CRYPTOCURRENCY FRAUD: LEGAL CHALLENGES IN INDIA

Varsha Rameshkumar, LLM, SRM School of Law, Kattankulathur

ABSTRACT

Because blockchain technology is decentralized and pseudonymous, crypto currency fraud has grown in importance inside the digital financial ecosystem. Phishing assaults, Ponzi schemes, rug pulls, pump-and-dump scams, and exchange hacks are just a few of the tactics used by scammers to defraud investors and steal money. Illicit acts are made easier by the irreversible nature of bitcoin transactions and the absence of thorough governmental control. The most prevalent types of crypto currency fraud are examined in this essay, along with the strategies employed by cybercriminals and the effects they have on investors and financial markets. It also looks at new technology, security frameworks, and current regulations that are intended to lessen fraudulent activity. Fostering a safer and more transparent bitcoin environment requires an understanding of these dangers and the application of proactive security measures.

Keywords: Crypto currency fraud, blockchain security, Ponzi schemes, phishing attacks, rug pulls, pump-and-dump scams, exchange hacks, regulatory oversight, financial crime, digital assets, fraud prevention.

INTRODUCTION

Cryptocurrency's decentralized, international, and safe transactions have completely changed the financial scene. Alongside its quick uptake, bitcoin fraud has become a serious problem that puts investors, exchanges, and financial institutions at serious danger. Due to blockchain transactions' pseudonymous nature and decentralized management, fraudsters now have more ways to take advantage of unwary consumers through a variety of fraudulent schemes.

Phishing attacks, Ponzi schemes, rug pulls, pump-and-dump scams, and exchange hacks are examples of common crypto currency fraud. These scams frequently cause investors to lose money and erode confidence in the ecosystem of digital assets. Additionally, it is challenging to successfully hunt down and prosecute fraudsters in the absence of adequate regulatory frameworks.

Examining the different forms of crypto currency fraud, their effects on investors and financial markets, and the effectiveness of current security protocols and legislative initiatives to stop fraudulent activity are the objectives of this research. Stakeholders may strive toward a more safe and open digital financial environment by being aware of the dangers of crypto currency fraud and putting strong preventive measures in place.

COMMON CRYPTO CURRENCY SCAMS

Crypto currency has transformed the global financial landscape, offering decentralized, fast, and borderless transactions. However, alongside its rise in popularity, various scams have emerged, exploiting the anonymity, lack of regulation, and irreversible nature of blockchain transactions. Scammers use different fraudulent schemes to deceive investors, steal funds, and manipulate markets. Here are the list scams using crypto currency .[1]

Phishing Scam

Phishing scams are one of the most prevalent threats in the crypto currency space, targeting users by tricking them into revealing their private keys, wallet credentials, or login details.

[1]Casey Murphy, *Cryptocurrency scams:how to spot,report,and avoid them,*INVESTOPEDIA (last visited 12/02/2025 5.45pm)
https://www.investopedia.com/articles/forex/042315/beware-these-five-bitcoin-scams.asp

These scams take advantage of the decentralized and irreversible nature of blockchain transactions, making it nearly impossible for victims to recover their stolen funds. Fraudsters use various phishing techniques, including fake websites, email scams, social media impersonation, and malicious software, to deceive unsuspecting users.

One common method of phishing in crypto currency is website spoofing, where attackers create fake websites that closely resemble legitimate exchanges or wallet services. Users who unknowingly enter their credentials on these sites provide scammers with direct access to their funds. Similarly, email phishing involves fraudsters sending deceptive emails posing as trusted crypto currency platforms, urging users to verify accounts or reset passwords through malicious links that lead to fake login pages. Another widespread tactic is social media impersonation, where scammers create fake profiles of well-known crypto influencers, projects, or companies to promote fraudulent giveaways. Victims are often tricked into sending crypto currency with the false promise of receiving a larger amount in return.

Ponzi and Pyramid Schemes

Ponzi and pyramid schemes have infiltrated the crypto currency market, exploiting investors' desire for high returns. These fraudulent investment schemes promise guaranteed profits but rely on funds from new investors to pay earlier participants, rather than generating actual revenue. Eventually, when recruitment slows down, the scheme collapses, leaving most investors with significant losses. The decentralized and anonymous nature of crypto currency transactions makes it easier for scammers to operate these schemes while avoiding detection and legal consequences.

A **Ponzi scheme** in crypto currency typically involves a fraudulent investment platform that guarantees high, risk-free returns. Scammers attract investors by claiming to use advanced trading algorithms, arbitrage strategies, or mining operations to generate profits. However, instead of making legitimate investments, they use funds from new investors to pay earlier participants, creating the illusion of a profitable venture. Over time, as recruitment slows or the scammer disappears, the scheme collapses, causing major financial losses for late-stage investors. Examples of crypto Ponzi schemes include BitConnect and PlusToken, both of which defrauded investors out of billions of dollars before being exposed.

