Cryptocurrencies, Blockchain, and Financial Crimes

Nikos Passas*

School of Criminology and Criminal Justice, Northeastern University, USA

Abstract: Cryptocurrencies and blockchain technology have revolutionized the financial sector, offering decentralized, secure, and efficient transaction mechanisms. However, these innovations have also introduced new challenges, particularly in the realm of financial crimes such as money laundering, illicit trade, and fraud. This paper explores the dual-use nature of cryptocurrencies, examining their potential for both financial innovation and criminal exploitation**,** with over $20 billion in illicit transactions recorded in 2023 (Chainalysis, 2023)**.** By reviewing case studies, regulatory responses, and technological solutions, this paper provides a comprehensive analysis of the risks and opportunities presented by cryptocurrencies and blockchain technology. Current regulatory frameworks, such as the EU's MiCA Regulation (2023) and FATF recommendations and guidelines, have significantly influenced cryptocurrency adoption by balancing innovation with risk mitigation. The paper concludes with actionable recommendations for enhancing regulatory frameworks, fostering international cooperation, leveraging AI and other technological advancements, and creating educational initiatives to mitigate financial crimes in the digital age.

Keywords: Cryptocurrencies, blockchain, financial crimes, money laundering, fraud, regulation.

INTRODUCTION

Cryptocurrencies, digital or virtual currencies that use cryptography for security, have emerged as a transformative force in the financial sector over the past decade (Nakamoto, 2008; Tapscott & Tapscott, 2016). Bitcoin, introduced in 2009 by an anonymous entity known as Satoshi Nakamoto, was the first decentralized cryptocurrency and remains the most widely recognized (Nakamoto, 2008). Since then, numerous cryptocurrencies, such as Ethereum, Solana, and Ripple, have been developed, each offering unique features and applications (Narayanan *et al*., 2016). The underlying technology of cryptocurrencies, blockchain, is a distributed ledger that records transactions across a network of computers, ensuring transparency, security, and immutability (Pilkington, 2016; Tapscott & Tapscott, 2016).

The adoption of cryptocurrencies has been driven by their potential for financial inclusion, efficiency in transactions, and as a store of value and investment vehicle (Böhme *et al*., 2015; Catalini & Gans, 2016). However, their rise in popularity has also brought to light significant challenges, particularly their potential misuse for financial crimes such as money laundering, fraud, and illicit trade (Childs, 2024; Das *et al*, 2025; Foley *et al*., 2019; Holt *et al*., 2023). The anonymity, decentralization, and borderless nature of cryptocurrencies make them attractive tools for criminal activities, including drug trafficking, terrorism financing, and ransomware attacks (Aldridge & Décary-Hétu, 2014; Browne, 2021; Fanusie & Robinson, 2018; Europol, 2019; FATF, 2014; Saha *et al*., 2024; Shin, 2022).

This paper aims to explore the complex interplay between cryptocurrencies, blockchain technology, and financial crimes, with a particular focus on money laundering and illicit trade. By reviewing case studies, regulatory responses, and technological solutions, this paper seeks to provide a comprehensive understanding of the challenges and opportunities presented by this new financial paradigm (Zohar, 2015). The dual-use nature of cryptocurrencies, as both tools for innovation and instruments for criminal activity, underscores the need for balanced regulation (Houben & Snyers, 2018). Effective measures must be developed to mitigate the risks associated with financial crimes while preserving the benefits that cryptocurrencies and blockchain technology offer (Campbell-Verduyn, 2018; Das *et al*, 2025; Weber *et al*., 2019).

Cryptocurrencies and blockchain technology have garnered significant attention from both academia and industry. The first section offers an overview of the literature on cryptocurrencies and blockchain. The paper then turns to financial crimes involving cryptocurrencies, especially money laundering and illicit trade. It then shifts attention to regulatory and enforcement issues, ending with a section on future directions and recommendations

UNDERSTANDING CRYPTOCURRENCIES AND BLOCKCHAIN TECHNOLOGY

1. Cryptocurrencies: An Overview

The literature on cryptocurrencies and blockchain is extensive and covers various aspects, including

*Address correspondence to this author at the School of Criminology and Criminal Justice, Northeastern University, USA;
E-mail: n.passas@northeastern.edu

E-ISSN: 1929-4409/25

technological advancements, economic implications, and societal impacts. Key themes include the evolution of blockchain technology, its applications beyond cryptocurrencies, and the challenges and opportunities it presents (Wang *et al*. 2021).

Cryptocurrencies are digital or virtual currencies that use cryptography for security and operate on decentralized networks based on blockchain technology. Unlike traditional fiat currencies, cryptocurrencies are neither issued nor controlled by central banks or governments. Bitcoin, the first and best-known cryptocurrency, was designed as a peer-to-peer electronic cash system to enable decentralized transactions without intermediaries (Nakamoto, 2008). Other major cryptocurrencies, such as Ethereum, Solana, and Ripple, have since emerged, each offering unique features and applications (Narayanan *et al*., 2016).

1.1. Bitcoin (BTC)

Bitcoin, launched in 2009, is the first and most well-known cryptocurrency. It was designed as a peer-to-peer electronic cash system to enable decentralized transactions without intermediaries. Key features of Bitcoin include its limited supply (only 21 million Bitcoins will ever be created), decentralization, pseudonymity (i.e., transactions are recorded on the blockchain without revealing users' identities, although they are traceable), and the use of a Proof of Work (PoW) consensus mechanism, which requires miners to solve complex mathematical problems to validate transactions (Nakamoto, 2008; Antonopoulos, 2014; Narayanan *et al*., 2016).

1.2. Ethereum (ETH)

Ethereum, launched in 2015 by Vitalik Buterin, is a decentralized platform that enables the creation of smart contracts and decentralized applications (dApps). Its native cryptocurrency, Ether (ETH), is used to power transactions and computations on the network. Ethereum's key features include smart contracts (self-executing contracts with terms directly written into code, enabling trustless agreements), programmability (including use cases, such as decentralized finance (DeFi) and non-fungible tokens (NFTs)), and its transition from Proof of Work (PoW) to Proof of Stake (PoS) with the Ethereum 2.0 upgrade, so that validators are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they "stake" (lock up) as collateral, thereby addressed critical issues such as energy consumption and scalability, while maintaining security and decentralization (Buterin, 2013; Hertig, 2018; Wood, 2014). Proof of Stake (PoS) is a type of consensus mechanism used by some blockchain networks to achieve distributed consensus. In PoS systems, validators (instead of miners in Proof of Work systems) are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they "stake" (hold and lock up) as collateral (Buterin, 2013; Tapscott & Tapscott, 2016).

1.3. Solana (SOL)

Solana, launched in 2020 by Anatoly Yakovenko, is a native cryptocurrency used for transactions, staking, and other activities within the ecosystem, as well as a blockchain platform designed for scalability and speed that provides the infrastructure for building decentralized applications. It aims to support decentralized applications and cryptocurrencies while maintaining low transaction costs. Solana's key features include high throughput (up to 65,000 transactions per second), Proof of History (PoH), and low fees (Yakovenko, 2017; Gervais *et al*. 2016; Gokal & Yakovenko, 2020).

Other major cryptocurrencies operating in niche markets include Ripple (XRP, which focuses on facilitating cross-border payments and remittances; Schwartz *et al*. 2014), Litecoin (LTC, offering faster transaction times and lower fees; Lee, 2011), Cardano (ADA, focusing on sustainability, scalability, and academic rigor, and aiming to provide a secure and scalable infrastructure for dApps; Hoskinson, 2017) and Binance Coin (BNB, used for payments on Binance and participation in token sales on the Binance Launchpad; Zhao, 2017).

