1; when the tampering is successful, X2 is at least Occurrence times, established as the difference between the actual number of occurrences of event X2 and the minimum number of circumstances, then the exact number of circumstances of X2 is; The probability of being on an honest node is

$$Q_t(h) = \sum_{m=0}^{m_{max}} \sum_{k=0}^{k_{max}} \left(\frac{u!}{m!\,(h+m+1+h)!\,(u-2m-h-1-k)!} \cdot Q_1 m Q_2^{(h+m+1+k)} Q_3^{(u-2m-h-1-k)}\right) \quad (3)$$

As shown in Figure 5, the ordinate is the success probability, the abscissa is the time t, the unit is N, and N is the average value of a new block generated by the honest nodes and time, calculated as.

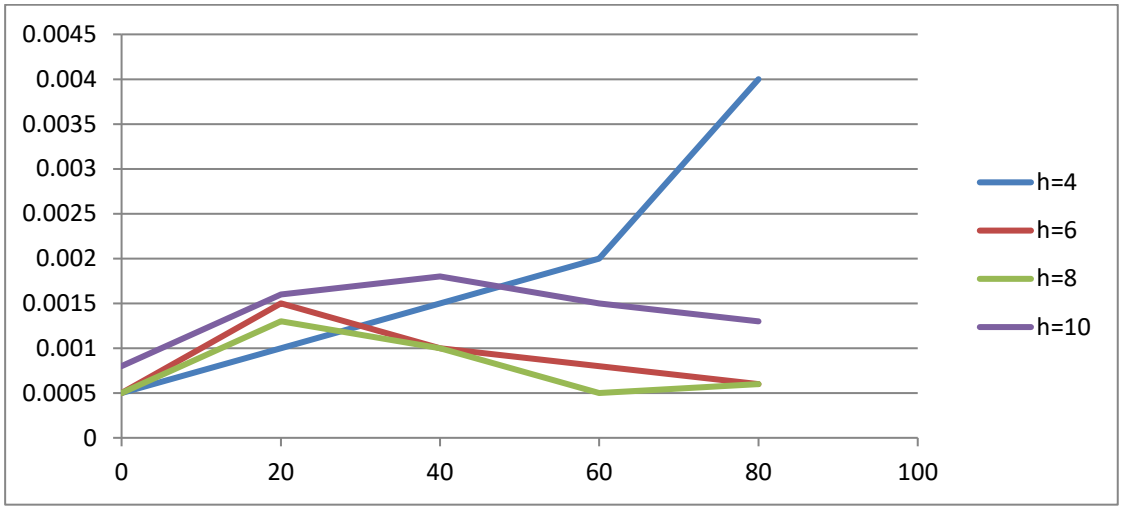
As shown from Figure 5 with table1a and 1b, the probability of the attacker's success decreases with the increase of the depth h of the tampered block. When the computing power of the attacker is less than that of the honest node, the attacker needs to calculate the hash value of h blocks first and then tamper with the union. The success probability gradually increases first and then decreases gradually until it is close to 0; when the attacker's computing power is greater than or equal to the honest node, the probability of successful tampering will gradually increase, but the increase rate becomes smaller. The attacker's computing power and honesty when the computing power of the nodes is equal, the success rate of tampering with blocks is higher. After some time, the success probability approaches 35%; when the computing power of the attacker is 50% of the computing power of the honest nodes, the maximum success probability of tampering with the first four blocks is less than 0.5% for secure intelligent contract. The computing power of Bitcoin and Ethereum is so mighty that it is almost impossible for an attacker to try to reach the same level of computing power as an honest node; even with the ability to achieve this level of computing power, the reward for block mining is much higher than the benefits of tampering with data for secure intelligent contract.

Table 1(a): When the attacker's computing power is 50% of the honest node's computing power

