Abstract: In the Internet of Things (IoT) system, data leakage can easily occur due to the differing security of edge devices and the different processing methods of data in the transmission process. Blockchain technology has the advantages of good non-tamperability, decentralization, de-trust, openness, and transparency, and it can protect data security on the Internet of Things. This research integrates the means by which data flow can be combined with blockchain technology to prevent privacy leakage throughout the entire transportation process from sender to receiver. Through a keyword search of the last five years, 94 related papers in Web of Science and IEEE Xplore were extracted and the complex papers and frameworks explained using a reconstruction graph. The data processing process is divided into five modules: data encryption, data access control, data expansion, data storage, and data visualization. A total of 11 methods combining blockchain technology to process IoT data were summarized. The blockchain application technology in the IoT field was summarized objectively and comprehensively, and a new perspective for studying IoT data flow was given.

Keywords: blockchain; Internet of Things; information security; reconstruction diagram

1. Introduction

With the arrival of the 5G era, the Internet of Things technology has been rapidly developed, the efficiency of information transmission dramatically improved, and people’s access to information gradually diversified. At the same time, the risk of privacy disclosure has also increased [1]. In 2019, American SR Lab carried out two attacks on voice agent software (VPA) and found that, after the exit command was issued, the subject’s conversations could still be eavesdropped [2]. In December 2020, the network security team found data leakage in SocialArks. The leaked database contained more than 408 GB of data and 318 million records. The number of affected users was about 214 million, mainly from three major social media sites: Instagram, Facebook, and LinkedIn, which seriously affected people’s lives; moreover, the data leakage seriously threatened the information security of the edge device owners of the Internet of Things.

Blockchain technology has anonymity protection and tamper resistance, effectively protecting information, user privacy, and the sharing of data in real-time [3]. It removes traditional third-party tools, does not rely on specific central nodes, realizes P2P transactions, and avoids the risk of privacy disclosure caused by a single point of failure. Blockchain features such as tamper resistance, decentralization, and traceability provide suitable conditions for data storage [4].

This paper mainly uses keyword extraction and reconstructed graph review methods to analyze the blockchain. A keyword extraction method was used to extract 82 representative papers published in the last five years from Web of Science and IEEE Xplore, which were combined with blockchain and Internet of Things technology. The 82 papers were divided into five modules by an inductive analysis, according to the different stages of data flow processing: data encryption module blockchain solution, data access control module blockchain solution, data extraction module blockchain solution, data storage module blockchain solution, and data visualization module blockchain solution.
module blockchain solution, and blockchain data visualization. The review method of reconstructed maps was used to simplify the complex models in the references and visualize them from the perspective of data flow processing. At the same time, some papers only propose ideas and methods, but no model diagram is conducive to the reader’s understanding. Due to this situation, a reconstructed diagram is presented to visualize and facilitate the reader’s experience.

By analyzing the overview papers on the combination of the Internet of Things and blockchain on the Web of Science and IEEE Xplore websites, we found that the current research reviews concern the application of blockchain technology in one or two data processing links of the Internet of Things. These reviews are one-sided and do not offer a comprehensive and objective assessment of all data processing links. The main contributions of this paper are as follows:

1. The entire process of IoT data flow from data receiving to data visualization is divided into five modules from the perspective of the data processing mode. There is no inductive method based on IoT data flow in the current research review.
2. This paper analyzes all data processing modules that combine IoT data and blockchain. Compared with the published overview papers in this field, the content is more comprehensive and the classification more specific.
3. The analysis method of the reconstruction diagram is adapted to display the various modules of the Internet of Things data stream processing data and to visualize the application of blockchain technology. The combination of graphics and text makes the expression more intuitive.
4. The research analyzed and summarized 82 papers from the past five years, showing the latest research progress of blockchain in the Internet of Things system.

2. Overview of Blockchain

Blockchain originated from Bitcoin, and since then, there have been alternative currencies with better privacy protection effects, such as Dashi Coin, Monroe Coin, and Zcash. Blockchain is a decentralized storage technology based on P2P network architecture. Its first description was in 2008 [5]. Between nodes, a unique information transmission mechanism was eventually adopted. The information is broadcasted to the entire domain. It abandons the traditional trust service relying on a reliable third party, supports point-to-point anonymous transactions throughout the process, greatly reduces the risk of network eavesdropping, and effectively protects user information security.

