An Overview of Blockchain Security Analysis

Hai Wang[1,2], Yong Wang[3], Zigang Cao[1,2], Zhen Li[1,2], and Gang Xiong[1,2(✉)]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
xionggang@iie.ac.cn
[2] University of Chinese Academy of Sciences, Beijing, China
[3] National Computer Network Emergency Response Technical Team/Coordination Center, Beijing, China

Abstract. The blockchain, with its own characteristics, has received much attention at the beginning of its birth and been applied in many fields. At the same time, however, its security issues are exposed constantly and cyber attacks have caused significant losses in it. At present, there is little concern and research in the field of network security of the blockchain. This paper introduces the applications of blockchain in various fields, systematically analyzes the security of each layer of the blockchain and possible cyber attacks, expounds the challenges brought by the blockchain to network supervision, and summarizes research progress in the protection technology. This paper is a review of the current security of the blockchain and will effectively help the development and improvement of security technologies of the blockchain.

Keywords: Blockchain · Network security · Cyber attacks · Network supervision

1 Background

1.1 Origin and Development of the Blockchain

The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008 [1]. It was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network.

Comparing to the rapid development of blockchain technology, relevant norms and standards on it are still incomplete. The first descriptive document on the blockchain is the "Bitcoin: A Peer-to-Peer Electronic Cash System" written by Nakamoto, in which blocks and chains are described as a data structure recording the historical data of the bitcoin transaction accounts. "A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get

X. Yun et al. (Eds.): CNCERT 2018, CCIS 970, pp. 55–72, 2019.
https://doi.org/10.1007/978-981-13-6621-5_5

into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it (Fig. 1)." The blockchain is also called the Internet of value [2], which is a distributed ledger database for a peer-to-peer network.

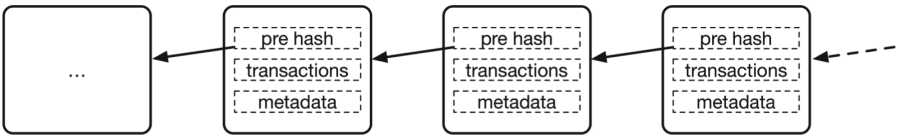

Fig. 1. The structure of blockchain.

As a rule, most innovations do not appear out of nowhere, nor does the blockchain. The blockchain is actually a natural result of that the ledger technology developed into distributed scenarios. Ledger technology has evolved from single entry bookkeeping, double-entry bookkeeping, digital bookkeeping to distributed bookkeeping. The blockchain structure (Fig. 1) naturally solves the problem of multiparty trust in distributed bookkeeping [3].

Due to its decentralization, tamper-resistance, safety and reliability, the block-chain technology has received extensive attention since its birth. After nearly 10 years developing, the blockchain technology has experienced the period of v1.0-bitcoin, v2.0-Ethernet and v3.0-EOS. Not only has the technology itself been greatly expanded and developed, but it has also been applied in many fields.

1.2 Blockchain Classification

According to the way users participate, blockchains can be classified into Public Blockchain, Consortium Blockchain and Private Blockchain, and also can be classified into main chains and side chains based on the relationship of chains. In addition, several blockchains can form a network. The chains in the network are interconnected in order to generate the Interchain [4].

Public Blockchain: a consensus blockchain that everyone can get an access to. He or she in the blockchain topology can send transactions and validated. Everyone can compete for billing rights. These blockchains are generally considered to be "completely decentralized", typical use like the bitcoin blockchain, in which the information is completely disclosing.

Private Blockchain: a blockchain in which the permission to write remain in one organization. The permission to read can be public or limited to some extent. Within a company, there are additional options, such as database management, audit, and so on. In most cases, public access is not necessary.

Consortium Blockchain: in between Public Chain and Private Chain, it refers to the blockchain whose consensus process is controlled by pre-selected nodes. For example, there is a system of 15 financial institutions, each of which

manages one node, and at least 10 of which must confirm each block to be recognized as valid and added to the chain. The right to read the blockchain can be open to the public, or limited by participants, or "hybrid". Such chains can be called "partially decentralized".

1.3 Paper Organization

At present, the blockchain has received much attention for its own characteristics, and has been applied in many fields including finance. However, there is little concern and research on its network security. Therefore, this paper introduces the birth, development and application of blockchain technology in detail, comprehensively searches and investigates various documents targeted on the security needs of blockchains, and systematically analyzes the security threats and defense technologies of blockchains.

The Sect. 2 of this paper introduces applications of the blockchain in different fields. The Sect. 3 focuses on the security threats in different layers of blockchains and summarizes common attacks. The Sect. 4 summarizes the research progress of blockchain security protection technologies. At the end of this paper, we summarize the work of the full paper.

