Cryptocurrency Frauds

Aryan Kasera

Abstract*: There are scams of millions of dollars happening on a daily basis in the world of cryptocurrency. Awareness and the latest 21st century technology- "Artificial Intelligence," may prove to be the key to fight this battle against Cryptocurrency scams. This research paper provides a comprehensive analysis discussing the various "Cryptocurrency scams" across the world, while giving case analysis of the biggest scams regarding the same, later exploring various solutions to this problem. This research paper, goes beyond the usual theft from hacking and ransomware attacks, and explores the in-depths of many of the frauds that have not been most commonly heard of. When we say 'Cryptocurrency frauds,' we directly associate with hacking and theft due to unauthorized access, but it goes more than that, and that is what this paper seeks to explore.

Keywords: Artificial Intelligence, Cryptocurrency, Frauds, Theft.

I. INTRODUCTION

Cryptocurrency, as unparalleled technology is invented every other day, is a financial innovation with the power to change the way finance is done. Since an anonymous Satoshi Nakamoto introduced the cryptocurrency in 2008, and primarily in the past few years, it has become an integral part of the financial and economic markets around the world; its success primarily owed to the 'decentralized' system it follows. The technology, has no stop to its exponentially growing popularity day-by-day, year-by year. While, it provides an innate benchmark for future investors to bank upon, there is no doubt that the technology brings to us, with all its benefits, high amounts of risks, and requires high amounts of security to curb the amount of cryptocurrency fraud happening in the world on a daily basis. While, one major factor that could help curb down the amount of cryptocurrency fraud, or with any cyber based fraud for that matter, is to help the users of the technology understand the potential risks involved and how exactly the technology functions. While, the cryptocurrency over the last few years has gained immense popularity, I think it is safe to say that many investors, or non-investors also, do not have a deep insightful knowledge as to what the underlying prevalent dangers are to the particular financial innovation. It is absolutely crucial to have a broadened understanding of a technology like the cryptocurrency while making investments in them. More often than not, investors don't know what hit them when they are duped of their long- hard earned only to discover later that they were victims of the highly affluential digital currency scam. We live in a time, as mentioned above, where every day we see new technology emerge into our lives.

We, as humans do undermine the chances of 'bad things' happening to us, and overestimate the probability of the least probable things (like winning the lottery), but the fact is that, there is a high prevalence of cyber-attacks in the world these days, and we should be aware of the potential threats and take several precautions to minimize the risks and exposures, while being 'on the net.' Well, this is the same for all the crypto-investors out there. Whilst, I am not saying that a person is very likely to get hacked and get all his/her cryptocurrency stolen away, or become a victim to a fraud, I am simply saying that caution and knowledge regarding these aspects, is a need of the hour. Whilst, Cryptocurrency scams are highly prevalent in the world, and while I do believe that an extensive knowledge about the sorts of scams happening and a knowledge about how to not fall into them is important, I also believe that, somewhere, the IT professionals in the world can also change the way cryptocurrency scams happen, by means of the state-of-the-art technology, "Artificial Intelligence," which has highly been proven helpful in many fields, and certain tools with the help of the technology can be built to curb the level of cryptocurrency scams. Cryptocurrencies, have succumbed to increasing amounts of frauds that result in investors losing millions of dollars every day. Ever since the inception of cryptocurrency, many people/investors have believed in the currency, as being the *'future,'* and a medium of investment that could, very well be the newest way of 'getting rich quick.' Many crypto-investors have indeed received large pay outs, especially with the rampant increase of the price of bitcoin in 2017-18 (with its peak coming in late 2017), and investors have also had substantial perks of having their capital invested in the decentralized exchange. However, there is a dark side to this extremely well-budding looking market. It is worth noting that cryptocurrencies, whilst being decentralized has its own benefits, it also has certain disadvantages. Cryptocurrencies, do not have the same legal protections as a normal debit or a credit card does. Once paid with cryptocurrency, you can only get it back if the sender sends it back.[1] Thus, it becomes imperative to know a seller's reputation, location and whom to contact if something goes wrong, before buying something using cryptocurrency. While, cryptocurrency transactions are anonymous, transactions maybe posted in a public ledger like the Blockchain, and the transaction amount and the wallet address could be used to identify the actual users of the currency. Studies have shown that many people are uneducated about the many potential dangers of cryptocurrencies. The number of people losing money on cryptocurrency markets, due to such frauds is constantly on rising, as the popularity of cryptocurrency increases. In 2018, a survey created by Bitcoin.com, stated that approximately $9 million are lost to cryptocurrency scams every day.[2] This figure continues to rise, as we move a couple of years ahead into 2020. A total of approximately $4 billion in scams was reported in 2019[3], while a total of $1.4

Revised Manuscript Received on July 28, 2020.

Aryan Kasera, Student, The Doon School, Dehradun, Uttarakhand, India.

1.
2.
3

billion in 2020 till date[4]. This is alarming! This just goes back to the fact that people need to be more educated about the cryptocurrency and about its scams, to better protect themselves from its trade-offs.

As we delve deeper into the research, we will come across the various ways in which cyber professionals attack these crypto-investors for monetary benefits.

