Cryptocurrency Ponzi schemes

Sanmoy Mukherjee, Charles Larkin, Shaen Corbet

1. Introduction:

Before the eponymous act by Charles Ponzi in 1919, the first recorded investment fraud of this type was recorded in the United States in 1872. Since then, such criminality has grown to become substantially more complex, aided substantially by the growth of communications and computer technology. Cryptocurrency Ponzi schemes exhibit similar behaviour to regular Ponzi's in the form of high yield investment program (HYIP) that promise potential investors a substantial return on investment (ROI) with little or no risk involved in a short time. We aim in this chapter to present an overview of cryptocurrency Ponzi schemes that have taken place over the past decade.

The cryptocurrency market is based on an encrypted peer-to-peer network that keeps transactions anonymous between users (Nakamoto, 2008). It was recorded that the market capitalization of cryptocurrency exceeded the $575 billion thresholds in November 2020, a dramatic rise since the inception of Bitcoin in 2009. Cryptocurrency Ponzi schemes started by *"Smart" Ponzi schemes*, which comprises of formulating computer programs whose authenticity is not backed by a credible source (Bartoletti *et al.*, 2019). In layman's term, these schemes exploit the gullibility of novice investors. A notable example is Amit Bhardwaj, who was accused of a $300 million Bitcoin Ponzi scheme in India, 2018. He was charged with fraudulently promising investors a 10% ROI for 18 months under the multi-level marketing schemes. Likewise, Belgium and France experienced substantial fraud, estimated to be approximately €6 million in Bitcoin due to the actions of a criminal group offering a 35% profit[1]. In addition, fake websites are a common approach used by scam artists, often possessing a domain name similar to the original is used.

2. A brief history of cryptocurrency Ponzi schemes:

In this section, we provide an overview of the macro-sized digital schemes that have taken place in recent years. Typically, early schemes in the cryptocurrency market were in the form of 'Bitcoin-only HYIPs'; there were 23 Bitcoin-only Ponzi schemes from January 2013-September 2014, which involved an amount of $843,000 (Vasek and Moore, 2015). According to *The Washington Post*, the latest conspiracy pioneered by John McAfee by March 2021 had a value of $13 million based on

[1] Article available here

promoting cryptocurrencies to investors and selling them when their prices inflated[2]. Such an example presents evidence of the scale of such theft in recent times. This is a lucrative scheme, and presents many opportunities for conspirators to remain largely anonymous. In the following subsections, we have highlighted some recent case studies.

2.1 OneCoin Ponzi scheme

OneCoin founded in 2014 is a Bulgarian-based company in which Ruja Ignatova aka ‘Cryptoqueen’ masterminded the scheme and deceived investors of $4 billion worldwide via a multi-billion-dollar pyramid scheme. Like other digital currencies, it had its digital wallet and the network comprised of 120 billion coins. The United States Attorney’s Office claimed that the growth in the value of the currency, which grew approximately 598% (from an initial value of €0.50 to €29.95 per coin) as of January 2019, was based on a bubble as it was not determined by market forces of demand and supply. The first red flag was raised in September 2016 by the Financial Conduct Authority (FCA), the United Kingdom regarding the probable risk the organisation posed to the investors in the UK. However, ten months later the warning was removed from its official website and the City of London Police retracted its criminal proceedings due to lack of evidence. Bitcoin.com accounts that Chelgate, a “crisis management PR company” and a London-based law firm bulldozed the FCA into dropping its efforts. The core members were charged with money laundering, having personally earned an estimated $400 million through a private equity fund, Fonero Funds. The entire fraud was valued at approximately $4 billion and as of 2019 thus far only Chinese authorities have recovered investor funds to the values of $267.5 million. In addition, Ignatov (Ignatova’s brother) was arrested on 6 March 2019 in Los Angeles on grounds of breaching the US Constitution and is facing up to 90 years in prison[3]. Sebastian Greenwood and Mark Scott were others who were also indicted.