2.1. Working Principle

The blockchain system consists of Block Header, Block Body, and Policy Header, which form a chain structure with the sequence in the form of a “series connection”. The block header encapsulates the version number, timestamp, hash value of the previous block, Merkle root, and random value of the solution. The block body records the number of transactions. In addition to the Genesis block, each block in the blockchain contains the hash value of the previous block [6]. Figure 1 is the specific structure of the blockchain, and its workflow is as follows:

1. The encrypted transaction information is uploaded through the node, and the current node broadcasts the information to the nodes of the whole network in the form of relay forwarding;
2. Miners verify the signatures of the collected transaction information and write the effective information into the block;
3. The transaction information in a given period is formed into a new candidate block, and the node obtains the workload proof meeting the target difficulty through the PoW consensus mechanism;
4. The blocks found by this node are broadcast to the whole network;
5. The whole network node verifies this node. When the transaction information is valid and has never existed, it will be added to the blockchain after verification, and a new block extension chain will be created behind this block.

Figure 1. Block structure reconstruction diagram.

2.2. Consensus Algorithm

The consensus algorithm was first used to study distributed problems. In 1982, Lamport put forward the “Byzantine General Problem”, that is, how to make all nodes reach a consensus when there are dishonest nodes in the network. In response to this problem, he proposed the Byzantine Fault Tolerance (BFT) algorithm. Later, Castro and others proposed a practical Byzantine Fault Tolerance (PBFT) algorithm, that is, when the dishonest nodes in the network are less than 1/3 of the nodes in the whole network, the whole network can reach a consensus. The PBFT algorithm has lower complexity and less computing power than the BFT algorithm, which reduces power waste to a certain extent. In 1993, Cynthia proposed the PoW (Proof of work, PoW) mechanism. Subsequently, Nakamoto Cong announced that it would apply the PoW consensus mechanism to Bitcoin transactions. This mechanism relies on powerful computing power to ensure the blockchain is secure and tamper-resistant. To tamper with the data in the block, more than 51% of the whole network’s computing power must be mastered, thus, ensuring the security of the transaction [7]. In 2012, Peercoin adopted the Proof of Stake (PoS) mechanism as the consensus mechanism and selected the node with the highest equity in the system, according to the currency age for bookkeeping. Compared with the PoW consensus, Peercoin improved the transaction efficiency and increased the throughput. In 2014, Dan proposed the Delegated Proof of Stake (DPoS). This mechanism is similar to the “Board of Directors”. Members of the “Board of Directors” are elected by democratic election. Members need to pay a certain margin and can benefit from transaction fees. This consensus mechanism guarantees node interests speed up the block out and enable rapid consensus verification [8].

3. Division of IoT Data Flow Module

The Internet of Things is a new technology paradigm derived from the Internet era, which uses the network to intelligently control various terminal devices [9,10]. A global or specific local area network can be formed according to specific needs to achieve the interoperability of people and things [11]. The Internet of Things technology can be used in various fields, such as medical care [12,13], agricultural science and technology [14], and the ecological environment [15].

Based on the transmission direction of the Internet of Things’ data flow from a new perspective, this research integrates how the data flow can be combined with blockchain technology to prevent privacy leakage during the whole transportation process from sender to receiver. It reconstructs the data flow of the Internet of Things at a new level and
visualizes the blockchain defense means with the reconstruction diagram analysis method. Figure 2 is the reconstruction diagram of the IoT data flow module division.

Figure 2. Division and reconstruction diagram of IoT data flow module.

4. Blockchain Solutions

4.1. Data Encryption Module Blockchain Solution

In the Internet of Things system, data at the encryption layer are vulnerable to the threat of privacy disclosure, such as device firmware leakage, side channel-based device exceptions, etc. Encrypting data based on the blockchain can effectively reduce the risk of data leakage at the encryption layer.