II. WHAT IS CRYPTOCURRENCY

A. Definition

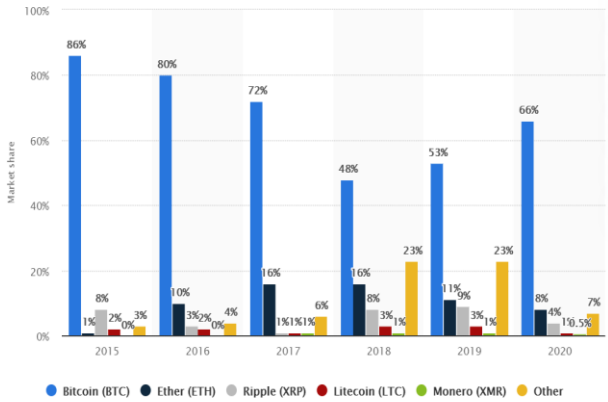
To understand the potential dangers limbering on this particular platform, I believe that it is imperative to first define what exactly a cryptocurrency is and understand the technology used behind its functioning.

Cryptocurrency, is a digital, virtual currency, which is secured using cryptography methods. In simple terms, a cryptocurrency is a digital asset designed to work as a medium of exchange, just like liquid cash, although, in a virtual/digital form.[5]. It is a 'decentralized' asset. [6]This aspect of being decentralized, allows the currency to exist outside the control of governments and central authorities, which is one of the main benefits that this asset possesses, and why it is becoming so increasingly popular amongst investors. The implemented technology in the cryptocurrency, ensures pseudo or full anonymity of the user transaction details.

B. Technology Used:

The blockchain, the main technology behind cryptocurrency, is where most records regarding the transactions in the cryptocurrency are stored. While going into more jargon, a blockchain is a distributed ledger (DLT), based on a peer to peer topology, that allows data to be stored globally on thousands of servers[7]…. While this may be exhausting, blockchain technology is maybe easier to understand in simple English. At the most basic level, the blockchain is literally a 'chain of blocks.' When I say a 'chain of blocks,' I am referring to a 'block'- which is the digital information, stored in a public database- the 'chain.'[8] That slightly simplifies it. The blockchain, being the cornerstone technology, to the existence of cryptocurrency, is used to keep an online transaction ledger of all the transactions that have ever taken place. The file is generally stored on multiple computers across a network, instead of being stored at one particular location, which allows the information to be and readable by anyone in the network. The blocks are linked using highly sophisticated cryptography tools, which involve complex mathematics and computer science. AN alteration in the blockchain is identifiable by the computers in the network as it disrupts the cryptographic links of data.[9] Maybe, investors feel secure knowing the excessive security of the blockchain. Yet, bad things happen. And there are scams across the globe regarding this virtual currency system.

That is the cryptocurrency in its most basic form. It is quite understandable as to why investors really find a crypto-investment to be a lucrative investment. An investment, as mentioned earlier, which portrays to be a quick and easy way of getting rich. Well, maybe it is, given the large benefits of the investment, although in a highly volatile market. After all, many people have become immensely wealthy by investing in the crypto market, due to its mega boom that it experienced in the past couple of years.

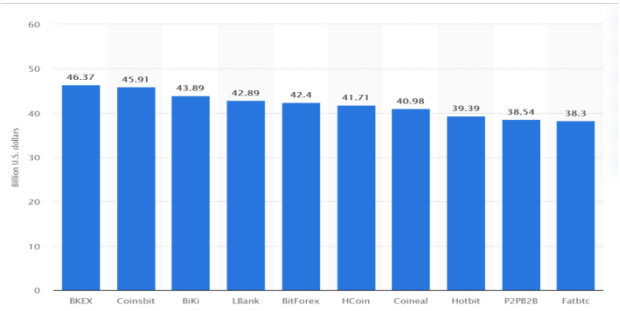


(Statista. 2020. Leading Cryptocurrencies By Market Cap 2020 | Statista.[online]Availableat:<https://www.statista.com/statistics/730782/cryptocurrencies-market-capitalization/>)

The figure provides an outlook as to the percentage of each cryptocurrency by its market capitalization from 2015-2020. The figure illustrates that the Bitcoin is the most popular cryptocurrency, while Ether being the second most by market capitalization.

C. Cryptocurrency Exchanges

It is important to have an explicit idea of how cryptocurrencies are traded, because more often than not, many frauds and scams, regarding cryptocurrencies, seem to happen at the most initial stages, during the trading of the cryptocurrency. Various scams, like the Ponzi scheme, are played out by traders of the cryptocurrency, although, more on that later, when I will be talking about all the cryptocurrency scams with a comprehensive case analysis for different types of scams, related to the same.



(Statista. 2020. Leading Cryptocurrency Exchanges By Volume 2020

Statista.[online]Availableat:<https://www.statista.com/statistics/864738/leading-cryptocurrency-exchanges-traders/#:~:text=This%20statistic%20presents%20the%20leading,the%20largest%20cryptocurrency%20exchange%20globally.>)

4
5
6
7.
8
9

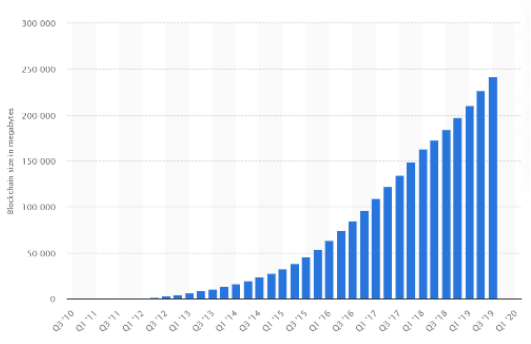
This statistic presents the leading cryptocurrency exchanges worldwide by 30-day volume as of January 2020. At that time, BKEX had a 30-day volume of 46.37 billion U.S. dollars, making it the largest cryptocurrency exchange globally.

