Crypto-Currencies how secure are they?

Gopal Vishwas Patil[1], Dr. Aniruddha S Rumale[2]

[1]M.Tech. Scholar, G H Raisoni COE&M, SFPU, Pune, Maharashtra, India
[2]Professor and HoD, Dept. of AI, G H Raisoni COE&M, SFPU, Pune, Maharashtra, India

---***---

Abstract - *A cryptocurrency is a digital or virtual currency that uses cryptography for security. Every cryptocurrency has its governance model, according to which it functions and secures its network. However, there are two factors that keep the cryptocurrency secure, i.e., the blockchain technology and consensus algorithm. However, there are issues with blockchain and crypto currency security that should be addressed. Also, if you are investing in popular and trusted cryptocurrencies then you are almost safe from the asset point of view. But what matters is where you store your cryptocurrencies which is important. There are various options like hot wallets, cold wallets, physical wallets to choose from with respect to security.*

Recently, cryptocurrencies have become the main topics in the financial industry. This paper elaborates different user privacy aspects, technology used for security, benefits, challenges, tips to avoid frauds using cryptocurrencies. Successful attacks on crypto currencies are possible and in action; it is important to understand the ways to save cryptocurrency. Many hackers are trying out new ways to counterfeit the cryptocurrency transaction processes and intending to draw the secured cryptocurrency. But being technologically advanced, it has become a challenge for hackers.

Key Words: cryptocurrencies, security, blockchain, financial fraud, ransomware

1.INTRODUCTION

This section discusses about what is cryptocurrency, how cryptocurrency works while transaction takes place with virtual currencies and cryptocurrency properties.

1.1 Cryptocurrency

A cryptocurrency is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets [1]. Cryptocurrencies are a type of digital currencies, alternative currencies and virtual currencies. If we takeaway all the noise around cryptocurrencies and reduce it to a simple definition, we find it to be just limited entries in a database no one can change without fulfilling specific conditions. Take the money on your bank account: What is it more than entries in a database that can only be changed under specific conditions? You can even take physical coins and notes: What are they else than limited entries in a public physical database that can only be changed if you match the condition than you physically own the coins and notes? Money is all about a verified entry in database of accounts, balances, and transactions.

1.2 How cryptocurrency Works

A cryptocurrency consists of a network of peers. Every peer has a record of the complete history of all transactions and thus of the balance of every account. A transaction is a file that says, "A gives X cryptocurrency to B" and is signed by A private key. After signed, a transaction is broadcasted in the network, sent from one peer to every other peer.

The term "virtual currency" refers to a medium of exchange existing entirely in intangible form that is not a legal tender but can be substituted for legal tenders. Older forms of "currency" that are not "legal tender" include paper-based currency substitutes, such as military scrip and depression scrip. In recent times, the term "virtual currency" has developed an added connotation that it exists only in an electronic or digital form and is used only as a medium of valid, ends up in a block in the blockchain for the purpose of transferring the ownership of an amount of cryptocurrency to a designated digital address. The diagram below (Fig.1) shows basic steps involved in a transaction.

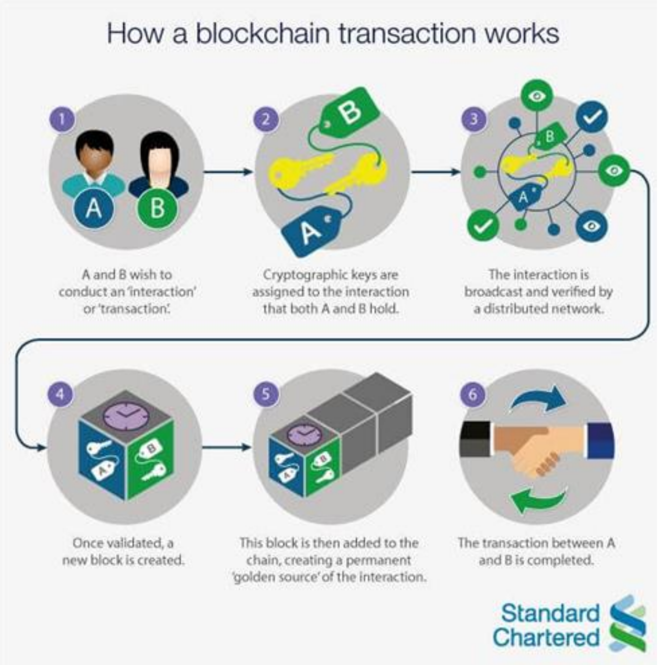
How a blockchain transaction works
1
A
B
A and B wish to conduct an 'interaction' or 'transaction'.
2
B
A
Cryptographic keys are assigned to the interaction that both A and B hold.
3
The interaction is broadcast and verified by a distributed network.
4
Once validated, a new block is created.
5
This block is then added to the chain, creating a permanent 'golden source' of the interaction.
6
The transaction between A and B is completed.
Standard Chartered

