

# Pseudonymous not Anonymous - The Forensic and Investigative aspect of Bitcoin Cryptocurrency

Dr. Deepak Raj Rao G.

Cyber Forensics Division

LNNJ National Institute of Criminology and Forensic Science

**Abstract** – Various new technological breakthroughs happened with the advent of Internet which made the Communication, Commerce, Banking and Governance, etc., easy and simple. Ecommerce, online banking, Digital Signature and Cloud Technology changed the Business and Commerce to new height. Online banking offers four benefits to the consumers like speedy, no queue, availability and digital and the invention of Bitcoin [1] in the year 2009 by Satoshi Nakamoto not only bring new avenue for financial transaction but also new challenges for the Law Enforcement Agencies in the investigation of crimes. There are so many myths such as all the transactions done using Bitcoin are anonymous and there cannot be any kind of digital evidence available if a Bitcoin is used while doing a crime. These myths about the Bitcoin need to be addressed for the performing better investigation in any crime done using Bitcoin. A study was conducted to find the availability of digital evidence that is created if Bitcoins are used to do any online financial transaction. This paper will provides the information found from the study on the various traces that gets created when using a Bitcoin for doing any kind of online financial transaction. Using these, it will be very helpful for the investigating officer in investigating the crimes in which Bitcoins are used.

**Keywords**– Bitcoin, Cryptocurrency, Blockchain, and Satoshi.

## I. BITCOIN THE CRYPTOCURRENCY

Bitcoin is a kind of digital cash that is created and transacted using mathematical formulas. The main difference between Bitcoin and other kind of cash is that there is no banking institution or third party to record or maintain the transactions. Bitcoins are created using open source cryptographic protocol in which all the transactions between the users will be computationally impractical to reverse and it is protected from frauds [2]. The transactions are done mainly through the Peer-to-Peer (P2P) protocol. In P2P, a network is built in such a way that the users will broadcast the transactions between each node computer independent of Internet Service Providers (ISPs). This is done to maintain the records of each transaction transparent and to avoid any kind of third party influence in the market value of Bitcoin. It has no intrinsic value like other currency and cannot be redeemed for any other commodity like gold, silver or precious metal.

The supply of Bitcoin cryptocurrency is not determined by any centralized financial institution such as Reserve Bank. It is totally governed based on the concept called Open Source and its entire network is decentralized [3]. Creation and supply of Bitcoin Cryptocurrency is entirely controlled by the algorithm created by Satoshi Nakamoto. Using this algorithm it is possible to create 21 million Bitcoins and it has got a time frame to by which it may

not exceed the year 2140. So far 16.8 million Bitcoins has been create or mined from the different parts of the globe [5].

The Bitcoin is created using a process called “mining” in which all the transactions done by the owners of Bitcoin are recorded and sealed by the cryptographic calculation known as “hashing”. The person who seals the transaction with the defined hash value will get one Bitcoin. It started with the first Bitcoin created by Satoshi Nakamoto in the P2P network that was connected with few computers. Now it has distributed all over the globe and all the transactions done across the globe using Bitcoin will be recorded at each mining computer to calculate the sealing hash value in order to earn a Bitcoin. If anyone wants to record a wrong or fraudulent transaction then the node computers which are involved in mining will reject this record. This indirectly means that all the transactions that are happing using Bitcoin are recorded and it will be available whenever it is required.

In USA, Bitcoin is legal but is not an approved currency and it can be considered a property but not as a currency according to Internal Revenue Service, US. In India, there is no legal validity to the Bitcoin Cryptocurrency and it is illegal to use for any purpose.

### 1. Storing the Bitcoin Cryptocurrency: Wallet

Generally expenses we keep some amount of case in our hand wallet so that our money can be kept safe from theft and robbery. Bigger amount of money is kept in the

saving account of bank where it can be accessed either physically or online mode. In cryptocurrency, a “Wallet” is equivalent of a bank account. Here, the wallet provides an easy mode for a person to use for all kinds of transaction and also provides the required security [4]. A wallet stores and manages the security keys required for the transaction that is private and public key along with the transaction details. It always checks the global block chains to receive any kind of transaction to be received or to send any kind of transactions to other wallets. Based on this information it will update the individual account details.

When a wallet holder wants to send his cryptocurrency available in his wallet to someone else, he will use the public key of the receiver as the address and release the funds of his public keys by signing the transaction with the corresponding private key [5].