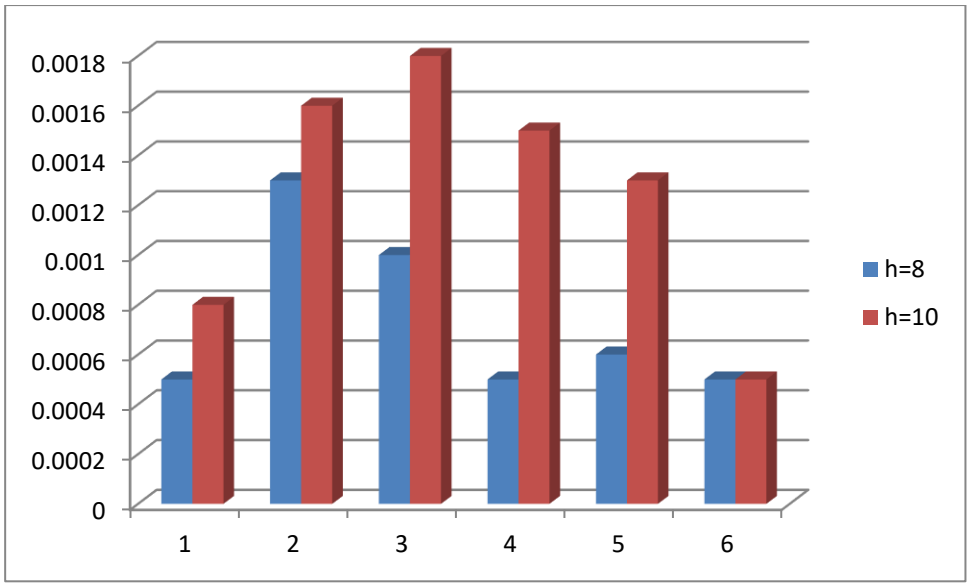
Serial	h=4	h=6	h=8	h=10
0	0.0005	0.0005	0.0005	0.0008
20	0.001	0.0015	0.0013	0.0016
40	0.0015	0.001	0.001	0.0018
60	0.002	0.0008	0.0005	0.0015
80	0.004	0.0006	0.0006	0.0013
100	0.0045	0.0005	0.0005	0.0005

Table 1(b):when the computing power of the attacker is equal to that of the honest nodes

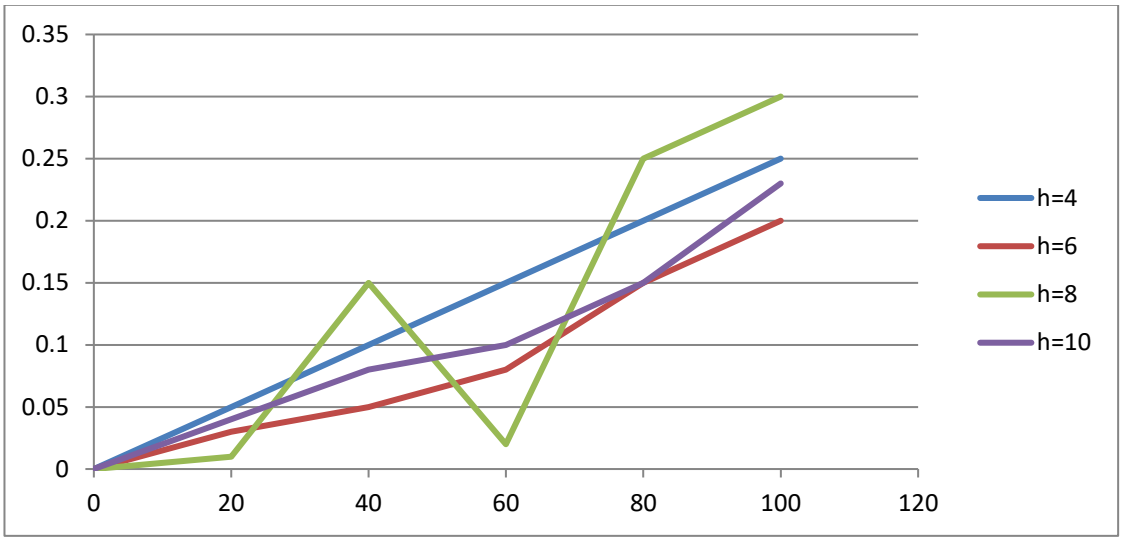
Serial	h=4	h=6	h=8	h=10
0	0	0	0	0
20	0.05	0.03	0.01	0.04
40	0.1	0.05	0.15	0.08
60	0.15	0.08	0.02	0.1
80	0.2	0.15	0.25	0.15
100	0.25	0.2	0.3	0.23



