RESEARCH ARTICLE OPEN ACCESS

Cryptocurrency Fraud:Challenges and Countermeasures in Fintechs

Anirudh Mustyala
Software Engineering, Plano - Texas
Email: anirudhmusthyala@gmail.com

----------**********----------

Abstract

Fintech companies in the crypto industry play a fundamental role by providing an alternative financial system and creating new investment opportunities for crypto enthusiasts. However, as these businesses grow and expand their services, they become more vulnerable to cryptocurrency frauds such as theft of cryptocurrencies in user accounts, Ponzi schemes, financial crimes, and pump-and-dump schemes. These frauds are enabled by the anonymity of cryptocurrency transactions, portability of cryptocurrencies, high transaction speed of cryptocurrencies, and the fact that cryptocurrencies are not backed by any government. This document discusses cryptocurrency fraud and strategies fintechs exploit to combat the problem.

Keywords: Crypto,Fintech,Data,financial crimes.

----------**********----------

I. INTRODUCTION

Since the advent of blockchain in the early 2000s, cryptocurrencies and their related applications have been among the most discussed technologies in the finance and technology sectors. Despite setbacks such as frequent market meltdowns and growing cybersecurity concerns, the crypto industry has continued to register massive growth in terms of customer base and overall market growth. Even though cryptocurrencies provide unique opportunities for digital investors and tech-savvies, this technology is susceptible to misuse by fraudsters. The penetration of cryptocurrencies in user communities has been characterized by the growing number of scammers who use digital currencies to scam people or execute illegal transactions. This piece of writing discusses cryptocurrency fraud and strategies fintechs can leverage to address the depravity.

II. BODY

Cryptocurrency Fraud

According to the US Federal Trade Commission (2022), cryptocurrency fraud is a form of scamming that leverages cryptocurrencies to steal money from unsuspecting people. Typically, cryptocurrency fraud involves scammers soliciting payments for undelivered services or promises via cryptocurrencies, scammers masquerading as cryptocurrency traders, and fraudsters accessing users' crypto wallets and transferring digital tokens from the wallets. Besides typical crypto fraud, advanced crypto frauds leverage scamming techniques such as pump-and-dump schemes and development of fake cryptocurrencies. According to a Vermont Department of Financial Regulation (2023), cryptocurrency fraud has increased by 900 percent since 2020 and is expected to continue growing with the increasing cryptocurrency use. Some of the common cryptocurrency frauds include;

Traditional theft

Even though crypto is an emerging industry, it can be used by typical thieves, such as hackers, to steal users' investments. Millions of crypto investors across the globe have lost their crypto investments to crypto hackers. According to the DeFi report (2023), in the second quarter of 2023 alone, the crypto sector lost $204.3 million to hackers. In the first quarter, the loss was double this figure, $462.3 million.

Ponzi schemes

Regulations around cryptocurrencies are still in their infancy. This allows fraudsters to launch crypto-based Ponzi schemes where new members are compelled to pay artificial returns to early adopters. Lack of proper crypto knowledge among people plays a significant role in the proliferation of Ponzi schemes in the crypto sector.

Financial crimes

Perpetrators of financial crimes such as tax evasion, money laundering, and bribery have found a haven in cryptocurrencies. Because of the nature of cryptocurrencies and how they operate, fraudsters have found digital currencies to provide an ideal environment for committing financial crimes. Today, many people with unexplained wealth describe themselves as crypto investors.

Pump and dump schemes

Pump and dump schemes are arrangements where investors in cryptocurrencies artificially raise the value of the target cryptocurrency, sell their investments, and leave the cryptocurrency to plummet. These schemes involve investors with huge shares hoarding the supply of the coin and hyping the currency to artificially raise its value and attract demand. With increased demand and value, they sell their share and dumb the coin.

In a nutshell, cryptocurrency fraud constitutes different types of fraud that involve the use of cryptocurrencies. They comprise scams executed via cryptocurrency payments and cryptocurrency exchanges,

crypto wallets takeover by hackers, and financial crimes that involve the concealment of transactions using cryptocurrencies.

Challenges Addressing Cryptocurrency Fraud

As aforementioned, fraudsters have found cryptocurrencies ideal for their operations due to the nature of cryptosystems and their mode of operations. Although various mechanisms have been put in place to regulate the use of cryptocurrencies, the spread of illegal activities in the crypto sector is still high. Some of the factors that motivate fraud via cryptocurrencies include;

Anonymity: One of the defining features of cryptocurrencies is the anonymity of transactions. Typically, crypto platforms do not collect identification information from their customers. Crypto transactions involve wallet addresses only. Even transacting parties have no means to know each other. The only information attached to wallet addresses is the list of assets and associated transactions. Anonymity allows online criminals to receive payments without their covers being blown (Bele, 2021).

Instant transactions: Cryptocurrency transactions are executed in a peer-to-peer environment. This implies there are no intermediaries to monitor transactions. Besides, unlike fiat-based systems where transactions are processed slowly, crypto transactions are instant. A person in Norway can send cryptocurrencies to a person in Australia in a matter of seconds. The lack of intermediaries and fast transaction speed make cryptocurrencies ideal for online criminals.

