© 2018 IJSRST | Volume 4 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Fraud Investigation Related to Cryptocurrency - Bitcoin- A Case Study

Manasa Sastry J. K, Astha Pandey*, M. S. Dahiya, Lawrence H. White M
Assistant Professor, Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, Gujarat, India

ABSTRACT

Background: From the time immemorial there have been several types of crimes. With the advancement in science and technology, digital crimes have become very prominent. One among which is Bit-Coin crypto-currency frauds which are gaining momentum in the types of frauds encountered by law enforcement agencies. Bit-Coin is a growing form of digital crypto-currency that is created and held electronically that has no centralized control systems, that governs the transactions. It is the most secretive form of money transfer between two anonymous people all over the world. It is on a superficial layer used to purchase or sell goods electronically, similar to the conventional dollars that are traded digitally where individual ledgers are maintained by all the bit coin users to have access to the building block-chain. However, a masked layer consists of a dark-net where enormous amounts of money are concealed in cold storage where illegal websites and illicit commerce like ATM/ Debit/ Credit Card scams subjecting to illegal transactions rule over the deep net by utilizing the innocent public money.

Case Presentation: The present study involves a case study where it was noted that innumerable ATM Debit/Credit Cards were skimmed and the illicit money was exchanged with this crypto-currency using an illicit website for bit coin mining and storing huge amounts of anonymous public money that was dictated by a few Nigerian Fraudsters running this racket all over the nation.

Keywords: Bit coin, Blockchain, ledger,Websites, ATM/ (Automated Teller Machine) Debit Card Scam

I. INTRODUCTION

Bitcoin is a worldwide crypto-currency and digital payment system[1] called the first decentralized digital currency, since the system works without a central repository or single administrator[1,2] .It was invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto[3] and released as open-source software in 2009[4]. The system is peer-to-peer, and transactions take place between users directly, without an intermediary.[1] These transactions are verified by network nodes and recorded in a public distributed ledger called a blockchain[5].

Bit coin is a form of digital currency that is created and marketed electronically with no centralized governing systems to monitor the humongous amounts of transactions[6]. It is the most secretive form of communication and money transfer between two anonymous people worldwide. Digital currency is the most fast growing technological makeover to the world that is the next replacement to the conventional paper currency. Bit Coins, as a cryptocurrency was apparently founded by **Satoshi Nakamoto** in 2009[7].

In the month of November 2016 the Indian Government has declared sudden demonetanization process due to which there was apnea of money felt

between many of the citizens as there was limit of money withdrawal from various ATMs (Automated Teller Machine). The main purpose of the government was to make India Digital and increase the number of digital transactions. Due to the above reasons many people have opted for online money transaction system i.e. Bitcoin as a safe store of value. But there are no laws related to regulation of Bitcoin and thus there are many chances of illegal work or transactions being done through this channel.

Thus with the increase in digital transactions and e-business there are many chances of cases like drug trafficking, human trafficking and money laundering cases to rise and one among them in digital frauds which is catching an eye of law enforcement agencies is frauds related to Bitcoin.

The biggest hack of bit coins is that no single financial institution controls the block chain of bitcoin network, but it is a digital file that is maintained on a ledger that contains names and balances and gain access to the available spendable balance as per the corresponding transactions. It completely works on peer-to-peer network but however these online financial transactions are made amongst impersonal users worldwide. A major featureof this is that the ledger is an open accounts book for all the users who additionally have an account of the bit coins spent or transacted between two users.

The entire understanding relies upon the cryptographic hashes that are assigned to particular bit coin user or account numbers that is attached to a bit coin wallet that has a respective address that dictates the authentic transfer of bit coins whose validation is done using computerized mathematical algorithms using a private key that determines the digital signature value to the message thereby encrypted by the sender whilst, the recipient uses their public key to decrypt the same and validate the transaction using a different algorithm. Transactions remain authentic and validated as the digital signature is transaction specific and the same bit coin cannot be bought or sold the 2nd time. Each bit coin user in the bit coin network has a global access to all the transactions as the loophole of this trade involves anonymity of end users and their transaction time stamps. Adding to this, there can be no trace of the transaction whatsoever, but is recorded on the block-chain that is encoded onto the bit coin itself. Bit coin mining is where bit coins are released to come to circulation that involves solving a computationally difficult equation/ puzzle to discover a new block that is added to the block chain to receive rewards as a few bit coins that gets bagged to the individual's wallets and the release of bit coins is reduced every 4 years to maintain the demand in the stock market.

