International Journal of Innovative Science and Modern Engineering (IJISME)
ISSN: 2319-6386 (Online), Volume-11 Issue-6, June 2023

A Review: Fraud Prospects in Cryptocurrency Investment

Janki Velani, Suchita Patel

Abstract: ***cryptocurrency is a digital or virtual currency that uses ryptography for security and operates independently of a entral bank. Its decentralized nature allows for secure and transparent transactions, making it an appealing alternative to traditional fiat currencies. Cryptocurrencies uses block chain technology, which is a distributed ledger that records all transactions on a network of computers. Bit coin was the first cryptocurrency to gain widespread attention, but today there are thousands of different crypto currencies with varying degrees of popularity and acceptance. Despite their potential benefits, cryptocurrencies are subject to volatility, regulatory uncertainty, and security risks, which have led to debates about their future role in the global economy. In this paper we are going to discuss different fraud prospects in cryptocurrency investment faces by users. Here we are listed possible scams happened in past and possibilities in future with cryptocurrency fund. Even we tried to discuss recent available detection & prevention methods for such scams. With the help of our future research perspective we are planning to provide technique to prevent such different scams and saving our valuable money.***

Keywords: Cryptocurrency, Fraud, Detection & Prevention

I. INTRODUCTION

Cryptocurrency or crypto is type of currency which in the digitally or form. We can do crypto transaction from anywhere in the world.it is entirely digital so, online database have the transaction data. So, when we have a transaction, it's been recording a public ledger. Basically, it uses encryption for verify the transition then it called the crypto currency. For the encryption there are advance coding done behind the system which provide the security. Cryptocurrency using block chain technology. Block Chain is a decentralized ledger of all transactions. Via this technology investor can do transaction without any authority.

A. How Block Chain Works - A Step by Step

As per diagram shown in Fig.1we can understand step by step process of Block chain working process.

1. User sends request for transaction and Authentication.
2. A block representing a transaction is created.
3. The block is broadcasting to all the nodes of network.
4. The block sent to every node of the network and validate all the transaction.
5. Node receives the cryptocurrency.
6. The block is added to the chain.
7. The transaction gets verified and executed.

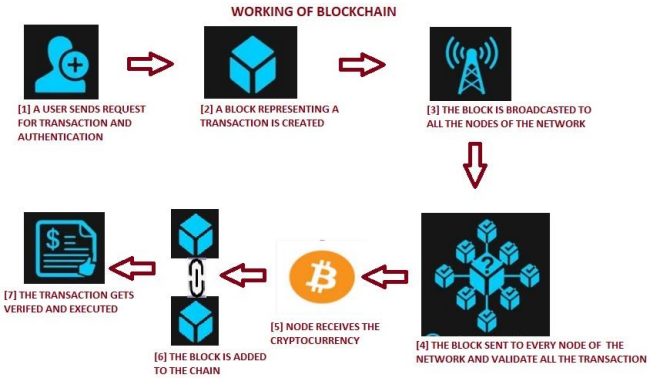

Fig. 1 Blockchain diagram

Further than it's very risky. After the transaction there Crypto is going to store your digital wallet. If you lost your wallet data for the access, you could lose your all investment in the cryptocurrency.

II. TYPES OF SCAMS

Table. 1 List of Possible Scams

LIST OF POSSIBLE SCAMS WITH CRYPTOCURRENCY
▪ INVESTMENT SCAM
▪ RUG PULL SCAM
▪ ROMANCE SCAM
▪ PHISHING SCAM
▪ MAN IN THE MIDDLE SCAM
▪ GIVEAWAY SCAM
▪ EMPLOYMENT OFFERS SCAM
▪ FRAUDULENT ICOS
▪ SHADY EXCHANGES
▪ FAKE WALLETS
▪ PYRAMID OR PONZI SCHEMES
▪ PUMP AND DUMP SCAM
▪ PUMP & DUMP GROUPS
▪ FAKE TRANSACTION SCAM

A.Investment Scam

This type's scam usually happens at social media and dating apps. Scammer tries to convince the victim to invest in the crypto [1]. They claim to be investment manager or a fake celebrity etc.