#### The different stages in Bitcoin Transactions

A transaction that needs to be done using Bitcoin has to be done from a place called Wallet. A wallet is nothing but a file in a computer especially the server which provides access to various Bitcoin addresses. An address of the Bitcoin is a string of letters and numbers (for ex. 1n6sLis8eOIilEe8kcleqtelnHwLG) which is a “Cryptographic Key Pair” generated by the algorithm that contains a public key and private key (Asymmetric Cryptography). Each address may have its own balance of Bitcoin available in it and this can be easily verified that to whom it belongs.

For Example: If a receiver wants the Bitcoin from the sender then the receiver needs to generate the address using the key generation mechanism available in the wallet. This will generate two keys that is, a Private key and Public Key. The private key is kept secretly in the wallet and the public key is sent to the sender of the Bitcoin. Once the sender receives this public key he will transfer the amount of Bitcoin to that address and sends it to the Transaction Verification where it is stored in a bundle called Transaction Block [5,6].

## 2. Blockchain

It is the bundle of transactions done by all the wallets in the whole network and stored for two different purposes, the first one for verification and other one for mining a new Bitcoin. As all the transactions are happening in the virtual medium, it is important to have a mechanism in which if there is any doubt on a particular transaction then it can be rechecked that between whom this transaction has taken place. This bundle of transaction provides the details of all the financial activities done using Bitcoin. If someone stores and processes the data then he needs to be rewarded but the reward needs more amount of computation and power [5,6].

In order to reward, the bundle of transactions must be calculated in such a way that it must create a unique type

of Hash Value. That is a particular number called “Nonces” need to be added to the bundle of transaction and when the hash from the total value must contain multiple zeros after decimal. If anyone gets the correct hash value then this bundle transaction called Block is completed and new Block is started to create the bundle from the hash value that was generated from the previous block. This way it is a continuous process making blocks and that is why it is called Block Chain. Since finding the Nonce value is a difficult task, the person who found it first will be awarded with one Bitcoin. The method of getting a Bitcoin is called “Mining” of Bitcoins.

In this transaction, it is clear that the information about the sender and receiver with time stamping is available in different locations called nodes. The investigating agency or the forensic expert needs to find which transaction has taken place between whom by analyzing the information stored in the nodes in the whole network.

#### Transactions of Bitcoin Cryptocurrency

Transaction is the important component that provides the information about the transfer of Bitcoin amount. It tells the network who is the owner of the particular Bitcoin and who has authorized the transfer of that Bitcoin denomination to the receiver [6,7]. In order to confirm the transfer of Bitcoins, the transaction must be recorded to the global ledger for everyone to see. This means that it is included in a block that will be mined on the Blockchain. To be included in a future block, this transaction must be propagated to many nodes of the network.

## 3. Handling the Scene of Crime with Bitcoin Cryptocurrency

The Bitcoin of the suspect needs to be preserved as a co-conspirator can access the wallet and drain out the Bitcoins. Before going to the scene of crime the Investigating Officer must have access to the Investigating Agency’s Wallet where the seized Bitcoins are and be transferred. It might not be possible to transfer the seized Bitcoins immediately to the agency’s wallet, in such a case the Investigating Officer must see to it that the electronic device i.e., Mobile Phone, Laptop, Desktop Computer etc, must be kept on and see to it that it might not get screen locked or go to sleep mode. If required, help from the expert may be taken to handle the devices.

## 4. Seizing the Bitcoins from the Encryption Protected Wallet

According to the Regional Organized Crime Information Centre, Special Research Report on Bitcoin and Cryptocurrencies Law Enforcement Investigative Guide the following step by step process needs to be followed for seizing the Bitcoins from the encryption protected wallet [5].

### Step 1

As in all cases involving evidence, responding personnel should thoroughly document the scene. When a Bitcoin

wallet is discovered, access to it is often protected by encryption. In the event the suspect's computer or mobile device is unlocked, follow best practices for maintaining the current state of the device to prevent it from locking inactivity [5].

#### Step 2

Ensure that the Investigating Officer has access to the Investigating Agency's Bitcoin wallet. All the required credential to access the wallet must be available with the IO. In case, if there is no existing Investigating Agency's Bitcoin wallet, DO NOT use a personal Bitcoin Wallet. Without an official Bitcoin wallet, it is not possible to proceed for seizing the Bitcoins of the suspect. So, follow the property seizing procedure [5].