2 Blockchain Applications

The large-scale digital currency system represented by the Bitcoin network runs autonomously for a long time, through which it supports the global real-time reliable transactions that are difficult to achieve in the traditional financial system. This has caused infinite imagination for the potential applications of the blockchain. If the business value network based on the blockchain gets real in the future, all transactions will be completed efficiently and reliably, and all signed contracts can strictly follow the agreement. This will greatly reduce the cost of running the entire business system, while sharply improving the efficiency of social communication and collaboration. In this sense, the blockchain might trigger another industrial revolution as the Internet did.

In fact, to find the right application scenario, we should proceed from the characteristics of the blockchain itself. In addition, you need to consider the reasonable boundaries of the blockchain solution. For example, blockchain applications for mass consumers need to be open, transparent, and auditable, which can be deployed on a borderless public chain or on a blockchain that is commonly maintained by multicenter nodes.

The application of blockchain in the financial services is the most concerned currently, and many banks and financial institutions around the world are the main promoters. At present, the processing after global securities trading is very complicated. The cost of liquidation is about 5–10 billion dollars. The post-trade analysis, reconciliation and processing costs exceed 20 billion dollars. According to a report by the European Central Bank [5], the blockchain, as a distributed ledger technology, can make a good deal with the cost of reconciliation and

simplify the transaction process. Relative to the original transaction process, the ownership of the securities can be changed in near real time.

Blockchain can be used for ownership and copyright management and tracking. It includes transactions of valuables such as cars, houses and artworks, as well as including digital publications and digital resources that can be tagged. For example, Factom tried to use blockchain to revolutionize data management and logging in business societies and government departments. Similarly, in response to the problem of food fraud, IBM, Wal-Mart and Tsinghua University jointly announced at the end of 2016 that blockchain will be used to build a transparent and traceable cross-border food supply chain [6]. This new supply chain will improve the traceability and logistics of food and create a safer global food market.

While enjoying the convenience of cloud storage, we will inevitably mention privacy concerns. This concern comes from two aspects. One is that the storage center may be attacked by hackers, causing their own data outflow, and the second is that the company wants to get more profits to abuse the privacy of users. Blockchain solves these problems perfectly. At present, there are many distributed cloud storage projects, such as Sia, Storj, MadeSafe, and IPFS in foreign countries, and FIGTOO and GNX in China. InterPlanetary File System (IPFS) is a global, peer-to-peer distributed file system, which aims to supplement (or even replace) Hypertext Transfer Protocol (HTTP), seeks to connect all computing devices with the same file system. Replacing domain-based addresses with content-based addresses to get a faster, safer, more robust, and more durable web [7].

The relationship between FIGTOO and IPFS: IPFS is a peer-to-peer hypermedia protocol and a distributed web and FIGTOO is developed on the basis of its open source. It is a branch of IPFS, which is equivalent to bitcoin and Ethereum in the blockchain. The infrastructures are all based on the blockchain. FIGTOO creates a shared trading market for free storage space and shares global storage resources through the shared economy model. It uses red chain technology to store files in slices, builds decentralized cloud storage and becomes the infrastructure of global red chain distributed file storage [8].

User Generated Content (UGC) is one of the important aspect of blockchain application. In the era of information explosion, how to quickly find the most important content from the overloaded information has become a core issue of the Internet. UGC Network is the world's first content value forecasting platform, a fair and value-driven content-incentive network with the mission of creating a content-driven blockchain value community that differentiates truly valuable content and achieves a reasonable return [9]. It committed to solving problems such as excellent content discovery and pricing on the UGC platform, unreasonable distribution of benefits, and centralized content storage.

Other UGC applications include YOYOW (You Own Your Own Word) - a blockchain-based UGC platform that all processes rely on interest-based implementation. It solves the problems in current content platform like lacking of high-quality content incentives, community pollution (piracy and Advertising)

serious [10]. BiHu - a token investor vertical community. In the BiHu, the user's contribution will be rewarded with the token (KEY) representing the BiHu and its surrounding ecological use rights [11].

Due to its decentralization, eliminating trust, tamper-resistance, safety and reliability characteristics, the blockchain technology has been used in lots of fields including financial services, credit and ownership management, trade management, cloud storage, user-generated content, copyright protection, advertising and games. In these cases, blockchain either solves the problems of multiparty trust in the transaction, or reduces the costs and risks of traditional industries.

3 Blockchain Security Analysis

3.1 Security Situation

With the blockchain technology has been widely used, various types of attacks have emerged. Such as from the more and more digital currencies have been stolen to the exchanges have been attacked and other events. According to the statistics of the BCSEC on the blockchain attack events, about 2.1 billion dollars of economic losses due to blockchain security incidents in 2018 [12]. These are only a part of the currently exposed, and as the value of blockchain increases, the number of attacks will continue to increase (Fig. 2).

