Digital Forensic Investigation on Ponzi Schemes

Babu Madhavan and N. Kalabaskar

Abstract The Ponzi scheme is an economic offence to lure investors by giving false assurance of huge returns with less risk. The money is provided to the older investors from the new investors in the form of payouts. Mostly the scheme would collapse or in the verge of collapse when the reduction of new investors. The scheme would try to retain later or the latest customers to reinvest or roll over the payouts into the scheme. Ponzi schemes are also performing as "Smart Ponzi Scheme" [1] where new technology (blockchain) cryptocurrency has been used indirectly. Some Ponzi scheme adopts a hybrid model without the knowledge of investors. Fugazzi financial securities are also given in the form of bonds with some security values, especially payouts are enticed to roll over again. The Ponzi scheme would initially be started and pretend to be a formal and genuine financial business and would certainly know the scheme would collapse. The scheme's brainchild or brainchildren would counter and prepare for the easy way outs. The accumulated money is invested in real estate, movable properties, Panama papers, gold investments, cryptocurrencies, smart contracts (Cryptocurrency), and offshore investments. The new and the latest investors were victimized a lot. The financial victimization will be more from the new investors to the initial or oldest investors. The fairness of identifying actual financial loss incurred by the investors has to be justified for a fair settlement. The nature of the Ponzi scheme itself is a discrete business and the brainchild/brainchildren behind the scheme have constructed business infrastructure in such a way that they cannot be caught or tracked or detected. They have chosen complex technological infrastructure to make the investigation process difficult. The Ponzi scheme is accomplished by complex infrastructure in a way digital forensics investigation process made so difficult to detect. Ponzi scheme identification and intelligence about people and infrastructure are to be collected properly else the break in the detection chain would end up in fragile evidence collection. Understanding of infrastructure of the Ponzi scheme model is crucial to gather all information and quantifying the actual amount and people who were involved in the Ponzi scheme. The magnitude

B. Madhavan (✉) · N. Kalabaskar
Department of Cyber Forensics and Information Security, University of Madras, Chennai, Tamil Nadu, India
e-mail: bob4u1985@gmail.com

S. J. Patel et al. (eds.), *Information Security, Privacy and Digital Forensics*,
Lecture Notes in Electrical Engineering 1075,
https://doi.org/10.1007/978-981-99-5091-1_14

of the Ponzi scheme scam would only be identified by the proper digital forensic investigation process. This paper discusses the complex infrastructure adopted by the Ponzi schemes. The hurdles and challenges faced by the investigation team and digital forensics Investigation team to detect the magnitude of the scam involved. This paper also addresses the lacuna of policy, enforcement, and regulatory lens on the Ponzi scheme with respect to the existing monitoring system and infrastructure.

Keywords Digital forensics · Economic offence · Ponzi scheme

1 Introduction

The Ponzi scheme is an economic offence to lure investors by giving false assurance of huge returns with less risk. The money is provided to the older investors from the new investors in the form of payouts. Mostly the scheme would collapse or in the verge of collapse when to the reduction of new investors. The scheme would try to retain later or the latest customers to reinvest or roll over the payouts into the scheme.

Ponzi schemes are also performing as "Smart Ponzi Scheme" [1] where new technology (blockchain) cryptocurrency has been used indirectly. Some Ponzi scheme adopts a hybrid model without the knowledge of investors. Fugazzi financial securities are also given in the form of bonds with some security values especially payouts are enticed to roll over again.

The Ponzi scheme would initially be started and pretend to be a formal and genuine financial business and would certainly know the scheme would collapse. The scheme's brainchild or brainchildren would counter and prepare for the easy way outs.

The accumulated money is invested in real estate, movable properties, Panama papers, gold investments, cryptocurrencies, and smart contracts (cryptocurrency).

The complex infrastructure of the Ponzi scheme is to be unraveled and busted with help of digital forensic investigation. Understanding of Ponzi scheme model and gaining actual information pertaining to the scheme to arrive real magnitude of the scam. The real magnitude of investors and money would certainly help fair disperse among invested victims.

1.1 History

The fraudulent scheme was named after "Charles Ponzi" [2, 3] who ran schemes such as "Postal reply coupon" selling with 100% return in 90 days. Though such fraud might occur prior to Charles Ponzi's contemporary this was well notified economical crime after Charles Ponzi was Busted.

1.2 *Famous Ponzi Scheme Cases*

Bernie Madoff [4] Ponzi scheme scam: Bernie Madoff was an American financial manager who ran a Ponzi scheme for more than two decades with a magnitude of more than 60 billion US dollars.

The center said that various programs and campaigns have been run by the government to sensitize people about various fraudulent and Ponzi Schemes.

Over the last 3 years, 8 cases involving 84 companies have been assigned to the Serious Fraud Investigation Office (SFIO) to inspect Ponzi schemes/multi-level marketing/chit fund activities, Minister of the State of Corporate Affairs, Rao Inderjit Singh, said in the Rajya Sabha on Tuesday [5, 6].

