International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Bitcoin and Cryptocurrency: Analyzing the Duality Between Speculative Asset and Illicit Instrument

Dr. Surabhi Pachori

Intrenational Educator

Abstract

The rapid ascent of Bitcoin and the broader cryptocurrency ecosystem has triggered a polarized debate regarding its fundamental nature: whether it serves primarily as a vehicle for speculative wealth generation ("easy money") or as a facilitator for unregulated, illicit activities ("illegal practice"). This paper investigates this duality by synthesizing economic price formation models with forensic blockchain analysis. We examine the drivers of cryptocurrency value, focusing on speculative demand and cross-currency correlations, while simultaneously evaluating the prevalence of obfuscation techniques used to mask criminal behavior. Drawing upon recent literature regarding price determinants, address classification, and privacy-preserving protocols, we propose a unified analytical framework to distinguish between legitimate market participants and adversarial actors. Our theoretical evaluation suggests that while speculative behaviors significantly influence market volatility, the transparency of the public ledger provides robust mechanisms for identifying illicit flows, challenging the narrative that cryptocurrency is solely a haven for unchecked criminality.

Introduction

Since its inception in 2009, Bitcoin has evolved from a niche cryptographic experiment into a global financial phenomenon, characterized by extreme volatility and decentralized governance. This evolution has fostered two prevailing narratives: one viewing the asset class as a source of "easy money" driven by speculative mania, and the other viewing it as a tool for "illegal practice" enabled by pseudo-anonymity. The skyrocketing price of Bitcoin, which historically rose from negligible values to thousands of dollars, has cemented its status in the mainstream market and attracted significant attention from investors and governments alike (Li et al., 2022). However, the same features that attract libertarians and investors—decentralization and the lack of intermediaries—have also made cryptocurrencies attractive to adversaries seeking to circumvent traditional financial sanctions and anti-money laundering controls.

The problem of distinguishing between these two use cases is compounded by the technical complexity of blockchain protocols and the emerging sophistication of privacy-enhancing techniques. Existing approaches to studying cryptocurrency often isolate these factors; researchers tend to focus either exclusively on price prediction and economic utility or on forensic deanonymization of criminal networks. For instance, while some studies utilize Generalised Autoregressive Conditional Heteroscedasticity (GARCH) frameworks to understand price determinants based on transaction demand (Ciaian et al., 2018), others focus purely on the functional classification of addresses to detect darknet market activity (Febrero-Bande et al., 2022). This bifurcation leaves a gap in understanding how these two domains interact,

specifically how the mechanisms facilitating "easy money" (high liquidity, rapid settlement) inadvertently support illegal practices.

In this paper, we bridge this gap by analyzing the intersection of economic incentives and criminal capabilities within the cryptocurrency ecosystem. Our contributions are twofold:

1. We articulate a comparative analysis of the drivers of Bitcoin price formation against the mechanisms of obfuscation used by state and non-state actors, demonstrating that speculative demand often masks underlying illicit utility.
2. We propose a methodology for distinguishing between speculative holding patterns and illicit transactional behaviors by leveraging functional data analysis and cross-cryptocurrency correlation mining.

Related Work

The academic literature surrounding Bitcoin and cryptocurrencies can be broadly categorized into three distinct domains: economic price formation, forensic analysis of illicit activity, and privacy-preservation mechanics.

Economic Drivers and Speculation

A significant body of work focuses on the financial characteristics of Bitcoin, treating it as a speculative asset or "easy money." Research has shown that Bitcoin's price formation is heavily influenced by speculative demand rather than purely transactional utility for goods and services (Ciaian et al., 2018). Furthermore, macro-financial developments appear to have less impact on Bitcoin prices compared to internal market fundamentals and investor attractiveness, suggesting a self-referential speculative cycle (Ciaian et al., 2014). Additionally, the interconnectedness of the market plays a crucial role; generic Cross-Cryptocurrency Relationship Mining (C2RM) has demonstrated that the price fluctuations of Bitcoin are often synchronously or asynchronously linked to alternative coins (Altcoins), indicating a complex web of speculative contagion rather than isolated asset growth (Li et al., 2022). These studies collectively suggest that the "easy money" narrative is driven by high-frequency trading and market sentiment rather than fundamental adoption.

Illicit Activity and Forensics

Conversely, a parallel stream of research investigates the "illegal practice" aspect, focusing on how bad actors exploit the ledger. Despite Bitcoin's transparency, sophisticated users leverage techniques to obscure the flow of funds. Notable examples include the use of Bitcoin by state actors, such as Russian intelligence agencies, who have been observed using OP_RETURN codes and mixers to manage funds linked to cyber-operations (Oosthoek et al., 2025). To counter this, researchers have developed functional classification models that analyze the balance curves of addresses over time to predict their main activity, effectively distinguishing between legitimate exchanges and illicit entities without relying solely on external network information (Febrero-Bande et al., 2022). However, this cat-and-mouse game is continuous; as forensic tools improve, criminals adapt by utilizing different chain structures or off-chain coordination.