International reach: Cryptocurrencies are universal. Their usage is not limited by international boundaries. The pertinence of cryptocurrencies in any country makes them perfect for international transfers. While the universal usability of digital currencies is meant to ease money transfers for legal

purposes, fraudsters are leveraging the quality for selfish reasons.

No government backing: Cryptocurrencies are not backed by any government. This implies the functioning and regulation of cryptocurrencies are not pegged to any state. Consequently, no government can be held responsible for the negative implications of cryptocurrencies.

Mitigating cryptocurrency fraud

Even though cryptocurrency fraud is incessantly growing and fraudsters seem to be a step ahead of fintechs, it is the role of fintech companies to install the necessary mechanisms to manage the menace. The good news is that most fintech firms are already taking steps to protect their customers from crypto scams. While these measures have not completely eroded the risk, they are at least showing signs of combating the problem. Some of the promising strategies fintechs are leveraging to address cryptocurrency scams include;

Know Your Customer (KYC) and Anti-money Laundering (AML) compliance

To help fintechs prevent fraud, governments across the globe have ratified KYC and AML laws. These laws mandate fintech companies to verify the identity of their customers before allowing them to use their systems (Campbell, 2018). They also compel fintechs to set transaction limits for customers. KYC regulations are meant to regulate the anonymity of crypto transactions. AML compliance is meant to address the use of cryptocurrencies for financial crimes.

Use of blockchain technology

One of the strategies cryptocurrency scammers use is tampering with fintech systems by deleting or modifying data. Fintechs can make their systems tamper-proof by building them on top of blockchain technology. Blockchain is a distributed ledger system that stores data in blocks on nodes (Pierro, 2017). For data to be modified, all the nodes must be in consensus. Besides, because data is stored in distributed nodes, it

is practically impossible for attackers to access and modify all the nodes. It is important to note that blockchain holds a permanent record of all transactions. Even when frauds manage to scam innocent crypto users, the transactions can be traced and reversed. Blockchain technology can also verify user identities, preventing identity theft.

Advanced authentication and verification system

User authentication and verification are some of the traditional mechanisms for protecting systems. To protect user accounts, fintech companies can use effective authentication and verification methods to keep unauthorized access at bay. Instead of using regular authentication factors, fintechs can leverage ultramodern secure factors such as biometrics. Authentication and verification systems can be further fortified by using multifactor authentication. For example, biometrics can be combined with a one-time PIN (OTP) sent to users via SMS or email.

Use of analytics in security

Artificial intelligence and machine learning technologies can be deployed in fintech systems to detect suspicious user account activities and stop them in real-time. Using data analytics, these technologies can learn about each customer account's behavior and detect frauds such as unwarranted crypto payments and account takeovers. Besides the ability to learn about customer accounts, these technologies can automate security processes, guaranteeing 24/7 monitoring of systems (Wirkuttis & Klein, 2017).

User awareness initiatives

Although technology plays an integral role in ensuring the security of IT systems, safety starts with the users of the platforms. Systems with high-end cybersecurity technologies are more likely to suffer frequent breaches if the users are not well-versed in the threats confronting them. Fintech firms can bolster the efficacy of their cybersecurity systems by educating users on cryptocurrency fraud.

This information can be disseminated together with ways of spotting cryptocurrency frauds and how to avoid them.

III. CONCLUSION

Fintech companies in the crypto industry play a fundamental role by providing an alternative financial system and creating new investment opportunities for crypto enthusiasts. However, as these businesses grow and expand their services, they become more vulnerable to cryptocurrency frauds such as theft of cryptocurrencies in user accounts, Ponzi schemes, financial crimes, and pump-and-dump schemes. These frauds are enabled by the anonymity of cryptocurrency transactions, portability of cryptocurrencies, high transaction speed of cryptocurrencies, and the fact that cryptocurrencies are not backed by any government. Fintech firms can combat the rising crypto frauds by adopting KYC and AML policies, employing analytics in security, leveraging blockchain technology, protecting user accounts with modern multifactor authentication, and keeping users aware of the cryptocurrency fraud threat. Fintech companies that employ these strategies are more likely to subdue cryptocurrency fraud.

REFERENCES

Bele, J. L. (2021). Cryptocurrencies as facilitators of cybercrime. In *SHS Web of Conferences* (Vol. 111, p. 01005). EDP Sciences.

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change*, *69*, 283-305.

Di Pierro, M. (2017). What is the blockchain?. *Computing in Science & Engineering*, *19*(5), 92-95.

Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. *Cyber, Intelligence, and Security*, *1*(1), 103-119.

Federal Trade Commission (2022), What To Know About Cryptocurrency and Scams. Retrieved From: https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams#scams

State of Vermont Department of Financial Regulation (2023), Investor Alert | NPR Report on Crypto Fraud Illustrates Need for Caution. Retrieved From: https://dfr.vermont.gov/consumer-alert/investor-alert-npr-report-crypto-fraud-illustrates-need-caution#:~:text=The%20promise%20of%20high%20returns,the%20start%20of%20the%20Pandemic.

DeFi (2023), De.Fi Rekt Report: Over $204m Lost in Q2 2023. Retrieved From: https://de.fi/blog/de-fi-rekt-report-over-204m-lost-in-q2-2023