2 The Technology Adopted by Ponzi Schemes

The complex infrastructure model has been adopted by Perpetrators who ran Ponzi schemes in India. The infrastructure model is apparent that it inherits an intricately maneuvered model whereby it can’t be unraveled and undetected by regulators and investigators.

3 Dissect and Understanding of the Ponzi Scheme Infrastructure

The perpetrators start a company with or without registration. Sometimes, the name of the company gets registered but hardly registers or associates with other regulatory bodies such as the Securities and Exchange Board of India (SEBI) and the Securities and Exchange Commission (SEC).

In the above hypothetical scenario (Fig. 1), the perpetrators’ head office located in Chennai has branches across the country. The Head office communicates with branches through Server and Client model ERP application whereby branch records are fed into the head office. The branch collects and records investors’ details such as name, identity, mobile number, email ID, and banking details. Branch may send all data to head office or selective records such as banking details, name, and mobile number. The Server/Client model ERP software is made with the front end in Dot Net and the Backend database in MySQL. The ERP software provider and support are from the Bangalore location and the application and database are hosted in a cloud server located in Dubai.

The selected records from branch data are fed to the head office. The data from different branches gets consolidated and further trimmed and send to the main database server. The main database server is hosted in a cloud server located in California which is an MS SQL Database with the front end of Python. The main

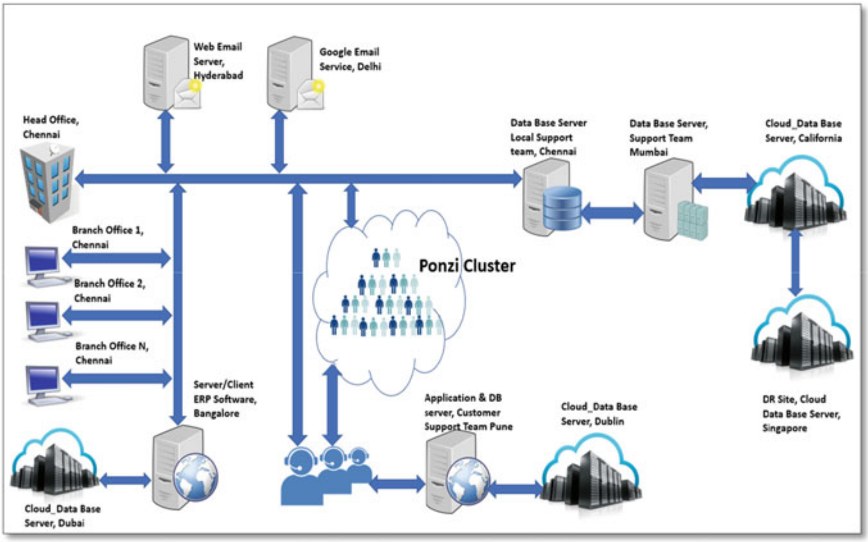
Web Email Server, Hyderabad
Google Email Service, Delhi
Head Office, Chennai
Data Base Server Local Support team, Chennai
Data Base Server, Support Team Mumbai
Cloud_Data Base Server, California
Branch Office 1, Chennai
Ponzi Cluster
Branch Office 2, Chennai
Branch Office N, Chennai
Server/Client ERP Software, Bangalore
Application & DB server, Customer Support Team Pune
Cloud_Data Base Server, Dublin
DR Site, Cloud Data Base Server, Singapore
Cloud_Data Base Server, Dubai

Fig. 1 Schematic diagram of Ponzi scheme IT infrastructure

database of consolidated records is hosted in a cloud server located in California and its DR (Disaster Recovery) site is located in Singapore.

The consolidated main database and applications have been taken care of and supported by a local vendor located in Chennai and the local vendor gets support from a database and cloud management service provider which is located in Mumbai each location has a copy of the data of the main database hosted in cloud server, California. The main database copy at each location may not be the same. The integrity of data should be checked to affirm the databases are the same.

Customer support team has taken care of providing services such as reaching new customers, notifications, and alerts to new customers, and answering customer queries. The front-end application is PHP and the backend database is Postgres DB. The team has been placed in Chennai and the customer support application and database are managed by a vendor located in Pune the application and database are hosted in a cloud server located in Dublin.

The perpetrators have used webmail and been hosted on a server located in Hyderabad. Google email service has also been used and the server is located in Delhi.

The perpetrators have also used NAS storage, laptops, mobile phones, printers, POS, and other digital gadgets which may have crucial evidence.

4 Digital Forensic Investigation of Ponzi Schemes

The digital forensic investigation deployed on the Ponzi scheme was either detected by the monitoring system after notification of several red flags or by complaints given by the victims. The intelligence should be gathered prior to the action against the perpetrator who runs the Ponzi scheme. The intelligence should be sophisticated enough to counter the people and technology involved in the scam. The vagueness in the intelligence would seriously affect the course of the investigation and might lose the plot of the whole magnitude involved in the scam.

The perpetrators who run the Ponzi scheme be definitely predetermined, scripted, and made their system more complex and not to get detected and caught. Understanding and dissecting their infrastructure is important to unravel the real magnitude involved in the Ponzi scheme. The search and seizure operation should be carried out with a high degree of caution without leaving the critical premises and persons inclusive of all gadgets associated with the scam.