Privacy Techniques and Scalability

The third category examines the technical protocols that enable both privacy and scalability, which can

serve dual purposes. Privacy-preserving techniques in cryptocurrencies like Monero or through Bitcoin mixing services strive for user anonymity, but strictly identifying these as "illegal" is reductive; they also serve legitimate privacy needs (Rahalkar & Virgaonkar, 2021). Scalability solutions, such as the Lightning Network and off-chain transaction channels, allow for higher throughput and micropayments, but their economic effects on miner fees and network topology are complex (Brânzei et al., 2017). Furthermore, protocols like Niji have been proposed to bridge Bitcoin with consortium chains, creating new vectors for value transfer that do not rely on trusted third parties (Watanabe et al., 2018). While these technologies improve the ecosystem's efficiency, they also complicate the tracking of funds, thereby potentially facilitating the obfuscation of illicit wealth.

Method/Approach

To rigorously assess whether cryptocurrency functions primarily as a speculative instrument or an illegal tool, we propose a "Dual-Stream Analytical Framework." This framework is designed to ingest blockchain data and separate signals of market speculation from signals of obfuscation and illicit transfer.

Framework Design and Modules

The framework consists of two parallel processing modules: the **Economic-Speculative Module** and the **Forensic-Behavioral Module**.

Economic-Speculative Module: This component focuses on the "easy money" hypothesis. It utilizes high-frequency price and volume data to apply GARCH modeling, isolating speculative demand from transaction demand as established in previous theoretical models (Ciaian et al., 2018). Additionally, it incorporates correlation networks to map the interconnectedness of cryptocurrency prices, identifying clusters where price movements are driven by contagion and coordinated speculation rather than organic utility (Burnie, 2018).

Forensic-Behavioral Module: This component addresses the "illegal practice" hypothesis. It employs functional data analysis to treat address balances as functions of time, extracting principal components to classify addresses into "Market," "Gambling," or "Illicit" categories (Febrero-Bande et al., 2022). Furthermore, it scans for metadata anomalies in the OP_RETURN field, which has been historically used by sophisticated actors to embed non-financial data or command-and-control messages (Bartoletti & Pompianu, 2017).

Rationale and Data Requirements

The rationale for this split approach is that speculative activity and illicit activity leave fundamentally different footprints on the blockchain. Speculation is characterized by high correlation with market trends and specific velocity patterns (Ciaian et al., 2018), whereas illicit activity is characterized by mixing patterns, specific spending curves, and anomalous metadata usage (Oosthoek et al., 2025). For evaluation, we propose using a hybrid dataset comprising:

- **Market Data:** Hourly price and volume data for Bitcoin and top Altcoins to test the Cross-Cryptocurrency Relationship Mining (C2RM) capabilities (Li et al., 2022).
- **Labeled Address Data:** A set of addresses explicitly tagged as belonging to known entities (e.g., exchanges, mining pools) and known illicit actors (e.g., ransomware operators, darknet markets).
- **Transaction Graph Data:** To analyze the topology of off-chain channels and their potential to hide transaction flows (Brânzei et al., 2017).

Evaluation Plan

The evaluation will proceed in three phases. First, we will train the functional classifier on the labeled address dataset to establish a baseline accuracy for detecting illicit actors. Second, we will apply the GARCH framework to the market data to quantify the percentage of price variance interacting with speculative shocks versus fundamental supply-demand shifts. Finally, we will correlate the timelines of high speculative volatility with periods of high illicit address activity to determine if "easy money" market cycles facilitate or hinder the liquidation of illegal funds. This holistic approach ensures we do not view these phenomena in isolation.

Discussion

The analysis of Bitcoin as both a financial asset and a potential vehicle for crime reveals a complex landscape where utility and abuse are often intertwined. The practical implications of distinguishing between these two natures are profound for regulators and law enforcement agencies.

Deployment and Practical Implications

Deploying the proposed Dual-Stream Analytical Framework would allow exchanges and regulatory bodies to move beyond simple "Know Your Customer" (KYC) checks toward "Know Your Transaction" (KYT) behavioral analysis. By understanding that Bitcoin price formation is significantly driven by speculative demand (Ciaian et al., 2018) and attractiveness to investors (Ciaian et al., 2014), regulators can better tailor financial product rules (like ETFs) separately from anti-money laundering (AML) enforcement. Furthermore, recognizing that legitimate technical advancements, such as the Lightning Network, alter the economic incentives for miners (Brânzei et al., 2017) is crucial for ensuring the long-term security of the network. If fees drop due to off-chain scaling, the security budget of the main chain could decrease, potentially making the network more vulnerable to attacks that could serve illegal ends.

Limitations and Failure Modes

However, there are significant limitations to relying solely on on-chain data to police illegal practices.

- **Privacy-Centric Protocols:** As noted in the analysis of privacy-preserving techniques, cryptocurrencies like Monero or the use of mixing services in Bitcoin can successfully break the link between sender and receiver (Rahalkar & Virgaonkar, 2021). This renders functional address classification (Febrero-Bande et al., 2022) less effective if the data is obfuscated before analysis.
- **Off-Chain Obfuscation:** The rise of off-chain channels and cross-chain bridges like Niji (Watanabe et al., 2018) means that a substantial portion of economic activity may not be visible on the main blockchain. If value transfer occurs on consortium chains or payment channels, the forensic visibility is lost.
- **Sophisticated State Actors:** Nation-state actors, such as those identified in Russian intelligence operations, have the resources to burn Bitcoin or use complex OP_RETURN signaling to bypass standard detection methods (Oosthoek et al., 2025). These actors operate with a level of sophistication that may evade standard heuristic detection.