Manuscript received on 11 May 2023 | Revised Manuscript received on 30 May 2023 | Manuscript Accepted on 15 June 2023 | Manuscript published on 30 June 2023.
*Correspondence Author(s)
Janki Velani, Student, M.Sc. (IT), ISTAR College, CVM University, V.V. Nagar. E-mail: jankivelani3@gmail.com
Dr. Suchita Patel*, Assistant Professor, Department of Computer Science, ISTAR College, CVM University, V.V. Nagar. E-mail: suchitapatelit@istar.edu.in, ORCID ID: 0000-0002-8034-5839

and also give the guarantee for the huge gain of the investment. Fake managers claim to have made millions investing in cryptocurrency and promise their victims that they will make money with investments. They promise to make high profit to your investment if you transfer your cryptocurrency to them [2]. And after you trusted them and transfer your money to them. They never go to give returns. so, you got the scam.

B. Rug Pull Scam

In such scams acts as Scammers who wants to do investment, nonfungible token (NFT) means buy coins to get money or funding. Once they get funding, they disappear with those money amount. A squid coin scam was very popular after Netflix series. In these games investors play games to earn crypto currency. They buy tokens for online games and exchange crypto currencies later. In such scams trading stopped then the money amount will become hidden. Here, token value reached to zero amounts or funding, when the persons attempted many times but failed to sell their all tokens. These scams also common for NFTs which are one type of digital assets.

C. Romance Scam

These scams also known as Dating scams. In such scams people finds dating person via online Dating apps. Involves long time to create trust between two party to convince and buy cryptocurrency. After getting fund or full amount, the party who are showing interest to date with another one will became sudden disappear and braking relationship. Also known as pig butchering scams.

D. Phishing Scam

Scammers send emails with links to a fake website to fetch the personal details like crypto account and wallet access details. Basically, every crypto wallet has the unique crypto key which allows wallet access. Scammer has the focus on it. Always go directly to the site secure site for the transaction of the crypto currency. Phishing scammers [4] often attract you into click on a link to website, where they can then steal your account details. They send an email to holders to a specially created website asking them to enter private key information. Once the hackers have acquired this information, they steal the crypto currency in those wallets.

E. Man In The Middle Scam

In this type of scammers steals user's private or sensitive information of cryptocurrency account details. When user shares such private details such as passwords, wallet keys and account details with public network, scammers steals those information via man-in-the-middle attack. As per experience if we need to prevent such scammers than we should block man-in-the-middle by using VPN, so malicious intruders cannot steal private details.

F. Giveaway Scam

Here, scammers give the lure of the victim to give the FREE crypto .and promise the sent them some amount of cryptocurrency. And some scammer also claims that if we give them some amount of the cryptocurrency after the short of the time, they will give us the more than amount which we give them. After the influence the scammer they cleverly get the information through us. And after they can access the whole fund of the wallet.

G. Employment Offers Scam

Here, IT freelancers seek online projects involves virtual currency and its exchange related works or jobs. Scammers will mimic as recruiters or job seekers to get accessibility of crypto accounts. Scams known as online hiring scams. Scammers give online jobs then hack into the systems to get funds which raise money for the DPRK.

These IT freelancers or workers always remain engaged with other IT related work and use their skills and expertise to gain access of currency accounts and enable DPRK's malicious attack.

H. Fraudulent Icos

Initial Coin Offering (ICOs) has yielded higher returns for investors who want to do startups for their companies or models. As compare to IPO, ICO is very young and risky. There are some lists of ICO categories such as Exit scam, URL scam, Bounty scam, White paper plagiarism scam, Exchange scam.

I. Shady Exchanges

Bitcoin, Ethereum, Ripple, Bitcoin cash, or Litecash are one or another heard about the most famous cryptocurrency exchanges which are not just unknown, but they are try to avoid publicity.

When a user connects their wallet to an online application and starts to do transaction, Hackers exploited a bridge between Ethereum and Blockchains and via warmhole attack redirected to a shady wallet.

