Blockchain and Cryptocurrency

Manu Mohan[1] , Dr.R. Savitha[2]

Department of Computer Application, RV College of Engineering, Bangalore, Karnataka, India

Abstract: This paper focuses on the blockchain technology that has enabled the existence of digital currency and also the cryptocurrency applications. A blockchain is an open and distributed ledger which are used to record the transactions between two parties in an efficient and permanent way. It consists of list of records called blocks where each block contains a cryptographic hash of the previous block and transaction data. These blocks are linked using cryptography. It uses peer-to-peer network for communication and allow the participants to confirm transactions without a need for the central authority. A cryptocurrency is a digital, encryption techniques used to verify the transfer of funds. The main focus of the paper is to explain the concept of blockchain and how cryptocurrency leverages its technology. Blockchain is a new approach in the information technologies field. One of its first implementation is the bitcoin cryptocurrency which has gained a lot of attention together with Ethereum and smart contracts. The paper gives a brief description about these topics.

Keywords: ledger, cryptographic hashing, bitcoin, smart contracts, mining

I.INTRODUCTION

Blockchain is also known as Distributed Ledger Technology (DTL). It uses decentralization and cryptographic hashing for transparent and unalterable transactions. It helps in increasing the capacity of the whole networks, proving better security, and creating immutable ledgers. The most basic application of the blockchain is to carry out the transaction through a secure network. It is a decentralized transaction and a well- known technology behind the success of Bitcoin cryptocurrency [2]. It tries to create an environment where no third party is in control of the transaction. This technology tries to solve the problem in a way for generating great business value. The most famous implementation of blockchain is Bitcoin.

Types of blockchain: There are mainly four types of the blockchains which are as follows:

- **Public blockchain**: It is a permission-less distributed ledger system. The main use of this type of blockchain is for exchanging cryptocurrencies and mining. Bitcoin is the most common example of public blockchain. It is secure if the users follow security rules otherwise it becomes risky.
- **Private blockchain:** It is a permission distributed ledger system which are operated only in a closed network. It is mainly used within an organization where security is within the hands of the organization. Only selected members are considered as the participants and is similar as public blockchain. It is mainly used for supply chain managements, digital identity, etc. Multi coin is the most common example of the private blockchain.
- **Consortium blockchain:** It is a semi decentralized ledger system mainly used by banks and government organization. It allows more than one organization to work together.
- **Hybrid blockchain:** It is a combination of the public and the private blockchain which providesthe users the facility of both the blockchains. Due to this reason, it is very much flexible.

Working of blockchain: The figure given below shows the entire flow of the blockchain from requesting transaction to validating then adding it to new block then finally completing the transaction.

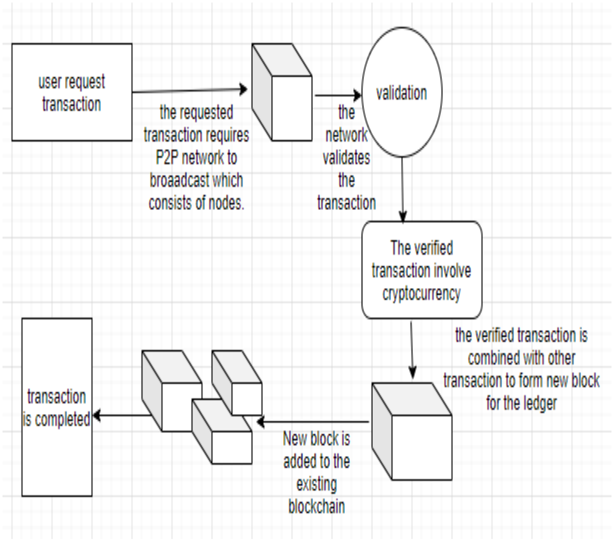
user request transaction
the requested transaction requires P2P network to broadcast which consists of nodes.
validation
the network validates the transaction
The verified transaction involve cryptocurrency
the verified transaction is combined with other transaction to form new block for the ledger
New block is added to the existing blockchain
transaction is completed

Figure 1.1 Working of blockchain

To make any transaction safer, it is very important to understand the concept of cryptocurrency.

Tools used to implement blockchain technology:

- **Remix IDE**: It is one of the easiest and browser based tools used for creating and deploying smart contracts using solidity programming language.
- **Truffle framework**: It is a framework for Ethereum (a type of cryptocurrency) which is used to offer a development environment for buildings Ethereum based apps.
- **Solc**: It is used to convert the solidity script which is a programming language into the readable format.
- **Geth**: It is a program which work as a node for the Ethereum platform ad is used for mining.
- **Embark**: It is a development framework for Ethereum based apps on decentralized technology. It is also used to manage smart contract.
- **Ganache**: This tool is used allow developers to create their own private Ethereum blockchain to test the apps. It allows to do testing without paying too much money.
- **EtherScripter**: It Provides an easy-to-use drag and drop interface that can be used in coding basic contracts.
- **Mist**: It is used to keep ether tokens and run smart contracts. It is available for Linux, Mac and Windows. Once it is set up, the password cannot be changed.
- **Blockchain Testnet:** It is used to test the app before deploying it on the main network.
- **Blockchain as a Service (BaaS**): It allow the users to use cloud based solutions for building, hosting and using their blockchain apps. It helps to solve the technical complexities and operational overhead within a company.
- **Metamask:** It acts as a bridge between Ethereum blockchain and chrome working as a browser extension.