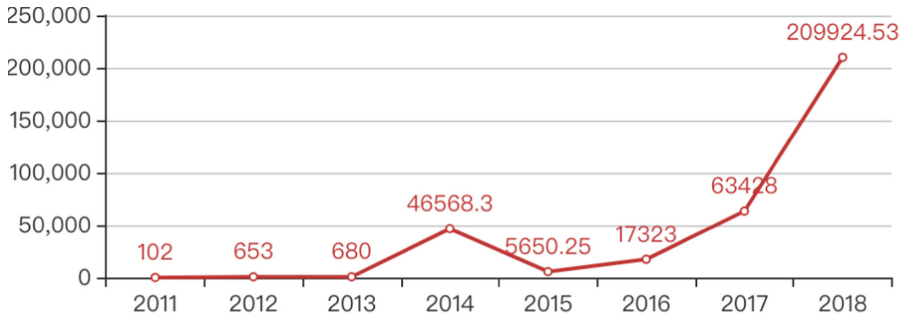

Fig. 2. Economic losses caused by blockchain security incidents (ten thousand dollars).

Blockchain technology itself is still in the initial stage of rapid development, and its security is far behind the needs of development. The risks may come from attacks by external entities or internal participants. The popularity of blockchain makes new demands on security and privacy protection on data storage, transmission and applications, and puts forward new challenges to existing security solutions, authentication mechanisms, data protection, privacy protection and Information regulation.

With the current recurrence of a series of digital currency theft, hacking of exchanges, and theft of user accounts, it is urgent to establish one or more collaborative security solutions to improve the security performance of the blockchain system.

3.2 Security Analysis of Each Layer of Blockchain

The current blockchain structure can be roughly divided into application layer, smart contract layer, incentive layer, consensus layer, network layer and data layer from top to bottom. The security analysis of each layer will be performed separately below.

Application Layer. Application layer security mainly covers the security issues of centralized nodes such as the exchanges which involve digital currency transactions and manage large amounts of funds. These nodes are at any point of failure of the entire blockchain network, and the attack yield is high and the cost is low, which is the preferred target of the attackers [13].

Unauthorized Access to An Exchange Server. Exchanges often deposit large amounts of money and are easily targeted. Once the exchange server authority is obtained and the key information is modified, the attacker can steal the funds key, tamper with the transaction amount or leak sensitive information, causing economic and reputational devastating blows to the exchange.

For example, the Youbit (formerly Yapizon) stolen event. On April 22, 2017, 4 hot wallets of Youbit were stolen, lost 3,816 BTC, with a total value of about $5,300,000, accounting for 36% of the exchange's funds. On December 19, 2017, Youbit announced that it was attacked again, lost approximately 17% of its assets, and at the same time announced the exchange closed and entered the bankruptcy process [14].

Exchange DDoS. Due to the high demand for network bandwidth in the trading platform, once a DDoS attack occurs, it is very serious for the platform and the entire industry. If the trading platform is attacked by DDoS, not only will itself suffer losses, but the transaction volume of the blockchain currency will also be greatly reduced, which will indirectly affect the rise and fall of the blockchain currency [15].

According to the report of global DDoS threat landscape Q3 2017 by Incapsula [16], although its industry scale is still relatively small, Bitcoin has become one of the top 10 industries which are most vulnerable to DDoS attacks. This reflects to a certain extent that the entire blockchain industry is facing serious DDoS security challenges. For example, from November 2017 to December 2017 Bitfinex announced that it had suffered the DDoS attack for three times, and all the services of the exchange had been shut down for a long time [17]. The attacker creates pressure on the server by creating a large number of empty accounts, causing related services and APIs to go offline for hours.

Employees Host Security. On June 20, 2011, the large Bitcoin exchange Mt.Gox was attacked. Its server was not compromised, but the attacker gained access to a computer used by an auditor of Mt.Gox, and got a read-only database file, resulting in about 60000 users' username, email address, and encrypted password [18] to be leaked. After obtaining this sensitive information, the attacker

cracked the password of one of the large accounts, issued a large sales message through this account, and sold 400,000 BTC [19] under it, trying to transfer funds through the legal transaction process. Fortunately, because the exchange protection measures are effective, it limits the maximum value of $1,000 BTC per account per day, so it does not cause much damage to this account. However, a large number of BTC sale requests caused the exchange BTC price to drop to 1 cent, resulting in an impact of approximately $8,750,000 in assets.

Malicious Program Infection. Once a malicious program is implanted into the exchange system, it is likely to cause a large amount of sensitive information leakage, including key and wallet files. The key is everything, and the leakage of sensitive information often means losing control of all assets. The exchange Mt.Gox was attacked in 2014. The key file of Mt.Gox was stored locally in clear text, and the key file wallet.dat leaked due to Trojan infection, resulting in a large amount of asset loss and eventually, Mt.Gox went bankruptcy [20]. It is worth noting that in this attack, the attacker used two years to gradually transfer assets in order to avoid the community recovering the loss through hard forks. The emergence of this type of APT attack means that monitoring of the threat of attack in the blockchain industry cannot rely solely on short-term anomaly transaction monitoring.