2. Blockchain Technology

Blockchain is the underlying technology that enables cryptocurrencies to function. It is a distributed ledger that records transactions in a secure, transparent, and immutable manner. Blockchain operates on a decentralized network of computers (nodes) that collectively maintain the ledger. Transactions are grouped into blocks, which are cryptographically linked to form a chain. Consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), are used to validate transactions and add new blocks to the chain. These mechanisms ensure agreement among nodes without the need for a central authority (Nakamoto, 2008; Tapscott & Tapscott, 2016).

2.1. Key Features of Blockchain

- **Decentralization**: Unlike traditional systems controlled by a central authority, blockchain

operates on a peer-to-peer network, reducing the risk of single points of failure and enhancing resilience.

- **Transparency**: All transactions on a blockchain are visible to participants, promoting accountability and trust.
- **Immutability**: Once a transaction is recorded on the blockchain, it cannot be altered or deleted, ensuring data integrity and preventing fraud (Swan, 2015).

2.2. Benefits and Potential of Blockchain

Blockchain technology has emerged as a transformative force with the potential to revolutionize industries by enhancing transparency, security, and efficiency across various sectors, addressing long-standing challenges and creating new opportunities. Below is summary of key areas where blockchain is making a significant impact.

FINANCE AND BANKING

Blockchain is reshaping the financial sector by enabling faster, cheaper, and more secure transactions. One of its most notable applications is in cross-border payments, where blockchain eliminates intermediaries, reducing substantially processing times and costs for international transactions (Mougayar, 2016). Furthermore, the rise of Decentralized Finance (DeFi) platforms leverages blockchain to offer financial services such as lending, borrowing, and trading without traditional intermediaries, addressing the issue of financial inclusion for vulnerable communities (Passas, 2018a and 2018b; Singer *et al*. 2017) and democratizing access to financial tools (Zetzsche *et al*., 2017). Another innovative application is the tokenization of assets, where physical assets like real estate and art are represented as digital tokens, enabling fractional ownership and easier transferability (Mougayar, 2016).

SUPPLY CHAIN MANAGEMENT

Blockchain enhances supply chain transparency and efficiency by providing end-to-end traceability of goods, allowing businesses and consumers to track the origin and movement of products (Kshetri, 2018). This capability is particularly valuable in industries like food and pharmaceuticals, where fraud prevention is critical. Immutable records on the blockchain reduce the risk of counterfeit products and fraudulent activities, ensuring product authenticity (Jamil *et al*., 2019; Saberi *et al*., 2019). Furthermore, smart contracts automate processes such as payments and inventory management, reducing administrative costs and improving operational efficiency (Kshetri, 2018).

HEALTHCARE

In healthcare, blockchain improves data security and interoperability, addressing critical challenges in the industry. For instance, blockchain enables secure data sharing among healthcare providers, improving care coordination and patient outcomes (Ekblaw *et al*., 2016). It also enhances drug traceability by tracking the production and distribution of pharmaceuticals, ensuring authenticity and reducing the risk of counterfeit drugs (Islam & Islam, 2024; Yue *et al*., 2016). Additionally, blockchain enhances the transparency and integrity of clinical trial data, bolstering trust in research outcomes (Ekblaw *et al*., 2016).

GOVERNMENT AND PUBLIC SERVICES

Blockchain can streamline government operations and enhance public trust through applications such as digital identity systems, which provide secure and verifiable identities, reducing identity theft and fraud (Ølnes *et al*., 2017). In voting systems, blockchain enhances transparency and security, reducing the risk of election fraud and increasing voter confidence (Kshetri, 2017). Another promising application is in land registry, where blockchain can streamline registration processes, reducing corruption and improving efficiency (Ølnes *et al*., 2017).

ENERGY

Blockchain is facilitating innovation in the energy sector by enabling peer-to-peer energy trading, which allows consumers to trade excess energy directly, promoting renewable energy adoption (Mengelkamp *et al*., 2018). It also improves grid management by enabling real-time data sharing and automated transactions, enhancing the efficiency and reliability of energy grids (Andoni *et al*., 2019).

ENTERTAINMENT AND MEDIA

Finally, blockchain empowers creators and improves content distribution by enabling content monetization through platforms like NFTs, reducing reliance on intermediaries and allowing creators to earn directly from their work (Dowling, 2021). Furthermore, smart contracts automate royalty payments, ensuring fair compensation for creators and streamlining the

distribution process (Tschorsch & Scheuermann, 2016).

In short, blockchain technology represents a paradigm shift in how we think about trust, data, and transactions. While cryptocurrencies like Bitcoin and Ethereum have drawn significant attention, the more significant potential of blockchain lies in its ability to transform industries by enhancing transparency, security, and efficiency. As the technology evolves, its applications are likely to expand, driving innovation and creating new opportunities across sectors. At the same time, realizing this potential will require addressing challenges such as scalability, regulatory uncertainty and harmonization, and energy consumption (Catalini & Gans, 2016; Werbach, 2018).

FINANCIAL CRIMES FACILITATED BY CRYPTOCURRENCIES

Cryptocurrencies have become a double-edged sword in the financial world. While they offer innovative solutions for decentralized finance and cross-border transactions, their anonymity, decentralization, and ease of use have also made them a preferred tool for financial crimes, leading to new regulatory approaches and issues of human rights (Rueckert, 2019; Trozze *et al*., 2022). In 2023, the Lazarus Group laundered $1.2 billion via cross-chain swaps and privacy coins (Chainalysis, 2024), demonstrating evolving tactics. As more illicit addresses are identified and incorporatd into the Chainalysis annual reports, the volume of inflows to illicit actors is growing by an estimated rate of 25% annually (Chainalysis, 2025).

Below is brief overview of how cryptocurrencies are implicated in money laundering, terrorism financing, illicit trade, sanctions violations, fraud and scams, ransomware, market manipulation, and dark web activities. This discussion is summarized in the crypto-crime typology below:

1. Money Laundering

Cryptocurrencies have attracted money laundering activities, as they offer decentralization and a perception of anonymity. Criminal offenders have used techniques such as tumblers and mixing services, peer-to-peer networks, and complex transaction chains in their efforts to obscure the origins of illicit proceeds (Alotibi *et al*., 2022) - cryptocurrency tumblers, also known as “mixers”, are services that attempt to obscure the origin of cryptocurrencies by mixing them with other cryptocurrencies (Foley *et al*., 2019). Detected cases, such as the BTC-e exchange and the PlusToken scam, highlight the ways in which money laundering activities involve cryptocurrencies (Fanusie & Robinson, 2018). Additionally, peer-to-peer networks serve as a means for laundering funds without traditional banking oversight (Hvidson, 2022). The complexities of transaction chains have grown, with cybercriminals employing sophisticated techniques to enhance opacity (Agarwal *et al*., 2023).