Fig.1: Steps involved in a cryptocurrency transaction.[2]

The transaction is known almost immediately by the whole network. But only after a specific amount of time it gets confirmed. Confirmation is a critical concept in cryptocurrencies. If a transaction is unconfirmed, it is pending and can be forged. When a transaction is confirmed, it is set in stone. It is no longer forgeable; it cannot be reversed. **Blockchain** is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved [3].

1.3 Properties of Cryptocurrency

Cryptocurrencies are built on cryptography. They are not secured by people or by trust, but by math. It is more probable that an asteroid fall on your house than that a cryptocurrency address is compromised. While most cryptocurrencies share a common set of properties, they are not carved in stone [4].

1) Irreversible: After confirmation, a transaction cannot be reversed. Not you, not your bank, not by anybody. If you send money, you send it. No one could help you, if you sent your funds to a scammer or if a hacker stole them from your computer. There is no safety net [4].

2) Pseudonymous: Neither transactions nor accounts are connected to real-world identities. You receive Cryptocurrencies on so-called addresses, which are randomly seeming chains of around 30 characters. While it is usually possible to analyse the transaction flow, it is not necessarily possible to connect the real-world identity of users with those addresses [4].

3) Fast and global: Transaction are propagated nearly instantly in the network and are confirmed in a couple of minutes. Since they happen in a global network of computers, they are completely indifferent of your physical location. It does not matter if I send Cryptocurrency to my neighbour or to someone on the other side of the world [4].

4) Secure: Cryptocurrency funds are locked in a public key cryptography system. Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers makes it impossible to break this scheme. A Cryptocurrency address is more secure than Fort Knox [4].

5) Permissionless: You do not have to ask anybody to use cryptocurrency. It is just a software that everybody can download for free. After you install it, you can receive and send Cryptocurrencies or other cryptocurrencies. No one can prevent you. There is no gatekeeper [4].

6) Controlled supply: Most cryptocurrencies limit the supply of the tokens. All cryptocurrencies control the supply of the token by a schedule written in the code. This means the monetary supply of a cryptocurrency in every given moment in the future can roughly be calculated today. There is no surprise [4].

7) No debt but bearer: The Fiat-money on your bank account is created by debt, and the numbers, you see on your ledger represent nothing but debts. Itis a system of IOU. Cryptocurrencies do not represent debts. They just represent themselves. They are money as hard as coins of gold [4].

2. Benefits and Challenges

This section discusses about benefits and challenges of using Cryptocurrencies.

2.1 Benefits

1) No Third-Party Seizure: No central authority can manipulate or seize the currency since every currency transfer happens peer-to-peer just like hard cash. Cryptocurrencies are yours and only yours, and the central authority cannot take your cryptocurrency, because it does not print it, own it, and control it correspondingly [5].

2) Anonymity and transparency: Unless Cryptocurrency users publicize their wallet addresses publicly, it is extremely hard to trace transactions back to them. However, even if the wallet addresses were publicized, a new wallet address can be easily generated. This greatly increases privacy when compared to traditional currency systems, where third parties potentially have access to personal financial data. Moreover, this high anonymity is achieved without sacrificing the system transparency as all the cryptocurrency transactions are documented in a public ledger [5].