Initial Coin Offering. Tampering Attack: When ICO raises funds, it usually hangs the receiving address on the project official website, and then the investor will transfer money to this address for the corresponding token. Hackers can tamper with the collection address through attacks such as domain hijacking, web vulnerabilities, or social engineering.

Phishing attack: The attacker uses social engineering and other means to impersonate the official, allowing the user to transfer money to the attacker's wallet address. For example, an attacker can use an approximate domain name and highly phishing website to defraud investors or use email to disseminate fake information, such as ICO project's payment address change notice, etc. or disseminate phishing information on social software and media to defraud investors.

Mining Machine System. The cyber security awareness of mining device manufacturers is uneven, and because of its closed source characteristics, the security of its code cannot be checked by the public. Once a cyber security issue occurs, the result is fatal. And whether the device manufacturer will intersperse the back door for remote control of the device, or steal the mining output, is still remain to be discussed.

0day: Most mining system is a general-purpose system. Once a mining system is found to have a 0 day vulnerability, the security barriers of the system will be broken in an instant. The attacker can use the vulnerability to obtain the modify permission and then tamper with reward receiving address and then hijack the user's reward.

Weak password attack: At present, the mining system in the market is based on the B/S architecture. Access to the mining system is usually through the web or other means. If the weak password is used, it will be vulnerable to intrusion.

Mining Pool. By June 2018, the top five Bitcoin mining pools in the world are BTC.com, AntPool, SlushPool, BTC.TOP and F2Pool. About 60% of the world's hash power is in the hands of Chinese miners [21].

Hash power forgery attack: The mining pool will test the actual hash power of the current miner through a certain proof of work test algorithm. The hacker can falsely report the hash power by finding the vulnerability of the algorithm, and then obtain the excessive reward that doesn't match the actual contribution.

Selfish mining attack: A malicious mining pool decides not to release the block it finds, and thus creates a fork. When the private fork is longer than the public chain, the malicious mining pool issues the private fork. Because the fork is the longest chain in the current network, it will be recognized as a legal chain by honest miners, so the original public chain and the honest data it contains will be discarded. The results of the study indicate that the malicious mining pools will yield more benefits normally by using selfish mining strategies. But such attacks usually require huge hash power as a support.

Centralization: The existence of the mining pool violates the principle of decentralization of the blockchain. Theoretically, if it can control at least 51% of the hash power of entire network, it will be able to monopolize the mining right, billing right and distribution right, which will affect the ecological security of the blockchain, so that the credit system of the cryptocurrency will cease to exist and the cryptocurrency system will be completely destroyed.

Possible Methods. It is impossible for any one party to respond to various attacks at the application layer. The application developers should ensure that the softwares don't contain discovered vulnerabilities and are thoroughly tested. As the central node, such as a trading platform, real-time monitoring of system health and some protected methods (e.g. data encryption storage, etc.) are required to ensure that the system is not subject to internal and external attacks. All employees should be systematically trained before they are employed to avoid becoming an attack portal. As a user, you should be able to keep your own account and key properly, distinguish between true and false information and be cautious in trading to avoid phishing attacks.

Smart Contract Layer. A smart contract is more than just a computer program that can be executed automatically. It is a system participant. It responds to the received message, it can receive and store value, and it can send out information and value [22]. For the security risks of smart contracts, the following attacks are summarized.

Reentrancy Attack. The essence of reentrancy attack is to hijack the contract control flow and destroy the atomicity of the transaction, which can be understood as a logical race condition problem. For example, The DAO was attacked,

and the attacker used the vulnerability in the contract to launch a reentrancy attack and gained 60 million dollars. In order to recover this part of the funds, the Ethereum community decided to perform a hard fork, roll back all the transaction records since the start of the attack and fix the contract vulnerabilities in the new branch. The vulnerability is described below. Here is a simplified version of The DAO contract:

```
contract SimpleDAO {
  mapping (address => uint) public credit;
  function donate(address to){credit[to] += msg.value;}
  function queryCredit(address to) returns (uint){
    return credit[to];
  }
  function withdraw(uint amount) {
    if (credit[msg.sender]>= amount) {
      msg.sender.call.value(amount)();
      credit[msg.sender]-= amount;
    }
  }
}
```

Participants call the donate function to donate their own Ether to a contract address, the donation information is stored in the credit array, and the recipient contract calls The DAO's withdraw function to receive funds. Before actually sending the transaction, The DAO checks if there is enough donation in the credit array, and after the transaction is over, the transaction amount is reduced from credit.