Very recently, in dark net and other deep websites, the online purchase of the illegal drugs and weapons occur via transactions that are run by bit coins in the illegal market and is currently growing to be a rampant form of cybercrime.

Case Presentation:

In one of the recent cases, in Bangalore City (India)[9], it was noted that innumerable ATM Debit/Credit Cards were skimmed and the illicit money was exchanged with this cryptocurrency using an illicit website for bit coin mining and storing huge amounts of anonymous public money that was dictated by a few Nigerian Fraudsters running this racket all over the nation. The technical analysts at our laboratory found the lead through a travel booking agent "via.com" as the source for ATM Fraud and an Indian accomplice who helped the fraudsters to store money in cold storage currency. Around 14 people were found as accused; however we were able to nab the rest eight correspondents.

MO (Method of Operation) of the accused

Most of the hard core criminals have their own modus operandi, i.e. method of operation. Even in this case

there was a specific signature which was noted. The main accusers female associate bought a magnetic card reader and prepared a card reader strip and later parceled it to the accused. He sold the same to his allies and the gang would insert it in various ATM Kiosks to read the magnetic data present on the innocent public's Credit/ Debit Cards. By doing so they were stealing the PIN (Personal Identification Numbers) numbers and later would remove the reader, prepare a duplicate of the card and swipe them at various goods selling business outlets and ATM Kiosks. Around ten (10) complaints were registered for Fund Misuse using Fake Cards at Banaswadi Police Station and the subsequently a suspicion rose that led to the investigation. The gang then struck a deal with a Bangalore resident and then transferred the money they had illicitly withdrawn, to his account and then received commission for every individual transaction.

II. MATERIALS AND METHODS

The chain of the fraud was found through their social networking site messages and their mobile artifacts. We used certain social media analysis tools and mobile extraction softwares/ applications to retrieve all the deleted and undeleted text messages from Facebook Messenger, WhatsApp and their mobile e-wallets of their bit coin accounts.

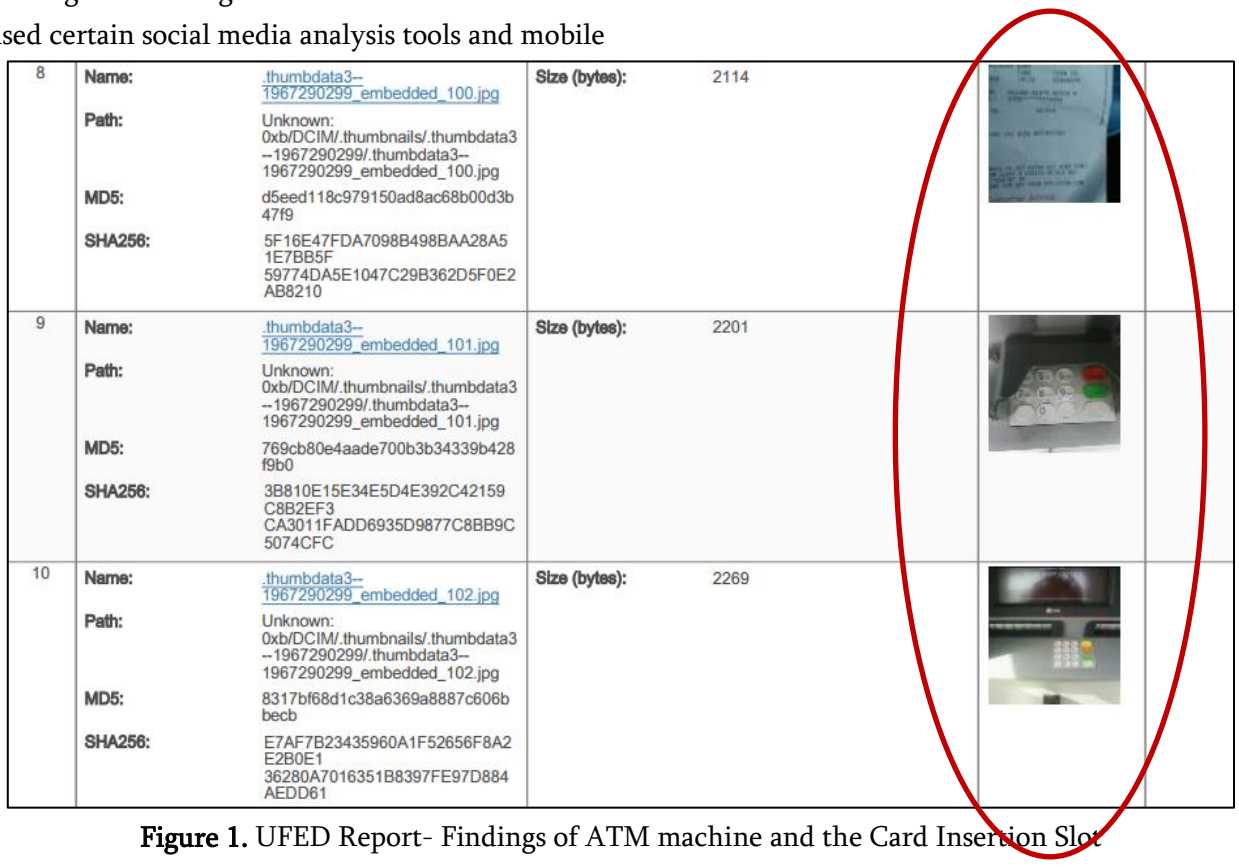
Tools and techniques used:

Technical Analysis for Mobile Data Retrieval:

1. UFED (Universal Forensic Extraction Device) Cellebrite 4PC(Extraction of deleted and undeleted messages and images related to magnetic card readers)
2. Magnet Axiom (Data recovery from all the mobile phones and the laptops)
3. EnCase Forensics (Hard Disk Imaging and Recovery of Deleted Data)

Social media Examination:

1. X1 Social Discovery (It was used for analysis of the Facebook Media and Messenger)



8	Name:	.thumbdata3--1967290299_embedded_100.jpg	Size (bytes):	2114	
	Path:	Unknown: 0xb/DCIM/.thumbnails/.thumbdata3--1967290299/.thumbdata3--1967290299_embedded_100.jpg			
	MD5:	d5eed118c979150ad8ac68b00d3b47f9			
	SHA256:	5F16E47FDA7098B498BAA28A51E7BB5F59774DA5E1047C29B362D5F0E2AB8210			
9	Name:	.thumbdata3--1967290299_embedded_101.jpg	Size (bytes):	2201	
	Path:	Unknown: 0xb/DCIM/.thumbnails/.thumbdata3--1967290299/.thumbdata3--1967290299_embedded_101.jpg			
	MD5:	769cb80e4aade700b3b34339b428f9b0			
	SHA256:	3B810E15E34E5D4E392C42159C8B2EF3CA3011FADD6935D9877C8BB9C5074CFC			
10	Name:	.thumbdata3--1967290299_embedded_102.jpg	Size (bytes):	2269	
	Path:	Unknown: 0xb/DCIM/.thumbnails/.thumbdata3--1967290299/.thumbdata3--1967290299_embedded_102.jpg			
	MD5:	8317bf68d1c38a6369a8887c606bbecb			
	SHA256:	E7AF7B23435960A1F52656F8A2E2B0E136280A7016351B8397FE97D884AEDD61			