3) No taxes and lower transaction fees: Due to its decentralized nature and user anonymity, there is no viable way to implement a Cryptocurrency taxation system. In the past, Cryptocurrency provided instant transactions at nearly no cost. Even now, Cryptocurrency has lower transaction costs than a credit card, PayPal, and bank transfers. However, the lower transaction fee is only beneficial in situations where the user performs a large value international transaction. This is because the average transaction fee becomes higher for very small value transfers or purchases such as paying for regular household commodities [5].

4) Theft resistance: Stealing of cryptocurrencies is not possible until the adversary has the private keys (usually kept offline) that are associated with the user wallet. Cryptocurrency provides security by design, for instance, unlike with credit cards you do not expose your secret (private key) whenever you make a transaction. Moreover, cryptocurrencies are free from Chargebacks, i.e., once cryptocurrencies are sent, the transaction cannot be reversed. Since the ownership address of the sent cryptocurrencies will be changed to the new owner, and it is impossible to revert. This ensures that there is no risk involved when receiving cryptocurrencies [5].

2.2 Challenges

1) High energy consumption: cryptocurrency blockchain uses PoW model to achieve distributed consensus in the network. Although, the use of PoW makes the mining process more resistant to various security threats such as sybil and double spending, it consumes a ridiculous amount of energy and computing resources [6]. Processing a cryptocurrency transaction consumes more than 5000 times as much energy as using a Visa credit card, hence innovative technologies that reduce this energy consumption are required to ensure a sustainable future for cryptocurrency. Furthermore, due to the continuous increase in network load and energy consumption, the time required for transaction processing is increasing [5].

2) Wallets can be lost: Since there is no trusted third party if a user lost the private key associated with his/her wallet due to a hard drive crash or a virus corrupts data or lost the device carrying the key, all the bitcoins in the wallet has been considered lost for forever. There is nothing that can be done to recover the bitcoins, and these will be forever orphaned in the system. This can bankrupt a wealthy cryptocurrency investor within seconds [5].

3) (Facilitate) Criminal activity: The considerable amount of anonymity provided by the cryptocurrency system helps the would-be cyber criminals to perform various illicit activities such as ransomware [7] tax evasion, underground market, and money laundering [5].

3. Security issues

This section discusses about security issues in Blockchain and Cryptocurrencies.

3.1 Security issues in Blockchain

Like any system, blockchain has points of vulnerability. Therefore, anyone planning on investing in cryptocurrency should be familiar with those points of vulnerability [12]. Any business dealing with blockchain must consider these issues with blockchain security:

1) The complexity of the technology: It is a difficult system to create from scratch (if you are trying to create a version for your own brand). One small misstep, and your entire system could be compromised. Of course, this is not a flaw with the system itself, but rather with its execution. Similarly, the complexity of the technology makes it more difficult for the average person to understand. Therefore, they may not properly understand the risks and function of the system [12].

2) The size of the network: For blockchain to work, there needs to beat least hundreds — preferably thousands — of nodes working in unison. This makes blockchain systems especially vulnerable to attack and corruption during the early stages of growth. For example, if a single user gets control of just 51percent of the nodes on a system, then they may be able to fully control its outcomes. On a scale of just 20 nodes, that is not an impossible feat [12].

3) The speed and efficiency of the network: The design of the block chain may also compromise its ability to process exchanges at a suitable rate. If a system grows too complex or in-demand before it develops an infrastructure that can support it, it can lead to data storage and transaction speed issues. This can negatively interfere with an otherwise efficient system. Therefore, it makes the list of issues with blockchain security [12].

4) The politics of execution: Though not a security issue with blockchain directly, the politics of the system could affect its execution and development. The fact that blockchain-based currencies are decentralized and international means that government-controlled currencies could become intrinsically less valuable. Accordingly, some national governments are working to introduce heavier regulations to the blockchain. They hope to control it before it threatens their economy or grows too powerful. As one of the many issues with blockchain security, this could postpone widespread adoption of the technology [12].

5) Third-party systems: For example, Nice Hash, a third-party Cryptocurrency mining marketplace, was recently hacked, losing more than 60 million dollars of cryptocurrency, because its platform was not secure. This was not a flaw with the blockchain. Instead, cybercriminals gained access to the system by using the blockchain [12].