The estimated amount laundered via cryptocurrencies surged to USD 23.8 billion in 2022, which represents a 68% increase from the previous year (Japinye, 2024). The use of mixing services and peer-to-peer networks makes tracking these transactions challenging (Leuprecht *et al*., 2022; Holt *et*

CRYPTO-CRIME TYPOLOGY

Crime Category	Description	Examples
1. Money Laundering	Obscuring the origins of illicitly obtained cryptocurrencies to make them appear legitimate.	Tumblers and mixing services, peer-to-peer networks, complex transaction chains.
2. Terrorism Financing	Using cryptocurrencies to raise and transfer funds for terrorist activities.	Transferring funds to wallets controlled by terrorist organizations.
3. Fraud and Scams	Deceiving individuals or entities to obtain cryptocurrencies through false pretenses.	Ponzi schemes (e.g., OneCoin), fraudulent ICOs, exchange collapses (e.g., QuadrigaCX).
4. Ransomware	Extorting cryptocurrency payments in exchange for decrypting data or restoring access to systems.	WannaCry attack, Colonial Pipeline attack.
5. Market Manipulation	Interfering with cryptocurrency markets to artificially inflate or deflate prices for profit.	Spoofing, wash trading, using stablecoins (e.g., Tether) to manipulate prices.
6. Illicit Activities and the Dark Web	Using cryptocurrencies to facilitate illegal transactions and trade on dark web marketplaces.	Sale of drugs, weapons, stolen data, and other illegal goods and services (e.g., Silk Road, AlphaBay, Hydra Market).

al., 2023; see also Nicholls *et al*. 2021 for illustrations and investigative approaches). Recent studies emphasize the emergence of advanced techniques such as cryptomixing, which obfuscate transaction paths and complicate traceability, posing significant challenges to regulatory bodies (Leuprecht *et al*., 2022).

2. Terrorism Financing

Designated terrorist organizations have also turned to cryptocurrencies for fundraising drawn by their pseudonymous nature and ease of cross-border transfers. Groups such as ISIS and the Al-Qassam Brigades, the military wing of Hamas, have used Bitcoin to raise funds for their operations, leveraging the anonymity of cryptocurrencies, in not very successful efforts to evade detection by financial authorities. Funds were transferred to wallets controlled by such organizations, often using privacy-focused cryptocurrencies like Monero and ZCash (Weimann, 2016; Greenberg, 2019).

In more recent cases, we have seen that illicit actors may transfer funds directly to wallets controlled by terrorist organizations, thereby circumventing traditional banking systems (Huey *et al*., 2024). Recent evaluations refer to the use of digital currencies like Bitcoin, where seamless transfer features play a role in funding extremist activities (Bhatnagar *et al*., 2023). Concerns among governments and international organizations have led to calls for more stringent guidelines and frameworks to monitor and impede such transactions (Al-Tawil, 2022).

3. Fraud and Scams

Cryptocurrencies have also become a breeding ground for fraudulent activities, such as scams, Ponzi schemes, and other misconduct. The decentralized nature of cryptocurrencies makes it difficult to recover stolen funds, and the lack of regulatory oversight has made ICOs a fertile ground for fraud (Vasek & Moore, 2015; Zetzsche *et al*., 2018). As shown in Figure **1**, the cases and losses in reported fraud cases related to cryptocurrency has been steadily rising in the USA.

Several high-profile case studies illustrate the scale and impact of cryptocurrency fraud. One of the most notorious examples of cryptocurrency fraud is the OneCoin scam, a fraudulent scheme that defrauded investors of over $4 billion. Marketed as a legitimate cryptocurrency, OneCoin was in fact a Ponzi scheme that used new investor funds to pay returns to earlier investors. The scheme claimed to have its own blockchain and cryptocurrency, but investigations revealed that no real blockchain technology or product existed. Instead, OneCoin relied on aggressive marketing tactics and false promises of high returns.

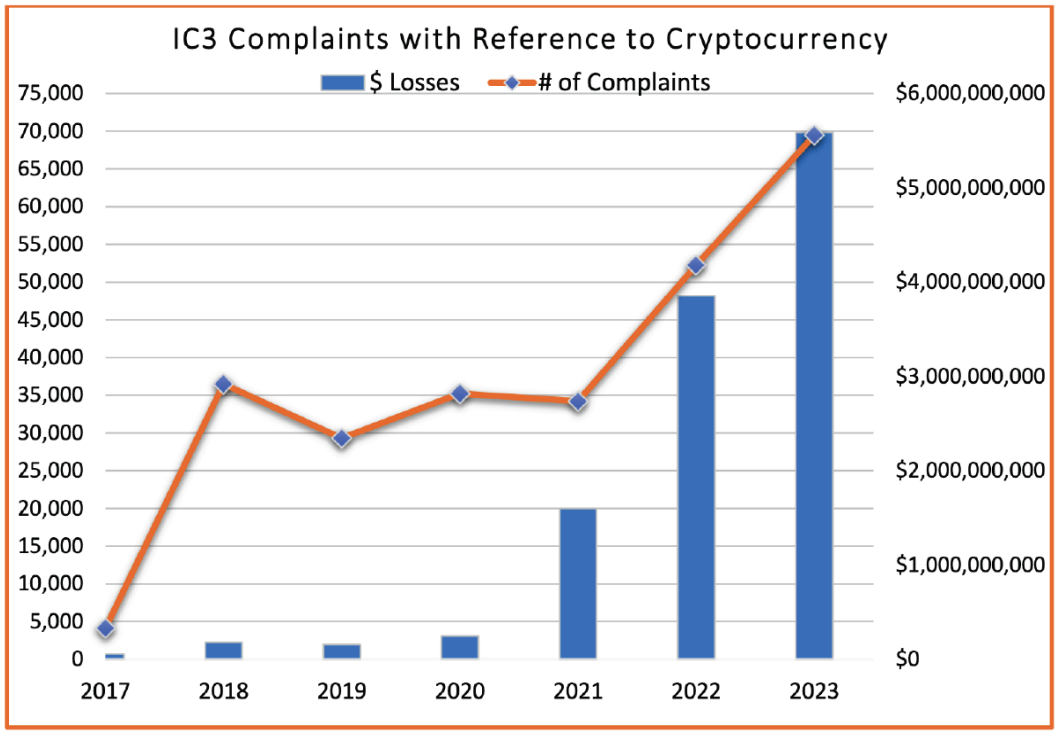

Figure 1: Reports received by the Internet Crime Complaint Center in the USA (Source: FBI, 2023).

The scheme eventually collapsed in 2019, leaving thousands of investors with significant losses (Zetzsche *et al*., 2018).

Another significant case is the QuadrigaCX collapse, which unfolded in 2019 and resulted in the loss of approximately $190 million in customer funds. QuadrigaCX was once Canada's largest cryptocurrency exchange, but its operations came to a sudden halt following the unexpected death of its CEO, Gerald Cotten. Cotten was the sole individual with access to the exchange's cold wallets, where the majority of customer funds were stored. His death left the exchange unable to retrieve the assets, leaving thousands of users unable to access their funds. Investigations later revealed mismanagement and questionable practices, including allegations that some funds had been misappropriated prior to the collapse (Bartoletti *et al*., 2021; Vasek & Moore, 2015). Both of these high-profile Ponzi schemes and fraudulent Initial Coin Offerings (ICOs) have caused significant financial losses for investors and serve as stark reminders of the risks involved in this emerging market.

More recent works consistently note that despite legislative efforts, criminals continuously innovate their methods to exploit unsuspecting individuals and investors (Saha *et al*., 2024). Notable is also the influx of new fraud techniques alongside growing awareness within cryptocurrency communities regarding these schemes (Childs, 2024). Adaptive scam methodologies continue to evolve in response to regulatory measures and community learning (Das *et al*., 2025). The encouragement of the "do your own research" mentality has become prevalent, emphasizing the need for individual and regulatory vigilance.

4. Ransomware

Ransomware attacks, where attackers demand payment in cryptocurrencies to unlock encrypted data and restore access to data or systems, have surged in recent years. Bitcoin is the preferred payment method for ransomware operators due to its pseudonymity and ease of use (Paquet-Clouston *et al*., 2019). Recent notable cases, such as the WannaCry ransomware attack and the Colonial Pipeline attack, highlight the role of cryptocurrencies in facilitating ransomware payments (Chainalysis, 2023; Saha *et al*., 2024).). In 2021 alone, the rise in ransomware payments in cryptocurrencies underscored a shift in the tactics of cybercriminals, leveraging the perceived anonymity of cryptocurrencies (Almaqableh *et al*., 2023).