4.1.1. Agent Re-Encryption Technology Based on Blockchain

Proxy re-encryption technology eliminates the dependence on third parties and decrypts data by transferring different keys to different users instead of using shared public keys as an intermediate link, which not only increases the security of information, but also reduces the complexity of operations [16–23]. Gao [16] proposed a combination of blockchain and proxy re-encryption technology for device communication and data sharing in the IoT community. Chen [17] proposed a threshold-based proxy re-encryption algorithm combined with the blockchain consensus algorithm, which eliminates the restrictions on the secure storage and distribution of private data in a distributed network and meets a wide range of data access needs. Manzoor [18] proposed a proxy re-encryption scheme to automate Internet of Things payments, transfer data from producers to consumers anonymously and securely, analyze the performance of hybrid systems by using an unlicensed Ethernet blockchain, and compare it with the IBM Super Accounting Structure, a licensed blockchain. Liyanage [19] proposed a proxy re-encryption scheme for data sharing in the Internet of Things. Data are only visible to owners and people in smart contracts, but the system lacks storage scalability. Pournaghi [20] proposed a proxy re-encrypted medical information sharing scheme based on blockchain and attributes, encrypted based on data attributes and stored on private blockchain, in contrast to public blockchain, which shares information on attribute fields, but the entire encryption process lacks a fine-grained division of privileges between individuals and hospitals. Figure 3 shows a reconstructed blockchain-based proxy re-encryption technique. Table 1 shows the abbreviated word in Figure 3.

Table 1. Notation.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ET</td>
<td>Ciphertext</td>
</tr>
<tr>
<td>IoT sensors</td>
<td>Data owner</td>
</tr>
<tr>
<td>Data consumers</td>
<td>Data user</td>
</tr>
<tr>
<td>GDC</td>
<td>Grade decision center</td>
</tr>
<tr>
<td>G</td>
<td>Identity level</td>
</tr>
<tr>
<td>C</td>
<td>Access condition-set</td>
</tr>
<tr>
<td>SKID</td>
<td>Secret key</td>
</tr>
<tr>
<td>RKID</td>
<td>Re-encryption key</td>
</tr>
</tbody>
</table>
Figure 3. Reconstruction of agent re-encryption technology based on blockchain.

4.1.2. Blockchain-Based Encryption Algorithm

In the aggregation process of Internet of Things data, various encryption algorithms can be used to encrypt the data [24–32]. During the aggregation process of distributed data, Louki [24] proposed to protect the privacy of aggregated data by combining blockchain with homologous encryption technology. Group-level aggregation can confuse IoT data, thus, complicating the inference of sensitive information from a single IoT device. Figure 4 is a reconstructed diagram of this scheme. Guo [25] discusses asymmetric encryption mechanisms on the blockchain, but each node in the blockchain is not completely anonymous. With the development of various anti-anonymous identity filtering and other technologies, it is still possible to locate and identify some key targets. Priyadarsini [26] proposed a hybrid chaotic encryption algorithm for medical images in the context of the Internet of Things. Guruprakash [27] proposed a hybrid elliptic curve algorithm and genetic algorithm to encrypt IoT data using blockchain technology, which greatly improves the overall performance of the IoT system. However, there is still room to improve the overall performance of consensus and physical identification mechanisms. Alshamrani [28] proposed a lightweight DNA-GA (DNA genetic algorithm) encryption method for resource-constrained Internet of Things devices on a blockchain, which improves data security and reduces encryption and decryption time. Abd-El-Atty [29] proposed a new blockchain-based quantum attack-resistant computer encryption algorithm for smart cities in the Internet of Things. The main advantage of the framework described is to help IoT nodes effectively share their data with other nodes and fully control their records.
cities in the Internet of Things. The main advantage of the framework described is to help IoT nodes effectively share their data with other nodes and fully control their records.

4.1.3. Hierarchical Encryption Based on Blockchain

Different ecosystems of the Internet of Things have different requirements for data processing architectures. Pavithran [33] proposes a Hierarchical Encryption of Identity (HIBE) Block Chain architecture for privacy protection in the Internet of Things and uses edge computing and cloud computing to protect data privacy. Zhang [34] proposed using low-consumption hierarchical key distribution to encrypt data in the medical care Internet of Things (H-IoT) system for medical information sharing on the blockchain. Figure 5 is a reconstructed hierarchical data-sharing diagram of the medical care Internet of Things based on blockchain.