The creation of the bubble was due to a lack of robust regulations from governmental agencies that were not imposing strict rules on digital currency. Even though the concept of ICOs and IPOs (the original equity market term that cryptocurrency marketers borrowed) are considered to be two sides of the same coin, the reality is far from it as the former lacks a robust regulation by the financial body.

2.2 BitClub

It was estimated that $722 million was embezzled by offering naive investors shares in mining pools in the BitClub Ponzi scheme. It encouraged investors by rewarding them with Bitcoins in exchange for

[2] Article available here

[3] The Department of Justice charged Ignatov on four counts; Conspiracy to Commit Wire Fraud, Wire Fraud, Conspiracy to Commit Money Laundering, Conspiracy to Commit Securities Fraud.

solving convoluted mathematical programs. From 2014 through 2019, the criminals used the BitClub Network to trap a group of funders from specific countries in Asia, Europe and Africa. Initially, the returns were exceedingly high after which it subsequently collapsed. In February 2015, the culprits altered the earnings manually from data mining by an upward trajectory of 60% as outlined by the Department of Justice[4]. Two years later they sold off BitClub shares gradually but did not use the capital to purchase mining tools despite claiming to mine coins. The group accumulated $722 million before the shutdown. Federal prosecutors arrested Matthew Goettsche, Jobadiah Weeks, Joseph Abel and Silviu Balaci on the grounds of conspiracy of wire fraud and selling unregistered securities without prior approval from the U.S. SEC. Silviu Catalin Balaci, a 35-year-old Romanian programmer pleaded guilty[5].

2.3 MMM Bitcoin Ponzi scheme:

MMM was a Russian Ponzi scheme in the 1990s engaged in shady "privatisation" deals and money laundering techniques. It is estimated that $1.5 billion was stolen with approximately 5 to 10 million Russians losing their savings. This scheme was ended by the Russian authorities in 1994 but re-emerged in 2011 as MMM Global (Boshmaf *et al.*, 2020). Initially, MMM was a community where participants offer help to each other and it transformed into a program that engages in financial help in the form of bitcoin with a threshold of $10K. Initially, they have zero Mavro and are only rewarded at a fixed rate to Bitcoin (1 BTC = 1 Mavro) along with a 30% monthly return once they provide monetary help to other members. Boshmaf, *et al* (2020) concluded from their dataset that between 2014 and 2016 the scheme generated up to $150 million per day. The Daily Net Difference exhibited a zero-sum payoff for the majority of cases, where the profits and losses of all the participants on a specific day are zero (Boshmaf *et al.*, 2020).

2.4 Ponzi schemes on Ethereum:

Ethereum has provided a new opportunity for scammers to commit financial fraud on *smart contract platforms* (Bartoletti *et al.*, 2019; Chen, 2019). Rubixi and LooneyLottery are some of the most fashionable Ponzi scheme contracts where Ethereum is used. Through the transaction history of LooneyLottery and Rubixi, it is seen that only 0.18% (13 out of a total of 733) and 22% (25 out of 112) of the transactions pay back to their investors respectively (Chen, 2019). The increase in blockchain technology has been a prominent catalyst for this and it is unravelled that there are more than 500

[4] Press release [Accessed on: 17/04/2021] available here

[5] Balaci faces a maximum of five-year sentence with a fine of $250,000

schemes that are in operation. It was estimated in a study that 45 out of 54 contracts are ETH based smart Ponzi schemes (Chen *et al.*, 2018). Table 1 articulates top Ponzi schemes arranged in ascending order, which occurred on this blockchain platform. The respective column in the dataset starts with the number of transactions that were monetary transaction amount in terms of both Ether followed by US dollars. Moreover, all these frauds fall under the category of *Chain-shaped* schemes[6] (Bartoletti *et al.*, 2019). The player is promised of doubling his investment for which 1ETH has to be paid as an entry fee.