A pattern of increasing sophistication in ransom ware tactics has emerged, where attackers leverage multi-layered encryption and threats to compel victims into compliance with their demands (Ramanathan *et al*., 2023). As cryptocurrency transactions are irreversible once completed, victims often find themselves at the mercy of their attackers, with few avenues for recourse available (Bhatnagar *et al*., 2023). Consequently, businesses and governments are forced to invest heavily in preventative measures and reactive strategies to mitigate these risks Truong *et al*. (2023).

5. Market Manipulation

Cryptocurrency markets are susceptible to manipulation, again due to a lack of regulation and transparency. This vulnerability has led to a range of manipulative practices that distort market prices, undermine investor confidence, and pose systemic risks to the broader cryptocurrency ecosystem. A well-documented form of manipulation in cryptocurrency markets is price manipulation, which includes tactics such as spoofing and wash trading. Spoofing involves placing large buy or sell orders with no intention of executing them, creating a false impression of market demand or supply to influence prices. Wash trading, on the other hand, involves trading with oneself to create artificial trading volume and activity (Gandal *et al*., 2018; Saha *et al*., 2024). These tactics have been relatively easy to execute due to the lack of regulatory oversight and the loosely organized nature of cryptocurrency exchanges (Ili, 2025). The prevalence of such tactics highlights a significant flaw in the mechanisms purported to promote fair trading practices within the market (Trozze *et al*., 2022).

Another case revolved around Tether (USDT), a stablecoin pegged to the US dollar, and raised concern for regulators (Alotibi *et al*., 2022; Saha *et al*., 2024). Griffin and Shams (2020) found evidence that Tether was used to manipulate Bitcoin prices during periods of market volatility and that large issuances of Tether were often followed by significant increases in Bitcoin prices, suggesting that Tether was used to prop up demand artificially. This type of financial crime not only distorts markets, but also raises questions about the integrity of the cryptocurrency ecosystem in general and undermines investor confidence.

6. Illicit Activities and the Dark Web

Cryptocurrencies have become the preferred medium of exchange for illicit activities on the dark

CASE EXAMPLE – Cryptocurrency laundromat washed out
ChipMixer, an unlicensed cryptocurrency mixer, was taken down in March 2023, for its alleged involvement in money laundering activities. Deposited funds would be turned into "chips" (small tokens with equivalent value), which were then mixed together - thereby anonymising all trails to where the initial funds originated. The investigation into the criminal service suggests that the platform may have facilitated the laundering of 152 000 Bitcoins (worth roughly EUR 2.73 billion in current estimations) in crypto assets. A large share of this is connected to darkweb markets, ransomware groups, illicit goods trafficking, procurement of child sexual exploitation material, and stolen crypto assets. Information obtained after the takedown of the Hydra Market darkweb platform uncovered transactions in the equivalent of millions of euros.

Box 1: Dark Web Markets (Source: Europol, 2025: 25).

web, facilitating the sale of drugs, weapons, stolen data, and other illegal goods and services. While law enforcement agencies have made significant strides in dismantling dark web marketplaces, the persistent emergence of new platforms and the growing use of privacy-enhancing technologies continue to pose challenges for investigators (Foley *et al.* 2019; Saha *et al*., 2024). The Hydra Market, shut down in 2023 for example, processed $5.2 billion in Bitcoin transactions for drugs and stolen data (Europol, 2023).

High-profile operations have led to the shutdown of several major platforms, including Silk Road and AlphaBay. Silk Road, one of the earliest and most notorious dark web marketplaces, operated from 2011 to 2013 and facilitated the trade of drugs, weapons, and other illegal goods using Bitcoin and allowing users to transact without revealing their identities (Agarwal *et al*., 2023). Its founder, Ross Ulbricht, was eventually arrested, and the platform was shut down, marking a significant victory for law enforcement (Christin, 2013). Similarly, AlphaBay, another major dark web marketplace, was dismantled in 2017 following a multinational law enforcement operation. At its peak, AlphaBay facilitated millions of dollars in transactions involving drugs, stolen data, and other illicit goods (Foley *et al*., 2019).

The dark web serves as a vital hub for illicit transactions, with a plethora of marketplaces facilitating the buying and selling of prohibited items including drugs, weapons, and counterfeit currencies, all typically using cryptocurrencies for payment. Various studies highlight that these marketplaces, such as AlphaBay and Dream Market, thrive on the dark web where anonymity is paramount for user protection against law enforcement actions (Bracci *et al*., 2021).

Recent studies have quantified extensive transactions occurring within dark web marketplaces, illustrating the lucrative nature of these environments. Marketplaces reportedly generate billions of dollars annually in revenue from illicit trades, fostering complex networks of user-to-user relationships in these trading environments (Nadini *et al*., 2022). This research also emphasizes the cumulative impact of these transactions on cryptocurrency values and the challenges faced in monitoring and controlling illegal activities within these platforms. Illustrative of the use of dark web market places for the commission of various offenses are the 2022 and 2023 cases of ChipMixer and Hydra Market.

Grappling with regulation, the academic discourse points to efforts toward enhanced monitoring and potential regulations within jurisdictions employing government-backed cryptocurrencies to disrupt illegal activities deeply embedded within these markets. Such regulatory frameworks aim to curb the excessive anonymity currently enjoyed by illicit actors on the dark web (Tewari, 2023).

REGULATORY AND ENFORCEMENT RESPONSES

1. International Regulations and Standards

The Financial Action Task Force (FATF) has been instrumental in shaping the regulatory environment surrounding cryptocurrencies, aiming to balance innovation with risk mitigation. In 2018, FATF amended Recommendation 15 and extended its financial vigilance standards to cover virtual assets (VA) and VASPs. This means, inter alia that, the FATF mandates the establishment of national regulatory frameworks to mitigate the risks associated with ML/TF activities through VASPs, including license and/or registration, robust customer due diligence (CDD), transaction monitoring, record-keeping, and reporting obligations within the digital asset sector. Since then, it has produced red flags, guidance updates as well as three reviews on the implementation of its standards on VAs and VASPs (FATF, 2019, 2020, 2021, 2023).

Additionally, the Basel Committee on Banking Supervision has proposed prudential standards for banks exposed to cryptocurrencies, considering them as high-risk and requiring higher capital reserves (Basel Committee, 2021), while the International Organization of Securities Commissions issued guidelines for regulating cryptocurrency markets, focusing on investor

Table 1: Overview of FATF Work on VAs and VASPs. (Source: FATF, 2024)

2018	• Recommendation 15 amended
2019	• Adoption of Interpretive Note to R.15 • Creation of the FATF Virtual Assets Contact Group (VACG) • Initial guidance for regulators: A risk-based approach to VAs and VASPs (updated in 2021)
2020	• 12 month review of the new FATF Standards: 1st12-month review • Report to the G20: FATF Report to the G20 on So-called Stablecoins • Risk indicators: List of Red Flag Indicators of ML/TF through VAs
2021	• Updated guidance: Updated Guidance for a Risk-Based Approach to VA and VASPs • 24 month review of the FATF Standards: 2nd12-month review
2022	• Report on R.15 compliance, with a particular focus on the Travel Rule, and emerging VA risks: • Targeted Update on Implementation of the FATF Standards on VA and VASPs
2023	• Report on ransomware, with focus on VA risks and trends: Countering Ransomware Financing • Report on implementation of R.15: VAs: Targeted Update on Implementation of the FATF Standards
2024	• Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity

protection, market integrity, and the prevention of fraud and manipulation (IOSCO, 2020).