#### Step 3

To transfer a suspect's Bitcoin to an Investigating Agency's Bitcoin wallet, the IO must have access to the private keys within the suspect's Bitcoin wallet. Getting the suspect to volunteer the encryption code is the easiest method of access. If the suspect will not volunteer the encryption code, the device on which the encrypted wallet exists should be seized by following the normal exhibit seizing procedure [5].

#### Step 4

Depending on the type of Bitcoin Wallet encountered, follow the below process [5].

**Mobile Wallets:** If the suspect is using a mobile wallet the process for making a transfer is relatively simple. In the suspect's wallet, navigate to the transfer or send tab. Enter the Investigating Agency's wallet's address or scan its QR code in the space labeled recipient. Enter the full value of the wallet as the amount to be transferred. Then press transfer or send to move the funds to the Investigating Agency's wallet [5].

**Software wallets:** Generally, funds can be obtained from a software wallet using the same method as mobile wallet. However, with a software wallet, the suspect's private key may be available either within the wallet or stored elsewhere on the device. Access to a suspect's private key gives indefinite access to the accounts associated with those keys. While it is not recommended that the officer attempt to access the private keys, it is important that the device is treated as encrypted device and seized, even if the officer can transfer the Bitcoin [5].

**Online Wallets:** If the suspect is using an online wallet, police can use the above method to transfer funds. Because online wallets use a third party to store Bitcoin funds, that third party can freeze account and assist in the seizure of funds left online. Police can do so using the same method to freeze traditional bank account [5].

**Hardware wallets:** Because hardware wallets are external memory or paper QR codes containing private keys they

must be loaded into a wallet that allows private keys to be imported. For an IO seizing the property of a suspect, it is sufficient to secure the hardware wallet and get it into the hands of the Chain of custody [5].

It is important to remember that a wallet may actually have multiple files that are holding Bitcoin separately. If an IO is transferring funds from an open or unencrypted wallet, they should ensure that there are not multiple files in the wallet. There should be a tab that allows all the wallets within the program to be viewed. It is possible that individual wallets may be separately encrypted within the program. If that is the case, then the device should be seized as an encrypted device [5].

### 5. Seizing the Bitcoins from the Encryption Protected Wallet

Regional Organized Crime Information Centre, in its Special Research Report on Bitcoin and Cryptocurrencies Law Enforcement Investigative Guide has also provided the step by step process need to be followed for seizing the Bitcoins from the not encryption protected wallet [5].

#### Step 1

As in all cases involving evidence, responding personnel should thoroughly document the scene. When a Bitcoin wallet is discovered that is not protected by encryption, the IO has got the complete access to all available Bitcoins. In the event the suspect's computer or mobile device is unlocked, follow best practices for maintaining the current state of the device to prevent it from locking from inactivity [5].

#### Step 2

Ensure that the IO has access to the Investigating Agency's wallet and know all the credential of the wallet. If there is no Investigating Agency's wallet, DO NOT use a personal Bitcoin wallet. Without an official Bitcoin wallet, it is not possible to proceed for seizing the Bitcoins of the suspect. So, follow the property seizing procedure [5].

#### Step 3

Depending on the type of Bitcoin wallet encountered, follow the same procedure followed in the encryption protected wallet [5].

#### Step 4

By successfully transferring Bitcoins from the suspect's wallet to the Investigating Agency's wallet, the suspect is no longer in possession of the Bitcoins. Investigating Agency's wallet should have controlled access to maintain accountability and integrity in the preservation of the digital evidence [5].

#### Tracing the Bitcoin using Forensic Tools

There exist various forensic tools to trace the transacting of Bitcoins and it is of both proprietary and open source.

Few tools those are openly available for the public use is discussed here as it may be easily accessible to the Investigating Officer [5].

### 6. Blockchain Explorer

Blockchain Explorer is accessible at <https://www.blockchain.com/explorer> and it provides lots of information and details about addresses, transactions and blocks. For example, IO can search by a public address to inspect the transactions associated with it. It has also got a feature to provide charts on Bitcoin statistics, such as the network hash rate and exchange rates. However, in order to carry out a forensic investigation, it will often be necessary to follow the path of funds between addresses, which would be simplified if it were possible to do this graphically; Blockchain Explorer does not provide a graphical interface [6].