Table 1: Top Ponzi schemes on Ethereum

Contract name	Transactions		ETH[7]		USD	
	In	**Out**	**In**	**Out**	**In**	**Out**
DynamicPyramid	444	143	7474	7437	84187	83541
DianaEthereum-x1.8	288	168	5307	5303	61166	61266
Doubler2	395	161	4858	4825	26376	26220
ZeroPonzi	627	499	4490	4489	49816	49770
Doubler	156	57	3073	3073	31292	35927
Government	723	846	2939	2939	35738	40066
Rubixi	686	66	1367	1363	16986	16775
ProtectTheCastle2	890	1257	1332	1332	186040	190802
EthereumPyramid	978	339	986	917	5044	5290
Total	18925	9100	43881	43332	630662	702878

2.5 CoinUp Ponzi scheme:

Launched in 2018, CoinUp, a South Korean cryptocurrency exchange, defrauded investors of $384 million. Kang Seok-Jung, head of the cartel aka "CashKing", was found guilty and charged with 16 years of imprisonment. The executives tempted investors with a promise of a return of 200% over a 1–2-month period and strategic marketing such as a falsified image of the CEO with the Korean president to add credibility. Moreover, a false statement was made in the form of the coins being listed publicly in the digital market that led to a high level of speculation.

[6] Under the taxonomy of *Chain-shaped* schemes, the investment is multiplied by a constant number that is homogenous for all users. The amount invested is fixed, free or with a minimum threshold and there is a percentage return of fee for each investment.

[7] ETH: Ethereum; USD: US dollar

2.6 PlusToken Ponzi scheme:

In September 2020, China saw a shock in the crypto market with a fraud of $6 billion committed by the PlusToken Ponzi scheme. PlusToken was set up by Chen Bo in 2018 and it attracted people by offering high returns to early investors from later investors while no business activity was involved. *The Wall Street Journal* states that the crime group lured in funding by selling pictures of a fake meeting between Price Charles and Leo who is the founder of PlusToken wallet Exchange[8]. It was used to make investors believe that the business was legitimate. The scammers promised a return in terms of the eponymous token (PLUS) and thereby managed to gather funds in over the equivalent of USD $2m in currencies like; 200,000 BTC, 26m EOS and 789,000 ETH. The number of transactions in and out of the system was conducted 24,000 times using 71,000 alternative IP addresses.

The liquidation of the PlusToken coins was estimated to have acted as a catalyst in causing the BTC price to fall. After the shutdown of PlusToken's operation in July 2019, there was a moderate fluctuation in Bitcoin's price. After 20th September 2019, the fraudsters made a large withdrawal of cash, $34 million, while the weighted traded volume also fell and immediately it created downward pressure on the price of Bitcoin from $10,000 to $8,000 on 25th September. Fortunately, the Chinese cyber law officers were able to recover 70% approximately of the total fraud amount ($4 billion). It also reported that there was a correlation between the plummeting of Bitcoin's value and the selling of previous gains from this scam. In the case of the PlusToken Ponzi scheme, it was an organized pyramid scheme consisting of 109 members, all of whom were arrested and six were prosecuted.

2.7 Cryptocurrency Exchange Scams:

Previous research has scrutinised how the crypto scams take place from the transfer of funds without prior credibility check, a violation of the know your customer (KYC) and anti-money laundering FATF regulations. We illustrate how these attacks are perpetrated on cryptocurrency exchanges via social media platforms (Phillips and Wilder, 2020; Xia *et al.*, 2020). Researchers employed the services of clustering-based content (DBSCAN) to identify phishing websites and advanced-fee scams (Phillips and Wilder, 2020). (For example, celebrity/exchange giveaway phishing scams using unique QR codes, payment addresses.)