While this may be a report from January 2020, a statistic from 2018, from Bloomberg news, shows quite different statistics, where other exchanges like Binance, Upbit, Bitfinex, Coinbase had the highest volume of trading done. Surprisingly, none of the top 10 exchanges of 2018, make it to the list of the top 10 exchanges in 2020.[10]

Take for example the case of the Mt. Gox, which was the largest cryptocurrency exchange platform back in 2014. In April, 2014, after suspending trading and closing its website, the exchange filed for bankruptcy. Any guesses as to why this happened.

It happened due to large thefts of bitcoins that were stolen straight out of Mt. Gox's hot wallet over time, beginning as early as in late 2011.

Cryptocurrencies are stored in digital wallets, which can be bought and sold via an exchange. The digital wallet of a particular user, acts as the medium of transaction between two parties. Although, the transaction is not final yet. The transaction is only final once it has gone through the process of mining- which allows 'tokens' to be created and the transaction is verified and added to the blockchain. Technically, it is traded like how stocks are traded in a stock exchange, apart from the fact being that this is virtual currency we are talking about, and a particular transaction has to go through significant technological processes while registering for a single transaction, which is linking the blocks in the chain.



(Statista. 2020. Bitcoin Blockchain Size 2010-2020 | Statista. [online]

Availableat:<https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/#:~:text=Bitcoin%20blockchain%20size%202010%2D2020%2C%20by%20quarter&text=The%20size%20of%20the%20Bitcoin,the%20end%20of%20March%202020.>)

The above shown bar graph shows the Bitcoin- the most famous cryptocurrency, and the way its blockchain has been growing over the past decade. It shows a clear exponential growth of the cryptocurrency, as previously talked about. The x-axis shows the time over the decade (2010-2020), while the y-axis shows the size of the blockchain storing bitcoin transactions.

It is rightly said that "A picture is worth a thousand words." Well, here it is. The above graph clearly depicts the growing popularity of the cryptocurrency. Imagine, a currency, growing at this rate, whilst having frauds worth millions of dollars every single day. Imagine, an economy losing $9 million a day. I mean, it is quite an incentive for the people committing cryptocurrency frauds, right. After all, the transaction details are anonymous, and yes, the chances of getting caught, quite less.

> **"It's bad enough realising that somebody's nicked £25,000 of your hard-earned cash. It's even worse when you realise there's little chance of getting it back."**
>
> - Published in the BBC news in 2019 when a tech journalist, Monty Munford, felt the wrath of getting his cryptocurrency stolen.

Further, FBI, in April, 2020 even predicted a surging increase in cryptocurrency scams, due to the coronavirus pandemic that has surrounded the world right now.[11] I believe that there are enough evidences stating that the cryptocurrency is ever-growing and the potential risks of fraud that the

cryptocurrency brings with it, is not something which should be taken very lightly, and it is definitely not something which should be overlooked. Which so much at stake, it is a problem, a problem which requires immediate answers, and which requires immediate awareness. Maybe modern technology can provide a solution to this underlying problem. Let's see, as we go ahead into this research, but first, more on the different types of scams and frauds played out by evolving fraudsters.

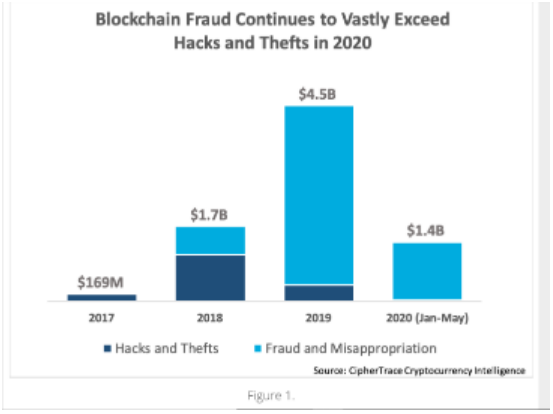
III. DANGERS OF CRYPTOCURRENCY

Customized Old-fashioned tricks and new tricks and tactics are used by crypto-criminals to highlight their prominence in this growing sphere. The crypto-criminals have found new ways of committing fraud, whether it be by simulating ponzi schemes or pulling various other schemes, meant to unlawfully steal money, from right under the noses of unsuspecting investors.

Cryptocurrency works at the integration of finance and technology. Hence, it is succumbed to the various crimes being played out in the financial as well as the technical world. While, technical scams do play a major role in the cryptocurrency market, we definitely cannot ignore the scams and frauds in the cryptocurrency market from a financial point of view, or frauds that are taken place similar to the ones in a traditional equity market. It is important to note that the way the prices of the cryptocurrency are based on, are not governed by a government, hence, market interactions are the major ways in which the price of a cryptocurrency is influenced. Which means the forces of demand and supply acting on the currency, without government interference. Thus, many scams and frauds that will be discussed are already of great prominence in traditional financial markets, and have been talked about frequently, although the applications of the particular scams to cryptocurrency are something which is not known to the common public.

10.

11



(Cipher Trace. 2020. *Cryptocurrency Anti-Money Laundering and Crime Report, Spring 2020*. [online] Available at: <https://ciphertrace.com/cryptocurrency-anti-money-laundering-and-crime-report-spring-2020/>.)

