National Conference on Recent Advances in Computer Science and IT (NCRACIT)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 1 | ISSN : 2456-3307

Blockchain, Bitcoin and Cryptocurrency: The Three Aspects of Modern Transactions

Tanvi Gupta[1], Aditya Gupta[2]

[1]Department of Computer Science and Engineering, SMVDU Katra, Jammu & Kashmir, India
[2]Department of Computer Science and Engineering, BGSBU Rajouri, Jammu & Kashmir, India

ABSTRACT

Blockchain, the distributed ledger technology has revolutionized the world of online transactions globally. It has various other uses but the most prominent one is the purpose of it serving as an underlying technology for the most popular and successful cryptocurrencies to this date known as the bitcoin. In this paper, we shall discuss about how the bitcoin, blockchain and the cryptocurrencies are integrated with each other and how they complement each other in order to make the online transaction phenomenon more friendly, accurate and efficient. We also review various security vectors and solutions that come across while deploying these techniques. The future possibilities and exploring probabilities of the three aspects is also very briefly discussed in this paper.

Keywords: Bitcoin, Cryptocurrency, Blockchain, Security Vectors.

I. INTRODUCTION

Bitcoin was deployed in 2009 and since its implementation; it has achieved unparalleled and unprecedented success [1]. Since bitcoin cryptocurrency has released more than 600 surplus cryptocurrency have been proposed [2]. Cryptocurrency is a system for exchanging tokens between users underpinned and mathematically verifiable i.e. settles exchange between counterparties that don't trust each other. The bitcoin being the most popular cryptocurrency records all the transactions in an open distributed public ledger i.e. blockchain [3]. The addition of blockchain makes it more interesting as it does not need a third party and the whole structure is thus decentralized. The blockchain is basically is list of records known as blocks which contains all the information related to a transaction and are linked and secured using cryptography. Introducing blockchain in bitcoin made it the first cryptocurrency which overcame an issue of double spending attack without the involvement of any third party or any authority which needs to be trusted or any central server. If blockchain become mainstream, anyone who can access internet can make transactions. Currently according to survey by the global agenda council of the world economic forum, a small part of the world's GDP (approximately 0.025%, or $20 billion) is held in the block chain. However, according to the survey of the forum, banks, insurance companies, high-tech enterprises see this technology as a way to speed up the settlement and reduce costs, so that this will increase significantly in the next years. Security and power are probably the most important characteristic of the currency, and the cryptocurrencies achieved using encryption techniques and decentralized approaches. Decentralization avoids both the point of failure but it is likely to offer forms of

disagreement between the parties [2]. To achieve agreement between the nodes, cryptocurrencies are taking advantage of dividing a mechanism that allows the maintenance of a single system overview of its situation, the blockchain [4]. Blockchain gives us a technology for establishing shared and immutable version between counter parties that are not relaying on each other and even has the potential to create a huge splash in any stream like financial and industrial that completely depends on the third parties. For better understanding the current ecosystem of block chain applications, a scalable proof of concept pipeline for analyzing multiple streams of semi-structured data is posted on social media is always demonstrated which is also based on open source components. Preliminary analysis suggested that the data which was found on deep web is complimentary to that which is available on conventional web. In future the system will scale to cloud based, real time, analysis of multiple data streams with information extraction and machine learning capabilities [5]. Cryptocurrency has been able to deal with peer-to-peer systems, blockchain technology has been developed and being used in financial, financing, and financial systems, but it doesn't have the power to sell [6]. There are 4 major protocols to increase awareness among the users and the investors who are investing in this. **Bitcoin:-**It was proposed by Satoshi nakamoto as a virtual electronic currency and it doesn't involve any third party as it is peer-to-peer cash system. In banking and finance it has been recognized as revolutionizing technology in terms of transaction and their security and privacy. Bitcoin has the following characteristics:

1. There is no involvement of third party for any transaction.
2. Non-reversible transactions are enabled.
3. Doesn't increase credit cost in minor casual transactions.
4. Doesn't increase transaction fees.
5. Double- attack is prevented.

A. Ethereum

It is a computer-aided, open source, and blockchain distributed computer network that includes intelligent contractual operations. The protocol has also provided a decentralized virtual machine called Ethereum Virtual Machine (EVM) and is also called the ether called a global network of nodes called turning-complete scripts [8].

B. Ripple Consensus Network

The Ripple Transaction Protocol has been issued in 2012 and developed on an open source distributed consensus ledger, internet protocol, and aboriginal currency known as XRP (ripples). Ripples basically enables fast, instant, safe and globally free transactions of any scale without any charge. This protocol supports fiat currency, token based currency, commodity, mobile minutes, etc. [8].

C. Hyperledger

It was introduced in 2015 by Linux Foundation as an open source blockchain platform to support blockchain based distributed ledgers. This protocol's ledger was developed to support international business transactions, technological and supply chain business, with the motive of improving performance and reliability aspects [8].

