Risk and analysis of Bitcoin and Blockchain

Shivam Gupta[1], Prof. Jamvant S. Kumare[2]
[1]Department of Cyber Security
[2] Department of CSE & IT
[1,2] MITS, Gwalior, India

Abstract- *In recent year digital cryptocurrencies like bitcoin, litecoin etc. has established as an safe and fast way of money transfer. That is because of its decentralized anonymous peer to peer system. The Bitcoin System is good but is widely being used in illegal activity. Bitcoin can be used in money transfer peer-to-peer without even using third party.*

This is a hot topic in research community of forensic invetigatrors to research on the anonymous system of bitcoin and revealing as much as ionformation they can so that it can help the cyber crime investigation process. Unfortunately, given the high volume of the introduced techniques, the literature lacks a comprehensive review of investigation techniques and methods for bitcoin..

Keywords- blockchain, bitiodine, litecoin

I. INTRODUCTION

Bitcoin is just another currency. The term Bitcoin refers to the entire currency system, whereas bitcoins are the basic units of the currency. As with dollars, euros, yen, and gold coins, you can save bitcoins, spend them on goods and services, and exchange them for other currencies. owever, Bitcoin is the world's first currency that is both digital and decentralized. A digital currency is one that can be easily stored and used on a computer. By this definition, even dollars can be considered a digital currency, since they can be easily sent to others or used to shop online, but their supply is controlled by a centralized bank organization. In contrast, gold coins are decentralized, meaning that no central authority controls the supply of gold in the world. In fact, anyone can dig for gold, create new coins, and distribute them. However, unlike digital currencies, it's not easy to use gold coins to pay for goods (at least not with exact change!), and it's impossible to transfer gold coins over the Internet. Because Bitcoin combines these two properties, it is somewhat like digital gold. Never before has there been a currency with both these two properties, and its impact on our increasingly digital, globalized world may turn out to be significant.

II. BITCOIN HISTORY

Until recently, people could not send digital cash back and forth to each other in a reliable way without a central mediator. A trusted central mediator such as PayPal can track payments and money transfers in a privately held account ledger, but it wasn't clear how a group of strangers who do not trust each other could accomplish the same transactions dependably. Sometimes referred to as the Byzantine Generals' Problem, this fundamental conundrum also emerges in computer science, specifically in how to achieve consensus on a distributed network. Satoshi described the solution to the Byzantine Generals' Problem and the invention of Bitcoin in a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." But the creation of the software that demonstrated the concept in practice was released a year later. Although the first version of the software was written by Satoshi, it quickly became a community project as the software was improved and maintained by hundreds of volunteers. Currently, the software is open source, and anyone can read and contribute to it. In January of 2009, the first bitcoins were distributed using the early Bitcoin software, and since then transactions have been running smoothly. Slowly but surely, an increasing number of people have started using Bitcoin, and what began as an experiment is now a multibillion dollar economy that processes hundreds of thousands of transactions per day (and is growing quickly).

III. THE WHITE PAPER

The Bitcoin whitepaper was released to the public on October 31st, 2008, a couple of months before Bitcoin's blockchain was launched. In the whitepaper, Satoshi explained how the blockchain could support a purely decentralized e-currency without the need for a central authority.

Satoshi writes:

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution.

The whitepaper mentions the issues with relying on the financial institutions as trusted third parties to process transactions. He particularly mentioned the costs of mediating reversible transactions which put merchants at risk of fraud, thus increasing transaction costs. The principal design goal was to ensure that whoever owns the keys controls the money.

The common scenario involves a buyer who orders an item from a merchant using a credit card. As fraud against the merchant, the buyer can dispute the payment or claim an unauthorized payment. In Bitcoin, reversing the transaction is not possible. Satoshi proposed a solution that relies on cryptographic proof. Transactions are signed and distributed on a public network. The design allows irreversible transactions sent directly between peers without centralized authority. He was able to deliver the solution, based on a new type of data structure called the blockchain.

Satoshi Nakamoto

Satoshi Nakamoto has remained anonymous since releasing Bitcoin. Records of his e-mails and forum posts exist from the end of 2008 through 2010. During that time, he worked with developers to release the source code and respond to the development topics. He also commented on relevant financial topics such as banking and fractional reserve lending. As quickly as he appeared, he vanished without much trace. To this day, we don't have much information on him. Many people have theorized about who Satoshi could be, yet nothing we have is conclusive.

IV. BLOCKCHAIN

The public ledger which records each Bitcoin transaction is built on a data structure called the blockchain. Transactions are grouped into blocks, and shared and validated by a network of nodes. Consensus on the network determines which blocks are accepted. Previously, the double-spending problem was difficult to solve without a trusted third party. To be able to accept a transaction, the available balance had to be validated by a central authority, ensuring synchronization between all the transactions. Implementing this in a decentralized way was difficult because of the complexities of sharing data between independent nodes. If two transactions were created at the same time, but with only enough funds available for the first transaction, the second must be rejected: the double spending problem.