While, in 2017, only scams related to Hacks and thefts were reported, it is appropriate to say the scamsters are developing and orchestrating new techniques to scam the cryptocurrency. It is also useful to observe from the figure on the left that as we progressed into 2020, the amount of thefts and hacks have reduced to a bare minimum, while there is a constant rise in the level of fraud and misappropriation of cryptocurrency.

A. Financial Frauds Related to Cryptocurrency

a) Ponzi Schemes:

The Ponzi Scheme, invented in 1920, by the infamous Charles Ponzi, sees millions of dollars of crypto- scams played out by the traders. This scheme, taking advantage out of people's lack of concrete awareness related to the cryptocurrency market accounted for around 92% of the stolen money in 2019,[12] having siphoned off a massive combining total of $8-10 billion. Charles Ponzi managed to work the ponzi scheme with postage stamps, well, it has been adapted into working with cryptocurrency. It is actually pretty easy to play out on cryptocurrencies given that the only things needed to implement the scheme is investments, which the cryptocurrency market seem to get plentiful. The main idea behind this underlying scheme is eventually paying off the old investors with the new investor's money. The new investors are wrongfully tied together using falsified reports, unrealistically high rates of returns and well, recommendations from old investors. Many people are indeed aware of this particular scheme given the high status and publicity that the Bernie Madoff case brought. However, due to the naïve approaches concerning cryptocurrencies amongst people, there may be unfamiliarity of the infamous ponzi scheme being applied to the cryptocurrency. The 'Crypto-ponzi' scheme perpetrated by the PlusToken, in 2019, which had a major following in Korea and China, was one of the biggest crypto ponzi schemes played out, costing investors more than $2 billion in total, while also being blamed for the fall in Bitcoin Prices in 2019, as stolen funds were sold via Bitcoin OTCs,[13] while the big one played out by OneCoin saw a fraud of around $4billion.[14] Some other "Crypto-ponzi" schemes were the scheme perpetrated globally by BitClub, costing around $0.7 million[15]. While I could go on and on about different ponzi schemes played out in the cryptocurrency market, and their respective damages, I would really like to concentrate my focus on one particular ponzi scheme played out by Bitconnect. Well, I could have chosen any big ponzi scheme for a case analysis, like the OneCoin or the PlusToken, although I particularly chose the ponzi scheme perpetrated by Bitconnect because, it was one of the first big ponzi schemes played out in the cryptocurrency market, which gives us the advantage, while analyzing it, of looking at the various approaches adopted by the cryptocurrency and the way the big scams related to ponzi schemes on cryptocurrency truly showed light. While, Bitconnect looked to be a pretty legitimate cryptocurrency, it was involved in, in 2018, when it shut down, in one of the biggest ponzi schemes played out in the cryptocurrency market. The exchange's Ponzi scheme relieved thousands of investors of their cash. Bitconnect, in order to render approximately 95% of the Bitconnect Coin's (BCC's) transaction on its said exchange, told its investors that they would be receiving an 'interest,' if they traded through the particular exchange. Apart from this, another significant red flag to the Bitconnect was that that the purchase of the BCC had to be paid in Bitcoins. While, the real reason for this is not known, but it is highly speculated that the reason for the condition could be the fact that it is easier to trace a cash transaction rather than a transaction done using Bitcoin or any other cryptocurrency for that matter. Bitconnect presented interest earnings report to its users to show how much they actually benefitted off interests while placing their faith in the Bitconnect.[16] For most of you out there, you might have already guessed as to how Bitconnect managed to show the significant interest earnings report and how they used to pay off the interest.[17] Well, it is of certainly no doubt that the interest was earned through the new investors coming in; thus, completing the vicious cycle of the Ponzi Scheme and providing a textbook definition of the same.

With the crypto-investors doubting that they had been duped of their money while placing their trust in the coin, and realizing that they had little to no chance of recovering their money, the price of the Bitconnect fell drastically by 80% in a short duration of time, from $400 per BCC to just around $27 per BCC.[18] Coming to the rather interesting part. By operating in an anonymously and requiring the payment of all BCC to be done with Bitcoin, they nearly made it impossible for the investigators to track them down. The Bitconnect scam is estimated to be around $2.6 billion[19] in worth making it one of the first and also, one of the biggest ponzi schemes in the cryptocurrency market. The Bitconnect scam, was definitely one of the most prominent scams in the market which was prominent enough to make crypto-investors to be aware of their investments in the cryptocurrency market and to be wary of where they are putting their money in. The question still remains as to what exactly was suspicious and how did the investors started having a doubt that they were getting duped off their money?

The answer lies in the large interest rates that they guaranteed. Well, the platform did say that it generated returns using a trading bot and a "volatility trading

12
13
14
15
16
17
18
19

software," which usually averaged around 1% per day. Obviously, profiting from the market fluctuations and volatility rates is a trading strategy used by many hedge funds and investment banks. Although, what indeed set the chain of suspecting the ponzi scheme run by Bitconnect was their sheer promise and payment of large guaranteed returns. This led many investors to believe that in fact, Bitconnect was running a ponzi scheme, that is using new investor's money to pay off old interests, in order to fulfil their 'immense' promise.[20]