4.1.4. Attribute Encryption Based on Blockchain

Attribute-based Internet of Things encryption protects private data while making targeted calls to the data [35–40]. Rahulamathavan [35] proposed a privacy protection architecture for the Internet of Things based on attribute encryption and blockchain technology, which fully guarantees the privacy of data. Figure 6 is a reconstructed flow diagram of the attribute encryption (CP-ABE) algorithm based on a ciphertext encryption strategy. Lu [36] proposed a blockchain privacy protection scheme based on the combination of attribute encryption and access control of the Internet of Things. Smart contracts are used to implement access control, and blockchain technology is used for privacy protection. Nakanishi [37] proposed attribute-based encryption (CP-ABE) in the Intelligent Internet of Things (IoTA) to upload tokens with attribute encryption to the database. Yu [38] proposed an updatable and revocable attribute encryption method for blockchain-based IoT systems to achieve two-way compatibility.
To protect the integrity and privacy of the data, a blockchain solution is introduced to the data access process. The blockchain-based access control architecture of the Internet of Things greatly reduces the risk of privacy leakage.

4.2. Attribute Access Control Based on Blockchain

Attribute-based access control can make control decisions [41–46] based on the access control policies and consensus algorithms that are created. Islam [41] proposed to combine attribute-based access control with blockchain-based access control to the Internet of Things (IoT) system. Intelligent contracts and distributed consensus provide access control to the Internet of Things. Yang [42] proposed using attribute-based access control to solve dynamic problems caused by dynamic access and data changes in the Internet of Things, and using blockchain technology to solve possible DDoS attacks. Ding [43] proposed the use of attribute-based access control for IoT systems to avoid single-point failures and data tampering, and the use of blockchain technology to record the distribution of attributes. Zaidi [44] is a distributed file system based on the Internet of Things. The effectiveness of
the Attribute Access Control model is analyzed using the Intergalactic File System as an example. Data owners store ciphertext on blockchain through smart contracts.

4.2.2. Functional Access Control Based on Blockchain

Function-based access control can more closely meet the availability and interoperability of the Internet of Things [47–53]. Sivaselvan [47] set the functionality as a token and performed all operations with a blockchain. It not only meets the interoperability of the Internet of Things, but also meet the different needs of enterprises. This method satisfies the interoperability of Internet architecture between different scenarios. Bouras [48] presented a distributed access control architecture based on functions, which solves the problem of weak interoperability between IoT Federation networks. Liu [49] proposed a feature-based access control architecture to address smart delivery in a variety of Internet of Things environments, using blockchain and various discrete identifiers to identify devices in the Internet of Things while protecting user privacy and security. To meet the scalability of Smart Internet, Xu [50] proposed a function-based joint delegation model, which supports the hierarchical and multipoint delegation of privileges, registers, and revokes privileges using blockchain smart contracts, as well as providing a more scalable Internet of Things system. In IoTA Open Source Distributed Accounts, Pinjala [51] proposed the use of a Functional Access Control Framework, which provides unpaid transactions for the Internet of Things while guaranteeing the integrity and privacy of functional tokens.

4.2.3. Blockchain-Based Identity and Role Access Control

Identity-based access control architecture [54–61] and role-based access control architecture [62,63] are suitable for solving identity management issues in the Internet of Things. In the access control system of the Internet of Things, Bouras [54] proposed the use of identity management to identify and authorize access rights and store the rights information on the federation chain to ensure that the information cannot be tampered with. Cui [55] classified nodes according to their functional differences, built a blockchain between different nodes to form hierarchical networks, authenticated ordinary nodes in the local blockchain, and authenticated collection nodes in the common blockchain.

4.2.4. Fine-Grained Access Control Based on Blockchain

Fine-grained access control allows the creation of smart contracts detailing data privileges based on the data owner’s wishes [64–69]. Ding [64] proposed a fine-grained access control framework using licensing blockchain technology to enhance trust in untrusted environments by implementing a trusted access control mechanism. Xu [65] proposed a hierarchical attribute encryption algorithm for fine-grained access control by authorizing different user attributes. To achieve fine-grained access control and compatibility between attribute update and revocation on blockchain in the Internet of Things, Yu [38] proposed a fine-grained attribute-based encryption algorithm to solve the update problem of blockchain data.