Figure 1. UFED Report- Findings of ATM machine and the Card Insertion Slot

546	**Name:** **Path:** **MD5:** **SHA256:**	IMG-20160914-WA0016.jpg Unknown: 0xb/WhatsApp/Media/WhatsApp Images/IMG-20160914-WA0016.jpg 4aa36c850bade53ebf2517f672c26f49 577C9821697ACAECAE8707CEE00E6201 75845E9E6743BDD05D78BA76883A214C	**Size (bytes):** **Created:** **Modified:** **Accessed:**	69556 14-09-2016 15:55:16 14-09-2016 15:55:16 23-11-2016 00:00:00		Yes
547	**Name:** **Path:** **MD5:** **SHA256:**	IMG-20160914-WA0017.jpg Unknown: 0xb/WhatsApp/Media/WhatsApp Images/IMG-20160914-WA0017.jpg 1faf1135760461992e0f93006141d0a8 9769D50221DF5CC0AF7967D3C BA81BA1 16CB31B2E54B2A5FF18FBC1F3E1B1027	**Size (bytes):** **Created:** **Modified:** **Accessed:**	16990 14-09-2016 15:59:24 14-09-2016 15:59:24 23-11-2016 00:00:00		Yes
548	**Name:** **Path:** **MD5:** **SHA256:**	IMG-20160914-WA0018.jpg Unknown: 0xb/WhatsApp/Media/WhatsApp Images/IMG-20160914-WA0018.jpg f1e3455333aeae5dbff1dd07efac44e0 BF77AFD1D37B1EEE2C5309C002B76402 49928C5848A7DE8A0861BF0D14ACC1C4	**Size (bytes):** **Created:** **Modified:** **Accessed:**	141071 14-09-2016 16:05:32 14-09-2016 16:05:32 24-01-2017 00:00:00		Yes
549	**Name:** **Path:** **MD5:** **SHA256:**	IMG-20160914-WA0019.jpg Unknown: 0xb/WhatsApp/Media/WhatsApp Images/IMG-20160914-WA0019.jpg 5298e18399f9fb9afc9206ebb461707e FEDBA168CD1D3A2B45B28C817D100220 5A89320DBDD47F641F9854A184AD3B34	**Size (bytes):** **Created:** **Modified:** **Accessed:**	33067 14-09-2016 16:05:20 14-09-2016 16:05:20 23-11-2016 00:00:00		Yes

Figure 2. UFED Report- Findings of ATM Kiosks and Skimmers and Magnetic Card Readers recovered from their phones

III. RESULTS AND DISCUSSION RESULTS AND DISCUSSION

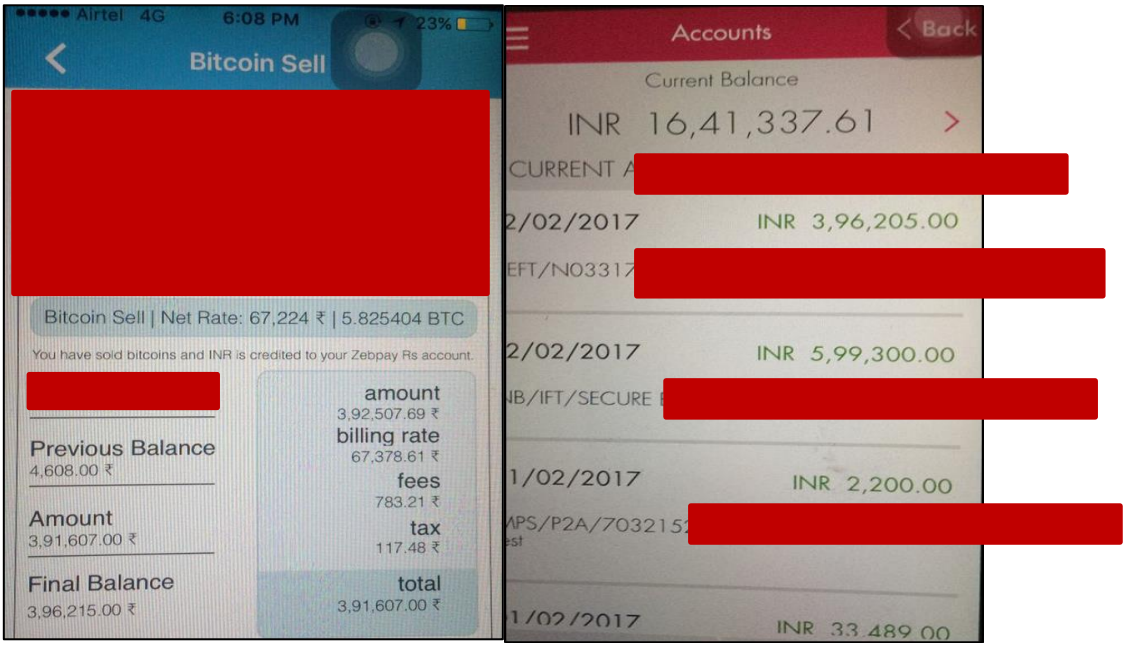


Figure 3. Snapshots of the e-wallet balances on their bit coin accounts wallets.

