Research on Three types of Economic Crimes under Blockchain Technology and Countermeasures

Yiqun Yao[a#], Jiaxuan Zhang[b#], Wenqi Jing*

Taiyuan University of Technology, Taiyuan China

[a]2372454228@qq.com; [b]15935759605@163.com;
*Corresponding author Email: 2322653520@qq.com
[#]These authors contributed equally to this work and share first authorship.

Abstract. Currently, technology is thriving, and blockchain technology, as an emerging technology, is flourishing, demonstrating an extremely important position in the field of computer innovation. Various industries, especially the finance industry, are currently more closely integrated with blockchain technology, showing a trend towards "blockchain+" development, and are being applied in more occasions and links. But everything has two sides. The characteristics of blockchain technology reflect the necessity and possibility of its application in the field of finance, but on the other hand, the loopholes and drawbacks caused by its characteristics also lay hidden dangers for illegal risks in blockchain financial activities. Many criminals use blockchain technology to rampant criminal behavior. Using virtual currency to carry out online pyramid schemes; Illegal fundraising through absorbing research and development investment and issuing virtual currency; Fraud under the guise of blockchain technology; Spread ransomware to claim Bitcoin and disrupt computer information systems; Using Bitcoin for cross-border currency evasion, concealing illegal assets, and so on. However, there is still a lack of regulatory and specialized laws and regulations in relevant departments in China, and there are still loopholes in network technology. We should improve and enhance it at the technical level and improve it at the regulatory system level.

Keywords: Blockchain crime, big data, virtual currency, criminal law risk

1 INTRODUCTION

With the popularity and application of the emerging blockchain technology, there have been some economic criminal activities, and the number of criminal cases is also increasing. While blockchain itself has advantages in terms of security and transparency, current laws do not specifically target criminal activity associated with the technology. On the contrary, they are treated as ordinary economic crimes and thus comply with the principle of punishment, so this paper combines the technical techniques and laws of three typical blockchain crimes. In practice, it explores the three types of crime countermeasures, the specific crime and punishment, and effectively reflects the principle

R. Magdalena et al. (eds.), *Proceedings of the 2024 9th International Conference on Social Sciences and Economic Development (ICSSED 2024)*, Advances in Economics, Business and Management Research 289,
https://doi.org/10.2991/978-94-6463-459-4_93

of legality. Starting with typical blockchain economic crimes, the author analyzes the importance and necessity of the particularity of related crimes. To provide important reference and basis for promoting the improvement and updating of relevant legislation and policies, to provide support for the revision and improvement of laws and norms, to help strengthen supervision and management, and to maintain the stability and safety of the financial market. To keep abreast of trends in crime and to anticipate new technological tools that may be used in crime, Strengthen the monitoring and prevention of potential crimes, analyze the motives and behavior patterns of criminals, develop more effective prevention strategies and security measures, reduce potential risks, and prevent possible crimes in advance.

As far as the basic laws are concerned, the criminal law norms applicable to blockchain mainly include the "crime of infringing citizens' personal information", "crime of refusing to fulfill the obligation of information network security management", "crime of illegally utilizing information network", "crime of helping information network criminal activities" and so on. "crime of violating citizens' personal information", "refusing to fulfill the obligation of information network security management", "illegal use of information network", "crime of assisting information network criminal activities", etc., while there are fewer crimes and provisions of general civil law applicable to the blockchain. During the rapid evolution of blockchain, the competent authorities have issued some non-regulatory notices and announcements for the sake of expediency, such as "Notice on Preventing the Risks of Bitcoin", "Notice on Preventing the Risks of Token Issuance and Financing", "Notice on Preventing Illegal Fund Raising in the Name of "Virtual Currency", "Blockchain", and so on. Risk Tips on Preventing Illegal Fundraising in the Name of "Virtual Currency" and "Blockchain", and so on. As they are not normative documents, they are not enough for regulations, and thus a large number of viewpoints on the three common blockchain crimes and a new situation in the field of judicial adjudication and practice have emerged in the academic community.

The research method used in the research process of this thesis is are Literature Review - a systematic review of the existing legal literature, regulations, and related literature on blockchain crimes, to understand the current situation in the field of blockchain research, to study this thesis in a clearer and more organized manner; Case Study - an in-depth analysis of one or more specific cases of blockchain that currently exist. existing blockchain one or more specific cases for in-depth analysis, to understand the legal issues, judgments, and impact of the case, in the process of understanding for this thesis to indicate the direction of the research; Policy Analysis (Policy Analysis) - to analyze the formation, implementation and effect of the legal policy to avoid blockchain crimes, to find the weak points, and to analyze the reasons for the emergence of the policy, to facilitate the subsequent emergence of legal provisions and research.

2 THREE TYPICAL TYPES OF BLOCKCHAIN ECONOMIC CRIMES

Blockchain is a decentralized distributed ledger with block-chain storage, tamper-proof, secure, and trustworthy. But its drawbacks such as the bad effects of its crypto-digital currencies in tandem with the dark web reflect the fact that it has many hidden dangers, according to the cluster diagram in the network. There is no relationship between the concept of economic crime and blockchain, but we do see links between blockchain and the economy and finance, such as "fraud" and "money laundering", so there is indeed an important causal relationship between the two concepts[1], In practice, economic crimes directly involving blockchain are mainly concentrated in fraud, illegal absorption of public deposits, fund-raising fraud and helping information network criminal activities. Among them, "cryptocurrency theft", "ICO financing fraud" and "smart contract loophole exploitation" are the most common, and it is necessary to conduct in-depth research.