A **pyramid scheme**, on the other hand, focuses on recruitment rather than investment returns. Participants are required to recruit new members and invest money to move up the pyramid structure. Each new investor's funds are distributed to those at higher levels, creating the illusion of earnings. Unlike Ponzi schemes, which rely on a central operator, pyramid schemes require continuous recruitment to sustain payouts. However, once recruitment slows, the structure collapses, leaving most participants at the bottom with heavy losses. Many crypto currency pyramid schemes disguise themselves as multi-level marketing (MLM) programs, promoting new tokens or mining programs while requiring members to bring in more investors to earn rewards.

Rug Pulls

Rug pulls are a deceptive form of exit scam in the cryptocurrency market, where developers create and promote a new digital asset or decentralized finance (DeFi) project, attract significant investment, and then suddenly withdraw all liquidity, leaving investors with worthless tokens. This type of fraud is particularly common in decentralized exchanges (DEXs), where tokens can be launched without stringent regulatory oversight. Rug pulls typically occur in newly created projects that promise high returns, innovative technology, or revolutionary financial solutions but lack transparency and accountability.

There are two main types of rug pulls **hard rug pulls** and **soft rug pulls**. A hard rug pull involves malicious developers embedding hidden loopholes in the project's smart contract, allowing them to steal investor funds once a certain amount of liquidity is reached. This often happens in projects where developers retain excessive control over token contracts, enabling them to mint unlimited tokens or disable users from selling. In contrast, a soft rug pull occurs when developers abandon a project after accumulating significant investor funds, without necessarily using malicious code. This can happen when a project's team overhypes their token, raises capital, and then disappears, leaving investors stranded.[2]

Pump-and-Dump Schemes

Pump-and-dump schemes are a form of market manipulation in the crypto currency space

[2]Allie grace garnett, *cryptocurrency scams:8crypto cons to avoid*,BRITANNICA MONEY, (last visited 12/02/2025 6.30pm)
https://www.britannica.com/money/cryptocurrency-scams

where fraudsters artificially inflate the price of a digital asset through misleading information, only to sell off their holdings once the price peaks, leaving unsuspecting investors with losses. These schemes often target low-liquidity or newly launched crypto currencies, where prices can be easily manipulated with coordinated buying activity. Organized groups, sometimes known as "pump groups," use social media platforms, private chat groups, and online forums to generate hype and attract retail investors, creating a fear of missing out (FOMO). As more people rush to buy the asset, its price skyrockets, at which point the orchestrators sell their holdings, causing the price to crash and leaving late investors with devalued tokens.

Pump-and-dump schemes typically unfold in several stages. First, scammers secretly accumulate a large amount of a low-value crypto currency before publicly promoting it through misleading claims, fake endorsements, or exaggerated predictions. Next, as retail investors buy in, the price rises rapidly, and scammers capitalize on the surge by dumping their holdings at a high price. Once they sell off their tokens, the artificial demand disappears, leading to a sharp price decline and significant losses for those who bought at the peak. Unlike traditional stock markets, where pump-and-dump schemes are illegal and monitored by regulators, the cryptocurrency market remains largely unregulated, making it easier for bad actors to execute these scams without legal consequences.

Exchange and Wallet Hacks

Crypto currency exchange and wallet hacks are among the most significant security threats in the digital asset space, resulting in millions of dollars in losses for investors and institutions. Unlike traditional financial systems, where transactions can be reversed or insured, stolen crypto currencies are often impossible to recover due to the decentralized and irreversible nature of blockchain technology. Hackers target exchanges and wallets by exploiting security vulnerabilities, weak authentication systems, or insider threats to gain unauthorized access to user funds. These attacks not only lead to financial losses but also undermine trust in the crypto currency ecosystem.

Crypto currency **exchange hacks** typically involve cybercriminals breaching an exchange's security systems to steal funds stored in hot wallets, which are always connected to the internet for liquidity purposes. Some of the most infamous exchange hacks include the Mt. Gox hack in 2014, where approximately 850,000 Bitcoin were stolen, and the Coincheck hack in 2018,

which resulted in over $530 million in losses. In many cases, exchanges that suffer large-scale breaches struggle to compensate users, leading to lawsuits and business closures. **Wallet hacks**, on the other hand, target individual users by exploiting weak passwords, phishing attacks, or malware infections. Scammers often use malicious software or social engineering tactics to trick users into revealing their private keys or seed phrases, granting full access to their wallets.