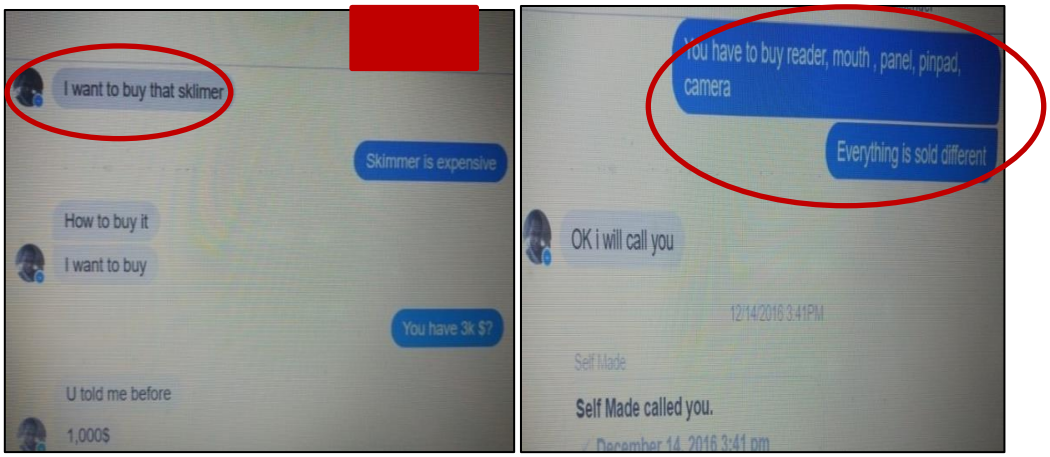


Figure 4. Facebook Messenger conversation between the accused

IV. RESULTS

Figure 4 describes about the Facebook Messenger conversation between the accused. It was noted that the fraudsters hadpreplanned the scam in India by co-ordinating with their Indian accomplice and their national's conman job well organized to spot their victims and hence paved a quick way to launder money. They made communications through social networking sites like Messenger and Facebook and finally integrated their money to the kingpin of this racket as shown in the figures named as Image 5 and Image 6.

The money obtained thereby has been refelected in their e-wallets on the involved person's bit coin account owned by another fraudster who helped them sequester huge amounts in the form of bitcoins as shown in the figures named as Image 3 and Image 4.

The UFED Mobile Extraction Report of the mobile phones of the accused aquitted at the Laboratory shows the transferred images of the ATM Kiosks, magnetic reader and other parts of the ATM Machines amongst the fraudsters and in turn these findings helped the Police Department to progress with the investigation of the mentioned Nigerian Financial Crime.

V. DISCUSSION

Ultimately using the evidences obtained from the extraction and data retrieval, we found a chain of suspects hailing from Nigeria who used the help of an Indian accomplice to store their illicit money that amounted to 21.4 lacs (approx.) on his unlicensed website in the form of bit coins.

For the purpose of our study, we have devised and used our corporate methodology and digital protocols using the emulated devices to provide a highly authentic and validated report on our respective findings/result obtained from the smart phones and the laptops.

VI. CONCLUSION

The above type of investigation is highly useful and eye opener to the law enforcement agencies. In the future there might be several cases related to drug trafficking, human trafficking related to digital crimes or say for that matter another bit coin case. Therefore prevention is better than cure, thus there should be stringent guidelines in terms of law and regulations related to Bit coin in India.

VII. ACKNOWLEDGEMENT

We are highly thankful to Incognito Forensics for all the needful for solving the case and helping in forensics digital investigation.

Conflict of Interest: The authors do not have any conflict of interest.

VIII. REFERENCES

[1]. Jerry Brito & Andrea Castillo "Bitcoin: A Primer for Policymakers" . Mercatus Center. George Mason University.

[2]. Sagona-Stophel, Katherine. "Bitcoin 101 white paper" November 2015

[3]. S., L. "Who is Satoshi Nakamoto?". The Economist. The Economist Newspaper2 November 2015.

[4]. Davis, Joshua "The Crypto-Currency: Bitcoin and its mysterious inventor". The New Yorker. 2011.

[5]. The great chain of being sure about things". The Economist. The Economist Newspaper Limited. 31 October 2015.

[6]. Retrieved fromhttp://www.investopedia.com/terms/b/bitcoin.asp

[7]. Nakamoto, Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2009. Unpublished Manuscript.

[8]. Refer the news update retrieved from http://www.deccanherald.com/content/595993/6-africans-among-7-arrested.html; 2017