2.1 Cryptocurrency theft

Cryptocurrency theft refers to the act of hackers or criminals obtaining another person's cryptocurrency through illegal means. This theft can be carried out in several ways, including but not limited to: Attacks on exchanges: Hackers break into the systems of cryptocurrency exchanges to steal the cryptocurrency assets of their users; Phishing sites and fraudulent campaigns: Criminals illegally obtain cryptocurrencies from people by tricking them into providing their private keys or mnemonics through phishing sites, fake ICOs (Initial Token Offerings) and fraudulent campaigns; Malware and phishing emails: hackers develop malware or send phishing emails to steal users' cryptocurrency private keys or access to cryptocurrency wallets.

As a result of the boom in emerging technologies in recent years, many cases of cryptocurrency theft have emerged, which has a rich guiding value in the direction of our blockchain research. It is estimated that between 2009 and 2018, around US$2.5bn was laundered via Bitcoin alone.[2] However, data on illicit activity via cryptocurrency are not reliable and one can assume that a large number of cases go undetected because they involve false identities or unregistered businesses.[3]Therefore, it can be seen that the study of this paper is of great significance. The behaviors committed by the perpetrators of the above-mentioned digital currencies can be divided into two categories. First, the manufacturing behavior (the so-called "mining"), that is, through the use of software on the computer (the so-called "mining machine") to create digital currency behavior, the behavior itself is not theft, the use of software actors did not transfer possession of digital currency, which does not meet the core definition of the act of theft - the core definition of the act of theft. This is not in line with the core definition of theft, which is to exclude others from the possession of property and to obtain possession of that property, and the actor's act of obtaining possession does not constitute the crime of theft.

In cryptocurrency theft, hackers or criminals obtain other people's cryptocurrencies through illegal means. This theft poses a serious threat to the property security of individuals and institutions by attacking exchanges, hacking into the systems of cryptocurrency exchanges, stealing the cryptocurrency assets of their users, etc. This will cause the victim to suffer huge economic losses, and the illegal property obtained by hackers to steal cryptocurrencies will eventually be used for illegal acts or fund illegal activities, which is not conducive to the development of social security.

2.2 Virtual Asset Fraud Based on the ICO Funding Model

ICO behavior is a new type of financing tool based on blockchain technology to issue virtual tokens in exchange for investment, and there are systemic financial risks such as information asymmetry, capital allocation mismatch, and underlying technology risks. Once the risk is realized, the damage result triggered by the act is serious and public. For example, in October 2018, the person in charge of Huizhong Blockchain "ran away", in the name of blockchain in the practice of pyramid schemes, the total amount of money involved in the case reached more than a billion yuan, of which more than 70 people's investment has reached 5 million yuan. Victims claim that such losses are unacceptable to the general public. In individual cases, according to the different legal attributes of the tokens, the act of attributing currency tokens may violate the crimes of illegal absorption of public deposits and fund-raising fraud, while the act of issuing asset tokens may violate the crime of unauthorized issuance of stocks, companies, and corporate bonds, and the act of issuing currency tokens may constitute the crime of counterfeiting currency.[4]

The techniques and practices related to ICO fraud are categorized into the following four types: firstly the first is fake projects, where fraudsters may release fake white papers, roadmaps, and technical specifications under the guise of fake blockchain projects or cryptocurrencies to attract the attention of investors and entice them to invest. Once funds are raised, the fraudster disappears or stops project development. Second False Promises: Fraudsters may publish exaggerated propaganda promising high returns or great future value-added potential to lure investors. Third-social engineering: deception through the use of social media, emails, or fake websites to spread false information as a way to trick investors into trusting and funding the project.

2.3 Smart Contract Vulnerability Exploitation

A smart contract is an automated contract executed on the blockchain, which is essentially a piece of code whose purpose is to specify how to automatically execute the payments in the contract when specific conditions are met. As smart contracts are in charge of huge digital assets on the blockchain platform, they are very likely to become important targets for attackers; the developers of smart contracts are unable to foresee the special environmental conditions that the contracts may face, resulting in the existence of potential security loopholes in the contracts written; it is even more difficult to test the security of the smart contracts written in Solidity language, etc., which makes it impossible to interrupt or terminate the execution of the contracts once the smart contracts are attacked. This makes it impossible to interrupt or terminate the execution of the contract once it is attacked.[5]