2. National and Regional Regulatory Approaches

Regulatory clarity in some regions (e.g., the U.S., EU, and Japan) has encouraged institutional investors to enter the crypto market. For example, the approval of Bitcoin ETFs and frameworks for crypto custody have made it easier for traditional financial players to engage with cryptocurrencies, while tax clarity was provided in the USA (IRS, 2021). On the other hand, some countries (e.g., China, India) have imposed outright bans or severe restrictions on crypto trading and mining, stifling adoption in those regions

Big economies, such as the United States and China or regions, such as the European Union, have thus adopted diverse regulatory approaches to address the risks posed by cryptocurrencies. The U.S. has adopted a multi-agency approach, with the Securities and Exchange Commission (SEC) regulating Initial Coin Offerings (ICOs) and cryptocurrency securities (US SEC, 2021), the Commodity Futures Trading Commission (CFTC) overseeing cryptocurrency derivatives (US CFTC, 2022), and the Financial Crimes Enforcement Network (FinCEN) receiving suspicious activity reports and enforcing AML/CFT requirements for VASPs (US FinCEN, 2021). Interestingly, SEC cryptocurrency-related enforcement actions reached their peak in 2023, while there was a 30% decrease in 2024 (Cornerstone Research, 2024).

China has taken a strict stance, banning cryptocurrency trading and mining while promoting its central bank digital currency (CBDC), the digital yuan (e-CNY), as part of its broader strategy to modernize the financial system and maintain monetary sovereignty (People's Bank of China, 2021). Japan has implemented a licensing regime for cryptocurrency exchanges under its *Payment Services Act*, requiring compliance with AML/CFT and cybersecurity standards (Financial Services Agency of Japan, 2021).

The European Union's (EU) *Fifth Anti-Money Laundering Directive* (5AMLD, Directive (EU) 2018/843) came into effect on July 9, 2018 and expanded the scope of the EU's AML/CFT framework to include cryptocurrency exchanges and wallet providers as "obliged entities." As a result, these service providers are now required to implement customer due diligence measures, monitor transactions, and report suspicious activities to their Financial Intelligence Units (European Commission, 2020).

Current regulatory frameworks, such as the EU's MiCA Regulation (2023) and FATF guidelines, have significantly influenced cryptocurrency adoption by balancing innovation with risk mitigation. The Markets in Crypto-Assets (MiCA) Regulation, adopted in 2023 as Regulation (EU) 2023/1114, aims to create a comprehensive framework for cryptocurrency markets within the EU. It establishes uniform rules for crypto-assets not currently covered by existing financial services legislation. Key provisions include transparency and disclosure requirements for the issuance and trading of crypto-assets, as well as licensing and supervision mandates for Virtual Asset Service Providers (VASPs) (European Parliament and Council, 2023).

3. Challenges and Limitations

Despite these regulatory efforts, challenges remain. The global nature of cryptocurrencies creates enforcement challenges, as criminals exploit regulatory gaps (Zohar, 2020). Privacy-focused cryptocurrencies like Monero and Zcash hinder transaction tracing, undermining AML efforts (Narayanan *et al*., 2021). Additionally, decentralized exchanges (DEXs) operate without a central authority, making it challenging to enforce Know Your Customer (KYC) and AML requirements (De Filippi, 2021).

FUTURE DIRECTIONS AND RECOMMENDATIONS

As cryptocurrencies and blockchain technology continue to evolve, addressing the challenges associated with financial crimes and regulatory oversight will require a multifaceted and coordinated approach. This concluding section outlines potential improvements in regulatory frameworks, technological innovations, collaborative efforts, and education initiatives to bring about a safer and more transparent ecosystem.

A critical aspect of regulatory improvement is the harmonization of global regulations, given that legal and law enforcement asymmetries have criminogenic effects (Passas, 1998; Dolliver and Love, 2021). Governments and international organizations must continue working towards unified standards to mitigate jurisdictional arbitrage. The FATF will play a central role in promoting consistent AML/CTF standards across jurisdictions (FATF, 2021, 2024). In addition, cross-border cooperation, including international agreements for information sharing and joint enforcement actions, can help combat transnational financial crimes (Zetzsche, Buckley, & Arner, 2020). A more adaptive and risk-based regulatory approach is necessary, tailoring oversight to the risk profiles of different cryptocurrency activities. High-risk sectors, such as initial coin offerings (ICOs) and decentralized finance (DeFi) platforms, require stricter oversight compared to lower-risk applications (Gensler, 2022). Regulatory sandboxes provide an avenue for testing emerging technologies and business models in a controlled environment, ensuring compliance while fostering innovation (Philippon, 2020). Furthermore, emerging technologies such as privacy-focused cryptocurrencies like Monero and Zcash necessitate specific regulatory guidelines that balance privacy with transparency (Brooks, 2021). The oversight of decentralized exchanges (DEXs) and DeFi platforms must also be strengthened, given their ability to operate without intermediaries (Easley, O'Hara, & Basu, 2019).

The complexity of some of these illicit transactions, highlighted the need for law enforcement agencies to devise innovative strategies (Das *et al*., 2025). Keeping pace with the rapid evolution of technology and criminal tactics necessitates the development of specialized teams and bolstered international cooperation (Trozze *et al*., 2022).

Technological advancements can significantly enhance monitoring, tracing and other enforcement capabilities in cryptocurrency markets. Acknowledging the influence of market sentiment and external news on volatility, researchers have begun to develop frameworks for anticipating and mitigating manipulative acts (Bhatnagar *et al*., 2023).

Figure 2: Blockchain tracing involves tracking transactions across distributed ledgers to identify sources, destinations, and intermediary wallets. This image illustrates key blockchain tracing instruments, such as:

- **Magnifying Glass & Connected Blocks**: Represents transaction analysis, highlighting the movement of assets between addresses.
- **Clipboard & Graph**: Symbolizes record-keeping and data visualization tools used to detect suspicious activity.
- **Barcode & Pie Chart**: Indicates forensic analytics techniques, such as address clustering, risk scoring, and transaction pattern recognition.

Figure **3** provides a concrete example of how the tracing process works in practice. It traces a ransomware payment through a mixing service to an exchange and finally to a bank account. It also