4.3. Data Extraction Module Blockchain Solution

4.3.1. Searchable Encryption

The technology that enables data to be searched in encrypted situations is called searchable encryption (SE) technology, which is divided into two types: symmetric searchable encryption technology and asymmetric searchable encryption technology. To share data in the Internet of Things, asymmetric searchable encryption technology called public-key encryption with keyword search (PEKS), is commonly used. Searchable encryption uses bilinear mapping to map groups G1 and G2 of prime P on two vectors to one vector. Define a bilinear map e: G1 × G1 → G2, conforms to the following characteristics:

- Non-degenerate: If A is a generator of G1, e (a, a) maps to a generator of G2, and b, c ∈ G1 exists, satisfying e(b, c) e ≠ 1.
• Bilinear: For any $a, b \in G_1$, there exists $x, y \in \mathbb{Z}_q^*$, so that the equation $e(ax, by) = e(a, b)x^y$ holds.

• Computability: For any $a, b \in G_1$, there is a valid algorithm to compute $e(a, b)$.

The Internet of Things (IoT) has changed our lives through massive data production. Liu [39] proposed a blockchain-assisted searchable attribute encryption (BC-SABE) with efficient revocation and decryption capabilities, in which the traditional centralized server was replaced by the distributed blockchain system responsible for threshold parameter generation, key management, and user revocation. Xiang [69] proposed that blockchain be used as a database and searchable encryption mechanism for searching keywords using the same encryption technology. Through comparative analysis, the security and search ability of this scheme are proved.

4.3.2. Key Decryption

Algorithm 1 decrypts the searched data to obtain the information on the chain, the PEKS decryption algorithm is as follows:

**Algorithm 1**: PEKS Decryption Algorithm

<table>
<thead>
<tr>
<th>Enter common parameters [params, g], public key, keyword, return ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trapdoor Generation Algorithm:</td>
</tr>
<tr>
<td>Enter the public parameter [params], Secret key, keyword to look up, return trapdoor</td>
</tr>
<tr>
<td>def Trapdoor (params, sk, word):</td>
</tr>
<tr>
<td>pairing = Pairing(params)</td>
</tr>
<tr>
<td>hash_value = Element.from_hash (pairing, G1, G2) Hash1(str(word). encode('utf-8')).hexdigest ()</td>
</tr>
<tr>
<td>return hash_value ** sk</td>
</tr>
</tbody>
</table>

4.4. Data Storage Module Blockchain Solution

The introduction of a decentralized consensus blockchain and the Intergalactic File System (IPFS) increases data storage and enables data expansion [70]. Ye [71] proposed to use IPFS and blockchain to store vehicle data in the Internet of Things together, so as to achieve the safe and effective storage of vehicle data. Sakakibara [72] proposed a cache technology based on a Field Programmable Gate Array (field programmable gate array) network interface card (NIC) to improve the storage of blockchain on the Internet of Things. The proposed system can reduce server overload. Xu [73] designed a non-dominant sorting genetic algorithm with clustering (NSGA-C). By adding clustering to ensure diversity, a suitable solution for different users is selected, which is superior to other improvements in local space consumption. Two-tier blockchain connects information on two different blockchains. Pal [74] proposed a dual-blockchain architecture, which moves the attribute storage and access of a public blockchain onto a secure private blockchain. Experiments show that the performance of this scheme has been greatly improved. Table 2 summarizes the current blockchain solutions for the Internet of Things data storage module.

### Table 2. Data storage blockchain solution.

<table>
<thead>
<tr>
<th>Blockchain Solutions</th>
<th>References</th>
<th>Performance Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interplanetary File System (IPFS) + Blockchain</td>
<td>[70,71]</td>
<td>Capacity expansion + secure storage</td>
</tr>
<tr>
<td>Network interface card (NIC) + blockchain</td>
<td>[72]</td>
<td>Reduce server overload + secure storage</td>
</tr>
<tr>
<td>Clustering (NSGA-C) + Genetic Algorithm</td>
<td>[73]</td>
<td>Minimum local space</td>
</tr>
<tr>
<td>Double-layer blockchain</td>
<td>[74]</td>
<td>Secure storage + Security Access + expansion</td>
</tr>
</tbody>
</table>
4.5. Blockchain Data Visualization

Blockchain data in the Internet of Things require some operation after collection to achieve the visualization purpose. Song [75] proposed a visualization tool to visualize the IoT sensor data stored as transactions through a series of data monitoring in the blockchain. Scarlato [76] proposed a scheme for inserting and visualizing travel data on the blockchain, which achieves the goal of data visualization by writing back-end and front-end infrastructure codes and replicating databases to maintain the same data. Table 3 is a summary of blockchain solutions for IoT data flow.