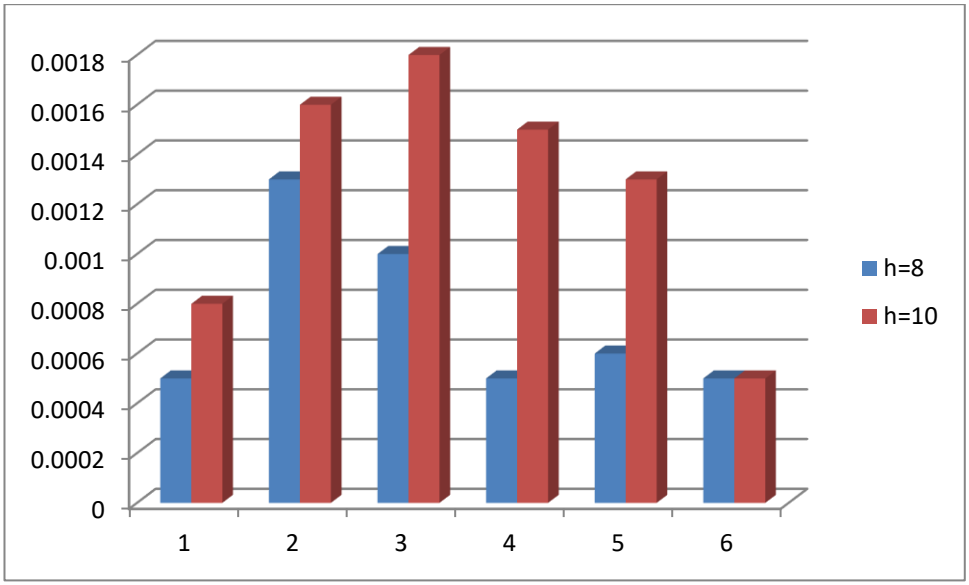
a) When the attacker's computing power is 50% of the honest node's computing power



b) Computing Power Of Most Honest Node



c) When the computing power of the attacker is equal to that of the honest nodes



d) Computing Power Of Most Like Hood Attacker Node

Fig 5 Attacker's success probability of tampering with block data

Honesty and computational prowess of the attacker, the success rate of tampering with blocks is higher when the nodes' compute power is equal. For example, the most excellent success probability of tampering with the first four blocks is less than 0.5% when the attacker's computational power is 50% of the honest nodes. Over time, the success rate reaches 35 %. Even if an attacker could match the processing power of a simple node, the benefits of data tampering would still be far outweighed by the rewards for block mining due to the overwhelming computational power of Bitcoin and Ethereum for secure intelligent contract.

4.4 Data fraud

Data fraud refers to the user changing the device clock and device timestamp, expecting to generate a large amount of false data in a short period for profit [37]. However, the block timestamp is also protected when the user saves the device data hash value in the DLMC contract. Data collectors can compare Block timestamp and data timestamp to verify whether the user forged data.

4.5 Equipment counterfeiting

Equipment counterfeiting means that the equipment manufacturer does not produce the equipment, only generates the public and private key pairs of the equipment, and uses the public and private keys of the equipment to upload forged data. As the equipment manufacturer, the equipment manufacturer is an entity with an entity, and the corresponding factory log on the blockchain has related Entity production records [35]. Therefore, data collectors can check the production records and credit records of the relevant equipment

manufacturers or check the data by checking the equipment factory logs and binding logs to determine whether the equipment manufacturer has committed equipment fraud [39].

4.6 Order Fraud

Order cheating means that the data collector does not submit a receipt to IoT-DOC after accepting the data to collect the data without generating the payment. The data collector submits the ticket to himself, creating the illusion of a large number of transactions [36]. Order cheating is not feasible The reason is that there is a lot of data-related information in the order, such as the total number of submitted data, the number of submissions, etc., and the cost of order fraud is relatively high; when the transaction result does not meet expectations, users will not continue to share data, and data collectors can only collect the data uploaded by the user for the first time, the order fraud outweighs the gain [38].

5. Method Feasibility Discussion

The IoT data capitalization method based on blockchain smart contracts aims to realize data capitalization and protect the rights and interests of individual users. The following discusses the way from four perspectives: data confirmation, data reliability, data realization, and user privacy protection, the Method can meet the requirements.

5.1 Ownership

The device signature transmission protocol collects data in the hands of users, ensures the user's data ownership, realizes the controllability of data assets, and confirms personal data rights. Users can store data locally or encrypt it and store it in a distributed database or other databases. When processing data, the user can choose to send it to the service provider for free to obtain the data analysis service provided by the service provider or send the data to the data collector for a fee through the IoT data order contract to realize data realization.