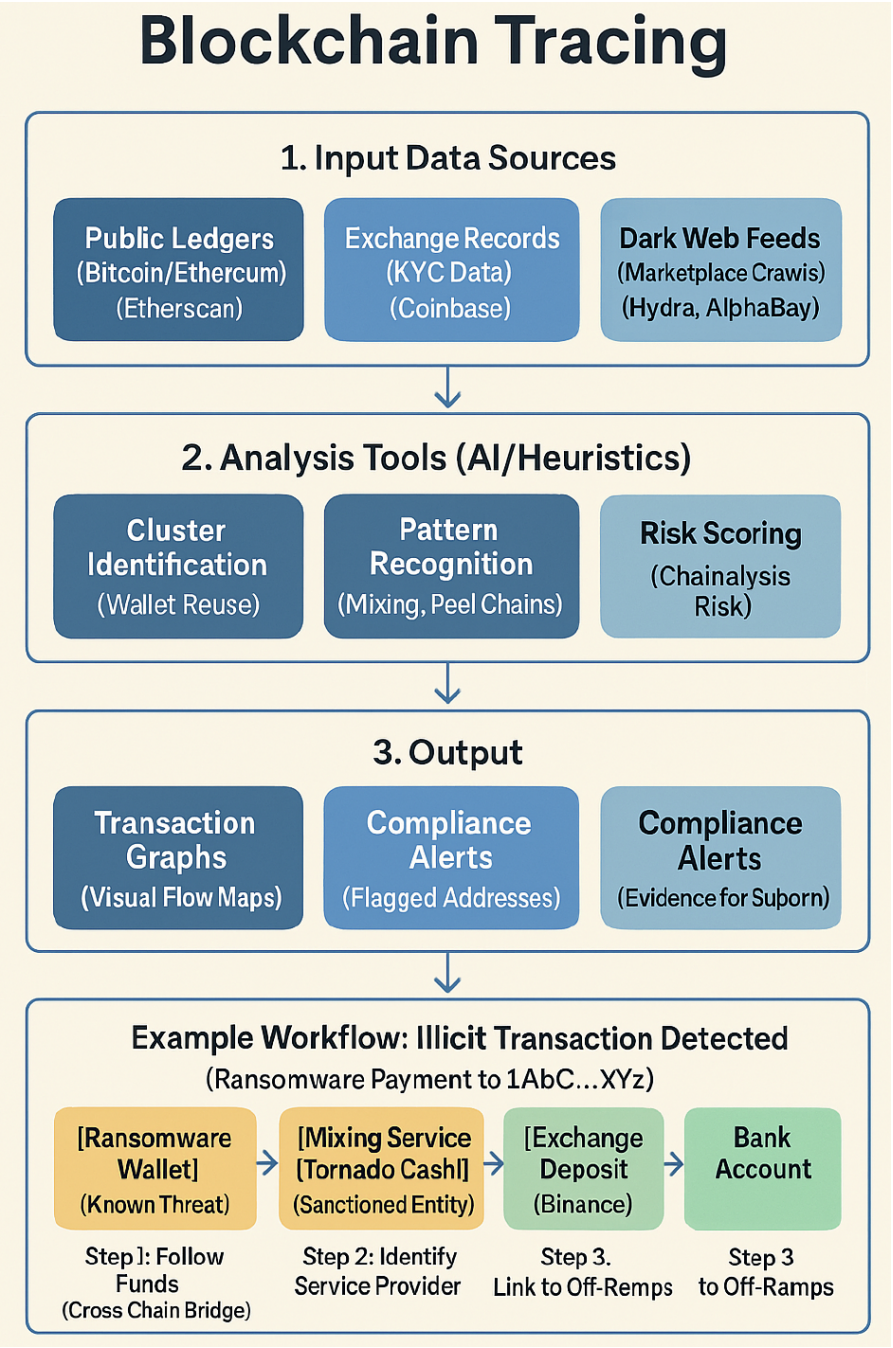

Figure 3: Blockchain tracing process (created by author with instructions to chat GPT.)

annotates each step with information about the nature of the entity or action.

All of these tools are crucial for law enforcement, compliance teams, and researchers monitoring illicit financial flows, fraud, and regulatory violations in blockchain ecosystems.

AI-powered blockchain analytics platforms, such as Chainalysis and Elliptic, assist regulators and law enforcement agencies in detecting suspicious patterns, tracing illicit transactions, and identifying bad actors (Foley, Karlsen, & Putniņš, 2019). Real-time monitoring using AI algorithms enables proactive intervention in cases of fraud or money laundering (Brenig, Accorsi, & Mueller, 2019). Smart contracts offer additional compliance mechanisms by automating regulatory requirements such as KYC checks and transaction limits, thereby improving efficiency and reducing compliance burdens (Werbach & Cornell, 2017). Blockchain-based systems can further enhance transparency by enabling automated reporting of suspicious activities to regulators (Schaupp & Festa,

Table 2: Tracing Techniques/Tools that Combine on-Chain data with off-Chain Intelligence to De-Anonymize Criminals

Key Tracing Techniques		
Method	**How It Works**	**Example Tools**
Address Clustering	Links wallets by common inputs/outputs	Elliptic, Crystal Blockchain
UTXO Analysis	Tracks unspent transaction outputs	Chainalysis Reactor
Privacy Coin Tracking	Uses timing/metadata flaws	CipherTrace (Monero tracing)

2018). Decentralized identity solutions provide secure and verifiable digital identity credentials, mitigating the risks of identity theft and fraud (Zhao & O'Mahony, 2018). The development of interoperable identity frameworks facilitates seamless KYC processes across jurisdictions and platforms, further strengthening regulatory compliance (Allen, 2021). As various jurisdictions tighten their anti-money laundering frameworks, they have begun adopting advanced technologies such as machine learning to detect suspicious transactions more effectively (Alekseenko, 2023; Das *et al*., 2025). This proactive approach is an essential step toward counteracting the burgeoning trend of crypto-enabled money laundering.

Global collaborations among governments, financial institutions, and technology companies is essential for effectively regulating cryptocurrency markets. Public-private partnerships can facilitate information sharing about emerging threats and best practices, enabling a more coordinated response to illicit activities (Bromberg, Godwin, & Ramsay, 2020). Joint task forces pooling resources and expertise can enhance investigative and prosecutorial efforts against cryptocurrency-related crimes (Europol, 2021). Industry self-regulation also plays a vital role in maintaining market integrity. Cryptocurrency exchanges and other stakeholders may wish to consider the development and adherence to a code of conduct that promotes transparency, security, and compliance (Hughes, 2020). Independent certification programs can verify that platforms meet established standards for security and regulatory compliance, building trust within the ecosystem (OECD, 2021). On a global scale, organizations such as Interpol, Europol, and the United Nations can facilitate international cooperation to combat cryptocurrency-related financial crimes (UNODC, 2022). Standard-setting bodies and industry consortia can further contribute by developing technical standards and best practices for blockchain and cryptocurrency systems (IOSCO, 2021).

Finally, education and awareness initiatives are critical to fostering a secure and informed crypto-currency integrity culture and environment. Public awareness campaigns should focus on educating consumers about the risks and benefits of cryptocurrencies while providing tools to identify and avoid scams (World Bank, 2020). Accessible fraud prevention resources, such as online guides and interactive tools, empower users to protect themselves from financial crimes (FINRA, 2021). Professional training programs for regulators and law enforcement agencies are also helpful, equipping them with the necessary technical knowledge and skills to monitor and investigate cryptocurrency-related activities effectively (IMF, 2021). Industry certification programs can further promote best practices and improve industry standards. Academic and research initiatives also play a crucial role in providing these and advancing the field. Universities and research institutions should develop specialized programs in blockchain technology, cryptocurrency regulation, and financial crime prevention (MIT Media Lab, 2021). Additionally, governments and private organizations should allocate funding for research into emerging trends, risks, and solutions in the cryptocurrency ecosystem (NSF, 2021).

A comprehensive approach encompassing regulatory refinement, technological innovation, collaborative efforts, and education is necessary to enhance the security and transparency of cryptocurrency markets. By leveraging these strategies, policymakers and industry stakeholders can help produce a regulatory environment that fosters innovation while properly controlling financial crimes and strengthening investor trust.

REFERENCES

Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2023). Blockchain and crypto forensics: investigating crypto frauds. International Journal of Network Management, 34(2). https://doi.org/10.1002/nem.2255

Aldridge, J., & Décary-Hétu, D. (2014). Not an 'eBay for drugs': The cryptomarket 'Silk Road' as a paradigm shifting criminal innovation. *British Journal of Criminology, 54*(4), 680-703. https://doi.org/10.2139/ssrn.2436643

Alekseenko, A. P. (2023). Model framework for consumer protection and crypto-exchanges regulation. Journal of Risk and Financial Management, 16(7), 305. https://doi.org/10.3390/jrfm16070305

Allen, C. (2021). Interoperable Identity Frameworks: Strengthening KYC Processes Across Jurisdictions. *Journal of Digital Identity*, 12(3), 45-60.

