

Risk Analysis of Digital Currencies and Their Response Strategies

Yue Zhang

Clermont School of Business,
Clermont-Ferrand, 63000, France
royang1108@gmail.com

Abstract:

With the development of information technology, digital currency has become increasingly familiar as a new type of financial tool. While it boosts the transaction rate, it also brings some hidden dangers. This article focuses on the risk analysis and response strategies of digital currencies. A case study is used to analyze the long-term risk of digital currency and propose countermeasures, summarizing the risks and measures. The decentralized nature of digital currencies is essentially different from that of traditional financial instruments. By analyzing the impact of digital currencies on financial stability, this study explores their risks and the adaptability of their response strategies to the financial regulatory system, starting from technical, market, and legal regulatory aspects, to provide references and suggestions for subsequent related academic research. From the perspective of market participants, this study analyzes the specific manifestations of technical and market risks of digital currencies, which can provide investors with a clear analysis, help them judge the investment value, reduce blind investment behavior, protect the legitimate rights and interests of investors, and maintain the order of the digital currency market.

Keywords: Digital currency, Risk analysis, Response strategy

1. Introduction

In the wave of the global digital economy, digital currencies are emerging. The birth of Bitcoin in 2008 marked the official debut of digital currency. It broke the centralized model of the traditional financial system based on features such as a distributed ledger and encrypted transmission. Subsequently, hundreds of digital currencies such as Ethereum and Litecoin emerged one after another, forming a huge

digital currency market. As of 2024, the global total market value of digital currencies has exceeded one trillion US dollars, attracting extensive attention from individual investors, financial institutions, and even at the national level [1]. The rapid development of digital currencies is inseparable from both technological progress and market demand. First, the maturity of underlying technologies such as blockchain blocks and encryption algorithms supports the security of digital currencies. Secondly, in areas such

as cross-border payments and inclusive finance, digital currencies, taking advantage of their own strengths, some countries have begun to gradually issue central bank digital currencies (CBDCS) in an attempt to include digital currencies in the legal tender system.

However, while digital currency is developing, its risks are gradually being exposed. From a technical perspective, it has exposed vulnerabilities in blockchain systems, mismanagement of private keys, and other vulnerabilities in the security of funds. From a market perspective, digital currency prices are affected by speculative sentiment, policy rumors, etc [2]. From a regulatory perspective, the legal positioning of digital currencies is not uniform globally, and there are regulatory gaps in some regions, which leads to illegal activities such as money laundering and illegal fundraising. This paper analyzes the multi-risk of digital currencies through case studies and proposes countermeasures, and summarizes the risks and measures.

2. An Overview of Digital Currency

2.1 Definition and Characteristics of Digital Currency

Digital currency is a new form of electronic money. Its main feature is that it relies on encryption algorithms and distributed ledger technology to achieve value storage and complete transaction flow. Its essential feature is virtuality, and the entire operation process is completely dependent on computer network systems to perform various functional operations.

Compared with traditional legal tender, digital currency presents the following core features:

Decentralization is a characteristic of digital currency, which is characterized by breaking away from the control of a single authority, relying on the collaboration of mul-

multiple nodes in a distributed network to create an open and transparent ledger system (like blockchain technology), and performing the verification and confirmation steps of transactions through a consensus mechanism, thus breaking through the inherent limitations of the traditional two-tier operating system of central banks and commercial banks [3].

The essential difference between anonymity and pseudo-anonymity shows that digital currency transactions generally do not have to be associated with the real identity information of users, but are executed based on encrypted addresses, which gives the participants a basic privacy protection function, that is, pseudo-anonymity. It should be noted that a completely anonymous state is difficult to achieve. Some cryptocurrencies (Monero) use more sophisticated algorithmic designs to enhance anonymity to address security risks.

Global and borderless features enable digital currencies to operate with the help of Internet technology, and their trading activities break geographical restrictions, allowing for instant payments and fund transfers on a global scale, breaking through the constraints of traditional foreign exchange regulation and the operating hours of financial institutions, and significantly improving the efficiency and convenience of cross-border capital flows.