5.2 Reliability

Suppose the user chooses to share the data for free. The user does not need to save the device information and data packet hash value in the blockchain through the DLMC contract, and the research institution can verify the device signature to ensure essential data reliability. However, suppose the user chooses to share the data for a fee, for data realization. In that case, the device information and data packet hash value must be saved to the blockchain. Furthermore, the hash value and timestamp of the data must be verified through the blockchain to ensure the data's reliability fully.

5.3 Shareability

The data can be shared for a fee through the IoT data order contract, which is convenient for users to realize the data in their hands and the value of the data. Users can obtain benefits by selling data and stimulating users' motivation to generate and share data; relevant research institutions can get data by issuing orders, Expanding the scope and volume of research data.

5.4 Privacy

The data does not contain the user's personal information (mobile phone number, email address, etc.). After the data collector collects the data, it can only judge whether the data source is consistent according to the user's public key address in the data and cannot obtain the user's private information. For unsafe or the public key address of personal information has been leaked, the user can change the public key address to avoid further personal information leakage. When the devices are different, users can use other public and private key pairs to prevent the association between public keys and confidential information. In addition, the data ownership is consistent. For devices with low sexual requirements (for example, health device data requires consistent attribution to have analytical value), users can enhance privacy by regularly replacing public and private key pairs.

6. Conclusion

The use of blockchain smart contracts in IoT data association solves the challenges of validating ownership of personal data, quantitative tracking of data assets, and the inability to efficiently execute value transfer in IoT systems. Based on blockchain innovative contract technology and digital signature technology, this research proposes data production, management and monetization methods centered on equipment signature transmission protocol, equipment life cycle management contract, and IoT data order contract, preliminarily realizing IoT The capitalization of data. The way in this paper can protect users' privacy and data ownership, maintain the authenticity of data, reflect the value of the data itself, and build a secure and reliable data trading platform that does not require third-party guarantees for secure intelligent contract. Users, equipment manufacturers, and a good connection between data collectors promote data sharing among the three and provide more extensive data for prominent research institutions. Future work will be devoted to the use of lightning network technology, plasma scalable autonomous intelligent contracts, an alliance chain and other methods to further reduce the cost of data sharing, establish a distributed data warehouse, and provide distributed data analysis services.

sReferences

[1] J. Ellul and G. J. Pace, "AlkylVM: A Virtual Machine for Smart Contract Blockchain Connected Internet of Things," 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018, pp. 1-4, doi: 10.1109/NTMS.2018.8328732.

[2] H. Cheng, Q. Hu, X. Zhang, Z. Yu, Y. Yang and N. Xiong, "Trusted Resource Allocation Based on Smart Contracts for Blockchain-enabled Internet of Things," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3114438.

[3] N. Zhang, N. Zhao and Y. Qu, "Research on the Integration System of Ubiquitous Power Internet of Things Based on Blockchain Technology," 2020 International Conference on Robots & Intelligent System (ICRIS), 2020, pp. 356-359, doi: 10.1109/ICRIS52159.2020.00094.

[4] M. Ur Rahman, F. Baiardi and L. Ricci, "Blockchain Smart Contract for Scalable Data Sharing in IoT: A Case Study of Smart Agriculture," 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), 2020, pp. 1-7, doi: 10.1109/GCAIoT51063.2020.9345874.

[5] D. Di Francesco Maesa, F. Tietze and J. Theye, "Putting Trust back in IP Licensing: DLT Smart Licenses for the Internet of Things," 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2021, pp. 1-3, doi: 10.1109/ICBC51069.2021.9461145.

A. Vangala, A. K. Sutrala, A. K. Das and M. Jo, "Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming," in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10792-10806, 1 July1, 2021, doi: 10.1109/JIOT.2021.3050676.

[6] V. Singla, I. K. Malav, J. Kaur and S. Kalra, "Develop Leave Application using Blockchain Smart Contract," 2019 11th International Conference on Communication Systems & Networks (COMSNETS), 2019, pp. 547-549, doi: 10.1109/COMSNETS.2019.8711422.

[7] L. Xu and Y. Li, "Internet of Things Access Control System Based on Smart Contract," 2021 IEEE International Conference on Artificial Intelligence and Industrial Design (AIID), 2021, pp. 659-662, doi: 10.1109/AIID51893.2021.9456510.