The DAO project was initiated by a blockchain company called Slock. it, which is in the business of combining blockchain technology with the Internet of Things (IoT). Slock. it initially wanted to utilize Ether to develop its Universal Sharing Slock. it initially wanted to use Ether to develop its "Universal Sharing Network" (UNSN), which allows users to share and rent various items such as bikes, cars, houses, etc. through smart contracts. Later, Slock. it found this decentralized sharing economy model promising and decided to create a more universal and open platform, The DAO. The DAO project started crowdfunding on April 30th, 2016, and lasted for 28 days. During the crowdfunding period, users were able to exchange Ether for DAO tokens (DAO Token), each of which is equivalent to approximately 1 to 1.5 Ether. The DAO Token not only serves as a medium of value but also as a right to vote. The DAO Token allows users to vote on a variety of project proposals, deciding which ones are worthy of funding and in what amounts. The DAO Project was so popular and supported that it raised over 12 million Ether, almost 14% of the total Ether at the time, and was valued at over $150 million at the time. With over 11,000 users participating in the crowdfunding, The DAO became the largest crowdfunding project at the time and one of the most innovative and influential projects in the blockchain space. However, shortly after the crowdfunding ended, some security experts discovered several vulnerabilities and flaws in The DAO smart contract and warned the community about them. One of the most serious vulnerabilities is the so-called "Recursive Vulnerability" (Recursive Call Vulnerability), which allows an attacker to call the same function multiple times in the same transaction, thereby repeatedly performing certain operations. This vulnerability was exploited by hackers to launch an attack on The DAO pool. The hacker first created a sub-DAO and transferred some Ether to it. Then, the hacker called the splitter function to request that his funds in The DAO be separated and transferred to the sub-DAO. In this process, the hacker exploited the recursive call vulnerability by repeatedly calling the splitter function over and over again, thus continuously separating more Ether from The DAO's pool of funds and transferring it to the sub-DAO. In this way, the hacker was able to exchange a lot of Ether for very little Ether, while the Ether in The DAO funding pool kept decreasing. The hack lasted a few hours and separated a total of 3.6 million Ether, which is a third of the total amount of Ether raised by The DAO. These Ether were transferred to a sub-DAO controlled by the hackers, but due to the rules of the smart contract, the hackers were unable to withdraw these Ether immediately and instead had to wait for a 28-day cooling-off period. This gave the community some time to figure out how to recoup their losses.

In recent years, a series of security vulnerabilities in the field of smart contract applications have occurred frequently, and strengthening the research on security vulnerabilities in smart contracts has become the focus of the industry's current attention. Currently, there are various vulnerabilities in smart contracts, including reentry vulnerability access control vulnerability, denial of service vulnerability, timestamp vulnerability, etc. Among them, reentry vulnerability and denial of service are two frequent vulnerabilities in smart contracts.[6]The attacker consumes computational resources or does not return the expected processing results, destroying the contract's logic in a short period or certain states, causing the contract to fail to execute normally or respond to normal service requests, thus "deadlocking". This leads to a huge difference between the actual results of the calculation and the expected results, which affects the normal logic of the contract and the loss of funds, and causes the increase of project tokens and the value to zero, seriously jeopardizing economic security.

3 EXPLORING THE CAUSES AND OPERATING MECHANISMS OF ECONOMIC CRIMES IN THE BLOCKCHAIN ENVIRONMENT

3.1 Causes of blockchain economic crime on and offline

Lack of relevant regulation

At present, blockchain technology is still in its infancy, and there is a large lack of regulation and governance for it, which has also found loopholes for lawless elements to utilize it for financial crimes. In terms of regulation, there is currently no unified global attitude towards the regulation of digital currencies. It is because of the legitimacy issue and the different attitudes of countries towards the regulation of virtual currencies that the regulation of the entire blockchain financial market is still in the exploratory period. But we can still see that some countries have made some efforts to achieve this, for example, the Department of Defense (DoD) of the United States launched a project to develop an affordable and highly secure supply chain risk management system that is enhanced by blockchain technology using the uniqueness of Physically Unclonable Functions (PUFs) .The wide range and diversity of blockchain applications in the financial field have increased the difficulty of coordinated regulation, from the linkage between sectoral laws such as the bill law, securities law, commercial banking law, company law, etc., to the coordination between different regulators within the financial market, to the consistency of cross-jurisdictional regulation by the same regulator, etc., all of which are facing a higher level and more scientific regulatory exploration. Financial market regulators lack a professional understanding of blockchain, which is an emerging technology, and thus lack potential risk prediction in the regulatory process. The anonymity and decentralization of blockchain also increase the difficulty of risk monitoring and regulation, which is difficult for existing regulatory technology to cope with and has limited regulatory effect.

Technical vulnerabilities and security issues.

The analysis of the overall blockchain ecosystem security report 2019-2022 of Ouko Cloud Chain (OKLink) can conclude that the distribution of security events is highly concentrated. 80% of the global security events occurred on the two public chains ETH and BSC, and nearly 85% of the losses were concentrated in the three chains ETH, SOL, and BSC; phishing attacks and network fraud are the most common attack techniques in blockchain security events. [7]At present, blockchain technology is now still in its infancy and there are still many loopholes. Compared with the traditional transaction mode, the security of the system applying blockchain technology will be improved because of the cryptography used in blockchain technology, but it is not invulnerable, as the computing power of supercomputers continues to progress, the weaknesses of the blockchain technology itself will be more and more obvious, for example, today's quantum computers are able to crack the encryption algorithms which are difficult to crack by the most powerful ordinary computers, and once the password is Once the password is cracked, the transaction information and even the digital signature may be tampered with, and then the secrecy of blockchain technology will be reduced to nothing, providing an opportunity for high-tech economic crimes.