I had previously talked about knowing cryptocurrency exchanges as they are the ones who more often than not are involved in a cryptocurrency scam. One such company/ exchange, which we will be talking about, Bitfinex, was involved in a ponzi scheme, whereby duping its investors off their money. Well, Bitfinex did start off as a legitimate company in 2012, although their scam started from whence their servers got hacked a significant amount of money was stolen off of Bitfinex.[21] Executives at Bitfinex, in an attempt to minimize the consequences of the theft, encouraged investors to convert their shares into equity within the company itself, thus, creating value out of nothing at all.[22] Once, most conversions were done by the investors, Bitfinex encouraged the investors to sell their equity as shares to new investors. Bitfinex then used the new investors' investments to pay off the investments of the old hack victims, thus creating a ponzi scheme of around $1 billion in value.

b) ICO:

Coming on to the next big scam perpetrated by fraudsters in the world of digital currency. This particular method is called the Fake ICO, (Initial Coin offering), which is in many ways similar to the Initial public offering in the stock market. Statistics in 2017 say that around 80% of the ICO's offered were scams[23] in an attempt to capitalize on investors fear of missing out on the next big pay check that they could receive by getting in on a new cryptocurrency. The ICO scams were responsible for stealing around $700 million out of investors pockets. While, the ICO, was one of the most prominent scams happening in the world in the cryptocurrency market in 2017-18, in the past couple of years, fewer funds are being raised through ICO's, primarily due to the crypto-market conditions, which has, fortunately, significantly reduced the amount of Fake ICO scams prevalent around the world. Although, as the scam was of utmost importance, which is why, it is important to know the types of scams happening in the crypto-market. PlexCoin, a fake cryptocurrency is the most notable example of the fake ICO, where PlexCoin promised astonishingly high returns (1300%) in the first 30 days, which captured the investors fear of missing out, thus leveraging high end investors into investing large amounts of money in a fake cryptocurrency. In total, there have been estimates in 2018, that the total value of the top 10 scammed ICO's, amounted to around $700 million, a definitely huge amount for something that does not even exist![24]

c) Pump And Dump

The next major cryptocurrency scam played out in the market is called the pump and dump scheme. This particular scheme is not very new and economic analysts date this scheme back to the 18th century. Much like scheme enacting with the traditional equity market, the pump and dump scheme is a huge contender in big cryptocurrency scams, and it is one to be particularly aware of.

The scheme is a price manipulation which is responsible for creating short term bubbles, featuring dramatic increases in price, volume and volatility. While the SEC considers the P&D scheme illegal in the stock markets, there are minimal rules are regulations concerning the same in the cryptocurrency market. In the cryptocurrency market, the scheme lasts only for a few minutes to be completely perpetrated. A study was done to typically estimate the time that the scheme lasts in the cryptocurrency exchange. The results were carried out using 500 different hand-picked cryptocurrency P&D schemes, and the results showed that in the first 70 seconds of the initial start of the scheme, the prices rose by 25%, on average, trading volumes increase a stunning 148 times, and the average 10-second absolute return reaches 15%.[25] The scheme involves selling off a purposefully highly inflated asset which was previously bought at a cheaper rate.

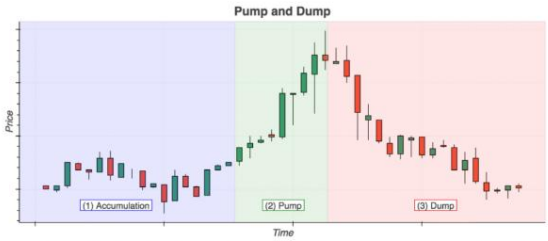


Figure 1: An example of the typical pump-and-dump shape and its phases (reproduced from Kamps & Kleinberg, 2018)

The above figure provides a representation of a sample P&D scheme, using the Candlestick analysis. This clearly shows that the prices of the asset have been inflated purposefully on a temporary basis so that it could be sold at a higher valuation than it is supposed to be sold at, and can immediately get back to the price that it was supposed to be sold for. Well, naturally it is visible that the fraudster makes a lot of monetary benefit by this particular scheme as the hike in the price, is the money which goes into his own pocket. That is surely an incentive for a fraudster to practice this, and while it is actually considered illegal in the stock market, it violates no such legal rule in the cryptocurrency market due to the lack of regulation in the market. And the inflated money, that comes from the buyer's pocket, eventually meaning that the fraudster is getting benefitted out of the naïveté attitude that the buyer had on the cryptocurrency market, again capitalizing on the buyer's fear of missing out. Such a scam, in a cryptocurrency market is organized via the use of "pump groups," using encrypted messaging apps like Telegram.[26]

One of the largest of such 'pump groups,' was reported by the journal which had nearly 74,000 followers, while newspaper reports suggested that around $222 million were made by the group in trades involving the particular scheme.[27]

One of the other major financial crime happening in the world of cryptocurrency is called the 'exit scheme, 'which has been described by Investopedia as a "fraudulent practice by unethical cryptocurrency promoters who vanish with the investors' money." In other

20
21
22
23
24
25
26
27

words, it is the practice of what could have been a legitimate business, due to some foreseeable insight of the business failing, manage to vanish into thin air, to avoid from paying the necessary debts back to the investors. While, naturally, just like in the case of the fake ICO, the investors are duped of their money as they are stolen away by the unethical perpetrators of the scheme. The particular scheme was famously perpetrated by a crypto-company by the name of Giza, which was believed to be a legitimate company due to its partnership with a Russian tech firm called Third Pin. Giza raised 2100 Ethereum coins, valued at around $2.4 million of that date. In February, 2018, after much worry from investors due to the cutting of ties of the both companies, the funds were transferred out, supposedly by the CEO of Giza, and no one was able to track down the CEO of the supposed firm.