The attacker first constructs a malicious contract Mallory, as follows:

```
contract Mallory {
  SimpleDAO public dao = SimpleDAO(0x354...);
  address owner;
  function Mallory(){owner = msg.sender; }
  function() { dao.withdraw(dao.queryCredit(this)); }
  function getJackpot(){ owner.send(this.balance); }
}
```

After Mallory deployed, the attacker calls The DAO's donate function to donate a bit of Ether to the Mallory contract. After triggering Mallory's fallback function (unnamed function), there are many trigger methods, such as transfer money to Mallory. The fallback function will call The DAO's withdraw function and extract all the funds that belong to it. It seems to be no problem so far. However, after msg.sender.call.value(amount)() in the withdraw is executed, Mallory's fallback function is automatically called after the transfer is completed due to the transfer operation feature, so the withdraw function is called again. Because credit is not updated at this time, so you can still withdraw money

normally, then you fall into a recursive loop, and each time you can extract a part of Ether in the DAO to the Mallory contract.

This loop will continue until one of three conditions occurs, gas is exhausted, the call stack is full, and The DAO balance is insufficient. An exception is thrown when one of the above conditions occurs. Due to the characteristics of the Solidity exception handling, all previous transactions are valid. Theoretically, repeating this operation can extract all the Ether of The DAO's to Mallory.

Unauthorized Access Attack. Most of this attack due to failure to make explicit function visibility, or fails to do sufficient permission checks, which can cause an attacker to access or modify a function or variable that should not be accessed.

For example, a multi-signature contract vulnerability in the Parity wallet was exploited by an attacker to steal a total of 153,037 Ether in three times. Then Parity official blog and Twitter released security alert [23] and updated the new version of the library contract. The bug comes from the Multi-Sig library file enhanced-wallet.sol written by Parity's founder Gavin Wood. The attacker exploited the bug to reset the wallet owner, took over the wallet and stolen all the funds. This is essentially a breach of authority in the contract.

Solidity Development Security. Possible bugs when writing smart contracts include:

Race condition: The biggest risk of calling an external function is that the calling behavior may cause the control flow to be hijacked and accidentally modify the contract data. This type of bug has many specific forms, such as reentrant and cross-function race conditions.

Transaction-Ordering Dependence: A attacker can construct his own transaction based on the order information contained in the pending transactions, and try to get his transaction to be written into the block before others.

Integer overflow and underflow: When programming, you should think about whether integer overflows can occur, how the state of uint variables will be transferred, and who has the authority to modify those variables.

Denial of Service Attack Based on Exception Rollback: For example, a crowdfunding contract gives a refund to a participant. The contract may need to traverse an array to process a refund for a group of users. The simple idea is that every refund is successful, otherwise the program should be rolled back. The consequence of this practice is that one of the malicious users forced the refund to fail and all users were unable to receive the refund. It is recommended to use a pull payment mechanism, which separates the refund operation into an independent function, which is called by the refund recipient to pull the refund.

Possible Methods. Once a smart contract is deployed in a distributed, decentralized network, it is difficult to change. It prevents data manipulation and establishes a trust mechanism based on the encryption algorithm. On the other hand, when the blockchain is facing a security attack, it lacks an effective correction mechanism and is difficult to reverse. Therefore, before the development of smart contracts, it is necessary to guard against the vulnerabilities that have

already occurred. It should conduct sufficient security tests before issued. Professionals perform code optimizations in a timely manner, conduct regular code audits, and monitor abnormal behavior of deployed contracts to reduce losses.

Incentive Layer. The purpose of the incentive layer is to provide certain incentives to encourage nodes to participate in the security verification of the blockchain. The security of the blockchain depends on the participation of many nodes. For example, the security of the Bitcoin blockchain is based on the great hash power that many nodes participate in the proof of work which makes it impossible for an attacker to provide a higher amount of computation. The verification process of a node usually consumes computing resources and electric power. In order to encourage node participation, the blockchain usually rewards participants in the form of virtual currency. Bitcoin, Litecoin, and Ether are all products of this mechanism.

Blockchain projects need to adapt to the market to automatically adjust the rewards, rather than simply reducing them. In the blockchain project reward mechanism, when the node's working cost is close to or greater than the income, they often choose not to work for this blockchain, which can easily lead to centralization problems.

Consensus Layer. The consensus mechanism gives the blockchain the soul to differentiate it from other P2P technologies. Commonly used consensus mechanisms are Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). The possible attacks include Bribe Attack, Long-Rang Attack, Accumulation Attack, Precomputing Attack and Sybil Attack. Table 1 shows the application scope of the attacks for the consensus mechanisms.

Table 1. Attack methods and application scope for consensus mechanism

Attack methods	PoW	PoS	DPoS
Bribe Attack	−	+	−
Long-Range Attack	−	+	+
Coin Age Accumulation Attack	−	+	+
Precomputing Attack	−	+	−
Sybil Attack	+	+	+

At present, the existing consensus mechanisms are not perfect, and it is necessary to explore a more secure and faster consensus mechanism while increasing the difficulty of existing attacks.

Network Layer. The information transmission of the blockchain mainly depends on the peer-to-peer network. The P2P network relies on nearby nodes

for information transmission in which it must expose each other's IP. If there is an attacker in the network, it is very easy to bring security threats to other nodes. The node of the public blockchain network may be an ordinary home PC, a cloud server, etc., and its security must be uneven. There must be a node with poor security, and attacking it will directly threaten the other nodes. The main attacks are as follows.