Abuse of darknet and anonymity.

With the development of society, the "advantages" of the "darknet" have been played to the fullest by network hackers. Due to the hidden nature of the "darknet" and its decentralized characteristics, it is mostly used by network hackers for trading all kinds of information. Bitcoin has become a popular exchange medium on dark web marketplaces.[8] Due to the hidden and decentralized characteristics of the "darknet", it is mostly used by network hackers to trade all kinds of information, and the supervisors can only collect and prevent all kinds of criminal information in the "darknet", but can't eliminate it completely, and the network hackers can set up a new site and use the more ingenious blockchain DNS after they are cracked down. [9]In addition, the activities of traditional fraud and pyramid schemes have begun to be carried out offline to online. In the blockchain era, even if the illegal and criminal activities on the chain are in fact organized and carried out by the subjects under the chain, due to the anonymity of the blockchain, the identities of the parties to the transaction are blurred, and the details of the transaction become difficult to trace, so it is difficult for traditional crime management methods to trace these subjects from the chain to the subjects under the chain. The combination of network marketing and network fraud with the false high returns of "blockchain" makes it easier for investors to be deceived and suffer huge losses. Blockchain "anonymity" will divide the world into two parts, that is, in addition to the user himself, it is difficult for other people to correspond to the chain on the chain and the chain off, this feature will greatly impede the accountability of criminal activities on the chain, which is a new challenge for the governance of crime in the blockchain era.

Social engineering attacks.

A social engineering attack is a kind of "social engineering" to implement the network attack behavior. Social Engineering, also known as information spying, was first proposed by Kevin Mitnick, a U.S. network security engineer, in The Art of Counter-Deception, with the starting point of letting people know how to protect information and avoid unnecessary losses caused by personal information leakage. In computer science, social engineering refers to a way of communicating legitimately with another person to psychologically influence them to perform certain actions or reveal confidential information. It is often considered as an act of defrauding others to gather information, cheating, and hacking into computer systems. In common law systems, this behavior is generally recognized as an invasion of privacy. In recent years, more hackers have turned to exploiting human weaknesses, i.e., social engineering methods, to carry out cyber attacks. The use of social engineering methods for information collection at the stamping stage, combining password blasting and locating the target's real information to break through the information security defense measures is also the principle of its attack on blockchain. Currently, this scenario has shown a rising and even proliferating trend. According to Rich Mogull, Director of Information Security and

Risk Research at Gartner Group, "Social engineering is the biggest security risk in the next 10 years, and many of the most destructive behaviors are due to social engineering rather than hacking or sabotage. " Some information security experts predict that social engineering will be an important area of confrontation between intrusion and counter-intrusion of information systems in the future.

3.2 Explore the operation mechanism from three major types of blockchain economic crimes

With the development of technology, the activities of criminals have evolved. With the development of privacy coins and hybrid coin technology, criminals may use blockchain more skillfully to conduct anonymous transactions, increasing the difficulty of regulation. Attacks against smart contracts are likely to increase, and hackers may focus on discovering and exploiting vulnerabilities in contracts for illicit gain.

Cryptocurrency theft

To keep cryptocurrencies safe, investors usually use cryptocurrency wallets, which are categorized into cold wallets and hot wallets, with cold wallets being more secure and hot wallets being suitable for frequent transactions. Criminals can invest or mine cryptocurrencies through phishing websites and lure victims to these websites through various methods. When users enter their wallet private keys on this website, fraudsters can easily transfer their assets, there are also some criminals through false identities and other fraudulent activities to lure people to provide their private key or mnemonic, to illegally obtain their cryptocurrency; malware and phishing emails: hackers to develop malware or send phishing emails to steal the user's cryptocurrency key or access to cryptocurrency wallet privileges.

ICO Funding Scams.

ICO financing scams are designed to raise money from investors, which may seem like an opportunity to get to the bottom of cryptocurrency and have a head start compared to other investors, but it's not. Zhifan Technology and Zhifan Academy released the "2022 Blockchain and Virtual Currency Crime Trend Research Report" (hereinafter referred to as the "Report"). The Report states that in 2022, the number of fraudulent money laundering cases will be at the top of the list, accounting for 30.5% of the total number, which is much higher than other types. The main currency involved is USDT, with the implementation of the "Criminal Law Amendment (XI)", there is a new understanding of money laundering crimes, USDT has gradually become a "self-laundering" of the hardest-hit area, and the perpetrator will be sold through the offline or online way of selling USDT, exchanged for fiat currencies, and then fiat currencies through the "whole to nothing". The mode of cash withdrawal, this mode realizes the conversion of USDT → fiat currency and blocks the traceability of the flow of funds by cash withdrawal, which belongs to the money laundering mode of Article 191, paragraph 1, item (2) of the Criminal Law, "Converting property into cash, financial instruments, and securities". Therefore, the formation of the ICO fund-raising fraud, USDT trading cash mode since the complete industry chain of money laundering.

Smart contract vulnerability utilization.

