Crypto Currencies: Issues and Challenges

Chandrasekaran G, Murugachandravel J, Neethidevan V

MCA Department, Mepco Schlenk Engineering College, India

***Abstract* - The popularly known *crypto currency* is a type of digital currency. It works as a medium of exchange that uses cryptography to secure financial transactions. *Cryptography* helps to keep the data secure. All data about the transactions are kept secure in a distributed ledger system called *Block Chain*. Crypto currencies use decentralized control as opposed to centralized digital currency and central banking system. Block chain serves as a public financial database system. Bit coin was the first introduced crypto currency, in 2009, by *Satoshi Nakamoto*. According to him, it is a Peer-to-Peer electronic cash system and further, it is decentralized with no server, or central authority. This paper focuses on the issues and challenges of crypto currencies.**

***Keywords* - crypto currency, cryptography, block chain, bitcoin, Distributed Ledger Technology**

I. INTRODUCTION

Crypto currency is a digital currency that uses cryptography for security. Crypto currency is a decentralized system based on block chain technology. It uses a distributed ledger enforced by a dissimilar network. The first block chain based crypto currency is the Bit coin. It is a Peer-to-Peer electronic cash system. It is decentralized and involves no servers and controlling authorities. One of the most important problems that any payment network has to solve is double-spending. It is a fraudulent technique which involves paying the same amount twice. To solve this problem, a third party centralized server that keeps record of the balances and transactions was used. But this method would exercise control over the users' funds and personal details. So, a decentralized network was introduced. In case of a decentralized network, a block chain, which is a public ledger of all transactions, is used. Each transaction is a file which consists of the public key of the sender, the recipient and the amount of coins transferred. The transaction has to be signed off by the sender with his / her private key. Before sending a transaction into the network, it must be confirmed. In the crypto currency network, only miners can confirm transactions by solving a cryptographic puzzle. They have to mark the transactions as legitimate and spread them across the network. Then each node of the network adds it to its database. When the transaction is confirmed, it becomes irreversible.

II. LITERATURE SURVEY

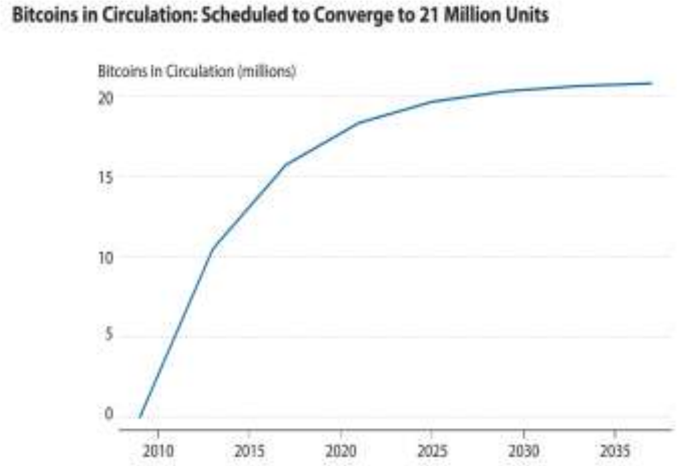
In [1], the features of crypto currencies are explained and they provide an easier way to transfer funds between two parties. Crypto currency acts as an alternate method of payment where, intermediaries may be replaced [2]. Crypto currency follows a peer-to-peer Electronic Cash System [3]. The important challenges faced by crypto currencies, especially, security and privacy are discussed in [4]. The functions, evolution of money, crypto currencies and bit coins, the challenges that they have to come across are discussed [5].

III. CRYPTOCURRENCIES AND BITCOINS

Crypto currencies and Bit coins provide alternative approach for exchanging goods, store value and act as a unit of account. They may have either centralized institutions or may be based on a decentralized network. In case of a centralized scheme, the digital currency is issued by an institution, which ensures that the digital coins can be used to buy and sell goods. In a decentralized currency scheme, central institutions are avoided and are built on a network of transaction partners. They can build trust by observing the behaviour of each other. If it is not possible to view each other, the solution lies in crypto currencies, which are decentralized currency schemes.

Bit coin users rely on the Bit coin protocol to send and receive payments over the internet. Participants who want to exchange Bit coins connect to a peer-to-peer network. Every partner is anonymous, only the enabling Bit coin protocol encrypts and verifies a transaction from one user's "wallet" to another. To avoid double-spending of Bit coins, each transaction is verified by Bit coin network nodes or "Miners", who have to solve a crypto graphical puzzle (calculation of a predefined hash value). The Miner who has solved the puzzle, includes the transaction into a public ledger, the block chain, and is rewarded with Bit coins. A copy of the block chain is stored at each node of the Bit coin network. Therefore, as the encryption, verification and transfer for each transaction is based on the Bit coin protocol, and transactions are publicly available through the ledger that is shared by peers in the network, there is no need for trust in any individual users and no central institution for money transactions is required. The Bit coin protocol, the Bit coin network and Bit coin are supported and enabled by a community of active supporters, who update the Bit coin protocol and ensure the healthiness of the Bit coin network. In addition, the first firms were formed to exchange Bit coins for fiat currencies like Dollar, Euro and Yen soon after the introduction of Bit coin. Today, around 80 000 merchants accept Bit coins as payment methods, with

Microsoft and Dell as the two largest Bit coin accepting retailers. The number of bit coin users is also increasing every year.