[8] G. Sawant and V. Bharadi, "Permission Blockchain based Smart Contract Utilizing Biometric Authentication as a Service: A Future Trend," 2020 International Conference on Convergence to Digital World - Quo Vadis (ICCDW), 2020, pp. 1-4, doi: 10.1109/ICCDW45521.2020.9318715.

[9] K. Peng, M. Li, H. Huang, C. Wang, S. Wan and K. -K. R. Choo, "Security Challenges and Opportunities for Smart Contracts in Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 8, no. 15, pp. 12004-12020, 1 Aug.1, 2021, doi: 10.1109/JIOT.2021.3074544.

[10] Q. Ren, K. L. Man, M. Li and B. Gao, "Using Blockchain to Enhance and Optimize IoT-based Intelligent Traffic System," 2019 International Conference on Platform Technology and Service (PlatCon), 2019, pp. 1-4, doi: 10.1109/PlatCon.2019.8669412.

[11] J. Hinckeldeyn and K. Jochen, "(Short Paper) Developing a Smart Storage Container for a Blockchain-Based Supply Chain Application," 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 2018, pp. 97-100, doi: 10.1109/CVCBT.2018.00017.

[12] W. Dandi and H. Jian, "Blockchain-based node data detection scheme for the Internet of Things system," 2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA), 2021, pp. 206-209, doi: 10.1109/CAIBDA53561.2021.00050.

[13] C. K. Da Silva Rodrigues and V. Rocha, "Towards Blockchain for Suitable Efficiency and Data Integrity of IoT Ecosystem Transactions," in IEEE Latin America Transactions, vol. 19, no. 7, pp. 1199-1206, July 2021, doi: 10.1109/TLA.2021.9461849.

[14] P. P. Ray, D. Dash, K. Salah and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," in IEEE Systems Journal, vol. 15, no. 1, pp. 85-94, March 2021, doi: 10.1109/JSYST.2020.2963840.

[15] J. Zhou, G. Feng and Y. Wang, "Optimal Deployment Mechanism of Blockchain in Resource-Constrained IoT Systems," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8168-8177, 1 June1, 2022, doi: 10.1109/JIOT.2021.3106355.

[16] N. Saquib, F. Bakir, C. Krintz and R. Wolski, "A Resource-Efficient Smart Contract for Privacy Preserving Smart Home Systems," 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI), 2021, pp. 532-539, doi: 10.1109/SWC50871.2021.00079.

[17] R. Xu, S. Y. Nikouei, Y. Chen, E. Blasch and A. Aved, "BlendMAS: A Blockchain-Enabled

Decentralized Microservices Architecture for Smart Public Safety," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 564-571, doi: 10.1109/Blockchain.2019.00082.

[18] E. S. Kang, S. J. Pee, J. G. Song and J. W. Jang, "A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid," 2018 3rd International Conference on Computer and Communication Systems (ICCCS), 2018, pp. 472-476, doi: 10.1109/CCOMS.2018.8463317.

[19] G. Si, Y. Sun, W. Chen and L. Chen, "Node Switching Method in Power Distribution Internet of Things based on Blockchain," 2020 International Conference on Computer Engineering and Intelligent Control (ICCEIC), 2020, pp. 291-295, doi: 10.1109/ICCEIC51584.2020.00062.

[20] G. Si, Y. Sun, W. Chen and L. Chen, "Node Switching Method in Power Distribution Internet of Things based on Blockchain," 2020 International Conference on Computer Engineering and Intelligent Control (ICCEIC), 2020, pp. 291-295, doi: 10.1109/ICCEIC51584.2020.00062.

[21] W. Xiao et al., "Blockchain for Secure-GaS: Blockchain-Powered Secure Natural Gas IoT System With AI-Enabled Gas Prediction and Transaction in Smart City," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6305-6312, 15 April15, 2021, doi: 10.1109/JIOT.2020.3028773.

[22] Y. Jiang, Y. Zhong and X. Ge, "Smart Contract-Based Data Commodity Transactions for Industrial Internet of Things," in IEEE Access, vol. 7, pp. 180856-180866, 2019, doi: 10.1109/ACCESS.2019.2959771.

[23] Bansal R., Gupta A., Singh R. and Nassa V. K., (2021). Role and Impact of Digital Technologies in E-Learning amidst COVID-19 Pandemic. 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), pp. 194-202.doi: 10.1109/CCICT53244.2021.00046.