B. Tech Frauds Related to Cryptocurrency

In addition to the frauds talked about earlier there are a few schemes, which can be categorized under cryptocurrency thefts. This field largely talks about the more heard of frauds related to cryptocurrencies. Crypto jacking, a significant fraud committed in the cryptocurrency world. This refers to the unauthorized use of someone else's computer to mine cryptocurrency. It is essentially hacking the processing speed of another computer which allowing all the infected systems to mine cryptocurrency for the fraudster, also providing a method giving higher returns and less risk of getting caught.[28] Hackers have become a prominent threat to the security of investor's cryptocurrencies. Numerous methods are used by hackers to steal the cryptocurrencies from the investor's accounts, and while investors are fairly confident on the security provided by blockchain as aforementioned, hackers manage to steal cryptocurrency every day, whether it be from cryptocurrency exchange markets such as the Binance hack of $40 million. Mt. Gox, as previously talked about in the paper was not hacked once but twice. The first hack took place in 2011, using the auditor's credentials which were supposed to be confidential. The first hack was a miniscule 2609 bitcoins relative to the amount lost during the second hack. The second hack in 2014, relived Mt. Gox of around 750,000 Bitcoins, which was around 6% of the bitcoins in circulation at that time. And as mentioned previously, Mt. Gox filed for bankruptcy in 2014.[29] Like Mt. Gox, many exchanges have had severe incidents of being hacked, in an attempt to steal the cryptocurrency exchanged in the market. From the smallest of exchanges to the largest of exchanges such as Bitfinex or Binance, the exchanges are vulnerable to hacks and have experienced various hacks in their systems previously. These hacks have the potential to completely wipe out an exchange from the market, like was done to Mt. Gox, which is another big risk that the investors are giving in to, while investing in cryptocurrencies. It took approximately 4 years for the culprit behind the Mt. Gox hack to be found and subsequently, some Bitcoins were retrieved from the culprit behind the hack.

IV. USE OF ARTIFICIAL INTELLIGENCE

Even though, the blockchain provides full transparency of transactions, it is difficult to track illicit financial flows. Many illicit transactions contain hundreds and thousands of transactions making manual inspection of the transaction data impracticable. Secondly, the number of illicit transactions is severely overnumbered by the number of legitimate transactions, thus making the task of finding the transactions like a 'needle in the haystack.'[30] Also, some cyber-criminals exploit various techniques in order to make the analyzing of the transaction much more difficult by using mixing tools to hide the actual existence of the illegal money.

Given that the cryptocurrency frauds are in such a meteoric rise, what exactly can be done using modern technology to curb down the frauds. I believe that Artificial Intelligence may have an answer to this question. Artificial Intelligence is a field in computer science which provide stimulation of the human intelligence to the machine that are programmed to think and mimic actions of humans.[31] This technology, plays an unparalleled role in our lives as we become more technologically centered. From algorithms which remove spam from mail inbox to recommending movies on Netflix, we are surrounded by the use of this technology in our daily lives. Now, the question is, can this technology help secure the cornerstone financial innovation of this decade.

Researchers from the Imperial College of London, studied the pump and dump scheme back in 2018-19, when thy published the first detailed account of how they work.[32]Apart from this, they also made a machine learning algorithm which could predict when the scheme is about to occur. Surely, the technical aspects of the algorithm are complex, and out of scope for this particular paper, but it is possible. It is possible to create algorithms which predict a scheme before it even takes place with large amounts of accuracy, and this can go a great way into curbing the level of fraud out there in the cryptocurrency world. Algorithms like the random forest model or the GML are able to predict the likelihood of a coin being pumped so as to temporarily increase its value.[33]

AI, is a self-learning technology, providing it the framework to recognize changes in patterns and transactions. AI, also evolves with changes in certain network conditions, which makes it difficult for the potential attacker to find vulnerabilities and loopholes to exploit. Looking at these facts, AI can be used excessively to recognize abnormality in the blockchain, which could help in the process of identifying a hack attempt and can be put to a stop before considerable damage has been done.

Alternatingly, AI can help protect the digital wallets used to store cryptocurrencies which are protected using crypto codes, however there have been several cases where a malware was able to obtain the codes in an attempt to break through the cryptographic methods and steal the funds.[34] Not only can AI help in making hack attempts more difficult, AI can also flag such attempts and constantly alert the user of such attempts which again could be a helpful tool in increasing the security of cryptocurrencies from the hands of professional cyber- criminals.

Exchanges like the Coinbase, use AI to Fight Fraud.

28
29.

30
31
32.
33
34

While methods using AI and Machine learning in the field of security of cryptocurrencies are prevalent to an extent, it requires a widespread approach and requires a global adaptation of the method which could help secure cryptocurrencies from frauds like the aforementioned ones. Fraud patterns are being detected by AI tools and can help in significantly reduce the cryptocurrency fraud
rates. Police also use certain AI tools to detect Ponzi Schemes in the market and can be made useful while working with Ponzi Schemes in the cryptocurrency market as well.[35]

V. RESULT AND DISCUSSION

The Paper provide a comprehensive and a viable solution to the prevalent cryptocurrency scams happening across the world.

The major highlights of the paper that need to be taken note of are:

1) Cryptocurrency scams are highly prevalent across the world and it goes beyond the regular hacking as presumed by most people.
2) There are millions of people being duped of their money and awareness is a key to help find a solution to this problem.
3) Along with the awareness, the proposed solution refers to using AI methodology, using clustering and classification algorithms that can essentially predict frauds before they happen.