Encryption security mechanisms and data immutability: Digital currencies use cryptographic techniques such as asymmetric encryption algorithms and hash functions to ensure the security of the transaction process and the clear definition of asset ownership. Once the transaction information is agreed upon through a network consensus and permanently recorded on the blockchain, its content cannot be modified or revoked, thus maintaining the authenticity and integrity of the ledger history, as shown in Tables 1, 2 below:

Table 1. The impact of increased efficiency and reduced costs of Cross-border payments with digital currency

Scene description	The extent of the reduction in transaction costs	Global cross-border traffic increase (trillion US dollars)
Benchmark scenarios	0%	0
Optimize scenes	60%	5.8
Scene Description	The extent of the reduction in transaction costs	Global cross-border traffic increase (trillion US dollars)
Benchmark scenarios	0%	0

Table 2. Impact of Cross-border Use of digital Currencies on Capital Flow Volatility

Scenario description	Increase in capital flow volatility	Capital outflow pressure in emerging markets (when the Federal Reserve tightens its policy)
No digital currency	0%	low
Have digital currency	20% - 30%	high

2.2 An Introduction to Common Digital Currencies

Depending on the issuer and credit endorsement, digital currencies can be classified into the following three major categories:

(1) Cryptocurrencies:

Bitcoin, proposed under the pseudonym Satoshi Nakamoto and first publicly released in 2008, is the world's first and most famous cryptocurrency, known as "digital gold". It aims to create a peer-to-peer electronic payment system that does not require the involvement of a central authority. It has notable features such as a limited supply (with a maximum issuance of 21 million), wide circulation, and high security, but its transaction processing speed and concurrent processing capacity still need to be improved. Created by Vitalik Buterin and his core development team in 2015, the most prominent feature of Ethereum is that it breaks the limitations of traditional cryptocurrencies and is committed to building an open blockchain platform that combines open source spirit with smart contract technology, providing strong technical support for the development of distributed applications. With the efficient issuance of tokenized assets based on the ERC-20 standard, it is of great significance for promoting blockchain technology innovation and expanding application scenarios.

(2) Stablecoins are an innovative type of digital asset that attempts to address the issues brought about by the large price fluctuations of traditional cryptocurrencies. These assets achieve a relatively stable value by establishing fixed peg connections with fiat currencies (such as the US dollar), precious metals, or other specific assets. Take Tether as an example. It is a typical stablecoin that dominates the market. It claims to maintain a 1:1 peg to the US dollar and is frequently applied to value storage in the digital currency field, serving as a medium of exchange and cross-border payments, etc. To some extent, it has alleviated the risk pressure caused by market uncertainty.

(3) Central bank digital currency is a digital form of fiat money, issued by the central bank and with credit guarantees, and has the basic characteristics of traditional money. Compared with decentralized crypto assets, CBDC shows more significant centralization, and its main task is to op-

timize the efficiency of the payment system operation and enhance the effect of monetary policy transmission. To promote the development of inclusive finance and safeguard the security of national monetary sovereignty, China's digital yuan and Sweden's electronic krona have both launched pilot or test projects, which have become one of the key research areas of concern for global central banks.

3. A Risk Analysis of Digital Currencies

3.1 Technical Risks

3.1.1 System stability issues

The normal operation of digital currency is an important foundation for achieving the expected functional value, and its underlying technical architecture still faces many reliability tests. Currently dominant blockchain platforms such as Bitcoin and Ethereum show significant underperformance under concurrent conditions.

3.1.2 It Could lead to hacking and loss

The digital currency ecosystem is too complex to be targeted by high-value digital assets, with technical flaws and cybersecurity concerns being the main risk factors. Mt.Gox, which was once the world's largest Bitcoin trading platform in 2014, eventually declared bankruptcy after about 850,000 bitcoins were stolen following a systemic security vulnerability attack [2]. The incident was seen as a signature security crisis in the blockchain field, which fully exposed the significant flaws in the risk management mechanisms of cryptocurrency exchanges. These will become weak links in the entire security, and if these problems are not completely resolved, they may prevent the digital currency industry from moving in a sustainable direction, and also have a negative impact on its promotion to social applications.

3.1.3 Loss of assets due to the loss of private keys

In a "self-sovereign" digital currency system, users achieve autonomous control over their assets with their private keys and bear all security protection responsibilities independently. If the private key is lost or illegally

obtained, the related funds will suffer irreversible and permanent losses. This is because it has the basic characteristic of decentralization. This is significantly different from the account protection and emergency services provided by traditional financial institutions [2]. In 2013, British programmer James Howells accidentally threw away the hard drive containing the private keys of 7,500 bitcoins as garbage. Although the market value of this wealth has now exceeded hundreds of millions of dollars, it has still

not been retrieved to this day. There are multiple technical factors that have led to the risk of asset loss [3]. This case deeply demonstrates the “wealth destruction” phenomenon caused by the interweaving of mismanagement of private keys and security vulnerabilities in smart contracts, highlighting the importance of enhancing users’ awareness of information security and standardizing their operations. As shown in Table 3:

Table 3. The Impact of Digital Currencies on Financial stability

Influencing factors	Specific impacts	Typical cases
Currency mismatch risk	Exacerbating currency mismatches and debt crises in emerging market countries	Latin American countries have lost their independent monetary policy space due to dollarization
Fluctuations in capital flows	Capital flow volatility rises by 20% to 30%	When the Federal Reserve tightens its policy, the pressure of capital outflow in emerging markets increases
Systemic risk contagion	Accelerate the international spread of financial crises	The risk of a repeat of the 2008 crisis has increased

3.2 Risks at the Market Level

3.2.1 Investment risk

The main risks faced by digital currency investment stem from the significant characteristics of its price fluctuations. During the bull market in 2017, the price of Bitcoin soared from less than \$1,000 to nearly \$20,000, attracting a large number of new investors. These investors, influenced by media hype and social networks, blindly followed the trend to buy Bitcoin, which eventually led to the bursting of the bubble. In early 2018, the price of Bitcoin plummeted, and many investors suffered heavy losses.