The Genesis block

September 15th, 2008 marked a defining moment for the finance industry, as Lehman Brothers, at that time the fourth largest investment bank, filed for chapter 11 bankruptcy after massive losses in stock price and assets. The collapse marked the beginning of the Global Financial Crisis of 2008. Shortly after, Bitcoin, a new type of virtual currency, was launched by an anonymous developer, or group of developers, under the name Satoshi Nakamoto. The software was built on a publicly-accessible transaction ledger, that is distributed and validated by a network of independent nodes. More importantly, its design was powerfully resilient to attacks. The mysterious developer launched Bitcoin at the beginning of 2009. Encoded in the first block of transactions was a message highly relevant to the state of global financial affairs at that time:

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

The first block of transactions, called the "genesis block", set forth Bitcoin, a new peer-to-peer digital currency. As the quoted headline was published by The Times on January 3, 2009, the message acts as proof that the block was indeed created after that time. From the intention of the comment on the failure of fractional reserve lending, we get a glimpse into the mind of its developer, Satoshi Nakamoto.

Simply put, fractional reserve banking allows a bank to lend more money than it has on reserve. The modern financial system largely accepts the practice of fractional reserve banking with policy controlled by a central bank. The central bank's primary method of control is through interest rates.

V. PREVIOUS WORK

1. Master thesis by Sevil Guler, 2015[16] outlines various method and solutions targeting growing security concerns, like increasing identity theft, user anonymity and also aims to understand their effectiveness. It also describe Secure Bitcoin wallet, standard Bitcoin transactions client, enhanced with various security features and services.

2. Drehmann et al, 2002 [7] Bitcoin has no legal tender status in any jurisdiction and very little academic literature to describe and analyze this phenomenon Even though Bitcoin might seem like a new-age innovation, the idea of virtual currencies and their benefit over fiat currencies has been discussed already for several decades.

3. Aaron Yelowitz and Matthew Wilson, 2015 [15] talks about characterstics of bitrcoin users. As per their work The anonymity of Bitcoin prevents analysis of its users. Author collect Google Trends data to examine determinants of interest in Bitcoin.Based on anecdotal evidence regarding Bitcoin users, they construct proxies for four possible clientele: computer programming enthusiasts, speculative investors, Libertarians and criminals. Computer programming and illegal activity

search terms are positively correlated with Bitcoin interest, while Libertarian and investment terms are not.

VI. RISKS IN BITCOIN

Double spending

More importantly, Bitcoin and its technology The Blockchain was released and open sourced to the world. The Bitcoin Blockchain was a solution to the difficult problem of preventing double spending when creating a distributed virtual currency. Double spending occurs when two transactions are accepted with an amount that exceeds the available balance. Up until that time, a decentralized solution to the double spending problem remained open. Satoshi's solution was the Blockchain.

Money Laundering

This is one of the most dangerous issue for government. For user the main risk is for the guarantee that the bitcoin will exist for life time. As there is no central government who controls bitcoin network, so if one day your all bitcoin disappear then you can't claim anyone for that. The decentralized is good as well as bad because it not guaranteed about the existence. The other risk is that the government will not allow you to use the bitcoin. Bitcoin is banned in many countries due to security and money laundering problem. The next one is that when you transact over bitcoin there are possible chances of man in the middle attack. The transaction is encrypted but in some manner it can be captured by attacker and your money can be lost.

Privacy

The Bitcoin payment network offers a highly decentralized mechanism for creating and transferring electronic cash around the world. Unfortunately, Bitcoin suffers from a major limitation: since transactions are stored in a public ledger (block chain) it may be possible to trace the history of any given payment — even years after the fact. Worse, since the Bitcoin ledger is public, any party can recover this information and data mine to identify users and patterns in the transactions. In other words: Bitcoin transactions are conducted in public.

VII. MY ANALYSIS

The invention of Bitcoin and Bloackchain is un-comparable to anything in some manner but in some situation it has lacks of security. There are several software available online and offline that analyze bitcoin transaction and track transactions. First of all we take an address of bitcoin and then analyze and generate a result based on transaction pattern. We use an online based tool named numisight bitcoin explorer for performing analysis

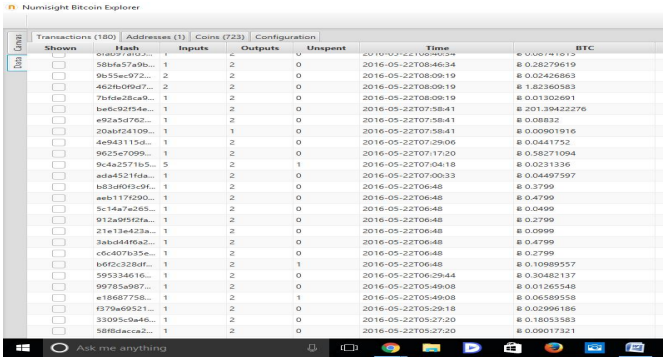
.