### 7. Chainanalysis

Chainanalysis is a company which has built a proprietary software solution for digital blockchain forensics. Though it is not clear how Chainanalysis provide the traces, or how, other than through the information used to advertise their product. It has 3 main categories of customers and describes features they can offer to target each type of customer individually. The types of customers and their associated features are:

Financial Institutions: Focus on meeting Anti-money laundering (AML) and Know Your Customer compliance obligations and a tool for due-diligence and detecting suspicious activity.

Cryptocurrency Exchanges: Focus on AML obligations and due-diligence (similar to financial institutions offerings)

Government: Features for suspect identification, criminal revenues and machine learning based pattern recognition [8].

### 8. Wallet Explorer

Wallet Explorer is a web based tool which provides similar capabilities to Blockchain Explorer in terms of inspecting addresses individually. It also provides a list of known entities and the public addresses which they are known to be mapped to. This is extremely useful information in understanding patterns of use and the main players in the Bitcoin network. However, this data is represented in quite a difficult to use format; it is not linked with network activity and therefore, on its own, it is not very useful in carrying out forensic investigations [9].

### 9. Blockpath

Blockpath is also a web based application that claims to be a Bitcoin accounting tool. The feature of this site that was the most interesting is the graphical explorer. The

graph allows exploring the relationship between addresses. However, there does not appear to be any mapping of multiple public addresses to a single entity (i.e. clustering), which would be vital to gaining real insights when performing forensic analysis.

## II. CONCLUSION

Much of the illegal purchase and sale of good takes place using the Bitcoin Cryptocurrency. They are traded in the Dark Web to make anonymize the criminal activities and illegal business but the transactions can ultimately be traced. Activities of bitcoin whether done through legitimate exchanges or personal or business financial records, all the money have a start and endpoint. Since all transactions to occur in Bitcoin are available to view by the public, Bitcoin can only offer pseudo-anonymity rather than real anonymity [6,10]. The forensic investigation done on the Bitcoin transaction shows that it is possible to de-anonymize Bitcoin transactions based on data that is publicly available [6,10]. In order to keep them anonymous like ToR, Mixing tools etc., and various other techniques were adopted by the criminals, by which their IP address, email id, etc., might have been spoofed or changed but still it can be traced based on the pattern of the activities [11]. Bitcoin Cryptocurrencies is Pseudonymous not Anonymous since the method adopted for doing the transaction using cryptocurrency, the user cannot totally be anonymous and the changed identity can be tracked back to the original user if proper forensic tools and techniques are used.

## REFERENCES

- [1]. Smith, C. 4 Advantages of Online Banking. Retrieved January 21, 2014, from Account Now: <http://www.accountnow.com/content/online-banking/4-advantages-of-online-banking-2/>
- [2]. Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash, Bitcoin.com (Nakamoto 2009), Accessed on Jan, 5 2020.
- [3]. Hochstein, Marc. Why Bitcoin Matters to Bankers, American Banker, March 14, 2014 edition.
- [4]. Shaw, R.. What is Bitcoin?, 2013, June 28. Accessed on Jan 6, 2020, from Infosec Institute: <http://resources.infosecinstitute.com/bitcoin/>
- [5]. Bitcoin and Cryptocurrencies Law Enforcement Investigative Guide, ROCIC Publication, 2018, (<https://www.iacpcybercenter.org/wp-content/uploads/2018/03/Bitcoin.pdf>). accessed on Feb 3, 2020.
- [6]. Eden, Callum, SherBlock Holmes: Digital Blockchain Forensics, Imperial College London, June 2019.
- [7]. Andreas Antonopoulos. Mastering Bitcoin, 2nd Edition. O'Reilly Media, Inc, 2 edition, Jun 21, 2017. ISBN 9781491954386.

- [8]. Max Baylis. Blockchain data analytics and health monitoring. Technical report, Imperial College London, September 7 2018.
- [9]. Walleexplorer.com: smart bitcoin block explorer, . URL <https://www.walleexplorer.com/>. Accessed: January 25, 2020.
- [10]. Malte Moser. Anonymity of bitcoin transactions an analysis of mixing services. 2013
- [11]. M. G. Reed, P. F. Syverson, and D. M. Goldschlag. Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communications, 16(4):482–494, May 1998. doi: 10.1109/49.668972.

### **AUTHOR'S DETAILS**

Dr. Deepak Raj Rao G., Assistant Professor. Cyber Forensics Division, LNJN National Institute of Criminology and Forensic Science, MHA, Government of India, Delhi-85. Email: [gdeepakrajrao@gmail.com](mailto:gdeepakrajrao@gmail.com)