Al-Tawil, T. N. (2022). Anti-money laundering regulation of cryptocurrency: uae and global approaches. Journal of Money Laundering Control, 26(6), 1150-1164. https://doi.org/10.1108/JMLC-07-2022-0109

Almaqableh, L., Wallace, D., Pereira, V., Ramiah, V., Wood, G., Veron, J. F., … & Watson, A. (2023). Is it possible to establish the link between drug busts and the cryptocurrency market? yes, we can. International Journal of Information Management, 71, 102488. https://doi.org/10.1016/j.ijinfomgt.2022.102488

Alotibi, J., Almutanni, B., Alsubait, T., Alhakami, H., & Baz, A. (2022). Money laundering detection using machine learning and deep learning. International Journal of Advanced Computer Science and Applications, 13(10). https://doi.org/10.14569/IJACSA.2022.0131087

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities. *Renewable and Sustainable Energy Reviews*, 100, 143-174. https://doi.org/10.1016/j.rser.2018.10.014

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* O'Reilly Media.

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: analysis and perspectives. IEEE Access, 9, 148353-148373. https://doi.org/10.1109/ACCESS.2021.3123894

Bhatnagar, M., Taneja, S., & Rupeika-Apoga, R. (2023). Demystifying the effect of the news (shocks) on crypto market volatility. Journal of Risk and Financial Management, 16(2), 136. https://doi.org/10.3390/jrfm16020136

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213-238. https://doi.org/10.1257/jep.29.2.213

Brenig, C., Accorsi, R., & Mueller, G. (2019). Real-Time Monitoring of Blockchain Transactions Using AI Algorithms. *Journal of Financial Technology*, 8(2), 123-140

Bromberg, L., Godwin, A., & Ramsay, I. (2020). Public-Private Partnerships in Financial Regulation: Enhancing Collaboration for Cryptocurrency Oversight. *Journal of Financial Regulation*, 6(1), 78-95.

Brooks, R. (2021). Privacy Coins and Regulatory Challenges: A Framework for Balancing Privacy and Transparency. *Journal of Financial Regulation and Compliance*, 29(3), 345-360.

Buterin, V. (2013). *Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform.* Ethereum Whitepaper.

Catalini, C., & Gans, J. S. (2016). Some Simple Economics of the Blockchain. *MIT Sloan Research Paper*, 5191-1. https://doi.org/10.3386/w22952

Campbell-Verduyn, M. (2018). *Bitcoin and Beyond: Cryptocurrencies, Blockchain, and Global Governance*. Routledge. https://doi.org/10.4324/9781315211909

Chainalysis. (2023). *The 2023 Crypto Crime Report.* Retrieved from https://www.chainalysis.com

Chainalysis. (2024). *The 2024 Crypto Crime Report.* Retrieved from https://www.chainalysis.com

Chainalysis (2025). *Crypto Crime Report: The rising role of cryptocurrency in all forms of crime and how its transparency is creating unique opportunities for investigation.* Retrieved from: https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf

Childs, A. (2024). 'I guess that's the price of decentralisation… ': Understanding scam victimisation experiences in an online cryptocurrency community. *International Review of Victimology*, 30(3), 539-555. https://doi.org/10.1177/02697580231215840

Christin, N. (2013). *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*. Proceedings of the 22nd International Conference on World Wide Web. https://doi.org/10.1145/2488388.2488408

Cornerstone Research. (2024). *SEC Cryptocurrency Enforcement 2024 Update*. Retrieved from https://www.cornerstone.com/wp-content/uploads/2025/01/SEC-Cryptocurrency-Enforcement-2024-Update.pdf

Das, B. N., Sarker, B. C., Saha, A., Bishnu, K. K., Das, B., Sartaz, M. S., … & Khan, M. A. (2025). Detecting cryptocurrency scams in the USA: a machine learning-based analysis of scam patterns and behaviors. Journal of Ecohumanism, 4(2). https://doi.org/10.62754/joe.v4i2.6604

Dolliver, D., & Love, K. (2015). Criminogenic Asymmetries in Cyberspace: A Comparative Analysis of Two Tor Marketplaces. *Journal of Globalization Studies, 5*(2), 75–96.

Dowling, M. (2021). Is Non-Fungible Token Pricing Driven by Cryptocurrencies? *Finance Research Letters*, 102097. https://doi.org/10.1016/j.frl.2021.102097

Easley, D., O'Hara, M., & Basu, S. (2019). *From Mining to Markets: The Evolution of Bitcoin Transaction Fees*. *Journal of Financial Economics*, 134(1), 91-109. https://doi.org/10.1016/j.jfineco.2019.03.004

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). *A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data*. MIT Media Lab.

European Commission. (2020). *Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu

European Parliament and Council. (2023) Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32023R1114

Europol. (2019). *Internet Organised Crime Threat Assessment (IOCTA) 2019.* Europol. https://doi.org/10.1016/S1361-3723(19)30114-9

Europol. (2021). *Joint Task Forces and Cryptocurrency Crime: Enhancing Investigative Efforts.* Europol.

Europol. (2025) *The Changing DNA of Serious and Organised Crime.* Europol.

Fanusie, Y. J., & Robinson, T. (2018). Bitcoin laundering: An analysis of illicit flows into digital currency services. *Center on Sanctions and Illicit Finance.*

FATF (2019) *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs)*, FATF, Paris.

FATF (2020), Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, FATF, Paris.

FATF, Paris FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris.

FATF (2024), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris.

FBI. (2023). *Cryptocurrency Fraud Report*. FBI: Internet Crime Complaint Center.

Financial Services Agency of Japan. (2021). *Amendment of the Payment Services Act and the Act on Prevention of Transfer of Criminal Proceeds*. Retrieved from https://www.fsa.go.jp

FINRA. (2021). *Fraud Prevention Resources for Cryptocurrency Users*. Retrieved from https://www.finra.org

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies, 32*(5), 1798-1853. https://doi.org/10.1093/rfs/hhz015

Gensler, G. (2022). *Remarks Before the Aspen Security Forum*. U.S. Securities and Exchange Commission. Retrieved from https://www.sec.gov

Gervais, A., Karame, G. O., & Capkun, S. (2016). *On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients*. IEEE Security & Privacy.

Gokal, R., & Yakovenko, A. (2020). *Solana: Scaling Blockchain for Global Adoption.* Solana Research Papers

Hertig, A. (2018). *Ethereum's Transition to Proof of Stake: Challenges and Benefits.* Blockchain Research Institute.

Huey, Y. C., Angeline, Y. K. H., Teng, Y. S., Melissa, T. T. T., Chin, W. S., & Saleh, Z. (2024). Text analytics on regulation of cryptocurrency. KnE Social Sciences. https://doi.org/10.18502/kss.v9i14.16140

Holt, T. J., Lee, J. R., & Griffith, E. M. (2023). An assessment of cryptomixing services in online illicit markets. Journal of Contemporary Criminal Justice, 39(2), 222-238. https://doi.org/10.1177/10439862231158004

Hoskinson, C. (2017). *Cardano Whitepaper: A Decentralized Public Blockchain and Cryptocurrency Project.* IOHK

Hughes, S. (2020). Self-Regulation in the Cryptocurrency Industry: Developing a Code of Conduct. *Journal of Financial Compliance*, 4(2), 112-130.

Hvidson, K. (2022). The influence of cryptocurrency on international relations and sanctions. Journal of Global Economy, Business and Finance, 4(2). https://doi.org/10.53469/jgebf.2022.04(02).10

İli, B. (2025). Analysis of complaints regarding cryptocurrency investment fraud: an evaluation from the perspective of new media literacy. Iğdır Üniversitesi Sosyal Bilimler Dergisi, (38), 214-229. https://doi.org/10.54600/igdirsosbilder.1580718

IRS. (2021). Virtual currency guidance. *Internal Revenue Service*. Retrieved from https://www.irs.gov/individuals/international-taxpayers/virtual-currency-guidance

IMF. (2021). *Professional Training Programs for Cryptocurrency Regulation*. Washington DC: IMF.