Money Laundering and Dark Web Transactions

Money laundering through crypto currency often follows a three-step process**: placement, layering, and integration**. In the placement stage, criminals convert illicit cash into crypto currency through peer-to-peer (P2P) platforms, unregulated exchanges, or by purchasing crypto with prepaid cards. The layering stage involves obfuscating the transaction trail using methods like **crypto tumblers (mixers), privacy coins (e.g., Monero and Zcash), or multiple wallet transfers** to break the link between the original funds and their final destination. Finally, in the integration stage, the laundered crypto currency is converted back into fiat currency through legitimate exchanges, online purchases, or real-world investments, making the illicit funds appear legitimate.[3]

The **dark web** further facilitates illegal crypto currency transactions by providing a marketplace for illicit goods and services, including drugs, weapons, stolen data, and hacking tools. Marketplaces like the now-defunct Silk Road and AlphaBay allowed users to conduct anonymous transactions using Bitcoin and other crypto currencies, making it difficult for authorities to trace criminal activities. Despite ongoing law enforcement crackdowns, new dark web marketplaces continue to emerge, utilizing enhanced privacy tools to evade detection.

Regulatory Challenges

Crypto currency fraud has become a growing concern for regulators and law enforcement agencies worldwide due to the decentralized, pseudonymous, and borderless nature of digital assets. While traditional financial systems have well-established legal frameworks to combat fraud, crypto currencies operate in a relatively unregulated space, making it challenging to enforce laws, track illicit transactions, and protect investors. The lack of uniform global

[3] what to know about cryptocurrency and scams(last visited 12/02/2025 7.30pm) https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.com

regulations and the rapid emergence of new crypto-related technologies further complicate efforts to prevent fraud and prosecute offenders.[4]

1. Jurisdictional ambiguity

Since crypto currency transactions occur on decentralized networks without central authorities, determining which country has legal authority over fraudulent activities can be difficult. Criminals exploit this loophole by operating in jurisdictions with weak or nonexistent crypto currency regulations, making it harder for authorities to take action.

2. Anonymity of crypto transactions

It presents enforcement challenges, as fraudsters use privacy coins, mixers, and decentralized exchanges to launder stolen funds, making it difficult to trace their identities.

3. Lack of investors protections Laws

Many fraudulent schemes, such as Ponzi schemes, rug pulls, and pump-and-dump schemes, exploit regulatory gaps, leaving victims with little legal recourse. Unlike traditional banking systems, where fraud victims may be reimbursed, crypto currency transactions are irreversible, meaning once funds are stolen, they are nearly impossible to recover. Regulators struggle to implement effective consumer protection measures without stifling innovation in the blockchain industry.

4. Cross border enforcement

Moreover, **the absence of standardized fraud prevention regulations** across countries leads to inconsistencies in enforcement. While some nations, like the United States and the European Union, have introduced stricter anti-money laundering (AML) and know-your-customer (KYC) requirements for crypto exchanges, others have minimal oversight, allowing fraudulent activities to thrive. Cybercriminals take advantage of these discrepancies, using unregulated platforms to move illicit funds across borders.

[4] Crypto and digital assets : regulatory challenges(last visited 12/02/2025 8.10pm) https://kpmg.com/us/en/articles/2022/ten-key-regulatory-challenges-2022-crypto-digital-assets.html

To address these challenges, governments and regulatory bodies are working to develop clearer frameworks for crypto currency fraud prevention. The implementation of global AML standards, mandatory KYC compliance, and enhanced blockchain forensic tools are key steps in reducing crypto-related fraud. However, as the industry continues to evolve, regulators must strike a balance between fostering innovation and ensuring a secure financial ecosystem. Collaborative efforts between governments, crypto businesses, and blockchain experts will be essential in mitigating fraud while maintaining the benefits of decentralized digital assets.

LEGAL IMPLICATIONS IN INDIA

In India, crypto currency is governed indirectly through various laws, as there is no specific legislation dedicated solely to digital assets. Some key acts that have legal implications for crypto currency include:

1. Prevention of Money Laundering Act (PMLA), 2002

In March 2023, the government brought cryptocurrency transactions under PMLA, making crypto exchanges, wallets, and intermediaries subject to anti-money laundering (AML) regulations. Crypto businesses must now follow Know Your Customer (KYC) norms and report suspicious transactions to the Financial Intelligence Unit-India (FIU-IND).[5]

2. Income Tax Act, 1961

The Finance Act, 2022 introduced a 30% tax on income from cryptocurrency transactions and a 1% Tax Deducted at Source (TDS) on transactions above a specified limit.Losses from crypto cannot be set off against other income.

3. Foreign Exchange Management Act (FEMA), 1999

FEMA regulates foreign exchange transactions, and cryptocurrencies, being cross-border in nature, may come under its purview. The government has not yet clarified whether crypto assets are considered foreign exchange, securities, or commodities, leading to legal uncertainty in international transactions.