For traditional financial institutions like commercial banks, the sharp fluctuations in the digital currency market can be transmitted to the existing financial system through many channels. If banks are involved and hold related assets, then the decline in asset quality and capital adequacy ratio due to the shrinking market value will indirectly increase their credit risk exposure. In 2021, a tweet by a certain celebrity directly caused a sharp fluctuation in the price of a certain digital currency, and many investors chased the high price, only to suffer a heavy blow.

3.2.2 The risk of investors blindly following the trend

In the digital currency market, retail investors are dominant, information asymmetry is prominent, and irrational “herd mentality” is likely to occur. Most people do not have a deep understanding of the essence of blockchain technology and the value of the project, and their invest-

ment decisions are often influenced by “fear of loss”, the words of opinion leaders, or the speculative atmosphere of the market. Rather than relying on strict fundamental analysis to make rational judgments, this kind of blindly following the trend to buy high and sell low has increased the volatility of the market and raised the potential risk level. During the bull market in 2017, the price of Bitcoin soared from less than \$1,000 to nearly \$20,000, attracting a large number of new investors. These investors, influenced by media hype and social networks, blindly followed the trend to buy Bitcoin, which eventually led to the bursting of the bubble. In early 2018, the price of Bitcoin plummeted, and many investors suffered heavy losses.

3.3 Risks at the Legal Regulatory Level

3.3.1 the global regulatory system is not uniform

At present, the global digital currency field is characterized by different legislation, diverse regulatory frameworks and governance models, and the absence of a unified international standard or coordination mechanism. This fragmentation can easily lead to regulatory arbitrage and jurisdictional conflicts, and some countries (Japan, Switzerland) tend to adopt more lenient regulatory policies, categorizing them under existing financial regulation. China has adopted a strategy of strict restrictions or even total bans. The uncertainty of the regulatory environment has hindered the normal development of the digital currency market and may become the breeding ground for

cross-border illegal activities, posing a threat to global financial security and stability [4, 5]. When developing and piloting legal digital currencies such as the digital yuan, China has adopted a policy orientation of cautious regulation of private crypto digital currencies. In the current rapid transformation of the global digital economy, how to create a regulatory framework that can both ensure security and promote renewal has gradually become a key issue that must be addressed [6].

3.3.2 The problem of regulatory gaps

The digital currency ecosystem is diversifying, with new models such as DeFi, NFTS, and algorithmic stablecoins constantly emerging, which poses a huge challenge to the traditional regulatory framework. The phenomenon of “technology ahead of legislation” is becoming increasingly prominent, and the existing legal system is difficult to effectively cover new business forms. The current financial regulatory system lacks specific provisions for decentralized applications driven by smart contracts, and there are obvious flaws in the division of responsibilities among DeFi protocol issuers, governance token holders, and liquidity providers. In 2017 and 2018, a large number of ICO projects emerged globally. Many of them raised funds without clear regulation. This leaves a large number of investors at risk of fraud and running away. In some countries such as the United States, although the SEC (Securities and Exchange Commission) has attempted to intervene and review certain projects, globally, many projects have taken advantage of regulatory gaps to raise funds from investors, ultimately resulting in significant financial losses.

3.3.3 There is a high risk of money laundering, illegal transactions, and other criminal activities

The pseudo-anonymity of digital currencies, along with decentralized communication methods, provides convenient conditions for their application in illegal activities such as money laundering, terrorist financing, and cross-border fund transfers. Criminals use mixing services, cross-chain interaction technologies, and converting illegal gains into more difficult-to-track cryptocurrencies (like Monero) to evade regulatory monitoring and tracking. The “Silk Road” dark web market poses a severe test to the global anti-money laundering/anti-terrorist financing (AML/CFT) system. This platform uses Bitcoin as a payment method, facilitating the conclusion of a large number of contraband transactions, with a cumulative transaction volume of up to 1.2 billion US dollars. This fully demonstrates the destructive power that such virtual asset trading platforms have caused to the traditional fi-

nancial order.

4. Strategies for dealing with digital currency risks

4.1 Technical response strategies

Technical security, as a key support for the operation of the digital currency system, serves as an important barrier against various risks. To enhance the overall security of the system, it is necessary to focus on promoting core technological innovation and continuous improvement, perfecting the design of the consensus mechanism, improving the proof-of-stake algorithm, improving the expansion plan, adopting state channels or sidechain architectures, and proactively laying out post-quantum encryption technology. To counter the potential threat of computing power attacks [7, 8].

4.2 Market-Level Response Strategies

To deal with the sharp fluctuations in the market and truly protect the rights and interests of investors, it is urgently necessary to establish a multi-dimensional regulatory and protection system. Regulatory authorities can use technological innovation to create a real-time monitoring and early warning platform, and dynamically track and promptly intervene in abnormal trading behaviors, market manipulation, and other illegal and irregular situations, so as to maintain the fairness of the market. Efforts should also be made to improve investor suitability management systems and risk education mechanisms [9].

4.3 Legal Regulatory Response Strategies

Building a clear and globally unified legal system is a key approach to regulating the order of the digital currency market and promoting its healthy development. Currently, it is urgently necessary to improve the legislative mechanism, clarify the relevant legal attributes and regulatory responsibilities of digital currencies. The central government can issue specialized laws and regulations to comprehensively clarify the legal status, asset attributes, and the functions of the competent authorities of various digital currencies. To fill existing regulatory loopholes, solve the problem of “having laws but not following them”, provide a solid legal foundation for law enforcement work, intensify efforts to crack down on currency-related crimes, public security, judicial, financial regulatory and other departments should deepen cooperation, rely on big data analysis and blockchain technology to track suspicious transaction clues, and effectively prevent people

from using digital currencies for money laundering, Fraud or illegal fundraising and the like [10].

In judicial practice, it is necessary to improve criminal legal norms in the field of digital currency, form unified standards for crime determination and sentencing, and enhance the deterrent effect and enforcement effectiveness of the law [11, 12].

5. Conclusions

At the technical level, there are mainly Performance bottlenecks in the blockchain system (such as slow transaction speed and TPS limitations), vulnerabilities in the consensus mechanism (such as 51% attack risk), and defects in private key management (loss or theft). Security needs to be enhanced by optimizing consensus algorithms (such as PoS replacing PoW), developing quantum-resistant encryption technology, and establishing code auditing standards. At the same time, tools like hardware wallets are promoted to reduce operational risks for users; At the market level, it is manifested as sharp price fluctuations, high policy sensitivity and irrational investor behavior (such as blindly following the trend). It is necessary to build a real-time monitoring and early warning system to track abnormal transactions, improve the investor access system (such as restricting leverage) and popularize risk education through official channels to guide rational investment and curb the “herd effect”.

References

[1] Meng T, Ouyang W, Shi Y, et al. China’s stablecoin development strategies in the digital RMB era: Building a new system of risk control, value anchoring and cross-border payments. *Rural Finance Research*, 2025: 1–13. Online publication date: 2025-08-24.

[2] Chen W, Han X, Ming Y. Risks and challenges of digital currencies, state regulation and global governance. *Northeast Asia Forum*, 2025, 34(4): 111–126+128.

[3] Yang D, Liu Z. Research on risk classification regulation of cryptocurrencies. *Journal of Guizhou University (Social Sciences Edition)*, 2025, 43(3): 74–84.

[4] Du Y, Zhou T. Research on the impact of legal digital currency on credit risk of commercial banks. *National Circulation Economy*, 2025, (8): 161–164.

[5] Hu X, Guo H. Research on risk user identification model of digital currency in financial institutions. *Jiangsu Communications*, 2025, 41(2): 102–107.

[6] Wu Z, Da T. Research on the development and regulation of digital currency in China. *Science & Technology & Finance*, 2025, (3): 76–83+94.

[7] Ma N. Research on countermeasures of the Chinese government to prevent virtual currency risks. *Heilongjiang University*, 2023.

[8] Xie Q. Research on the application risk prevention system of legal digital currency in inclusive finance. *Southwest University of Political Science and Law*, 2023.

[9] Tian J. Research on legal issues of regulation of legal digital currency in China. *Shanxi University of Finance and Economics*, 2023.

[10] Zhou F. The trend of digital finance: Unveiling the multidimensional network of cryptocurrency risk propagation. *Applied Economics*, 2025, 57(38): 5924–5941.

[11] Lu J, Zhang Y, Xiao J. Risks and preventive mechanisms of digital currency and financial security. *Modern Economics and Management Forum*, 2025, 6(2).

[12] Wu S, Wang Y. Research on taxonomies, security risks and policies of digital currency: Based on the perspective of literature review. *Electronics Science, Technology and Applications*, 2025, 12(1).