Table 3. Summary of Internet of Things data flow blockchain solutions.

<table>
<thead>
<tr>
<th>Module Division of IoT Data Flow</th>
<th>Technology or Method</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Encryption Module</td>
<td>Agent Re-encryption Technology Based on Blockchain</td>
<td>[16–23]</td>
</tr>
<tr>
<td></td>
<td>Blockchain-Based Encryption Algorithm</td>
<td>[24–32]</td>
</tr>
<tr>
<td></td>
<td>Hierarchical Encryption Based on Blockchain</td>
<td>[33,34]</td>
</tr>
<tr>
<td></td>
<td>Attribute Encryption Based on Blockchain</td>
<td>[35–40]</td>
</tr>
<tr>
<td>Data Access Control Module</td>
<td>Attribute Access Control Based on Blockchain</td>
<td>[41–46]</td>
</tr>
<tr>
<td></td>
<td>Function Access Control Based on Blockchain</td>
<td>[47–53]</td>
</tr>
<tr>
<td></td>
<td>Identity and Role Access Control Based on Blockchain</td>
<td>[54–61]</td>
</tr>
<tr>
<td></td>
<td>Fine-grained Access Control Based on Blockchain</td>
<td>[64–67]</td>
</tr>
<tr>
<td>Data Extraction Module</td>
<td>Searchable Encryption Technology</td>
<td>[68,69]</td>
</tr>
<tr>
<td></td>
<td>Key Decryption</td>
<td></td>
</tr>
<tr>
<td>Data Storage Module</td>
<td>IPFS + NIC + NSGA-C + Double-Layer Blockchain</td>
<td>[70–74]</td>
</tr>
<tr>
<td>Blockchain Data Visualization</td>
<td>Visualization Tools</td>
<td>[75,76]</td>
</tr>
</tbody>
</table>

5. Challenges and Application

5.1. Blockchain Challenges

Internet of Things security faces challenges in authentication, authorization/access control, availability, confidentiality integrity [77], reading the information, identifying malicious nodes, illegal exploitation, etc. The main challenges are as follows:

1. Security (75%), privacy (62.5%), resource limitation (50%), and scalability (50%) are the most important issues in block-based Internet of Things research [78].
2. In the blockchain-based Internet of Things, there is a bottleneck in the research process for edge-device distributed trust management [79].
3. According to the mapping between the characteristics of the Internet of Things and the blockchain, there is space for each terminal device in the Internet of Things to achieve absolute decentralization through the blockchain. When the blockchain network acts as a complete or lightweight node, different consensus mechanisms will change the effectiveness of the integration of the Internet of Things [80].
4. Blockchain technology is used when there are only a few nodes. As it takes some time to read information from the blockchain, it may slow down the speed of information reading.
5. Malicious nodes join the blockchain and use the consensus algorithm to obtain all information on the public ledger.
6. Blockchain technology is used by the dark net to engage in illegal activities.
5.2. Blockchain Application Scenarios

The Internet of Things is the integration of the physical world into the network world. It can provide related services according to different scenarios. The integration of the Internet of Things and blockchain can be applied in various fields. Tapia concluded from 164 papers that security and privacy (31.08%), health care (19.59%), and energy (9.46%) are the three most widely used areas [80]. We have categorized some application scenarios of blockchain, and Figure 7 shows other potential areas of blockchain, which are not limited to the applications discussed in this paper.

In addition to the application areas shown in the figure, the application scenarios include private data storage, education, banking, taxation, media, smart homes, etc. Figure 7 shows that blockchain is widely used in people’s lives, and blockchain can be utilized in various areas of life to protect data privacy. Blockchain applications in different areas improve data security and protect people’s privacy.