6) Blockchain transactions make use of a public and private cryptographic key: Those keys are nearly impossible to crack on their own, but a cybercriminal could get a hold of those keys through more conventional, easier means. For example, they could get them if you store the keys on an in secure platform. If someone finds your email password, they will have access to your entire inbox. In the same way, if someone finds your blockchain keys, they can impersonate you on the blockchain. This is one of the main issues with blockchain security to ponder [9] [10] [12].

7) Traditional scams: Users on the blockchain are also vulnerable toother traditional scams. However, these are not inherent security weaknesses of the blockchain. For example, if you get an email from someone who convinces you they have a worthwhile investing opportunity, they may trick you into delivering them cryptocurrency without delivering the products or services they promised [12].

3.2 Security issues in Cryptocurrencies

1) Spoofing and Phishing Payment Information: As with the ordinary e-money, phishing attacks also affect cryptocurrency users as they can be redirected to a fake website requiring them to enter user id and passwords of their crypto-wallet. While spoofing of transaction can be performed by an attacker when a user tries to copy the wallet address for transaction which is replaced by malware and the user is not aware of the changes since not everyone is vigilant to double check a long address copied by them [11].

2) Error in User Address: There is also a risk of potential loss when an error is made in the recipient address which can results in loss of money. For example, in case of Ethereum, if some of the last digits of the recipient address is entered wrong by mistake, the money will disappear into void or would be transferred to the exact address but the multiplied by 256 in value intended will be transacted [11].

3) Loss of a Wallet File: One of the major problems in the cryptocurrencies is the loss or the theft of local wallet files due to hard disk crash or other interruptions. So, it is generally advised to make paper wallet to store local passwords or a backup hardware wallet [11].

4) Insecure ICOs: Investing in cryptocurrency Fundraising through virtual currencies can be done via Initial Coin Offering (ICO). An ICO is generally issued to raise a lump sum amount of funds through buying and selling of cryptocurrency which requires just an Internet connection. Absence of risk-free access mechanism to regulate the cryptocurrency market to track down and de-anonymize a payee on the cryptocurrency market is another hurdle when handling virtual currencies [11].

5) Payment Gateway Hacking: Hacking can be done through convincing the hosting provider that they are the real domain owners and then intercepting the cash flows. Many well-known financial services have fallen prey to such kind of tactics employed by hackers [11].

6) Fraud at the Trading Exchange: With the popularity and recent price rise of cryptocurrency, many future exchange and trading platforms are budding out across the globe. These trading exchanges store public and private keys of all their customers' wallets in their local servers. If in any case, a trading exchange provider decides to run away with all their users' cryptocurrencies. Then due to lack of regulations and legal frameworks, there is not much that can be done against such crimes, which in turn puts all traders into vulnerable situation [11].

3.3 Tips for cryptocurrency holders and crypto investors

Some suggestions and precautionary measures for cryptocurrency holders and crypto investors are given below,

1) Always verify a Web wallet's address and avoid following suspicious links to an Internet bank or Web wallet.

2) Before transacting, always double-check the recipient's address, the amount entered, details of transaction fees and other charges.

3) Prepare a secondary option to recover forgotten account passwords and other details as well as keep them safe and private.

4) Crypto investment is risky. So common practices must be followed while investing like diversified investment, reliability of the providers and a strong mind-set to deal with unforeseen circumstances.

5) Use cryptocurrency hardware wallets and paper wallets is advised.

6) Use good antivirus programs to protect the computers and devices used to access crypto-wallets, and other activities involving cryptocurrencies.

4. SUMMARY

Most Virtual Currency use around the world is under a void in terms of legality and regulated in the moment. Some countries have incorporated it into their financial system, but some have banned them completely. If the popularity of Virtual Currencies increases further, more and more countries may regulate it, although it is not the case where many are considering prohibitions on it. With the growing user base and recent upsurge in Cryptocurrency's value which is one of the most famous virtual currency available, there are more and more hurdles like need of a legal framework and regulating authority, awareness about the use of wallets, transaction processing as well as risks involved in virtual currency transaction are rising.