In such type of scam, a user always redirected to a attacking website where seed phrase would be stolen and funds directly pass on to a shady wallet or account. There are multiple remote access or live stream techniques are followed for direct help.

J. Pyramid Or Ponzi Schemes

In such schemes most of scheme organizers often promise high returns with little or no risk. Instead, they use money from new investors to pay earlier investors and may steal some of the money for themselves. A Ponzi cryptocurrency app is now attracting in many bank customers and scamming them by gifted them high returns. Most of Ponzi schemes share common characteristics like High returns with little or no risk; unregistered investments; unlicensed sellers; those who are facing issues with paperwork; and facing difficulty receiving payments.

K. Pump And Dump Scam

Classic dump and pump are the cleverest technique to do the scam. Where the holder pretends the value of the crypto is going to high. After this all try to sell their holding. And scammer gets the crypto at the cheap price. And you lose your investment. Crypto holder claimed the hyped via fake email and social media posts like Twitter, Facebook, or the other social media platform.

Then some holder who saw that posts they try to sell their crypto. Cause of that they make a huge profit among the other holders. It's happened within a fraction of the minute.

L. Fake Transaction Scam

Scammer lures the crypto holder to give the good exchange or some extra crypto. But they try to scam them. Holders do not know its fake until after they lose their deposit. Cause of the block chain it is the hard to recover the funds. Fake crypto products return on investment and users are typically required to pay a high initial fee and then frequently asked to invest more and more. When you try to withdraw your funds, you'll likely find they've vanished. Stick to known crypto exchange markets such as Coin base, Crypto.com and Cash App. Scammer always try to scam you in new way so you should know that only scammer demand to send the crypto in advance or Scammer give the guaranteed profits and the high returns. Don't trust that people who try to convince you to make profit quick and easily. Don't try to merge your online dating app personal life with the crypto kind investment. Never give your personal account details to another person or the Unknown sites.

III. DETECTION AND PREVENTION METHODS

Here, some prevention method you should follow for protect your crypto investment: Current eras of AI and ML there are different tools [3] available to beat cybercriminals means detection and prevention methodologies that can boost detection rates and providing protection by automated systems.

A. Phishing Scram Solution

If we discuss about phishing scram involves have grabbed lots of money and adds highest level of insecurity as in financial level. To deal with such issues graph based cascade feature extraction method based on transaction records and a light GBM-based usual-sampling Ensemble algorithm to build the identification model.

One more solution Block chain Phishing Scam detection using Multi-Channel graph classification such as random walk or graph neural network (GNN). A multi-channel graph classification model (MCGC) with multiple feature extraction channels for GNN where The transaction pattern graphs and MCGC are more able to detect potential phishing scammers by extracting the transaction pattern features of the target users.

B. Fake Check Scam Solution

Fake check scam is very common and very costly damaged fraud for victims due to high amount of lose as well as being exposed to legal records. There is no any current solution to authenticate cheques and detect fraud instantly. Due to 24 hours waiting time to detect scam victim has to loss large amount of financial funds.

C. Read & Throughly Understand Team

If we want to avoid very serious issues related to ICO scams than gaining deeper knowledge regarding whitepaper is necessary. We need to generate timeline, SWOT analysis, building a model before project, checkpoints for goals, objectives, and strategies. To resolve such a serious problem, we propose a block chain-based scheme to authenticate checks and detect fake check scams. Moreover, in this approach allows the revocation of used checks. More precisely, such approach helps the banks to share information about provided checks and used ones, without exposing the banks' customers' personal data. We demonstrate a proof of concept of our proposed approach using Name coin and Hyper ledger block chain technologies.

D. Protect Your Wallet

You need a wallet with unique keys. If anybody asks about the key its high chance to get the scam. Keep your key is very secure. Make sure your wallet is developed by the reputable company. For the first time of transaction send some small transaction and you notice some malicious things then uninstall the app. Don't logging in the site with the public Wi-Fi. Like in real life our wallet should be secured. Bit coin such a great feature concerns or demands highest level of security. Below figure-2 represents our roles and responsibility to adopt and protect our money stored in the forms of cryptocurrency wallet.

