SURVEY ON CRYPTOCURRENCY TECHNOLOGY

K.Subhashini Spurjeon[1] Shubham Kumar Sahu[2] Anupriya Dutta[3]
Department of Information Technology
Bhilai Institute of Technology, Durg, 491001
[1]ksubhashinispurjeon@gmail.com, [2]sksdbest@gmail.com,
[3]anu.dutta345@gmail.com

Abstract

Cryptocurrencyis a digital assetdesigned to work as a medium of exchangethat uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. Cryptocurrencies are classified as a subset of digital currenciesand are also classified as a subset of alternative currenciesand virtual currencies.Bitcoin, created in 2009, was the first decentralizedcryptocurrency.
This paper presents the three generations of cryptocurrencies, their features and uses.

Keywords: Cryptography, Blockchain , Decentralized, Distributed, Hash functions

1.INTRODUCTION

The paper summarizes the results of the systematic study of different digital currencies. Why should we use cryptocurrencies? The answer to this question is simple.We should use cryptocurrencies since it is a step in the right direction for global trade where everyone can be involved. To neglect the idea of Cryptocurrencies on a decentralized network today is like neglecting the idea of Internet and the Hypertext Transfer Protocol (http) back in the early nineties. People who understands this technology or people who can get a clear picture how it works can easily see the benefits for mankind. It's the peoples money.
Bitcoin was the first prominent cryptocurrency to gain the public's attention, but it is doubtful that it will be the last. In the wake of Bitcoin's popularity, many coin developers have sought to improve upon the basics of Bitcoin and offer a more fulfilling and feature rich experience to newcomers.
The future appeal of cryptocurrencieslies in allowing users ultimate control over their money, with fast secure global transactions, and lower transaction fees when compared to all existing currencies. When used properly and fully understood the virtual currency ultimately serves its purpose.

1.1 TRANSACTIONS

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

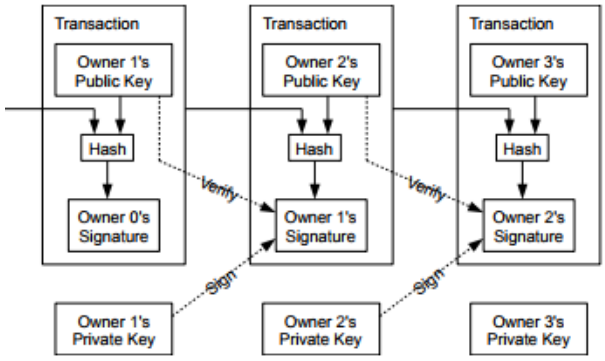

Figure 1: Blockchain Transaction model

A transaction is a transfer of Bitcoin value that is broadcast to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs. Transactions are not encrypted, so it is possible to browse and view every transaction ever collected into a block. Once transactions are buried under enough confirmations they can be considered irreversible. Standard transaction outputs nominate addresses, and the redemption of any future inputs requires a relevant signature. All transactions are visible in the blockchain, and can be viewed with a hex editor. A blockchain browser is a site where every transaction included within the blockchain can be viewed in human-readable terms. This is useful for seeing the technical details of transactions in action and for verifying payments.

2. LITERATURE REVIEW

There are three generations of cryptocurrencies till now namely first generation, second generation and third generation.

2.1.FIRST GENERATION

The example of first generation of cryptocurrency is Bitcoin. This generation represents the peer-to-peer accounting system. It is a border less currency. Peer-to-peer technology allows us to do transactions without need of any centralised third party such as bank i.e. first generation is a decentralised technology. But, the first generation currencies have scale issues. The bitcoin scalability problem is a consequence of the fact that blocks in the blockchainare limited to one megabytein size.
The most popular first generation currency is bitcoin.

Bitcoin: Bitcoin is the first decentralized digital currency, as the system works without a central bankor single administrator.Bitcoin was invented by a person or group of people under the name Satoshi Nakamotoand released as open-source softwarein 2009.Bitcoins are created as a reward for a process known as mining.