Eclipse attack: The node is kept in an isolated network by hoarding and occupying the victim's slots. This type of attack is designed to block the latest blockchain information from entering the eclipse node, thereby isolating the nodes [24].

BGP hijacking: At present, the security researchers have proved the conceptual feasibility of the attack. From November 5, 2015, to November 15, 2016, through the analysis and statistics of the node network, most of the bitcoin nodes are currently hosted in a few specific Internet Service Providers (ISP), while 60% of Bitcoin connections are in these ISPs. Therefore, these ISPs can see 60% of Bitcoin traffic, and can also control the traffic of the current Bitcoin network. The researchers verified that at least two attacks are conceptual feasible through the hijacking scenario, and given validation code [25].

The security defense for the network layer can be mainly improved from two aspects: P2P network security and network authentication mechanism. In the transmission process of the network, a reliable encryption algorithm is used for transmission to prevent malicious attackers from stealing or hijacking the node network. Strengthen the validity, rationality and security of data transmission in network. Client nodes should do the necessary verification for important operations and information.

Data Layer

Block Data. Malicious information attack: Write malicious information, such as virus signatures, politically sensitive topics, etc. in the blockchain. With the data undelete feature of the blockchain, information is difficult to delete after it is written in the blockchain. If malicious information appears in the blockchain, it will be subject to many problems.

A team of researchers at the RWTH Aachen University and the Goethe University Frankfurt in Germany pointed out that among the 1,600 documents added to the Bitcoin blockchain, 59 files contained links to illegal children's pictures, politically sensitive content or privacy violations [26]. Currently, only a few Bitcoin blockchain transactions contain other data. In the Bitcoin blockchain, about 1.4% of the 251 million transactions contain other data, that is, only a few of these transactions contain illegal or undesirable content [26]. Still, even such small amounts of illegal or inappropriate content can put participants at risk.

Signature and Encryption Method. Cryptography is the key to ensure the security and tamper resistance of blockchain, and blockchain technology relies heavily

on the research results of cryptography, which provides a key guarantee for the information integrity, authentication and non-repudiation of the blockchain.

As a mainstay of the blockchain, the encryption technology is particularly important. For example, the MD5 and SHA1 hash algorithms popular in previous years but have been proved to be insufficiently secure. At present, the SHA256 algorithm is widely used in bitcoin. So far, this algorithm is still safe, but with the development of new technology and research, it may not be safe in the future. Therefore, when designing blockchain applications, it is important to carefully choose the encryption method. Current mainstream signature methods include aggregate signature, group signature, ring signature, blind signature, proxy signature, interactive incontestable signature (IIS), blinded verifiable encrypted signature (BVES), and so on.

Attacks on cryptographic algorithms, especially the hash functions, include brute-force attack, collision attack, length expansion attack, back door attack and quantum attack.

3.3 Network Supervision of Blockchain

While blockchain brings technological innovation, it also brings huge challenges for network supervision. The traditional supervision mode is mostly centralized management. How to use the blockchain technology and the current legal system to supervise the application of the blockchain is one of the problems that the government and the industry pay attention to.

In order to overcome the problems of blockchain in network supervision, it is necessary to cross the underlying technology and think about how to combine the specific cases of technology application with supervision. At present, by classifying application cases, they can be divided into three categories, "Recycling Box", "Dark Box" and "Sandbox" [27]. The application cases in each category bring many challenges for the legal, supervision and decision-making departments. The three categories are fully analyzed below.

3.4 "Recycling Box"

"Recycling box" are those cases that attempt to solve industry pain points through blockchain solutions in a better, faster, and cheaper way. Their goals are not illegal, and the motivation is simple. In the process of the application launched, the network supervision authorities can implement supervision only by making minor modifications to the current supervision framework.

The most typical example is the interbank settlement system developed by Ripple. The payment solution uses a single distributed ledger to connect the world's major financial institutions and cross-bank transactions that occur between each other can be done in real time. Compared with the traditional method, it not only saves a lot of time, improves efficiency, but also saves a service fee [27].

3.5 "Dark Box"

"Dark box", its source is similar to "dark net". Cases belonging to this category, without exception, all contradict the current law. Such cases are numerous, for example, the online drug market, the arms market or other illegal goods market, human trafficking networks, terrorist financing and communication networks, money laundering and tax evasion can all be classified as such. These illegal services have existed in the dark network for a long time. Nowadays, because of the application of blockchain technology, some of them are like discovering the New World. It's easy to identify the "dark box", but it can be difficult to try to stop them [27].

The reason why the "dark box" is difficult to be stopped is that in recent years, the digital currency has become an important tool for money laundering, illegal transactions, and escaping foreign exchange control due to its anonymity and decentralization. Digital currency does not require a credit card and bank account information. Criminals can avoid the supervision agencies and cannot trace the source and destination of funds through traditional capital transaction records, which makes traditional supervision methods malfunction.