II. BITCOIN WALLET

Bitcoin wallets contain private key, secret codes that allow you to spend bitcoins. Basically it's not bitcoins that need to be stored instead it's the private key that needs to be stored, which gives excess to bitcoins. A bitcoin wallet is actually an application, website, or device that manages bitcoin private key. There are two types of wallet:

1. Hardware wallet
   a. Ledger nano s
   b. Trezor
   c. Keepkey
2. Hot wallet

A. Hardware wallets

These are physical electronic device which are built for the sole purpose of securing bitcoins. This hardware wallet must be connected to your mobile or tablet before spending bitcoin. Wallets are the easiest way to secure bitcoin, easy to backup, setup is even easy for non-technical users. These hardware wallets are not free as in we need to buy them with money.

B. Hot wallet

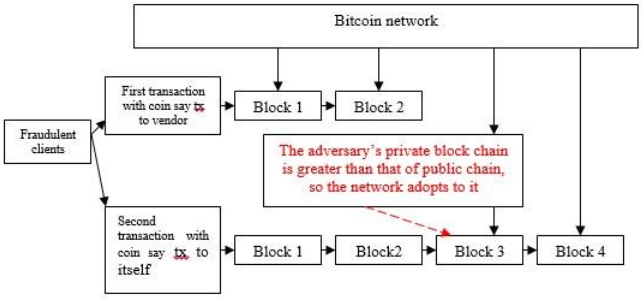
These wallets run on internet connected devices. These wallet generate private key on internet which makes them more secure. They can store small amount of bitcoins, these are convenient i.e. receiving and spending payments are easy and fast. These are not good for storing secure large amount of bitcoins. The following table shows different kinds of wallet [3].

III. ATTACKS

A. Double Spending Or Race Attack

This attack occurs when same Bitcoin has been spent in multiple transactions. Two conflicting transaction has been send in rapid succession. This attack is primarily targeted to either seller or merchants. In this attack the sellers has to go through the loss as they lose away the product which creates block chain forks [9]. To overcome this attack we can insert observers in the network, communications alerts must be there among peers, nearby peers can also notify about the double spending attacks to merchants, merchants can disable the direct communication or direct incoming connections [10]. The following table shows how double send attack can happen [9]

Finney attack: - The finny attack considers a deceitful and immoral miner who specifies and shows a pre mined block so that when the product is received from a merchant, the double spending mischief is achieved [3]. The attack is primarily targeted at sellers or merchants. The attack has adverse effects on the sellers and merchants who not only lose their products but also their customers. Remedial measures such as the presence of a network observer, disabling the direct incoming connections can help to countermeasure the nature of such attacks.



B. Brute force attack

Brute force attack is also an attack which considers the blunder of double spending. It is done by privately mining the blockchain fork [10]. This also is primarily targeted at merchants and sellers. The counter measuring to this attack can be done by confirming the transactions repeatedly.

C. Vector 76 Or One-Confirmation Attack

Vector 76 or one confirmation attack is the collaboration of the double spending and Finney attacks [3]. The primary target of such attacks are the bitcoin exchange services.

D. Block Discarding Or Selfish Mining

Block discarding or selfish mining is the process of misusing the feature of bitcoin forking so as to achieve an unfair reward in a deceitful manner [3]. The miners who are honest and proper are effected by such attacks. Techniques such as zero block technique can be used as remedies.

E. Block withholding

Block withholding is an attack where the miner submits only the ppows (proof of work) and not the fpows in a respective pool [10]. These attacks facilitate the wastage of useful miner resources and also slash the revenue of the pool. To counter these attacks only trustworthy miners should be given

admission into a pool and the pool should be closed when unexpected slashing of revenue occurs.

II. METHODS AND MATERIAL

An easy way to comply with the conference paper formatting requirements is to use this document as a template need to refer to an Internet email address or URL in your paper, you must type out the address or URL fully in Regular font.

III. CONCLUSION

Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. Authors are strongly encouraged not to call out multiple figures or tables in the conclusion these should be referenced in the body of the paper.

IV.REFERENCES

[1] SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, Joseph Bonneau,2015,ieee

[2] Cryptocurrency Networks: A New P2P Paradigm, Sergi Delgado-Segura, 2017, Hindawi

[3] A Survey on Security and Privacy Issues of Bitcoin, Mauro Conti, 2017, ieee

[4] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies, Princeton University Press, Princeton, NJ, USA, 2016.

[5] Rapid Prototyping of a Text Mining Application for Cryptocurrency Market Intelligence, Marek Laskowski ,2016,ieee

[6] Blockchain, blueprint for a new economy, Swan Melanie,2015, O'Reilly Media Inc

[7] On Bitcoin markets (in)efficiency and its evolution, Ladislav Kristoufek,2018,Elsevier

[8] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto,2016,ieee

[9] A Survey on Security and Privacy Issues of Blockchain, Sandeep Kumar E,2017,ieee

[10] Have a snack, pay with bitcoins, T. Bamert,2013,ieee

[11] Theoretical bitcoin attacks with less than half of the computational power (draft), L. Bahack,2013, Elsevier

[12] Securing smart cities using blockchain technology, K. Biswas,2016,ieee