![Figure 7. Blockchain Application Scenarios.](image)

5.3. Other Data Privacy Protection Methods

Blockchain technology is widely used in all aspects of IoT information flow because of its good protection of information. Its consensus mechanism can handle many security issues, such as multi-party issues, lack of trusted third-party platforms, and the need to monitor activities between entities in real time. In addition, it can also resist a variety of attack types, such as replay attacks and witch attacks. In addition to blockchain technology, there are many ways to protect data privacy in the process of processing data. The following is a collation of other privacy protection methods:

Data perturbation technology [81]: The purpose of protecting data privacy is achieved by perturbing the original data. The data obtained by the attacker are not real; they are also distorted. In the data perturbation method, the localized differential privacy technology is the most widely used technology. It distorts the original data by adding noise to achieve the purpose of protecting data privacy. However, in the process of interference, the information loss is too large and the data availability is reduced. This process can use distributed ledgers to improve the data transmission speed and capacity and reduce data loss [82].

Data encryption technology: By encrypting the original data to achieve the purpose of protecting data privacy, common encryption methods include the Advanced Encryption Standard (AES) algorithm [83], RSA public key cryptography system, elliptic curve cryptosystems (ECC) algorithm [84], and homomorphic encryption algorithm [85]. However, in
the encryption process, third-party servers are prone to privacy leakage. The decentralized characteristics of blockchain technology can be used to protect the security of data [86].

Data anonymization [87]: Data can be anonymized and selectively published according to its sensitivity, thereby reducing the risk of data privacy leakage. Common technologies include k-anonymity [88], L-Diversity [89], and T-Closeness [90]. However, the anonymous algorithm requires significant calculation, involves a large amount of data processing overhead, and is vulnerable to background knowledge attacks.

Federal Learning [91]: Based on the distributed framework, by using artificial intelligence algorithms, data modeling is realized under the mechanism of data non-sharing and encryption, and the built sharing model can be used by all participants. However, some work shows that federated learning can be easily leaked by third-party attackers, or by central servers in the process of training parameter update iteration.

Table 4 compares the differences between blockchain privacy protection methods and other privacy protection methods from four aspects. The comparison shows that the blockchain privacy protection method can better protect the privacy of data than other privacy protection methods.

The technical director of the US Department of Homeland Security (DHS) has created a flowchart to help people determine whether blockchain technology is needed. The comparison results in Table 4 show that blockchain is an appropriate way to manage data streams under very limited conditions [92]. However, other privacy protection methods have some pitfalls, and their degree of protection is lower than blockchain technology.

Table 4. Comparison of blockchain technology with other data privacy protection methods.

<table>
<thead>
<tr>
<th>Privacy Protection Method</th>
<th>Technique</th>
<th>Small Data Loss</th>
<th>Trusted Third Party</th>
<th>A Small Quantity of Computation</th>
<th>Difficult to Be Attacked by a Third Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain Privacy Protection Data Perturbation</td>
<td>Consensus Algorithm, Smart Contract</td>
<td>YES</td>
<td>---</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Data Perturbation Privacy Protection Data Encryption Privacy Protection Data Anonymous Privacy Protection Federal Learning Privacy Protection</td>
<td>Local Differential Privacy</td>
<td>NO</td>
<td>---</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Data Encryption Privacy Protection Data Anonymous Privacy Protection Federal Learning Privacy Protection</td>
<td>AES, RSA, ECC</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Data Anonymous Privacy Protection Federal Learning Privacy Protection</td>
<td>K-anonymity, L-Diversity, T-Closeness</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Data Anonymous Privacy Protection Federal Learning Privacy Protection</td>
<td>Deep Learning</td>
<td>YES</td>
<td>---</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>

5.4. Blockchain Considerations

Blockchain should be selectively applied based on a full understanding of the technology. The technical director of the US Department of Homeland Security (DHS) has created a flowchart to help people determine whether blockchain technology is needed. The flow chart lists six questions to help those who are interested in using blockchain determine whether it is necessary; if the given six problems are met at the same time, it is necessary to use blockchain technology.