2.2 SECOND GENERATION

The second generation of cryptocurrency is known to be smarter than bitcoin.
The example for currency that was found in this generation is etherum. This currency has two major things different. The first thing is that it allows to use some programming language on the blockchain. The code is used for smart contracts and for decentralised applications. It makes transactions smaller. It makes the transactions secure for both the

end i.e. one can receive money when he /she has done the job. The second generation also has a small amount of scalability problem.
The coins of second generation sparkle coin, sky coin, etherum.

Etherum: Ethereum is an open-source, public, blockchain-based distributed computingplatform featuring smart contract(scripting) functionality.It provides a decentralized Turing-completevirtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes. Ethereum also provides a cryptocurrencytoken called "ether", which can be transferred between accounts and used to compensate participant nodes for computations performed.

2.3 THIRD GENERATION

There is not any exact example of third generation cryptocurrency. All the currencies are competing to come in this generation and some are in horizon. The main objectives of this generation is a need of governance system, reduced scalability and interoperability. Interoperability helps us to interact with other blockchains or with other cryptocurrencies. Some of the coins on the horizon of third generation are cardano and Iota.

Cardano: Cardano is considered a 3rd generation cryptocurrency, and ranks as of January 10 2018, at Coinmarketcap.com among the top 10 traded values, with a market cap of $19,726,196,786. The BitMex, Bittrex, Upbit, Binance and Coinnest currency exchanges list Cardano ADA futures.Cardano was launched by blockchain development firm Input Output Hong Kong (IOHK), lead by Charles Hoskinson, former CEO of Ethereum. Cardano develops their currency around a Recursive InterNetwork Architecture (RINA). Cardano facilitates the Ouroboros algorithm which is Provably Secure Proof of Stake, enabling multiple blockchain creation at any given time running parallel, and with the ability to handle humongoustransactions. The biggest advantage of Cardano is that unlike Bitcoin, it's built with two layers.

Iota: IOTA is an open-sourcedistributed ledger(cryptocurrency) focused on providing secure communications and payments between machines on the Internet of Things. Using directed acyclic graph(DAG) technology instead of the traditional blockchain, IOTA's transactions are free regardless of the size of the transaction, confirmation times are fast, the number of transactions the system can handle simultaneously is unlimited, and the system can easily scale.IOTA was founded in 2015 by David Sønstebø, Sergey Ivancheglo, Dominik Schiener, and Dr. Serguei Popov.

For an IOTA user to send out a transaction, the user must validate two other, randomly selected transactions. A sent transaction must accumulate a sufficient level of verification (i.e. must be validated a sufficient number of times by other users) in order to be accepted as “confirmed” by its recipient. IOTA works with a single administrator called the Coordinator which confirms all transactions in a set of released milestones.

3. CONCLUSION

- Digital currency is still not being used as a common currency and hence cryptocurrency is not acceptable completely.
- As it is a currency i.e. we can purchase stuffs by paying it but there is no such system in most of the countries that accepts cryptocurrency.
- The rate of the coins changes day by day. It has not a fixed amount and hence one may experience profit or loss.

- The miners of a specific cryptocurrency are mining coins and these coins are not accessible by the normal people.
- From the government point of view cryptocurrencies should be banned as there is no record of transactions.

4. FUTURE SCOPE

There are limitations of every coin,no coin serves to completely satisfy aim of the cryptocurrency or replace the original currency. Therefore, in future we need a cryptocurrency that can work as a normal currency for normal people and with cryptocurrency its property of the currency that it privacy is most important who sended money to whom only the sender and receiver knows and no one else can ever know , but people are using this property to serve illegal purpose we need to find a way to stop this. Also, we need a system that can serve as a digital currency acceptor so that the normal public can bring the digital currency in their daily use and can know about its features. To make the people aware about these digital currencies special sort of technique is needed to be developed.

5. REFERENCES

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[3]"ethereum"*GitHub*. Retrieved 11 January 2018.

[4]Iota: a cryptocurrency for Internet-of-Things. http://www.iotatoken.com/,and https://bitcointalk.org/index.php?topic=1216479.0

[5]Sergio Demian Lerner (2015) DagCoin: a cryptocurrency without blocks. https://bitslog.wordpress.com/2015/09/11/dagcoin/

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

[7]Cryptocurrencies: A Brief Thematic ReviewArchived 25 December 2017 at the Wayback Machine.. Social Science Research Network. Date accessed 28 august 2017.

[8]https://www.cardanohub.org/en/home/