Compared with the traditional contract, smart contract not only solves the trust problem but also carries a huge amount of digital asset transactions. However, at present, the improper coding and security loopholes of smart contracts have been utilized by lawless elements, which has caused many security problems. Therefore, this paper takes an Ethernet smart contract as an example, and its operation principle is shown in Figure 1:

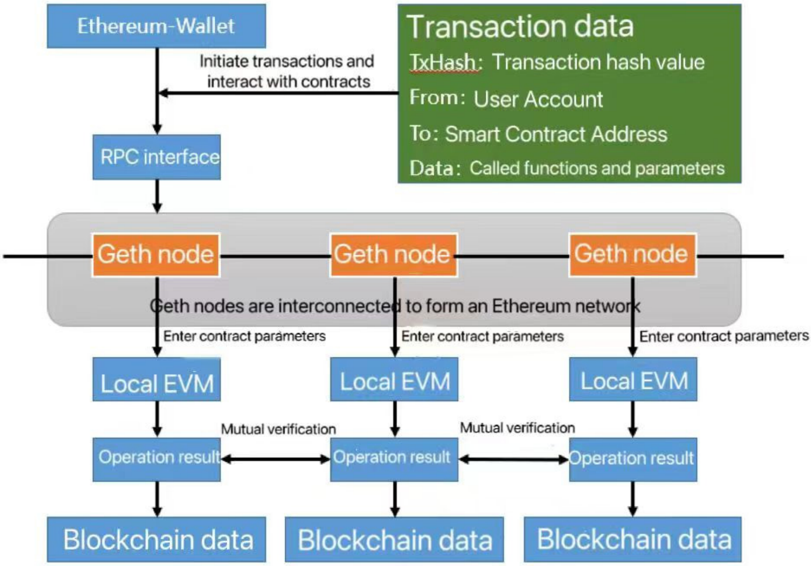
Ethereum-Wallet
Initiate transactions and interact with contracts
Transaction data
TxHash: Transaction hash value
From: User Account
To: Smart Contract Address
Data: Called functions and parameters
RPC interface
Geth node
Geth node
Geth node
Geth nodes are interconnected to form an Ethereum network
Enter contract parameters
Enter contract parameters
Enter contract parameters
Local EVM
Local EVM
Local EVM
Mutual verification
Mutual verification
Operation result
Operation result
Operation result
Blockchain data
Blockchain data
Blockchain data

Fig. 1. -Ether smart contract operation principle

Based on this operating principle, the common security vulnerabilities are:

Denial of Service.

The use of software defects, protocol loopholes, resource suppression of services, and making it reduce or lose availability is known as denial of service (DoS), and the attack behavior that causes DoS is also called DoS attack, the principle is shown in Figure 2. The same as the computer network, smart contracts are also facing the threat of DoS attacks, but the object of the attack from the server to the contract, when the contract has the corresponding security vulnerabilities, the attacker by consuming computing resources or not return the expected results, can be in a short period or in some states to destroy the contract's logic, resulting in the contract can not be executed normally or can not respond to normal service requests, thus "Deadlock".

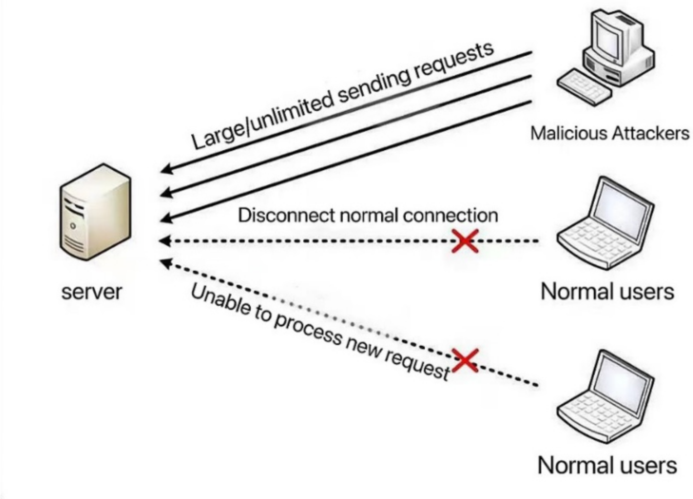
Large/unlimited sending requests
Malicious Attackers
server
Disconnect normal connection
Normal users
Unable to process new request
Normal users

Fig. 2. -Principle of DoS attack

Code Reentry.

In Ethernet smart contracts, reentry vulnerability is possible in any case of passing Gas redundancy because contracts can call each other. Simply put, an external malicious contract controlled by an attacker interrupts the normal execution logic of the target contract by initiating an unintended external call, bypasses the restrictions in the code, and re-enters again and again into the internal execution of the target contract to perform sensitive operations, thus triggering a reentry attack, which is essentially similar to the idea of recursive calls. For example, in August 2021, Cream Finance, a DeFi protocol on Ether, was attacked by a reentry vulnerability, in which the hacker operated a large amount of funds for transactions through a flash loan, resulting in a loss of more than $18 million for the project side. As show in figure 3.

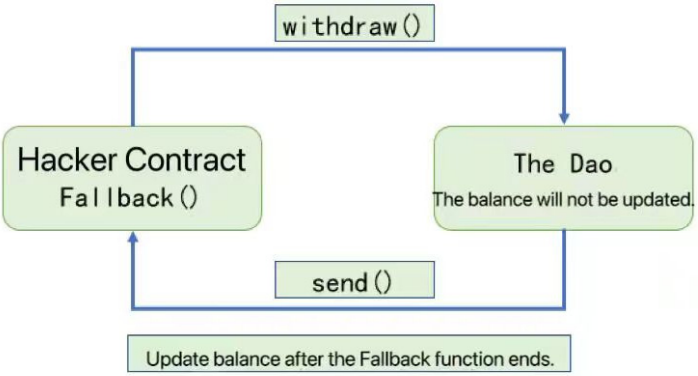
withdraw()
Hacker Contract
Fallback()
The Dao
The balance will not be updated.
send()
Update balance after the Fallback function ends.

Fig. 3. - C ode Reentry Principle

4 COUNTERMEASURE SUGGESTIONS FOR BLOCKCHAIN ECONOMIC CRIMES IN PRACTICE

4.1 Formulation of Relevant Laws and Regulations

Initially, efforts focus on extending existing legislation to encompass real-world issues associated with blockchain technology. Furthermore, regulations should be amended to broaden the scope of legal supervision, such as integrating various forms of digital asset transactions into anti-money laundering regulations. Moreover, institutional measures for governing blockchain crime should absorb beneficial experiences from abroad and merge them with China's national conditions. Finally, while designing legislation, attention should be given to the following: prioritize cybersecurity, emphasize the protection of personal information, manage data throughout its entire lifecycle, and regulate cross-border data flow to safeguard national public interests and the rights of all parties. Also, maintains legal moderation, integrates technology into regulation, and prevents excessive regulation from hindering technological innovation by balancing and defining the relationship between law and technology in the top-level design.

4.2 Enhancement of Tangible and Intangible Regulatory Mechanisms

Regulating blockchain finance should not solely rely on legal norms but should be approached through the entire regulatory system. Initially, it is crucial to embrace the concept of "penetrative" supervision. With the emergence of decentralized, cross-departmental, and cross-jurisdictional financial complexities, there is a need to transcend the institutional regulatory function rigidity, transitioning from regulatory competition to regulatory coordination. Moderate centralization should be adopted to design different permissions for regulators, financial institutions, industrial and commercial departments, judicial departments, and other specific nodes, to meet the needs for judicial inquiries and freezing. Regulatory agencies demand the real-name authentication of specific accounts and require intermediaries to fulfill their duty of good faith. Secondly, it is imperative to fully leverage the "regulatory sandbox" model, as it guarantees the government's regulatory position over businesses, promotes product innovation, and safeguards consumer interests. Lastly, the regulatory function of self-disciplinary organizations should be fully released. This includes leveraging advantages in unifying blockchain technology standards, formulating industry regulations, and standardizing specific operations to effectively complement legal regulation. For this reason, many governments around the world are now looking to regulate for cryptocurrencies, and thus provide an opportunity to audit their flows.[10]

It is important to focus on smart contract auditing and vulnerability repairs. Smart contracts utilize technological means to ensure the complete, timely, and sufficient fulfillment of contracts, using digital code to guarantee trust and low-cost solutions to credit issues in economic activities. It creates a new pathway for resolving credit issues using data. However, the decentralization, lack of regulation, and automatic execution characteristics of smart contracts establish a perfect breeding ground for criminal activities, leading to the emergence of new criminal modes. This presents risks and challenges to the criminal justice system, highlighting the necessity to elevate the safety standards of smart contracts. Establishing and promoting safety standards for smart contracts, instituting review mechanisms, and ensuring developers adopt best practices, will diminish the prevalence of smart contract vulnerabilities.

Additionally, to intensify supervision and regulation of ICO financing fraud, regulatory agencies should enhance oversight of the ICO market, strictly ensuring transparency and compliance. Moreover, the establishment of relevant regulations to penalize non-compliance behavior and the creation of dedicated complaint channels for investigating and promptly addressing investor complaints about ICO projects should be implemented. Furthermore, swift actions should be taken on projects found to engage in fraudulent activities. Meanwhile, it is essential to enhance investor education and raise their awareness of the risks associated with ICO investments. Investors should seek an understanding of critical information such as the project team, and whitepapers, and exercise caution towards projects that promise high returns and excessive hype. Investors should conduct thorough due diligence, and evaluate project credibility, and potential risks by verifying information from multiple sources.

Moreover, it is crucial to strengthen the protection measures for cryptocurrencies. According to the Prosecutor General of the Russian Federation I. Krasnov, the number of crimes in the field of information technology has increased by 25 times and amounted to 294 thousand over the past five years, while only a quarter of them was solved.[11] Therefore, the majority of cryptocurrencies should be stored in offline cold storage devices to prevent network attacks, and funds should only be transferred to hot wallets for transactions when necessary. Additionally, the utilization of multi-signature technology, which requires authorization from multiple private keys to complete a transaction, and the use of hardware security modules to store private keys during usage enhance physical key security. To improve security, introduce two-factor or multi-factor authentication for transactions and account access. Higher-level authentication methods such as biometric technology or hardware tokens can also be utilized.

4.3 Enhance blockchain data mining and analytics technology

Furthermore, to address the increased complexity in tracking virtual currencies due to mixing pools, privacy computing, zero-knowledge proofs, and other techniques involved in the entire process of fund transfer and circulation, it is crucial to intensify research and application of blockchain analysis tools. Investing in and continuously developing advanced blockchain analysis tools will enhance the monitoring, tracking, and analytical capabilities of transactions on the blockchain. Examples include more efficient data storage and retrieval, as well as more advanced data analysis algorithms to extract useful information from massive amounts of data, and more advanced privacy protection technologies to ensure that user's personal information and transactional privacy are adequately protected. For example, technologies such as Zero-Knowledge Proofs (ZKPs) can help authenticate without exposing detailed information. At the same time, analytics tools need to provide more compliance support, including features to meet anti-money laundering (AML) and know-your-customer (KYC) regulations.

Additionally, through the use of blockchain analysis tools, at the initial stage of case assessment, essential indicators of the case's fund pool (such as the scale of the fund pool, freezable fund pool scale, recoverable fund pool scale) and the primary virtual currency transaction paths are identified. Based on this, a case assessment report is generated to aid investigative personnel in quickly grasping significant case clues, opening up case analysis approaches, and making informed case decisions. During the investigation and evidence collection phase, a vast collection of virtual currency address labels is used to trace the funds' origin and to determine if they are linked to criminal activities. This facilitates the identification of individuals associated with the addresses involved and aids in generating evidentiary letters based on the analysis results. In the phase of assessing the funds involved in the blockchain, the transaction behavioral relationships between virtual currency addresses are visually presented to meticulously delineate the complete fund routes and conduct detailed analysis until the comprehensive address relationships are fully restored.

4.4 Enhance the risk perception and security awareness of the public and practitioners

Financial institutions and their regulators should strengthen publicity and education, relying on the large coverage group of financial institutions, popularize blockchain financial knowledge in various forms, enhance the financial literacy and risk awareness of the general public, and avoid blindly participating in the so-called blockchain financial projects under half-knowledge, especially for the timely warning of the prominent risks, for example, the U.S. Securities and Exchange Commission (SEC) has reminded the public through the official website several times that For example, the SEC has repeatedly reminded the public through its official website that ICOs carry market operation risks and high risks of fraud. Relevant government departments should also release relevant information to the public promptly to publicize and educate the public and remind them of the risks, for example, the net credit department should produce some easy-to-understand publicity materials for blockchain technology to enhance the public's knowledge of blockchain; public security authorities should release to the public promptly the cases related to blockchain finance to warn the public of the risks; and the industry and commerce department should strengthen the statistical analysis on the establishment, modification and cancellation of relevant enterprises and provide timely warnings to the public of the risks involved. The industrial and commercial departments should strengthen their statistical analysis on the establishment, change, and withdrawal of relevant enterprises, and make early warning for high-risk enterprises. At the same time, it is important to focus on risk education for blockchain financial institutions to make them clear about their obligations in safeguarding national interests and protecting users' rights and interests, so that they can comply with the law without jumping over the red line, avoid blockchain technology from being used as a tool for crime by improving internal control mechanisms and standardizing business operation processes, and protect the privacy and other legitimate rights and interests of users.

4.5 Promotion of international cooperation and information sharing

Furthermore, promoting international collaboration and information sharing is a crucial measure for combating the frequent occurrence of domestic and foreign money laundering crimes involving virtual currencies. The emergence of widespread money transfer routes across multiple countries has highlighted the need to strengthen communication and cooperation between countries and regions that engage in virtual currency exchange. Establishing a mechanism for anti-money laundering cooperation among organizations such as the Financial Action Task Force (FATF) and its member countries is a vital component of global governance. Strengthening domestic and international cooperation requires deep international collaboration in areas such as information sharing, evidence collaboration, fund tracking, jurisdiction definition, and distribution of work in countries and regions involved in virtual currency money laundering. This multi-faceted collaboration process necessitates the establishment and integration of an anti-money laundering database based on risk assessment models for suspicious virtual currency transactions. This database should be connected online internationally to facilitate improved information exchange and intelligence cooperation. Additionally, advancing judicial assistance, after duly considering legal and regulatory differences, is essential to achieving consensus on issues such as case jurisdiction, regulatory boundaries, and control measures for apprehending criminal suspects. Only through cross-border mutual legal assistance can effective judicial cooperation be achieved. Lastly, an increase in the circulation of digital currencies between countries is unavoidable in the age of virtual economies and would contribute to a certain extent to diminishing the anonymity of virtual currencies, moving towards enhancing anti-money laundering collaboration between different countries.[12]

5 CONCLUSIONS

The emergence of blockchain technology has offered increased tran sparenc y, security, and decentralization to economic transactions. However, as demonstrated in this paper, blockchain-based economic activities are not immune to criminal activities. Although technological nature makes fraud more challenging, there are still challenges and vulnerabilities that enable wrongdoers to exploit blockchain for a variety of criminal behaviors.