Fig. 2 Good Practices to protect Cryptocurrency Wallet.

E. Take Your Time

Scammer makes you in the rush to sell them to your crypto currency. It gives you panic via the false news or the time limits in discount. If you are in this situation, please take time to understand what is happen with you.

F. Use Multi-Factor Authentication

If you use the multi-factor authentication [8] it prevents to fetch your login details or the wallet details throughout the hackers. Hacker will not be able to get your wallet details. Before they get into the wallet some code is going to share in your phones or the mails. Without the code they are not able to retrieve the data of your account or the wallet.

IV. RESULT AND DISCUSSION

Detection and Prevention is better than cure term indicates before money loss if we aware regarding all such fraud or scam possibilities or methodologies, we never be a victim. There are millions of dollars/financial loss due to scams happens every year. Also current 21st century era of Internet of Things as well as Artificial Intelligence tools always fruitful to provide awareness of how to deal with such big cryptocurrency fraud problems. There are many cryptocurrency fraud prevention methods available in market today such as Stay Vigilant, Secure your Wallet, Take a Step Back as well as Remain Sceptical But due to less awareness and lack of knowledge till date many financial scams happened. Also whenever customer starts to does currency transfer transaction via cryptocurrency wallet, trust factor matters lot so we are planning to proposing prevention and detection methodology based on transactions trust factor. [5,6,7]

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

V. CONCLUSION

In this digital era, we can conclude that crypto is good for investment and make future financial strong but if you don't get the write reference or write flow how to invest in it or sound knowledge of which websites are most preferable for the security purpose then you got the scam, and you lose all your money. In this paper we would like to share review knowledge for various possibility of cryptocurrency frauds and different ways to secure our financial assets and very basic practices to save and secure crypto wallet. However we are also proposing prevention and detection method [5,6,7] in our future research which was MANET security so people can get benefit and be safe own funds even before the investment check one more time what you are going to do. In short we can make our account or wallet plan journey safer and secure.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors have equal participation in this article

REFERENCES

1. Yukun liu, aleh tsyvinski, Risk and returns of cryptocurrency, national bureau economic research.
2. Ryan Farrell, An analysis of the crypto industry, Wharton research Scholars
3. Dr Garrick Hileman & Michel Rauchs, Global Cryptocurrency Benchmark study, 2017 [CrossRef]
4. Weili Chen1,2 , Xiongfeng Guo 1,3 , Zhiguang Chen 1,2 , Zibin Zheng 1,3 and Yutong Lu 1" Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem", International Joint Conference on Artificial Intelligence (IJCAI-20)
5. Suchita Patel, Priti Srinivas Sajja, Samrat Khanna, Enhancement of Security in AODV Routing Protocol Using Node Trust Path Trust Secure AODV (NTPTSAODV) for Mobile Adhoc Network (MANET), Information and Communication Technology for Intelligent Systems (ICTIS 2017) [CrossRef]
6. Dr. Samrat O. Khanna Suchita Patel, Black Hole Attack – VULNERABILITY to AODV Routing Protocol in MANET, Proceedings of National Seminar on Future Trends in Information Technology on 21st March, 2015
7. Suchita B Patel, Samratvivekanand O Khanna, 2-Tier Trust Based Model Forintrusion Detection System in Mobile Adhoc Network, International Journal of Research and Innovation in Applied Science (IJRIAS), 2016
8. Ankur Gupta, Dushyant Kaushik, Swati Gupta, "Integration of Biometric Security System to Improve the Protection of Digital Wallet" Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020 [CrossRef]

AUTHORS PROFILE

Ms. Janki Velani is a student of Master of Science in Information Technology department of ISTAR College, CVM University, V.V. Nagar, Anand, and Gujarat. Her research area of interest is Internet of Things, Network Security. jankivelani3@gmail.com

Dr. Suchita Patel has been working as an Assistant Professor in Computer Science department of ISTAR College, CVM University, V.V. Nagar, Anand Gujarat since year 2012. Her area of interest is Network Security, Cloud Computing, and Internet of Things, Mobile Application Development. She has published more than 17+ research paper publications in various national and international journals and conferences.