Therefore, it can be said that Cryptocurrencies have got a great potential to become a global currency. Even in countries where its use is banned by the authorities, it is still an issue to restrict the use entirely without internet censorship. So, it can be ascertained that there is a huge growth potential and benefits of incorporation of Virtual Currencies into legal frameworks and to the already existing financial system. Indian Banking and Finance sector are

ready to leverage from the capabilities of blockchain technology and distributed ledgers in transaction processing. There are likely to be more debate over the legality and acceptance of cryptocurrencies is going to be happening in the next few years surrounding digital currencies.
The key legal issues surrounding cryptocurrencies have been discussed in this paper and these are the main concerns countries must consider when creating legislation for Virtual Currencies.

After looking at the security issues highlighted in this report one cannot help but wonder if blockchain and cryptocurrencies are safe or not. The system itself is airtight, so long as it has been executed properly, and has a decent network of users on the system. However, any system has some vulnerability, and the blockchain is no exception. The key thing to remember here is the vast majority of blockchain security breaches are related to human error. When properly executed and protected, the blockchain is transparent and tamper-proof. And that is about as "secure" as a technology can get. In doing so, we will be able to leverage the benefits without worrying about issues with blockchain security.

REFERENCES

[1] Carylyne Chan - What Are Cryptocurrencies?
[2] UURIINTUYA BATSAIKHAN AND BRUEGEL- Cryptoeconomics – the opportunities and challenges of blockchain
[3] What is blockchain technology?
[4] Ameer Rosic - What is Cryptocurrency? [Everything You Need To Know!]
[5] Mauro Conti, Senior Member, IEEE, Sandeep Kumar E, Member, IEEE, Chhagan Lal, Member, IEEE, Sushmita Ruj, Senior Member, IEEE - A Survey on Security and Privacy Issues of Bitcoin
[6] P. Fairley, "Blockchain world - feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous," IEEE Spectrum, vol. 54, no. 10, pp. 36–59, October 2017.
[7] K. Liao, Z. Zhao, A. Doupe, and G. J. Ahn, "Behind closed doors: measurement and analysis of cryptolocker ransoms in bitcoin," in 2016 APWG Symposium on Electronic Crime Research (eCrime), June 2016, pp. 1–13.
[8] Ramis Jamali, CFA Sherwin Li, P. Eng. Rodrigo Pantoja - cryptocurrency | digital asset class of the future – bitcoin vs ethereum?
[9] Blockchain support
[10] Demiro Massessi - Blockchain Public / Private Key Cryptography In A Nutshell
[11] Paras Vishwakarma1, Mr. Zohaib Khan2, Dr. Taruna Jain3 - Cryptocurrency, Security Issues and Upcoming Challenges to Legal Framework in India
[12] Peter Daisyme - Issues with Blockchain Security
[13] https://cpomagazine.com/tech/how-secure-are-cryptocurrencies/
[14] https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency
[15] https://www.financialexpress.com/market/why-warren-buffett-wants-to-stay-away-from-bitcoin-even-as-cryptocurrency-has-grown-6x-in-5-months/2216877/
[16] https://en.wikipedia.org/wiki/Cryptocurrency_and_crime
[17] https://en.wikipedia.org/wiki/Cryptocurrency
[18] https://wall-street.com/the-pros-cons-of-ryptocurrency/cryptocurrencies

BIOGRAPHIES

Mr. Gopal V Patil is having 15 years of IT experience in banking domain and currently working as Technical lead and Sr. Solutions Architect in Technical excellence and Innovation team at Citi development center. He is strong professional with Full stack experience, skilled in Java, J2EE, Spring, Python, Big data, AI/ML. He is currently pursuing MTech at G H Raisoni College of Engineering and Management, Wagholi, Pune.

Dr. Aniruddha S Rumale is having 23 Years of academic experience and currently working as Head of Department Artificial Intelligence and Dean Entrepreneurship Development Cell & Institute's Innovation Council at G H Raisoni College of Engineering and Management, Wagholi, Pune. He has authored more than 30 papers in various international/national journals and conferences, more than 4 books. He also has a YouTube Channel Tutor (https://www.youtube.com/c/TutorASRumale) dedicated to Technology teachings. His Primary research interest is in Cloud Computing, AI and ML, DIP, & Software Engineering.