This paper has primarily focused on the discussion of typical economic crimes related to blockchain, presenting a comprehensive analysis of the technical means and criminal possibilities. It has summarized the causes of blockchain economic crimes and relevant strategies, advocating for comprehensive action across various aspects such as raising public awareness, enhancing technical tools, and strengthening regulations to efficiently prevent economic crimes in the blockchain. The significance of this dissertation research not only lies in the constructive theoretical opinions on blockchain-related to economic crimes but also in making certain contributions to the improvement of related laws, which is conducive to the maintenance of economic security.

REFERENCES

1. Grosu,V.,Botez,D.,Melega,A.,Kicsi,R.,(2022)Bibliometric analysis of the transformative synergies between blockchain and accounting in the uprooting of economic criminality. Entrepreneurship and Sustainability Issues.,9:77-105. DOI:10.9770/jesi.2022.9.4(3)
2. Canellis,D.,(2018)Here's how criminals use Bitcoin to launder dirty money. https://thenextweb.com/hardfork/2018/11/26/bitcoin-money-laundering-2/
3. Foley,S.,Karlsen,J.， Putninš,T. (2018), Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed through Cryptocurrencies?. https://www.emerald.com/insight/1368-5201.htm
4. Li,X.,Ye,Q.,(2023)On the criminal law system of ICO behavior and tokens under blockchain technology.J.,25:,90-100. https://kns.cnki.net/kcms2/article/abstractv=HR7ide6_o4Trio4oHm8trFNh2L8ihpdTs1bNJFEojBQhZ6Qp0s0mwB9W8QjCEx vH8etGSBowAj-dpT_1Dc2_4wXEqM9WAN1zopDE0E5yqCzVgbroA7AYwYxzKVOr44Wl8er8J6yyk=& uniplatform=NZKPT&language=CHS
5. Shen C. (2023)Research status of security vulnerabilities in intelligent contracts. Information Security Research, 9:1166-1172. https://kns.cnki.net/kcms2/article/abstract?v=HR7ide6_o4Rkb2bMCrOFkVMQvZJgrg4BZemuTkiOdKqogGxM1eWkes6fd9U hN6OV_siZWoJKnR4hWRq-zPnEkZKo63p 2OoG fkxkQi9UfL2vjJUEf0nRO3yaXrFL4LGW9TYfwT9gmn1M=&uniplatform=NZKPT&language=CHS
6. Shi, Z., Shi，Z., Liu , D., Lei，H., Gong，X. Multiple attention mechanism graph isomorphic network intelligent contract source code vulnerability detection [J/OL]. Computer Engineering and Applications: 1-10. https://kns.cnki.net/kcms/detail/11.2127.tp.20240104.1048.012.html
7. Li, D., Sun, J., Jiang, Z., Peng, Y. (2023)Review of Research on the Situation and Security Governance of Virtual Currency Crime. Police Technology, 2: 33-41. https://kns.cnki.net/kcms2/article/abstract?v=HR7ide6_o4Sn1-SnG-WTaZFt-QerfGflsMULUtwn2jgTpdwMx8ZfVPJW9_0t0_NHiWmASJ7LWwyxct-rybJnAe_S1qK5Bq3MHSbXNKQxmYHg8tXo3wlbEH-qUTo9emWT5Fm4dK3bxd7c=&uniplatform=NZKPT&language=CHS
8. Davis,J.,(2011)The crypto-currency, Bitcoin and its mysterious inventor. https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency
9. Wang,J.,Jin,W., Wang,S.,(2020) Analysis of Blockchain Crime Prevention and Control Strategies.J.,34: 42-49, https://kns.cnki.net/kcms2/article/abstractv=HR7ide6_o4S5htexSE6biYqYVQxLiM23K1Uduptab48RrzFOQeDZ4XJ4Ut95k7 556jTSctz2FfkMeAWlK0jIGvAJRx-8aYVbnLWE0S1MxjUgL8cpaIlwUxE-reQk3ZTV636pZfXMcWZM8tWqr5uGwQ==&uniplatform=NZKPT&language=CHS
10. Dyson,S.,Buchanan,W.J.,Bell,L.(2018)The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime.The Journal of The British Blockchain Association,1:1-6. https://doi.org/10.31585/jbba-1-2-%288%292018
11. Egorov, I. (2021) Prosecutor General spoke about the increase in the number of cybercrimes in Russia by 25 times. https://rg.ru/2020/07/17/genprokuror-rasskazal-o-roste-chisla-kiber-prestuplenij-vros sii-v-25-raz.html

12. Feng,C.,(2021)Practice and Conception of Using Big Data Resources and Blockchain Network Security.J., S1: 50-53. https://kns.cnki.net/kcms2/article/abstract?v=HR7ide6_o4Qc_oWGjHAvB2y_UBFx3-SDwiSskjjddPOCGf8BQP7BOVxyG73oZ4iCueIP1HqDMf9B2wjIr_9AJz9PXqaQxYY61PRJ2KAq25QwolCbDpJzr6L8z1f3fQVfv_jvxJz07d1yMv7m0OTw==&uniplatform=NZKPT&language=CHS