IOSCO. (2021). *Technical Standards for Blockchain and Cryptocurrency Systems*. Retrieved from https://www.iosco.or

Islam, I., & Islam, M. N. (2024). A blockchain based medicine production and distribution framework to prevent medicine counterfeit. *Journal of King Saud University - Computer and Information Sciences*, *36*(1), 101851. https://doi.org/10.1016/j.jksuci.2023.101851

Jamil, F., Hang, L., Kim, K., & Kim, D. (2019). A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. *Electronics*, *8*(5), 505. https://doi.org/10.3390/electronics8050505

Japinye, A. (2024). Integrating machine learning in anti-money laundering through crypto: a comprehensive performance review. European Journal of Accounting Auditing and Finance Research, 12(4), 54-80. https://doi.org/10.37745/ejaafr.2013/vol12n45480

Kshetri, N. (2017). Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. *Telecommunications Policy*, 41(10), 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003

Kshetri, N. (2018). Blockchain's Roles in Meeting Key Supply Chain Management Objectives. *International Journal of Information Management*, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Lee, C. (2011). Litecoin: An Open Source P2P Digital Currency. Litecoin Whitepaper.

Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. Journal of Financial Crime, 30(4), 1036-1054. https://doi.org/10.1108/JFC-07-2022-0161

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing Microgrid Energy Markets: A Case Study. *The Brooklyn Microgrid*. *Applied Energy*, 210, 870-880. https://doi.org/10.1016/j.apenergy.2017.06.054

MIT Media Lab. (2021). *Academic Programs in Blockchain Technology and Cryptocurrency Regulation*. Cambridge, MA: MIT.

Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *White Paper.*

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEE Access*, *9*, 163965–163986. https://doi.org/10.1109/ACCESS.2021.3134076

NSF. (2021). *Funding for Research on Cryptocurrency Trends and Risks*. Washington, DC: NSF.

OECD. (2021). *Independent Certification Programs for Cryptocurrency Platforms*. Paris: OECD.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. *Government Information Quarterly*, 34(3), 355-364. https://doi.org/10.1016/j.giq.2017.09.007

Passas, N. (1999). Globalization, Criminogenic Asymmetries and Economic Crime. *European Journal of Law Reform, 1*(4), 399-423. https://doi.org/10.1108/JFC-06-2017-0058

Passas, N. (2018a). Report on the debate regarding EU cash payment limitations. *Journal of Financial Crime, 25*(1), 5-27.

Passas, N. (2018b). Cash, Crime and Common Sense: Effective and Non-effective Ways of Tackling Illicit Financial Flows. In I. Gloerich, J. Hart, G. Lovink, C. Nevejan, & I. Verkerk (Eds.), *Flying Money 2018: Investigating Illicit Financial Flows in the City* (pp. 70-84). Amsterdam: Amsterdam University of Applied Sciences and City of Amsterdam.

People's Bank of China. (2021). *Notice on Further Preventing and Disposing of the Risks of Virtual Currency Trading and Speculation*. Retrieved from http://www.pbc.gov.cn

Philippon, T. (2020). On Fintech and Financial Inclusion. *Journal of Financial Economics*, 137(2), 234-251.

Ramanathan, V., Tripathi, S., Bhattacharya, S., & Varshney, S. (2023). Public health perspectives on cryptocurrency: the good, the bad and the ugly. Indian Journal of Community Health, 35(3), 372-374. https://doi.org/10.47203/IJCH.2023.v35i03.023

Rueckert, C. (2019). Cryptocurrencies and fundamental rights. *Journal of Cybersecurity*, *5*(1), tyz004. https://doi.org/10.1093/cybsec/tyz004

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain Technology and Its Relationships to Sustainable Supply

Chain Management. *International Journal of Production Research*, 57(7), 2117-2135. https://doi.org/10.1080/00207543.2018.1533261

Saha, S., Hasan, A. R., Mahmud, A., Ahmed, N., Parvin, N., & Karmakar, H. (2024). Cryptocurrency and financial crimes: a bibliometric analysis and future research agenda. Multidisciplinary Reviews, 7(8), 2024168. https://doi.org/10.31893/multirev.2024168

Schaupp, L. C., & Festa, M. (2018). Blockchain-Based Reporting Systems for Regulatory Compliance. *Journal of Information Systems*, 32(3), 45-60.

Schwartz, D., Youngs, N., & Britto, A. (2014). *The Ripple Protocol Consensus Algorithm.* Ripple Labs Inc.

Singer, D., Demirguc-Kunt, A., Klapper, L., & Singer, D. (2017). *Financial Inclusion and Inclusive Growth: A Review of Recent Empirical Evidence*. World Bank, Washington, DC. https://doi.org/10.1596/1813-9450-8040

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.* Penguin.

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1), 1. https://doi.org/10.1186/s40163-021-00163-8

Truong, V. T., Le, L. B., & Niyato, D. (2023). Blockchain meets metaverse and digital asset management: a comprehensive survey. IEEE Access, 11, 26258-26288. https://doi.org/10.1109/ACCESS.2023.3257029

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials*, 18(3), 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

UNODC. (2022). *International Cooperation to Combat Cryptocurrency-Related Financial Crimes*. Vienna, UNODC.

U.S. Commodity Futures Trading Commission (CFTC). (2022). *CFTC Backgrounder on Crypto-Assets*. Retrieved from https://www.cftc.gov

U.S. Financial Crimes Enforcement Network (FINCEN). (2021). *FinCEN Guidance on Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*. Retrieved from https://www.fincen.gov

U.S. Securities and Exchange Commission (SEC). (2021). *Framework for "Investment Contract" Analysis of Digital Assets*. Retrieved from https://www.sec.gov

Vasek, M., & Moore, T. (2015). There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In R. Böhme & T. Okamoto (Eds.), *Financial Cryptography and Data Security* (Vol. 8975, pp. 44–61). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-47854-7_4

Wang, G., Zhang, S., Yu, T., & Ning, Y. (2021). A Systematic Overview of Blockchain Research. *Journal of Systems Science and Information*, *9*(3), 205–238. https://doi.org/10.21078/JSSI-2021-205-34

Weber, R. H., Staub, S., & Hardy, R. (2019). Blockchain technology and digital trade: Challenges and opportunities. *Journal of International Economic Law, 22*(2), 237-259. https://doi.org/10.7551/mitpress/11449.001.0001

Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press

Werbach, K., & Cornell, N. (2017). Contracts Ex Machina: How Smart Contracts Automate Compliance. *Duke Law Journal*, 67(2), 313-350

World Bank. (2020). *Public Awareness Campaigns on Cryptocurrency Risks and Benefits*. Washington DC: World Bank.

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *Journal of Medical Systems*, 40(10), 218. https://doi.org/10.1007/s10916-016-0574-6

Zhao, J. L., & O'Mahony, D. (2018). Decentralized Identity Solutions for Secure Digital Credentials. *Journal of Cybersecurity*, 4(1), 1-15.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2017). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. University of Luxembourg Law Working Paper. https://doi.org/10.2139/ssrn.3072298

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2020). *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*. *New York University Journal of Law & Business*, 14(2), 393-446.

Zhao, C. (2017). *Binance Whitepaper: Building the Crypto Ecosystem.* Binance

Zohar, A. (2015). Bitcoin: Under the hood. *Communications of the ACM, 58*(9), 104-113. https://doi.org/10.1145/2701411

Received on 15-02-2025 Accepted on 20-03-2025 Published on 18-04-2025

https://doi.org/10.6000/1929-4409.2025.14.08