3.6 "Sandbox"

The "sandbox" is one of the most exciting and headaches for legislators in these three categories, and many of the most disruptive and public interest cases fall into this category. The term "sandbox" was taken from a recent initiative by the Financial Conduct Authority (FCA) called "Regulatory Sandbox". Application cases belonging to this category have very valuable business objectives, but the current situation is that due to the various characteristics of the distributed ledger technology, most of these cases cannot meet the existing supervision requirements. Their common feature is what the business pursued is legal, but it may cause various risks, so the government will not let it go and will have appropriate supervision.

The typical case is peer-to-peer(P2P) funding. It is necessary to mention the venture capital fund The DAO based on the blockchain. Although The DAO's ICO is no different from ordinary venture capital, their goals are all to invest in a startup. It seems to have nothing to do with illegality. However, the way The DAO works is not normal at all, which is one of the reasons why it will be incompatible with the existing legal system.

The DAO has no physical existence, no legal status in any jurisdiction, no leadership, management, or even employees. All operations are automatically done by the blockchain in a decentralized manner. It is not responsible to anyone except those anonymous donors. TechCrunch commented on such organizations as "completely transparent", "shareholders have full control", and "unparalleled flexibility and self-governance".

At present, the skills possessed by most of the regulators are highly specialized, and they are only suitable for a certain place. The applications of blockchain are mostly global, and the coverage area is very wide. This also explains why the

FCA's proposed regulatory sandbox program has suffered a cold spot as soon as it was launched, and many blockchain startups have expressed no interest in it.

4 The Current Status of Blockchain Security Protection

Blockchain technology is currently in the early stage of development. There are many security issues from the underlying technology to the upper application. The third chapter has analyzed the vulnerabilities of each layer of the blockchain and the possible attacks. At present, when studying blockchain security, most of the scholars mainly focus on integrity, privacy protection and scalability [4].

Defenses against these attacks have been given in some papers. In the blockchain integrity protection aspect, for example, for selfish mining attacks, Eya [28] and Heilman [29] both proposed defensive measures. The existence of Proof of Work mechanism and the large number of honest miners make the blockchain integrity protected.

Although the blockchain provides anonymization, it is not completely anonymous. The attacker can still perform certain mapping by analyzing network traffic and transaction information. In the literature [30–32], scholars analyzed and advanced a hybrid mechanism. It's main idea is that the user sends some bitcoin from an address and puts the bitcoin into another address in such a way that it is difficult to find the correspondence between the input and output addresses of the same user. At present, there are two main types of methods for blockchain privacy protection: One is to add an anonymous protection mechanism to an existing blockchain through a technology such as "secure transmission". Another possible approach is to create a new blockchain that is incompatible with the Bitcoin system, such as Zerocash, which provides anonymity by using new primitives in its block [33]. In fact, some more forward-looking technologies have been studied to obtain a better anonymity guarantee, such as Coin join solutions, software that provides anonymous functionality (e.g. Mimble wimble) and next-generation encryption technology represented by attribute-based encryption.

Cryptography is the cornerstone of blockchain technology. Once the hash function or encryption algorithm is no longer secure, the security of the blockchain will no longer exist. The hash function SHA256 and the encryption algorithm elliptic curve cryptography used for the blockchain are still safe, but with the development of new technologies (e.g. quantum computing), its security remains to be discussed. Therefore, we should pay attention to new research results in a timely manner and actively seek more secure algorithms.

Blockchain technology currently has many security problems, but any innovative technology needs a process of continuous problem solving from birth to maturity, so as the blockchain. What's more, features of the blockchain like eliminating the center, eliminating trust, and tamper-resistance, can solve problems exist in many industries.

5 Conclusion

As an emerging technology, the inherent data security and effective privacy protection make the blockchain industry be used more and more widely. However, it is worth noting that with the expansion of its application, more and more new types of security threats are emerging targeted on the blockchain. The way to strengthen the security protection of the blockchain needs further research indeed.

The second chapter of this paper introduces the application scenarios of blockchain technology in different fields and analyzes the corresponding projects. The third chapter focuses on the security analysis of the technology and application of each layer of the blockchain, and summarizes the vulnerabilities and possible attacks. The fourth chapter summarizes the current status of blockchain security protection, it shows that more research is needed on the security aspect.

According to a large number of papers have been researched, most users and researchers of the blockchain pay more attention to the application of blockchains and technology itself, but less attention and researches to security. We think blockchain anonymity research and upper-level security, especially smart contract layer and application layer security requires continuous attention and research. I hope that the work of this paper can alert the practitioner "network security of the blockchain is still waiting for deeper research".