IV. DISTRIBUTED LEDGER TECHNOLOGY

Distributed Ledger Technology (DLT) enables different parties with common goals to co-create a permanent, immutable and transparent record of exchange and processing, while making the database more secure and resilient. Distributed ledger may be publicly available or not. They can vary in terms of which set of verifiers are authorized to validate transactions, viz., permissionless or permissioned. In both types of ledgers, all participants are allowed to submit transactions and validate them and they are expected to be authorized. These types of ledgers are appropriate for highly controlled and regulated environments where all participants need to be known, hence, lack the pseudo-anonymity and decentralisation of authority associated with permissionless ledgers but offer higher transaction rates, and settlement times at lower costs than current public permissionless systems. The sustainability and success of DLT depends on trust, usability, transparency and legitimacy. Based upon this, DLT has to face certain challenges, like, *regulation*, *privacy*, *scalability*, *volatility* and *incentives*. A good reputation system creates a safe environment for network participants to interact and it would attract more participants. On the other hand, a bad reputation would make the participants to ignore the system. Regulation plays an important role in correcting faulty information. Regarding privacy, it is a big challenge for the public permissionless block chains which disclose all transactions, smart contract code and state. Nowadays, many block chains, have been designed to solve this problem. Many block chain protocols scale lesser transactions because of block size and transaction complexity. Volatility represents the challenge of storage of value. To address this issue, stable-coins are introduced. Fixing of right incentives helps to achieve mutual gains when parties involved in a relationship have differing goals and possess varied knowledge.

V. ISSUES AND CHALLENGES

Crypto currencies make us face so many issues and challenges. Some of them are discussed below.

Price Manipulation

The prices of crypto currencies on exchange platforms rise and fall dramatically over a short period of time. When the price of a tradable asset drops, then the volatility of the market will be high. Regular investors will notice this change and interpret it to mean an imminent price increase. Once this happens, the price of the crypto currency will increase. The important reason why this sort of asset price manipulation is possible is due to the lack of position price limits.

The Activities of Cybercriminals

The crypto currency market has been challenged by the hackers and cybercriminals. There have been a number of crypto currency hacks that have resulted in millions of dollars being stolen. Traders and investors have lost funds and some platforms have ceased to operate. The price of particular crypto currencies has dropped considerably. Transactions on a block chain are immutable and as such if funds get stolen, there is little chance of ever recovering such funds. Crypto currency trading platforms constantly have to improve their security framework in order to stay ahead of the hackers and thieves.

Lack of Price Uniformity

It is often necessary to develop price charts in order to carry out investment analysis and develop trading strategies. The problem here is the price of a crypto currency, which can vary considerably on the different exchange platforms. With such extreme price differences for the same crypto currency, price charting becomes a difficult task.

Transaction Delays

The crypto currency market is beset with delays across almost every type of transaction. From opening a trading account to verifying your identity and being able to make deposits and withdrawals, the system seems to be quite slow. Block chain technology ought to make transactions occur faster but it seems to take forever for transactions to be approved on various chains.

Expensive transactions

The transactions are subject to a transaction fee which also creates a queue of pending transactions. The order of implementation depends on the highest amount that is paid as transaction fee. Therefore, for a person who wants to send money across immediately will have to pay an excessive transaction fee which will in turn make his transaction unnecessarily expensive. Due to this problem, people are seeking fast and cheap alternatives to Bit coin to free themselves of slow and expensive transactions.

Poor mobile platform support

Most of the companies, like Apple, Google don't allow dealings with bit coins on their mobile platforms. Recently, Apple had decided to ban bit coin wallets on the App Store. Furthermore, Google too does not allow in-app payments with bit coin. Some developers create mobile applications for bit coins, but it is harming the ecosystem. So they emulate what restrictive governments do at least within their platforms. Bit coin is an excellent method of remote payment. It is a much better way to send and receive payments instead of using QR codes.

Privacy

Lack of privacy on public block chain is a major challenge faced by crypt currencies. For example, bit coin is a private system, which is not the case in reality. A Bit coin transaction is not encrypted. However, it is hashed. Every transaction that takes place is available for public scrutiny and analysis.

Scalability

Scalability is another challenge for crypto currency. It is potentially keeping this crypto asset out of the hands of potentially a larger user base. The problem of scalability arises due to Bit coin's nature of essentially having a limit on the number of transactions that can occur within a certain time frame. This limit is placed in order to prevent the block chain size from going out of control. As of now, the network has never hit this limit, but it will happen eventually if Bit coin becomes a mainstream form of payment.

VI. CONCLUSION

So far, we have discussed about features of crypto currencies, bit coins and Distributed Ledger Technology. We have seen the important challenges faced in the field of crypto currencies. Any form of money needs to be easy to transact with, easily recognizable or verifiable by users, and easy to carry for it to work well as a payment system. Many objects that are currently utilized to store wealth are not easy to carry or transfer. Bit coin offers a new alternative.

REFERENCES

[1]. Ashish Mohod, Anmol Mannarwar, Kaustubh Badukale, “What is the future of Cryptocurrency in India”, International Journal of Research in Science and Engineering, Vol.4, Issue.1, Jan-Feb 2018

[2]. Marcel Morisse, Department of Informatics, University of Hamburg, “Cryptocurrencies and Bitcoins: Charting the Research Landscape”.

[3]. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”

[4]. Mauro Conti, Sandeep Kumar E, Chhagan Lal, “A Survey on Security and Privacy Issues of Bitcoin”, Deecember2017

[5]. Dr. Zeynep Gurguc, Prof. William Knottenbelt, “Cryptocurrencies: Overcoming Barriers to Trust and Adoption”. Imperial College, London

[6]. https://en.wikipedia.org/wiki/Cryptocurrency

[7]. https://www.genesis-mining.com/cryptocurrency-list

[8]. https://medium.com/aditusnetwork/8-challenges-to-overcome-to-enable-cryptocurrency-payments-c7a49e379d61

[9]. https://blockgeeks.com/guides/what-is-cryptocurrency/

[10]. https://cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies