Global Economic Perspectives Vol 3 Issue 4 2025

Original Research Article

Open Access

Omniscient Pte.Ltd.

An Analysis of the Double-Edged Sword Effect of Blockchain Technology on Financial Crime Governance

Ye-Wei Sun*

University of Murcia, Murcia, 30003, Spain

***Correspondence to:** Ye-Wei Sun, University of Murcia, Murcia, 30003, Spain, E-mail: 1157485898@qq.com

Abstract: Blockchain technology, characterized by features such as decentralization, is transforming the financial system and providing new tools for financial crime governance. However, its characteristics like anonymity are also exploited by criminals, giving rise to new types of financial crime. This paper analyzes its "double-edged sword" effect from a financial professional perspective: first, it outlines the technical principles and current applications; then, it explores its empowering mechanisms as a "sharp sword" in anti-money laundering, combating terrorist financing, and enhancing transaction transparency. Subsequently, it analyzes its abuse as a "dark blade" in criminal activities such as cryptocurrency money laundering. Employing the financial regulation "trilemma" framework, the paper argues for the necessity and challenges of seeking a balance between decentralization, privacy protection, and effective regulation. It proposes comprehensive governance pathways, including building an adaptive regulatory framework that synergizes "RegTech" and "Compliance Tech." The research indicates that guiding blockchain technology to serve financial security and stability requires acknowledging and mastering its dual nature.

Keywords: Blockchain; Financial Crime; Anti-Money Laundering; RegTech; Double-Edged Sword Effect

Introduction

The 21st century has witnessed accelerated financial innovation, with disruptive technologies like blockchain reshaping the global financial landscape. As the underlying technology of Bitcoin, blockchain, through its distributed ledger and other features, constructs a value transfer network that requires no central authority, showing great potential in areas like payment settlements and Central Bank Digital Currencies (CBDC). However, technological innovation always brings risks and challenges. In financial crime governance, blockchain exhibits a "double-edged sword" characteristic: transparency and traceability benefit regulatory tracking, while the emphasis on anonymity can provide a breeding ground for illicit activities. For financial professionals, understanding and mastering this dual effect is of significant importance, relating to institutional compliance, risk management, and the stability of the financial system. Traditional financial crime governance frameworks are largely based on centralized financial intermediaries, which are being fundamentally challenged by blockchain and the Decentralized Finance (DeFi) ecosystem. From a finance professional perspective, this paper will move beyond technical discussions to analyze how blockchain impacts

financial crime governance across multiple dimensions and explore the construction of a future financial governance system that balances innovation with risk prevention and control.

1. The Core of Blockchain Technology and Its Application Landscape in the Financial Sector

The core of blockchain technology lies in constructing a "trust machine." Its three pillars—decentralization, immutability, and traceability—collectively reshape the methods of value transfer and agreement execution. Decentralization eliminates reliance on a single authoritative institution. Immutability ensures data authenticity through cryptographic hashing and a chain structure, while traceability makes every transaction permanently recorded and traceable. Smart contracts further codify agreement logic, enabling automatic execution, and encryption technology, while ensuring security, grants users pseudo-anonymity [1]. In the financial sector, blockchain has evolved from the payment function of cryptocurrencies like Bitcoin to encompass a vast ecosystem including Decentralized Finance (DeFi), stablecoins, Security Token Offerings (STOs), and Non-Fungible Tokens (NFTs). DeFi, relying on smart contracts, provides intermediary-free lending, trading, and insurance services, embodying "code is law." Stablecoins act as value-anchored tools, becoming the mainstream medium within DeFi. STOs and NFTs promote the tokenization of traditional assets and unique rights, respectively. These innovations enhance efficiency, reduce costs, and increase financial inclusivity, while simultaneously posing new challenges to the existing regulatory and anti-financial crime systems.

2. The "Sharp Sword": The Positive Effects of Blockchain in Empowering Financial Crime Governance

Despite the inherent risks, the underlying characteristics of blockchain offer new approaches to addressing pain points in the traditional financial system.

2.1 Enhancing Transaction Transparency and Traceability to Decipher Money Laundering Puzzles

Money laundering activities within the traditional financial system often obscure the source and destination of funds through multi-layered shell companies, complex cross-border transfers, and cash transactions, creating a "black box." In contrast, the ledger of public blockchains (such as Bitcoin and Ethereum) is open, and all transaction records can be queried. This means that once law enforcement agencies can link a wallet address to a real-world identity (e.g., through KYC information from exchanges), they can trace the entire transaction history of that address, mapping out a clear flow of funds. This "God's-eye view" significantly restricts criminals' operational space, making traditional money laundering techniques like "layering" exceptionally fragile on the blockchain.

2.2 Enhancing Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Efficiency

Traditional AML/CFT compliance heavily relies on financial institutions acting as "gatekeepers," performing Customer Due Diligence (CDD) and submitting Suspicious Transaction Reports (STRs). However, this model suffers from information silos, delayed responses, and high costs. Blockchain technology offers the potential for building a more efficient compliance system.

Shared KYC (Know Your Customer): Multiple financial institutions can build a secure, authorized KYC information sharing platform based on blockchain. With a single authorization from the customer, their verified identity information can be securely shared among members of the consortium chain. This avoids repetitive verification, reduces compliance costs, and ensures the timeliness and consistency of information [2].

Automated Compliance (Embedded Compliance): Smart contracts can be programmed to automatically enforce AML rules. For instance, if a transaction involves an address from a sanctioned country or exceeds a specific threshold, the contract can automatically freeze the transaction and send an alert to regulators. This "embedded compliance" integrates rules directly into business processes, enabling real-time, dynamic risk monitoring.

2.3 Providing a Technical Foundation for Regulatory Technology (RegTech)

The combination of blockchain with artificial intelligence (AI) and big data analytics has given rise to powerful on-chain analytics tools. Professional blockchain analysis companies (such as Chainalysis, Elliptic) use techniques like graph theory and machine

learning to perform cluster analysis on massive amounts of on-chain transaction data, identifying clusters of addresses associated with known illicit entities like dark web markets, ransomware, and mixers. These tools have become standard equipment for law enforcement and regulatory agencies globally in combating cryptocurrency-related crime, significantly improving the efficiency and precision of criminal investigations.

3. The "Dark Blade": The Negative Effects of Blockchain Abuse in Financial Crime

3.1 Abuse of Anonymity and Pseudonymity: A New Breeding Ground for Money Laundering and Terrorist Financing

Although public blockchain transactions are transparent, the pseudonymity of addresses provides a first layer of protection for criminals. They can further enhance anonymity through the following methods:

Mixers/Tumblers: Services like Tornado Cash allow users to mix their cryptocurrencies with funds from other users before withdrawal, thereby severing the direct on-chain link between the original funds and the destination address, significantly increasing tracing difficulty. Although Tornado Cash has been sanctioned by the US Treasury Department, similar services continue to emerge.

Privacy Coins: Privacy-focused cryptocurrencies like Monero and Zcash use advanced cryptographic techniques such as ring signatures and zero-knowledge proofs (zk-SNARKs) to completely hide transaction amounts, senders, and receiver information while ensuring transaction validity, making on-chain tracing virtually impossible. This provides a perfect "safe haven" for high-risk illicit funds.

3.2 The New Frontier of Crime in Decentralized Finance (DeFi)

The "permissionless" and "censorship-resistant" nature of DeFi makes it an ideal tool for financial crime.

Flash Loan Attacks: Attackers can utilize uncollateralized flash loans provided by DeFi protocols to borrow huge sums, manipulate the price of a particular token within a very short timeframe to arbitrage on other protocols, then repay the loan and abscond with the profits. This entire process occurs within a single transaction, making it difficult for traditional risk control systems to intercept.

Protocol Exploits and "Rug Pulls": Because DeFi protocol code is open source, hackers can find and exploit logical vulnerabilities in smart contracts to steal funds from protocol treasuries. More egregious are "Rug Pull" scams, where project developers abruptly withdraw liquidity and disappear after attracting substantial investor funds, leaving investors with nothing [3]. Such crimes are difficult to prosecute due to the lack of a clear liable entity (project teams are often anonymous).

Cross-Chain Bridge Risks: Cross-chain bridges, acting as hubs connecting different blockchains, have become prime targets for hackers due to the large assets they hold and their complex security models, resulting in several incidents causing losses amounting to hundreds of millions of dollars.

3.3 The Facilitation of Ransomware and Illicit Payments

In recent years, ransomware attacks have surged, and cryptocurrencies (especially Bitcoin) have become the preferred method for ransom demands by extortionists. The reasons are: the payment process is fast, cross-border, and difficult to freeze or reverse through the traditional financial system. Criminals leverage the characteristics of cryptocurrencies to create an efficient, low-risk closed loop for the extortion economy.

3.4 Challenging the Foundations of the Traditional Regulatory Framework

The FATF's "Travel Rule" requires Virtual Asset Service Providers (VASPs), such as exchanges, to transmit originator and beneficiary identity information during transfers. However, in the DeFi context, users interact directly with smart contracts, and there is no traditional VASP involved. This makes the "Travel Rule" nearly impossible to apply in the DeFi space, creating a significant regulatory gap. A profound structural contradiction exists between the decentralized nature of blockchain and the traditional regulatory paradigm that targets centralized institutions.

4. Moving Beyond Binary Opposition: Building an Adaptive Framework for Financial Crime Governance

4.1 Revisiting the Financial Regulation "Trilemma"

In the context of blockchain, financial regulation faces

a dilemma akin to an "impossible trinity": complete decentralization, absolute user privacy, and effective financial crime regulation are difficult to achieve simultaneously. Overemphasizing decentralization and privacy provides shelter for crime; whereas excessive regulation may stifle innovation, contradicting the original intent of blockchain. Therefore, the goal of regulation should not be to pursue an absolute optimum for all three, but rather to find a dynamic and acceptable equilibrium point based on specific developmental stages and risk appetites.

4.2 Constructing an Adaptive Framework Driven by the Synergy of "RegTech" and "Compliance Tech"

Develop Advanced On-Chain Regulatory Tools: Regulatory authorities should heavily invest in independent on-chain data analysis capabilities and collaborate with private-sector blockchain analytics companies to establish a national-level cryptocurrency tracking and risk early-warning system. Simultaneously, explore the use of privacy-enhancing technologies like zero-knowledge proofs to prove transaction compliance to regulators without disclosing all user transaction details (e.g., proving that a transaction did not interact with a sanctioned address).

Promote the Standardization of "Embedded Compliance": Encourage DeFi protocol developers to embed basic compliance logic (such as address screening) as optional modules within smart contracts. Regulators can formulate relevant technical standards and offer incentives like "regulatory sandboxes" or exemptions to protocols that adopt "Embedded Compliance" and meet certain security standards [4].

Clarify Regulatory Boundaries and Liability for DeFi: For protocols that, while claiming to be "decentralized," still have identifiable development teams or governance token holders capable of exerting significant influence, explore bringing key participants (such as front-end interface operators, core developers) under the regulatory scope of VASPs, requiring them to fulfill corresponding AML/CFT obligations.

4.3 Strengthening International Cooperation and Standard Harmonization

The cross-border nature of blockchain dictates the limitations of unilateral regulation. Regulatory agencies from various countries must strengthen cooperation, promoting global consensus on the definition of crypto-assets, the scope of VASPs, the implementation details of the Travel Rule, and stances on privacy coins and mixers. The FATF should continue to play a leading role by updating its guidance to cover emerging sectors like DeFi.

4.4 Fostering a Responsible Financial Innovation Ecosystem

Financial institutions, tech companies, and academia should work together to internalize financial security and compliance as core values of blockchain financial innovation. Through industry self-regulation, sharing best practices, and joint research, a healthy ecosystem that both stimulates vitality and effectively prevents and controls risks should be built.

Conclusion

The impact of blockchain technology on financial crime governance represents a profound structural transformation, not a simple binary of advantages and disadvantages. It can serve as a "Sharp Sword" aiding penetrative supervision, yet also become a "Dark Blade" for criminals to evade scrutiny. Financial professionals should discard simplistic technological determinism and discern the complex economic, legal, and social factors behind technology application. The future of financial crime governance is not merely a contest between regulators and criminals, but a game involving different technological paradigms, governance philosophies, and global interests. Constructing a flexible, intelligent, and globally-minded adaptive framework is key to successful governance. This framework must leverage the transparency advantages of blockchain, utilize the deep integration of RegTech and CompTech to achieve risk preemption and intelligent management, while simultaneously, through prudent rule design and international cooperation, block criminal opportunities under the premise of protecting legitimate innovation and privacy.

References

[1] Li Chengni, Wei Lanlan. Research on the Prevention and Control of Mobile Financial Crime Based on Blockchain Technology [J]. Journal of Henan Police College, 2023, 32(06): 54-62.

[2] Deng Liang. Criminal Risks and Their Prevention and Control in Blockchain Finance [J]. Journal of

Jiangxi Police College, 2023, (02): 22-29.
[3] Guo Ying. The Financial Crime Governance System from the Perspective of Blockchain: Taking Illegal Absorption of Public Deposits by P2P Lending Platforms as an Example [J]. Legality Vision, 2022, (10): 152-154.
[4] Zhang Chenghu, Li Pengxu. Research on a Multi-Chain Blockchain-Based Information Sharing Model for Internet Financial Crime Intelligence [J]. Journal of Intelligence, 2021, 40(06): 65-70+136.