References

1. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
2. Zhao, G.: Blockchain: the cornerstone of the value Internet. Publishing House of Electronics Industry, Beijing (2016)
3. Yang, B., Chen, C.: Blockchain Principle, Design and Application. China Machine Press, Beijing (2017)
4. Fang, W., Zhang, W., Pan, T., et al.: Cyber security in blockchain: threats and countermeasures. J. Cyber Secur. **3**(2), 87–104 (2018)
5. Distributed ledger technologies in securities post-trading. https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf. Accessed 4 July 2018
6. IBM News. https://www.ibm.com/news/cn/zh/2016/10/19/D468881I72849Y25.html. Accessed 4 July 2018
7. Benet, J.: IPFS - Content Addressed, Versioned, P2P File System. https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf. Accessed 4 July 2018
8. RedChain White Paper. https://cdn.thiwoo.com/RedChain/reeed_white.pdf. Accessed 4 July 2018
9. U Network: A Decentralized Protocol for Publishing and Valuing Online Content. https://u.network/U_whitepaper_en.pdf. Accessed 4 July 2018
10. YOYOW White Paper. https://yoyow.org/files/white-paper3.pdf. Accessed 4 July 2018
11. BIHU White Paper. https://home.bihu.com/whitePaper.pdf. Accessed 4 July 2018
12. BCSEC Security Trend Analysis. https://bcsec.org/analyse. Accessed 4 July 2018
13. CHAITIN TECH, ConsenSys.: Blockchain Security Guide. https://chaitin.cn/cn/download/blockchain_security_guide_20180507.pdf. Accessed 4 July 2018

14. Youbit Files for Bankruptcy After Second Hack This Year. https://www.ccn.com/south-korean-exchange-youbit-declares-bankruptcy-after-second-hack-this-year. Accessed 4 July 2018
15. Blockchain Security v1. https://bcsec.org/report. Accessed 4 July 2018
16. GLOBAL DDOS THREAT LANDSCAPE Q3 2017. https://www.incapsula.com/ddos-report/ddos-report-q3-2017.html. Accessed 4 July 2018
17. Bitfinex Attacked Statement. https://twitter.com/bitfinex/status/940593291208331264. Accessed 4 July 2018
18. MtGox Account Database Leaked. https://news.ycombinator.com/item?id=2671612. Accessed 4 July 2018
19. LulzSec Rogue Suspected of Bitcoin Hack. https://www.theguardian.com/technology/2011/jun/22/lulzsec-rogue-suspected-of-bitcoin-hack. Accessed 4 July 2018
20. Bitcoin Trading Platform Mt.Gox Filed for Bankruptcy Protection. http://www.bbc.com/zhongwen/simp/business/2014/02/140228_bitcoin. Accessed 4 July 2018
21. Pool Distribution. https://btc.com/stats/pool?pool_mode=month. Accessed 4 July 2018
22. Smart Contract Wiki. https://github.com/EthFans/wiki/wiki/%E6%99%BA%E8%83%BD%E5%90%88%E7%BA%A6. Accessed 4 July 2018
23. Parity Security Alert. https://paritytech.io/security-alert. Accessed 4 July 2018
24. Heilman, E., Kendler, A., Zohar, A., et al.: Eclipse attacks on Bitcoin's peer-to-peer network. In: Usenix Conference on Security Symposium (2015)
25. BGP Hijack-btc. https://github.com/nsg-ethz/hijack-btc. Accessed 4 July 2018
26. Matzutt, R., Hiller, J., Henze, M., et al.: A quantitative analysis of the impact of arbitrary blockchain content on bitcoin. In: 22nd International Conference on Financial Cryptography and Data Security. Springer, Curaçao (2018)
27. Depth Long Text Interpretation of Blockchain and Supervision: "recycling boxes", "black boxes" and "sandboxes". https://www.pintu360.com/a49882.html?s=87&o=1. Accessed 4 July 2018
28. Eyal, I., Sirer, E.G.: Majority is not enough: bitcoin mining is vulnerable. Commun. ACM **61**(7), 95–102 (2018)
29. Heilman, E.: One weird trick to stop selfish miners: fresh bitcoins, a solution for the honest miner (poster abstract). In: Böhme, R., Brenner, M., Moore, T., Smith, M. (eds.) FC 2014. LNCS, vol. 8438, pp. 161–162. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44774-1_12
30. Valenta, L., Rowan, B.: Blindcoin: blinded, accountable mixes for bitcoin. In: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (eds.) FC 2015. LNCS, vol. 8976, pp. 112–126. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48051-9_9
31. Bissias, G., Ozisik, A.P., Levine, B.N., et al.: Sybil-resistant mixing for bitcoin. In: Proceedings of the 13th Workshop on Privacy in the Electronic Society. ACM (2015)
32. Meiklejohn, S., Orlandi, C.: Privacy-enhancing overlays in bitcoin. In: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (eds.) FC 2015. LNCS, vol. 8976, pp. 127–141. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48051-9_10
33. Sasson, E.B., Chiesa, A., Garman, C., et al.: Zerocash: decentralized anonymous payments from bitcoin. In: Security and Privacy, pp. 459–474. IEEE (2014)