Typosquatting[9] and *App clones* are two techniques that are used for various scam attacks. Xiao *et al.* (2020) mentions that the first *Fake App* exchange app was created in November 2013 and 323 apps

[8] Article available here

[9] Typosquatting involves formulating a domain with a name similar to the original one. It hangs on to the typing mistakes users make while searching for the correct website.

dealt with 38 exchanges. In *Typosquatting*, some 83% of exchanges are targeted by 1,595 fraudulent domains. They are criminal platforms for trading scams, phishing, referral fraud[10], and gambling. These platforms have a short existence, disappearing rapidly after starting, but only after taking the client's BTCs with them. Due to this reason, they are found out quickly and have a moderately low level of success in defrauding investors, estimated to be around 45% (Chohan, 2018). Table 2 depicts embezzled amount from various exchange platforms from 2011 to 2017. These examples relate to frauds that have resulted in the ultimate closure of the exchanges involved. The loss of $581.180 million from Mt. Gox, had contributed to its failure. (Mukhopadhyay *et al.*, 2016).

Fake apps are on the rise and a recent incident on Trezor has raised high concerns on the loopholes on Apple's safety net. An example of this fraud is that of Phillipe Christodoulou who lost 17.1 BTCs that was roughly estimated to be $600k.

Table 2: Significant cases of embezzlement from exchange platforms

Date	**Exchange Platform**	**Embezzled Amount (USD)**
Jun-11	*Mt.Gox*	8,750,000
Jul-11	*Bitomat*	220,000
Aug-11	*MyBitcoin*	800,000
Aug-12	*Bitcoinica*	460,000
Aug-12	*Bitcoin Savings and Trust*	5,600,000
Sep-12	*Bitfloor*	250,000
Apr-13	*Instawallet*	4,600,000
Oct-13	*Inputs.io*	1,000,000
Oct-13	*Global Bond Limited*	5,000,000
Feb-14	*Mt.Gox*	390,000,000
Jan-15	*Bitstamp*	5,100,000
Feb-15	*Bter*	2,100,000
Jan-16	*Cryptsy*	3,300,000
May-16	*Gatecoin*	2,000,000
Aug-16	*Bitfinex*	72,000,000
Dec-17	*Nicehash*	80,000,000
Total		581,180,000

The identification of a fake app is verified by the certificate signatures of the respective developers. Nevertheless, there are phishing apps that develop fake versions of websites like Poloniex and Binance (Xia *et al.*, 2020). It gathers information from the users, such as their email address, that

[10] Referral fraud refers to how a buyer in the crypto exchange platform tries to manipulate the current offering in the official exchange websites by hacking the process for various incentives. It forwards the user to the official exchange platform and implementing codes that helps them earns the profits by the official platforms.

ultimately leads to theft. Binance acted as the most commonly traded digital asset trading platform whose volume is approximately twice compared to the next largest (28.85 vs 14.44 billion USD).

2.8. Demographics:

We also must discuss the demographics of scammed investors (Bryans, 2014; Glaser *et al.*, 2014). Evidence suggests[11], the majority of crypto users were 21-30 years old (57.1%) while there is no other age cohort that dominates. Economic theory justifies this finding as younger cohorts are more risk-tolerant (especially technology-driven) and they have a regular inflow of income with the opportunity to increase its threshold.[12] Last year, researchers have claimed that cryptocurrencies are high-risk assets and according to studies 9.2% of the German population invest in digital currencies (Ante *et al.*, 2020). Table 3 outlines the demographics of the Germans who experienced the highest average relative returns (2449%) along with the highest absolute return (€ 478,100) in Ante *et al.* (2020).

In a study of a cohort comprising of European and North American cryptocurrency users, their level of confidence was measured on a scale of 1-5 in the context of crypto assets (Abramova *et al.*, 2021). In addition, the descriptive metrics in that study disclosed that out of the 395 crypto users, 88% were men and they were in the age group of 25-44 with a minimum of 3 years of trading experience. Most of the users' crypto wallets comprise Bitcoin and Ethereum.

Moreover, studies have shown that a significant portion of the male population has a bias towards risky investments and that acts as a catalyst in the case of cryptocurrencies. (Lammer, Hanspal and Hackethal 2019) (Powell and Ansic, 1997).