VI. CONCLUSION

With the help of new research and methods of implementing AI, it is plausible to connect it with the cryptocurrency sphere in an attempt to make crypto investors more secure and making blockchain more secure than it is already portrayed to be. We have the framework, we need the application, and it is indeed the need of the hour.

I have talked about the rampant growth in the cryptocurrency world, discussing in relevant detail about the major scams happening across various platform in the dimension. I have also talked about how, AI provides us an empirical framework to identify such frauds happening, providing details on how AI has the power to change the cryptocurrency sphere by ensuring more security for the same.

We have seen a lot of frauds happening in the crypto-sphere and its time that we recognize the importance and become aware of it.

Whilst, AI and technology in general might be helpful in controlling the frauds related to cryptocurrency, it is quintessential to have a deeper understanding of the cryptocurrency world, when thinking about investing or associating with the field. It is a relatively new field, with a large potential, and with the potential there are many challenges that are to be faced by this particular platform. It is a technology aimed to create a better life, a world where decentralized currency is used widely for transactions, although there are misdemeanors in the crypto-sphere which people are unaware about and it is high time that people explore the in depths of their crypto-investment before heading straight into it. It is also important to note that I am not commenting on the merits of a cryptocurrency investment, I am just trying to say that in the world of new technology and innovation, like the cryptocurrency and blockchain, it becomes important to have an understanding of the underlying dangers that are prevalent in the field.

REFERENCES

1. Consumer Information. 2020. *What to Know About Cryptocurrency*. [online] Available at: <https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency#:~:text=Cryptocurrency%20Scams,
2. Bitcoin News. 2018. *$9 Million A Day Is Lost in Cryptocurrency Scams |Security Bitcoin News*. [online] Available at: <https://news.bitcoin.com/9-million-day-lost-cryptocurrency-scams/>.
3. Seoul, P., 2020. *Cryptocurrency Scams Took in More Than $4 Billion In 2019*.[online]WSJ.Availableat:<https://www.wsj.com/articles/cryptocurrency-scams-took-in-more-than-4-billion-in-2019-11581184800>
4. Finextra Research. 2020. *Crypto Crime Reaches $1.4Bn So Far In 2020*. [online]Availableat:<https://www.finextra.com/newsarticle/35949/crypto-crime-reaches-14bn-so-far-in-2020>
5. Cointelegraph. 2020. *What Is Cryptocurrency?*. [online] Available at: <https://cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies>.
6. Investopedia.2020. *Cryptocurrency*. [online]Availableat:<https://www.investopedia.com/terms/c/cryptocurrency.asp>.
7. Mearian, L., 2020. *What Is Blockchain? The Complete Guide*. [online] Computerworld.Availableat:<https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html>
8. Investopedia. 2020. *Blockchain Explained*. [online] Available at: <https://www.investopedia.com/terms/b/blockchain.asp>
9. IG. 2020. *What Is Cryptocurrency Trading And How Does It Work?*. [online] Available at: <https://www.ig.com/en/cryptocurrency-trading/what-is-cryptocurrency-trading-how-does-it-work#:~:text=Cryptocurrency%20trading%20involves%20speculating%20on,and%20what%20moves%20the%20markets.>
10. CoinMarketCap. 2020. *Top Cryptocurrency Spot Exchanges | CoinMarketCap*.[online]Availableat:<https://coinmarketcap.com/rankings/exchanges/>
11. Alford, T., 2020. *Bitconnect Scam: The $2.6 BN Ponzi Scheme [2020 Update] - Totalcrypto*. [online] TotalCrypto. Available at: <https://totalcrypto.io/bitconnect-scam/>
12. Bitcoin News. 2020. *The Fallout From Onecoin's Ponzi Scheme Continues To Impact Investors | Bitcoin News*. [online] Available at: <https://news.bitcoin.com/the-fallout-from-onecoins-ponzi-scheme-continues-to-impact-investors/>
13. Boxmining. 2020. *Plus Token (PLUS) Scam - Anatomy of A Ponzi*. [online] Available at: <https://boxmining.com/plus-token-ponzi/>
14. Cipher Trace. 2020. *Cryptocurrency Anti-Money Laundering And Crime Report, Spring 2020*. [online] Available at: https://ciphertrace.com/cryptocurrency-anti-money-laundering-and-crime-report-spring-2020/
15. CoinDesk. 2020. *Alleged Architects Of $720M BitClub Ponzi Request Jail Release Over Coronavirus Risk - CoinDesk*. [online] Available at: <https://www.coindesk.com/alleged-architects-of-700m-bitclub-ponzi-request-jail-release-over-coronavirus-risk>
16. Coppola, F., 2020. *Bitfinex: Cryptocurrency's MF Global*. [online]Forbes.Availableat:<https://www.forbes.com/sites/francescopcoppola/2019/04/29/the-cryptocurrency-mf global/#:~:text=It%20is%20being%20investigated%20for,unregulated%20payment%20processor%2C%20Crypto%20Capital
17. En.wikipedia.org. 2020. *Bitconnect*. [online] Available at: <https://en.wikipedia.org/wiki/Bitconnect>
18. Finder UK. 2020. *What Is Bitconnect (BCC) And How Does It Work? | Finder UK*. [online] Available at: <https://www.finder.com/uk/bitconnect>
19. Hard Fork | The Next Web. 2020. *Bitconnect Is Shutting Down Its Lending and Exchange Platform*. [online] Available at: https://thenextweb.com/hardfork/2018/01/16/bitconnect-shut-down-closed/