Blockchain technology also faces some problems in different application scenarios. In the field of medicine and healthcare, if patient data are shared and stored, problems such as excessive information, insufficient storage space, and slow information search speed arise. Therefore, a double-layer blockchain is proposed to solve this problem. In the field of Internet of Things, each IoT system uses its own alliance chain; that multiple Internet of
Things systems realize multi-party information security sharing is a problem worthy of study. In the field of artificial intelligence, machine learning requires significant computing power; thus, how to generate high throughput in the case of a large number of concurrent requests needs further research.

6. Conclusions

The Internet of Things (IoT) system has a wide range of applications, and the interaction between devices is complex. The data flow faces multiple security threats in each module of data processing. Blockchain technology can defend against various threats, so it is applied in all aspects of data processing. In this paper, the keyword extraction method is used to extract 94 latest documents from the last five years. From a new perspective of data processing, these representative works are divided into five modules by inductive analysis; then, each module is visualized by a reconstruction graph. This paper summarizes 11 methods of processing IoT data combined with blockchain technology. The results show that blockchain technology can be applied to the entire transmission process of IoT data flow, but the degree of application is different. It is most widely used in data encryption and data access control. In the process of data visualization, the method is single, and there is still space for further research.

The most popular feature of blockchain technology is its non-tamperability. However, in the future, some work will likely involve modifying the data on the blockchain, requiring us to develop new technical means to solve it. Our future work will be devoted to studying how to selectively change the data on the blockchain to make more rational use of blockchain technology.

Author Contributions: Conceptualization, J.L. and X.Z.; formal analysis, J.L. and W.S.; investigation, J.L. and W.S.; data curation, J.L.; writing—original draft preparation, J.L.; writing—review and editing, J.L. and X.Z.; supervision, X.Z.; funding acquisition, X.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by grants from the National Natural Science Foundation of China (No.61802161), the Scientific Research Project of Liaoning Provincial Department of Education (No. JZL202015404, LJKZ0625), and the Applied Basic Research Program of Liaoning Province (No.2022JH2/101300280).

Data Availability Statement: The study did not report any data.

Conflicts of Interest: The authors declare no conflict of interest.

References
4. Yao, Q.; Zhang, D. Overview of identity management technology in block chain system. J. Softw. 2021, 32, 2260–2286. [CrossRef]


31. Pang, Z.; Yao, Y.; Li, Q.; Zhang, X.; Zhang, J. Electronic Health Records Sharing Model based on Blockchain with Checkable State and attribute-based encryption. *J. Ind. Inf. Integr.* 2020, 2, 122001. [CrossRef]


42. Yang, Q.; Zhang, M.; Zhou, Y.; Wang, T.; Xia, Z.; Yang, B. A Non-Interactive Attribute-Based Access Control Scheme by Blockchain for IoT. *Electronics* 2021, 10, 1855. [CrossRef]

43. Ding, S.; Cao, J.; Li, C.; Fan, K.; Li, H. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. *IEEE Access* 2019, 7, 38431–38441. [CrossRef]


45. Wang, P.; Yue, Y.; Sun, W.; Liu, J. An Attribute-Based Distributed Access Control Framework for Blockchain-Enabled IoT. In Proceedings of the 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 21–23 October 2019; pp. 1–6. [CrossRef]


60. Fotohii, R.; Allee, F.S. Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT. *Comput. Netw.* 2021, 197, 108331. [CrossRef]


62. Ameer, S.; Benson, J.; Sandhu, R. An Attribute-Based Approach toward a Secured Smart-Home IoT Access Control and a Comparison with a Role-Based Approach. *Information* 2022, 13, 60. [CrossRef]


69. Xiang, X.; Zhao, X. Blockchain-assisted searchable attribute-based encryption for e-health systems. *J. Syst. Arch.* 2022, 124, 102417. [CrossRef]


71. Ye, H.; Park, S. Reliable Vehicle Data Storage Using Blockchain and IPFS. *Electronics* 2021, 10, 1130. [CrossRef]


73. Xu, M.; Feng, G.; Ren, Y.; Zhang, X. On Cloud Storage Optimization of Blockchain With a Clustering-Based Genetic Algorithm. *IEEE Internet Things J.* 2020, 7, 8547–8558. [CrossRef]