Table 3: Demographics for German Crypto Investors

Country	Age	Gender	Amount invested	Amount realized	Occupation	Income
Category 1	38	Male	€ 500	€ 1,80,000	Commercial/trade training	€ 2000-2999
Category 2	38	Male	€ 5,500	€ 1,85,000	PhD	More than €5000

3. Concluding Comments

When analysing how the cryptocurrency Ponzi schemes have shaped over the past decade across the globe, it is apparent that the scammers have manipulated the risk-seeking behaviours of novice

[11] Available here
[12] Ibid.

investors. Evidence suggests that more or less all the schemes have utilised a multi-level marketing scheme to encourage investors to participate in risky investment programs. The majority of the Ponzi schemes mentioned in this paper have a low recovery rate except for PlusToken Ponzi that had a remarkably high recovery of 70% of investor funds. In PlusToken Ponzi, evidence of price manipulation was found, involving OTC brokers who dealt with illegal funds. Thus, it can be inferred that scammers wanted to drive down BTC prices down to allow for their digital currencies to rise. Lack of monitoring and government regulations have amplified these events. To limit this, investors need to be educated on cryptocurrency dangers before making investments.

It is necessary to point out a few limitations in this cryptocurrency-related literature. Firstly, we present an overall idea of cryptocurrency Ponzi schemes without discussing the flaws of blockchain technology in-depth that leads to leakage. Secondly, we have not talked about the contagion effects of these Ponzi schemes on the stocks like the S&P 500 index and gold coin sales. Thirdly, Bitcoin and others operate on the digital platform for which electricity is a crucial input in the production process. It is not extrapolated here how much energy these schemes are consuming and its environmental impact. Fourthly, the lack of a coherent understanding of cryptocurrencies as a legal form of money is significant. Finally, a statistical analysis of the percentage of crypto-based Ponzis schemes to the total number of financial sector Ponzi schemes over the last decade will help us understand the extent of cryptocurrency as a means of defrauding people. We must continue to note that in Bitcoin-based Ponzi schemes cites that only 21% of the revenues have been recovered from Bitcoin-based schemes (Vasek and Moore, 2015). As long as Ponzi schemes remain lucrative in cryptocurrency markets, and their benefits outweight the perceived countermeasures in place against thieves, they will continue to become more frequent and sophisticated.

References:

Abramova, S. *et al.* (2021) 'Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users', in *Conference on Human Factors in Computing Systems*. New York, USA, p. 26. doi: https://doi.org/10.1145/3411764.3445679.

Ante, L. *et al.* (2020) *Returns from Investing in Cryptocurrency: Evidence from German Individual Investors*, *BRL Working Paper Series*. doi: 10.2139/ssrn.3540876.

Artzrouni, M. (2009) 'The mathematics of Ponzi schemes', *Mathematical Social Sciences*, 58(2), pp. 190–201. doi: 10.1016/j.mathsocsci.2009.05.003.

Bartoletti, M. *et al.* (2019) 'Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact', *Future Generation Computer Systems*, 102, pp. 259–277. doi: 10.1016/j.future.2019.08.014.

Baur, D. G., Hong, K. and Lee, A. D. (2018) 'Bitcoin: Medium of exchange or speculative assets?', *Journal of International Financial Markets, Institutions & Money*, 54, pp. 177–189. doi: 10.1016/j.intfin.2017.12.004.

Boshmaf, Y. *et al.* (2020) 'Investigating MMM Ponzi Scheme on Bitcoin', in *Proceedings of the 15th*

ACM Asia Conference on Computer and Communications Security, ASIA CCS 2020, pp. 519–530. doi: 10.1145/3320269.3384719.

Bryans, D. (2014) ‘Bitcoin and Money Laundering : Mining for an Effective Solution’, *Indiana Law Journal*, 89(1).