[24] Dushyant, K., Muskan, G., Gupta, A. and Pramanik, S. (2022). Utilizing Machine Learning and Deep Learning in Cyber security: An Innovative Approach", in Cyber security and Digital Forensics, M. M. Ghonge, S. Pramanik, R. Mangrulkar,D. N. Le, Eds, Wiley, https://doi.org/10.1002/9781119795667.ch12

[25] Gupta A., et. al, (2020). An Analysis of Digital Image Compression Technique in Image Processing. International Journal of Advanced Science and Technology, 28(20), 1261 - 1265. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/3837

[26] Kaushik, K., Garg, M., Annu, Gupta, A. and Pramanik, S. (2021). Application of Machine Learning and Deep Learning in Cyber security: An Innovative Approach, in Cybersecurity and Digital Forensics: Challenges and Future Trends, M. Ghonge, S. Pramanik, R. Mangrulkar and D. N. Le, Eds, Wiley, 2021.

[27] Pandey, B.K. et al. (2022). Effective and Secure Transmission of Health Information Using Advanced Morphological Component Analysis and Image Hiding. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore.https://doi.org/10.1007/978-981-19-0151-5_19

[28] Pathania, V. et al. (2022). A Database Application of Monitoring COVID-19 in India. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_23

[29] Veeraiah V., Rajaboina N. B., Rao G. N., Ahamad S., Gupta A. and Suri C. S., (2022).Securing Online Web Application for IoT Management. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1499-1504.doi: 10.1109/ICACITE53722.2022.9823733.

[30] V. Jain, S. M. Beram, V. Talukdar, T. Patil, D. Dhabliya and A. Gupta, "Accuracy Enhancement in Machine Learning During Blockchain Based Transaction Classification," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 536-540, doi: 10.1109/PDGC56933.2022.10053213.

[31] V. Talukdar, D. Dhabliya, B. Kumar, S. B. Talukdar, S. Ahamad and A. Gupta, "Suspicious Activity Detection and Classification in IoT Environment Using Machine Learning Approach," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 531-535, doi: 10.1109/PDGC56933.2022.10053312.

[32] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Scalable Platform to Collect, Store, Visualize and Analyze Big Data in Real- Time," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118183.

[33] M. Dhingra, D. Dhabliya, M. K. Dubey, A. Gupta and D. H. Reddy, "A Review on Comparison of Machine Learning Algorithms for Text Classification," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1818-1823, doi: 10.1109/IC3I56241.2022.10072502.

[34] D. Mandal, A. Shukla, A. Ghosh, A. Gupta and D. Dhabliya, "Molecular Dynamics Simulation for Serial and Parallel Computation Using Leaf Frog Algorithm," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 552-557, doi: 10.1109/PDGC56933.2022.10053161.

[35] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Review on Application of Deep Learning in Natural Language Processing," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1834-1840, doi: 10.1109/IC3I56241.2022.10073309.

[36] V. V. Chellam, S. Praveenkumar, S. B. Talukdar, V. Talukdar, S. K. Jain and A. Gupta, "Development of a Blockchain-based Platform to Simplify the Sharing of Patient Data," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118194.

[37] Veeraiah V., Ahamad G. P, S., Talukdar S. B., Gupta A. and Talukdar V., (2022) Enhancement of Meta Verse Capabilities by IoT Integration. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1493-1498.doi: 10.1109/ICACITE53722.2022.9823766.

[38] Gupta A., Singh R., Nassa V. K., Bansal R., Sharma P. and Koti K., (2021) Investigating Application and Challenges of Big Data Analytics with Clustering. 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), pp. 1-6.doi: 10.1109/ICAECA52838.2021.9675483.

[39] Natalia Volkova, Machine Learning Approaches for Stock Market Prediction , Machine Learning Applications Conference Proceedings, Vol 2 2022.

[40] M, A. ., M, D. ., M, A. ., M, V. ., I, S. T. ., & P, K. . (2023). COVID -19 Predictions using Transfer Learning based Deep Learning Model with Medical Internet of Things . International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 43–50. https://doi.org/10.17762/ijritcc.v11i3.6200

[41] Sherje, N. P., Agrawal, S. A., Umbarkar, A. M., Dharme, A. M., & Dhabliya, D. (2021). Experimental evaluation of mechatronics based cushioning performance in hydraulic cylinder. Materials Today: Proceedings, doi:10.1016/j.matpr.2020.12.1021