[5] cryptocurrency in india : legality, AML regulations , and taxation (2024) (last visited 12/02/2025 9.00pm) https://sumsub.com/blog/cryptocurrency-in-india/

4. Information Technology Act (IT Act), 2000

While the IT Act governs electronic transactions and cyber security, it does not explicitly cover cryptocurrencies. However, crypto currency exchanges and wallets must comply with data protection, cyber security, and electronic contracts under this law.

5. Companies Act, 2013

Crypto currency-related businesses registered in India must comply with the Companies Act, ensuring transparency in financial reporting and governance. Non-compliance with financial disclosures related to crypto holdings could lead to penalties.

6. Consumer Protection Act, 2019

Since there is no specific regulation for investor protection, crypto-related frauds may be addressed under the Consumer Protection Act, which deals with unfair trade practices and disputes.

7. The Banning of Unregulated Deposit Schemes Act, 2019

This act prohibits unregulated deposit schemes and Ponzi schemes. If any cryptocurrency project or exchange operates as an unregulated deposit scheme, it may face legal action under this law.

Upcoming Legislation: Cryptocurrency and Regulation of Official Digital Currency Bill

The Indian government has proposed a bill that could either regulate or ban private crypto currencies while promoting the Digital Rupee (CBDC) issued by the Reserve Bank of India (RBI).The bill has not yet been introduced in Parliament, leaving the legal status of crypto currency in limbo.

CASE STUDIES

The **IAMAI vs. RBI (2020 SCC online SC 275)**[6]

This case was a landmark judgment in India's crypto currency landscape. In April 2018, the

[6] IAMAI V.RBI (2020 SCC online SC 275)

Reserve Bank of India (RBI) issued a circular prohibiting banks from providing services to crypto currency businesses, severely impacting crypto exchanges and traders. The **Internet and Mobile Association of India (IAMAI)** challenged this ban in the **Supreme Court,** arguing that the RBI had no legal authority to impose such restrictions, as crypto currencies were not classified as legal tender. IAMAI also contended that the ban violated **Article 19(1)(g) of the Indian Constitution,** which guarantees the right to trade and business. The RBI defended its decision, citing risks to financial stability, consumer protection, and potential misuse for illegal activities. On **March 4, 2020,** the **Supreme Court ruled in favor of IAMAI,** striking down the banking ban as **disproportionate and unconstitutional**, stating that the RBI failed to provide sufficient evidence to justify its decision. The judgment **revived crypto currency businesses** in India by restoring their access to banking services. However, while the ruling prevented an outright ban, crypto currency remained **unregulated,** leading the government to later introduce **strict taxation laws** in 2022 and bring crypto transactions under the **Prevention of Money Laundering Act (PMLA) in 2023.** The government is still considering a formal **Crypto currency and Regulation of Official Digital Currency Bill,** which could further shape India's crypto landscape. The case remains a significant milestone in balancing financial regulation and digital innovation in India.

CONCLUSION

The rise of cryptocurrency fraud in India highlights significant legal challenges due to regulatory uncertainty, enforcement difficulties, and jurisdictional conflicts. While efforts have been made to regulate digital assets, the lack of a dedicated legal framework complicates the prosecution of fraud cases. Issues such as the anonymity of transactions, cross-border crimes, and the absence of clear consumer protection laws make it challenging for authorities to curb illicit activities.

Despite existing laws like the Prevention of Money Laundering Act (PMLA**)** being applied to crypto-related crimes, they remain insufficient in addressing the unique complexities of digital currencies. Without stronger regulations, increased awareness, and better enforcement mechanisms, cryptocurrency fraud will continue to exploit legal loopholes, posing risks to investors and the financial system. To mitigate these risks, India must establish comprehensive crypto laws, enhance inter-agency coordination, and adopt advanced technological solutions for monitoring and tracking fraudulent transactions.

REFERENCE :

1. Casey Murphy, *Cryptocurrency scams: how to spot, report, and avoid them,* INVESTOPEDIA (last visited 12/02/2025 5.45 pm) https://www.investopedia.com/articles/forex/042315/beware-these-five-bitcoin-scams.asp

2. Allie grace garnett, *cryptocurrency scams:8crypto cons to avoid*, BRITANNICA MONEY (last visited 12/02/2025 6.30 pm), https://www.britannica.com/money/cryptocurrency-scams

3. what to know about cryptocurrency and scams (last visited 12/02/2025 7.30pm) https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.com

4. Crypto and digital assets: regulatory challenges(last visited 12/02/2025 8.10pm) https://kpmg.com/us/en/articles/2022/ten-key-regulatory-challenges-2022-crypto-digital-assets.html

5. Cryptocurrency in India legality, AML regulations, and taxation (2024) (last visited 12/02/2025 9.00 pm) https://sumsub.com/blog/cryptocurrency-in-india/