Chen, W. *et al.* (2018) ‘Detecting ponzi schemes on ethereum: Towards healthier blockchain technology’, in *The Web Conference 2018 - Proceedings of the World Wide Web Conference, WWW 2018*. Creative Commons Attribution 4.0 International (CC BY 4.0) license, pp. 1409–1418. doi: 10.1145/3178876.3186046.

Chen, W. (2019) ‘Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum’, *IEEE Access*, 7, pp. 37575–37586. doi: 10.1109/ACCESS.2019.2905769.

Chohan, U. W. (2018) *The Problems of Cryptocurrency Thefts and Exchange Shutdowns The Problems of Cryptocurrency Thefts and Exchange Shutdowns*. Canberra: SSRN. doi: https://dx.doi.org/10.2139/ssrn.3131702.

Corbet, S. *et al.* (2019) ‘Cryptocurrencies as a financial asset: A systematic analysis’, *International Review of Financial Analysis*, 62(August 2018), pp. 182–199. doi: 10.1016/j.irfa.2018.09.003.

Corbet, S. *et al.* (2020) ‘The destabilising effects of cryptocurrency cybercriminality’, *Economics Letters*, 191, p. 108741. doi: 10.1016/j.econlet.2019.108741.

ElBahrawy, A. *et al.* (2017) ‘Evolutionary dynamics of the cryptocurrency market’, *Royal Society of Open Science*, 4(11). doi: 10.2139/ssrn.2969708.

Fletcher, E., Larkin, C. and Corbet, S. (2021) ‘Countering money laundering and terrorist financing: A case for bitcoin regulation’, *Research in International Business and Finance*, 56(October 2020), p. 101387. doi: 10.1016/j.ribaf.2021.101387.

Gandal, N. *et al.* (2018) ‘Price manipulation in the Bitcoin ecosystem’, *Journal of Monetary Economics*, 95, pp. 86–96. doi: 10.1016/j.jmoneco.2017.12.004.

Glaser, F. *et al.* (2014) ‘Bitcoin - Asset or currency? Revealing users’ hidden intentions’, *ECIS 2014 Proceedings - 22nd European Conference on Information Systems*, pp. 1–14.

Lammer, D., Hanspal, T. and Hackethal, A. (2019) *Who Are the Bitcoin Investors? Evidence from Indirect Cryptocurrency Investments, SSRN Electronic Journal*. doi: 10.2139/ssrn.3501549.

Mukhopadhyay, U. *et al.* (2016) ‘A brief survey of Cryptocurrency systems’, in *2016 14th Annual Conference on Privacy, Security and Trust, PST 2016*, pp. 745–752. doi: 10.1109/PST.2016.7906988.

Nakamoto, S. (2008) ‘Bitcoin: A Peer-to-Peer Electronic Cash System’. doi: 10.1162/ARTL_a_00247.

Phillips, R. and Wilder, H. (2020) ‘Tracing Cryptocurrency Scams : Clustering Replicated Advance-Fee and Phishing Websites’, in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. Toronto, ON, Canada: IEEE. doi: https://doi.org/10.1109/ICBC48266.2020.9169433.

Powell, M. and Ansic, D. (1997) ‘Gender differences in risk behaviour in financial decision-making : An experimental analysis’, 18.

Sountra, M. (2019) ‘Cryptocurrency as a Modern Technique of Money Laundering and Terrorism Financing’, *International Journal for Electronic Crime Investigation*, 3(4). Available at: http://www.ojs.lgu.edu.pk/index.php/ijeci/article/download/339/297.

Vasek, M. and Moore, T. (2015) ‘There’s No Free Lunch, Even Using Bitcoin’, *International Financial Cryptography Association*, 8975, pp. 44–61. doi: 10.7910/DVN/28561.

Xia, P. *et al.* (2020) ‘Computers & Security Characterizing cryptocurrency exchange scams’, *Computers & Security*, 98, pp. 1–17. doi: 10.1016/j.cose.2020.101993.