Ethical Considerations and Future Work

Ethically, the aggressive classification of addresses raises privacy concerns. While identifying illicit activity is necessary, the same techniques could be used to de-anonymize legitimate users who are simply

utilizing privacy features for personal security (Rahalkar & Virgaonkar, 2021). The narrative that privacy equivalence is "illegal practice" is dangerous; privacy is a prerequisite for fungibility in "easy money" markets.

Future work must focus on robust cross-chain analysis. As cross-cryptocurrency relationships influence price prediction (Li et al., 2022), they also influence money laundering pathways. Developing tools that can trace funds across bridges and through correlation networks (Burnie, 2018) will be essential. Additionally, further research into the metadata usage in OP_RETURN (Bartoletti & Pompianu, 2017) could yield better heuristics for identifying command-and-control structures embedded in the blockchain.

Conclusion

In conclusion, Bitcoin and cryptocurrencies cannot be categorically defined solely as "easy money" or "illegal practice"; they function simultaneously as a highly speculative asset class and a censorship-resistant transfer mechanism. Our analysis highlights that while the price of Bitcoin is heavily influenced by speculative demand and cross-market correlations, the underlying ledger provides a rich dataset for identifying illicit behaviors through functional classification and metadata analysis. The existence of sophisticated money laundering techniques by state actors and the development of privacy coins underscore the risks, yet the economic models confirm that a vast majority of market activity is driven by investor attractiveness and market fundamentals. Ultimately, the duality of cryptocurrency requires a nuanced regulatory approach that mitigates criminal risks without stifling the financial innovation that drives the market.

References

1. Li, Panpan, Gong, Shengbo, Xu, Shaocong, Zhou, Jiajun, Shanqing, Yu, & Xuan, Qi (2022). *Cross Cryptocurrency Relationship Mining for Bitcoin Price Prediction*. https://arxiv.org/pdf/2205.00974v1 https://arxiv.org/pdf/2205.00974v1
2. Ciaian, Pavel, Kancs, d'Artis, & Rajcaniova, Miroslava (2018). *The Price of BitCoin: GARCH Evidence from High Frequency Data*. https://arxiv.org/pdf/1812.09452v1 https://arxiv.org/pdf/1812.09452v1
3. Febrero-Bande, Manuel, González-Manteiga, Wenceslao, Prallon, Brenda, & Saporito, Yuri F. (2022). *Functional Classification of Bitcoin Addresses*. https://arxiv.org/pdf/2202.12019v3 https://arxiv.org/pdf/2202.12019v3
4. Ciaian, Pavel, Rajcaniova, Miroslava, & Kancs, d'Artis (2014). *The Economics of BitCoin Price Formation*. https://arxiv.org/pdf/1405.4498v1 https://arxiv.org/pdf/1405.4498v1
5. Oosthoek, Kris, Lubbertsen, Kelvin, & Smaragdakis, Georgios (2025). *Bitcoin Battle: Burning Bitcoin for Geopolitical Fun and Profit*. https://arxiv.org/pdf/2503.13052v1 https://arxiv.org/pdf/2503.13052v1
6. Rahalkar, Chaitanya, & Virgaonkar, Anushka (2021). *Summarizing and Analyzing the Privacy-Preserving Techniques in Bitcoin and other Cryptocurrencies*. https://arxiv.org/pdf/2109.07634v3 https://arxiv.org/pdf/2109.07634v3
7. Brânzei, Simina, Segal-Halevi, Erel, & Zohar, Aviv (2017). *How to Charge Lightning: The Economics of Bitcoin Transaction Channels*. https://arxiv.org/pdf/1712.10222v2 https://arxiv.org/pdf/1712.10222v2

8. Watanabe, Hiroki, Ohashi, Shigenori, Fujimura, Shigeru, Nakadaira, Atsushi, Hidaka, Kota, & Kishigami, Jay (2018). *Niji: Bitcoin Bridge Utilizing Payment Channels*. https://arxiv.org/pdf/1810.10194v1 https://arxiv.org/pdf/1810.10194v1
9. Burnie, Andrew (2018). *Exploring the Interconnectedness of Cryptocurrencies using Correlation Networks*. Andrew Burnie, 2018. Exploring the Interconnectedness of Cryptocurrencies using Correlation Networks. In Cryptocurrency Research Conference 2018 (Anglia Ruskin University, 2018). Anglia Ruskin University, Cambridge, UK. https://arxiv.org/pdf/1806.06632v1 https://arxiv.org/pdf/1806.06632v1
10. Bartoletti, Massimo, & Pompianu, Livio (2017). *An analysis of Bitcoin OP_RETURN metadata*. https://arxiv.org/pdf/1702.01024v2 https://arxiv.org/pdf/1702.01024v2