[35]

20. Medium. 2020. *Bitfinex Never 'Repaid' Their Tokens, Bitfinex Started A Ponzi Scheme.*. [online] Available at: <https://medium.com/@bitfinexed/bitfinex-never-repaid-their-tokens-bitfinex-started-a-ponzi-scheme-86a9291add29>
21. MIT Technology Review. 2020. *Millions of People Fell For Crypto-Ponzi Schemes In 2019*. [online] Available at: <https://www.technologyreview.com/2020/01/30/275964/cryptocurrency-ponzi-scams-chainalysis/>
22. Techcrunch.com. 2020. *TechCrunch Is Now A Part Of Verizon Media*. [online]Availableat:<https://techcrunch.com/2018/01/16/bitconnect-which-has-been-accused-of-running-a-ponzi-scheme-shuts-down/>
23. The Conversation. 2020. *How Cryptocurrency Scams Work*. [online] Available at: <https://theconversation.com/how-cryptocurrency-scams-work-114706>
24. Baker, T., Morrison, E., Saavedra, A., Judge, K., John C. Coffee, J., Awrey, D., Judge, K., Doty, J., John C. Coffee, J. and Tao Li, B., 2020. *Cryptocurrency Pump-And-Dump Schemes*. [online] CLS Blue Sky Bio available: <https://clsbluesky.law.columbia.edu/2019/01/07/cryptocurrency-pump-and-dump-schemes/#:~:text=In%20a%20new%20paper%2C%20we,falls%20and%20investors%20lose%20money.>
25. Finance Monthly | Monthly Finance News Magazine. 2020. *The 10 Biggest ICO Scams Swindled $687.4 Million*. [online] Available at: <https://www.finance-monthly.com/2018/10/the-10-biggest-ico-scams-swindled-687-4-million/>
26. Hackernoon.com. 2020. *AI Proving To Be An Integral Part Of Cryptocurrency High Volume Transaction Security | Hacker Noon*. [online] Available at: <https://hackernoon.com/ai-proving-to-be-an-integral-part-of-cryptocurrency-high-volume-transaction-security-cc20a40d23c7>
27. Investopedia. 2020. *How Artificial Intelligence Works*. [online] Available at: <https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp#:~:text=Artificial%20intelligence%20(AI)%20refers%20to,as%20learning%20and%20problem%2Dsolving.>
28. Investopedia. 2020. *'Pump And Dump' Hits Cryptocurrency Market*. [online] Available at: <https://www.investopedia.com/news/pump-and-dump-hits-cryptocurrency-market/#:~:text=One%20of%20the%20largest%20identified,only%20to%20sell%20minutes%20later.>
29. McMillan, R., Chokkattu, J., Barrett, B., Grey, J., Lewis, B., Levy, S. and Simonite, T., 2020. *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*. [online] WIRED. Available at: <https://www.wired.com/2014/03/bitcoin-exchange/>
30. Medium. 2020. *The Five Biggest ICO Scams*. [online] Available at: <https://medium.com/@tozex/the-five-biggest-ico-scams-54967ec92b87>
31. MIT Technology Review. 2020. *Machine Learning Identifies Cryptocurrency Scams Before They Happen*. [online] Available at:<https://www.technologyreview.com/2018/12/04/1771/machine-learning-identifies-cryptocurrency-scams-before-they-happen/>
32. Nadeau, M., 2020. *What Is Cryptojacking? How To Prevent, Detect, And Recover From It*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html>
33. Osborne, C., 2020. *Police Use AI To Track Down Cryptocurrency Ponzi Scheme Swindlers | Zdnet*. [online] ZDNet. Available at: <https://www.zdnet.com/article/police-use-ai-to-track-down-cryptocurrency-ponzi-scheme-swindlers/#:~:text=Police%20use%20AI%20to%20track%20down%20cryptocurrency%20Ponzi%20scheme%20swindlers,-Live&text=The%20alleged%20criminals%20behind%20a,assistance%20from%20artificial%20intelligence%20systems.>
34. Sagar, R., 2020. *As Cryptocurrency Pump & Dump Schemes Grow, Here's How To Avoid The Scam With Machine Learning*. [online] Analytics India Magazine. Available at: <https://analyticsindiamag.com/cryptocurrency-pump-dump-schemes-avoid-the-scam-with-machine-learning/> (Journal Online Sources style) K. Author. (year, month). Title. *Journal* [Type of medium]. Volume(issue), paging if given. Available: http://www.(URL)

AUTHORS PROFILE

Aryan Kasera is a student at The Doon School with a keen interest in Math, Economics, and Computer Science. He has had experiences in the field of Cybersecurity through his internships with the Gurugram Police Cybercell, where he was also exposed to many cryptocurrency related forensics and investigations, while also enthusiastically engaged in spreading cyber awareness amongst people. Along with that he has had experiences by working as a Java Developer in Optimize IT Systems, Kolkata. He is an avid reader of Economics, and Finance, and has found himself working as the CFO in The Youths Lens. He has had research experiences during his journey in the form of Environmental Data Science and Tea Export Analysis. He aims to pursue his higher education in the upcoming years. Through this research paper, he aims to reach to the masses to create an awareness about Cryptocurrency, and propose solutions that could be kept in place to reduce frauds.