Suppose Address to be investigate is –

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

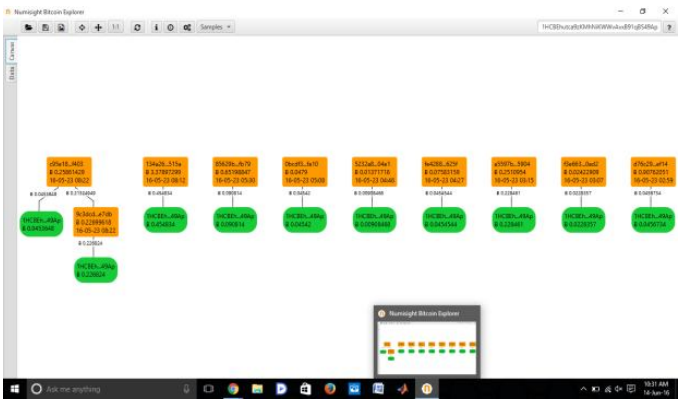
By attaching the address, it will lookup whole the transaction by fetching data from blockchain.

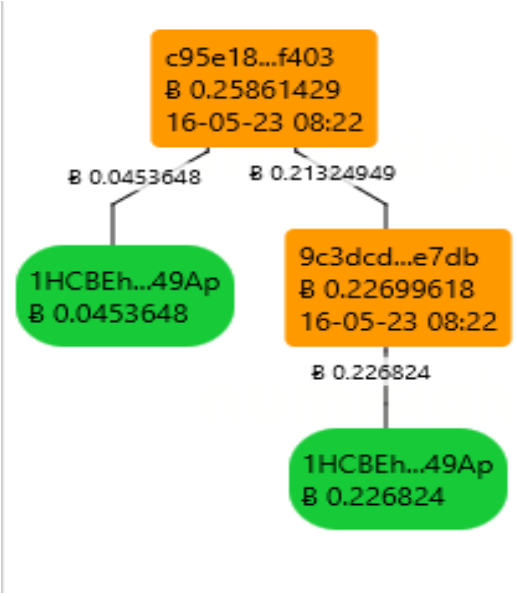
After inserting addresss which we want to investigate, it begins the process



VIII. RESULT AND FUTURE SCOPE

Bitcoin analysis gives us all the transaction detail of that address from beginning to last in list as well as graphical form. The graphiocal representation shows every single transaction in which red color shows the sender while greeen represent reciever.





By analyzing an address we are able to track down the list of transaction and can stop money laundering as well. In future this process can further be extending by identifying user based on the pattern and transactions.

IX. CONCLUSION

This paper concludes that nothing in this world is fully secured. May be today bitcoin gaining popularity but it is difficult for it to be fit in this world as permanent virtual currency. Block chain can gain wide adoption because of its decentralization property which can be used for future implementation of security based techniques.

REFERENCES

[1] Decentralizing Privacy: Using Blockchain to Protect Personal Data-2015 IEEE CS Security and Privacy Workshops

[2] Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk Tyler Moore1 and Nicolas Christin2

[3] Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. Oct 2008.

[4] Joseph Poon, Thaddeus Dryja "The Bitcoin Lightning Network: Scalable O_-Chain Instant Payments" Version 0.5.9.1, (2015)

[5] Saifedean Ammous, "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation, and International Development" The Journal of Private Enterprise 30(3), 19–50, (2015)

[6] Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin "Zerocoin: Anonymous Distributed E-Cash from Bitcoin" IEEE Symposium on Security and Privacy (2013)

[7] Drehmann M., Goodhart C. and M. Krueger, "The challenges facing currency usage: will the traditional transaction medium be able to resist competition from the new technologies?." Economic Policy, 17(34), page 193-228 (2002)

[8] Eli Ben-Sasson, Alessandro Chiesay, Christina Garmanz, Matthew Greenz, Ian Miersz, Eran Tromerx, Madars Virzay, "Zerocash: Decentralized Anonymous Payments from Bitcoin" IEEE Symposium on Security and Privacy, (2014)

[9] F. Reid, Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System" IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing (2011)

[10] Patrick McCorry, Siamak F. Shahandashti, Dylan Clarke and Feng Hao "Authenticated Key Exchange over Bitcoin" (2015)

[11] Tyler Moore, Nicolas Christin "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk"(2014)

[12] Sevil Guler, "Secure Bitcoin Wallet" UNIVERSITY OF TARTU, Master Thesis, (2015)

[13] Narayanan and V. Shmatikov, "Robust De-anonymization of Large Sparse Datasets," in Proceedings of the 29th Symposium on Security and Privacy. IEEE, pp. 111–125(2008)

[14] R. Puzis, D. Yagil, Y. Elovici, and D. Braha, "Collaborative Attack on Internet Users' Anonymity," Internet Research, vol. 19, no. 1, pp. 60–77, (2009)

[15] Aaron Yelowitz* and Matthew Wilson, "Characteristics of Bitcoin users: an analysis of Google search data" in Applied Economics Letters, 2015 Vol. 22, No. 13, 1030–1036

[16] Sevil Guler, "Secure Bitcoin Wallet" UNIVERSITY OF TARTU, Master Thesis, (2015)