The identification of systems and gadgets present in the head office and branches are easier when compare to the servers managed and located in the different parts of the jurisdiction. The time-lapse in the action among the target location may lead to a breaking in the chain of investigation as well as loss of evidence.

The confiscation of digital gadgets associated with perpetrators may provide lead to miss may be missed by pre-intelligence. Forensic imaging and analysis of collected digital devices and gadgets have to be performed.

The cloud server and the servers located in the remote location have to be imaged. Webmail and other email server data have to be forensically imaged or copied.

The analysis of all the data from the individual's mobile, pen drive, or laptop to the organization's application, database, and email data.

Cloud server logins and IPs associated with cloud service provider needs to be identified and probed further to check if any other instances or databases are running. Collect cloud logs to identify any deletion activity that took place before or after the action. Identify any column or table or record that has been deleted, removed, or dropped in the database. If found to be deleted or suspected to be deleted or tampered prompt for the backup database from the respective vendors.

The database and other data associated with the Ponzi scheme are subjected to a credibility check. Since the Ponzi scheme involves huge money and people the victims should not be impersonated as perpetrators and perpetrators should not be impersonated as victims.

The digital sweep (screening of all electronically stored information (ESI) associated with the entity) should be deployed to find any "Smart Ponzi scheme" also running under the regular parent scheme. If found deploy proper detection tools to identify such smart Ponzi schemes with blockchain technology.

The complexity of data redundancy and fragility in different servers and databases analysis so difficult. The database used here is MSSQL, MySQL, and Postgres DB and the application used here is Dot.NET, Python, and PHP so the knowledge to interpret the data and evaluate the overall scam is tedious. The perpetrator might delete an important table or column even the database if any of the premises gets missed or can be accomplished remotely or accomplished in lapse time during action.

The database analysis should provide maximum pristine data whereby actual consolidated figures involved in the scam can be figured out. The payouts have already been made and the payouts have to be made need to be assessed in the pool of investors who have received more than what they have invested and the pool of investors who have not received part or full from their investments.

The proper database analysis with other corroborative evidence would give proper figures where victims can be benefitted without any hitches.

5 Hurdles in the Forensic Investigation

5.1 People

The Ponzi scheme is a predetermined scam thus people who are involved as brain children will definitely flee or abscond thus getting investments out of such scams would be difficult to trace and confiscate.

5.2 Infrastructure

By nature, the scheme would fall sooner or later so made the infrastructure systematically difficult to trace and detect.

5.3 Technology

Technological feasibility is exploited here by accomplishing complex infrastructure. Technological versatility needs to investigate such complex technological systems. “Media”—laptop, desktop, server, and mobiles to “Data” Database and Email to “Information” Documents and Spreadsheets to “evidence” Final reporting File.

5.4 Jurisdiction

Policy and law always have a problem when handling jurisdictional tyranny.

6 Trends and Challenges

- Smart Ponzi schemes have come and detection of such would be easier but the identification of source code is challenging [7].
- Tracking of investments particularly in cryptocurrencies is difficult as it's decentralized and peer-to-peer in nature.
- Smart contracts are also hard to track so investment in such platforms by perpetrators would certainly be hard to detect.
- Regular Ponzi schemes and smart Ponzi schemes together made a hybrid model which involves combined traditional investments and crypto investments.

7 Conclusion

The Ponzi scheme is not new eventually identified way back in the 1920s executed by the scamster "Charles Ponzi". The contemporary form of the Ponzi scheme will float always with time to time. Now, technological advancement provides new avenues to accomplish the scam by the perpetrators.

The technology will also help the investigation team, especially digital forensics investigations to detect Ponzi schemes but the nature of the scheme itself scam and the fleeing nature of perpetrators would be made investigations less smooth. The multi-jurisdiction and extra-terrestrial investigations need a lot of time, money, and manpower.

Pre-intelligence prior to Search and Seizure action is so important, especially the scams like the Ponzi scheme.

Proactive is better than reactive or detect. Policy and laws should be amended with respect to the technological phase, crimes, and frauds.

The regulatory bodies have to be vigilant and any red flags raised by the monitoring system should be addressed and investigated and if the absence of red flags with the apparent scams, then the monitoring system should be updated to compete with a phase of the technology, crime, and perpetrator.

References

1. https://www.researchgate.net/publication/324509423_Detecting_Ponzi_Schemes_on_Ethereum_Towards_Healthier_Blockchain_Technology#pf2
2. https://internationalbanker.com/history-of-financial-crises/charles-ponzi-1920/
3. https://en.wikipedia.org/wiki/Ponzi_scheme
4. https://www.investopedia.com/terms/b/bernard-madoff.asp
5. https://www.hindustantimes.com/india-news/84-firms-involved-in-8-ponzi-scheme-cases-in-3-years-centre-in-parliament-101649161707682.html
6. Source: Hindustan Times Published on Apr 05, 2022, 05:58 PM IST
7. https://ieeexplore.ieee.org/document/9407946