II. CRYPTOCURRENCY

A cryptocurrency is a digital currency that is derived from the encryption techniques which are used to secure the network secured by cryptography. It is a form of money which is not regulated, controlled and tracked by any centralized authority or institutions. : It is very important to know some basic terms before knowing how cryptocurrency works.

- **Public ledgers:** It consists of confirmed transactions which are stored in the public ledger.
- **Transactions**: It is the transfer of funds between two digital wallets.
- **Mining:** It is the process of confirming transactions and adding them to public ledger.

Some of the key features of cryptocurrency are:-

- Most cryptocurrencies have a pre-determined and limited supply of the cryptocurrency which is coded into its algorithm when created. It has the facility of creating scarcity to prevent currency manipulation over the time.
- The cryptocurrency provides the features of irreversible immutable transaction means the transactions cannot be changed and modified once it is saved in the blockchain.
- It provides the feature of anonymous digital identity. So, there is no need for the users to identify themselves when transacting with the system.
- It uses distributed and decentralized network of computers all around the world for transactions.

Types of cryptocurrency: Some types of cryptocurrencies are discussed below:

- **Bitcoin (BTC):** It is one of the first and most commonly known cryptocurrency. It was created in 2009 by Satoshi Nakamoto. It allow the user to make peer-to-peer transactions using blockchain technology as blockchain provide secure transaction even when many users can see the transaction. But they can decrypt by the owner of that transaction using private key. It does not require any central authority.

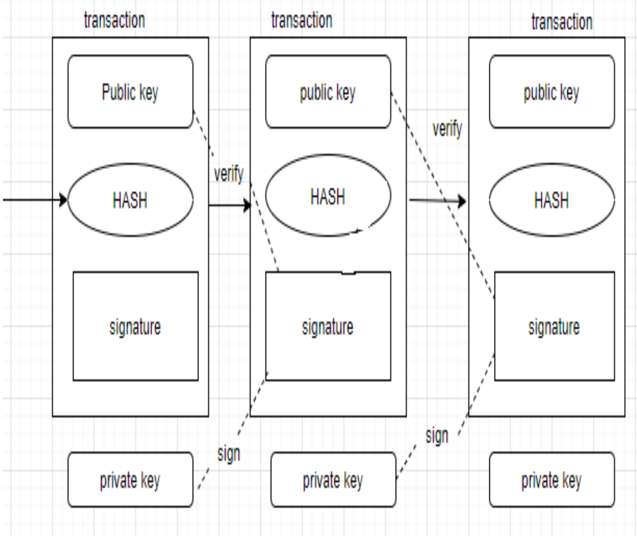

Figure 2.1 Structure of bitcoin

The figure above presents a system with P2P distributed server which serves as a proof of the order of transactions. A chain of digital signatures are called electronic coin whereas each transactions is defined as a set of digitally signed hash of previous transactions and public key of the owner. It describes the structure of transaction in a bitcoin blockchain where public key is used for verification purpose and private key is used for signing purpose.

- **Bitcoin Cash:** It was developed to improve the features of Bitcoin like increasing block size, faster processing, etc.
- **Litecoin (LTC):** It was developed in 2011 as an alternative to bitcoin. Like bitcoin, it doesn't require any central authority. It is also open and decentralized system used for global payments.
- **Ripple (XRP**): It was launched in 2012 for transferring money faster. It acts as cryptocurrency and digital payment network for financial transactions**.**
- **Ethereum (ETH):** It was launched in 2015 based on blockchain technology**.**

III. SOCIETAL PROBLEM THAT CRYPTOCURRENCY SOLVES

There are so many problems that cryptocurrencies tries to solve. The paper presents some of the societal problems that are solved by using cryptocurrency. It tries to solve the cross border payment issues by enabling users to undertake safe cashless transactions without paying high charges. It tries to solve the problem inflation because money decreases its value with time and allows people to travel worldwide. In some places people do not have their bank accounts. Thus, cryptocurrency helps the people to do cashless payments worldwide by using smartphones. The multicurrency mobile wallet makes it possible for cryptocurrency users to exchange currencies, store altcoins and buy tickets. It also solves the issue of intermediation charges and provide the feature of Bitcoin which emerges as a warrantor of trader's privacy. It helps in matching the physical cash so that there is no demand for the seller to identify the consumer or the source of money. Blockchain provides a powerful verification method that do not let the cryptocurrency users double spend means it does not allow redundant transactions for a single coin. Since cryptocurrencies are digital, they only exist as states in a global ledger where all transactions are carried out. The order of the transaction is done by classifying them into kind of blocks and connecting them into a chain. It is impractical to interchange the block to execute the transactions thus, it helps in removing or editing the information via illegal channels. It helps the users to send any information in a precise way without giving extra information. Since , the blockchain is kept in a decentralized database it is difficult for the hacker to obtain the information. In some situation, if somebody shares their valuable information to other it involves huge risk,. By using cryptocurrency and blockchain technology these problems can be resolved as they provide effective and efficient solutions.

IV CONCLUSION

The paper gives details about several concepts of blockchain and cryptocurrency. It also presents the most popular implementation of the blockchain that is Bitcoin and the provides the solution for the problems that the society are facing. In the past few years , there is a rapid growth in the number of cryptocurrencies. So the paper also focuses on the types of cryptocurrencies available and tools available to implement the blockchain.

References

[1] Marko Vukoli´c. 2015. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International Workshop on Open Problems in Network Security. Springer, 112–125.

[2] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).

[3] Vitalik Buterin et al. 2014. A next-generation smart contract and decentralized application platform. white paper (2014).

[4] Giuseppe Destefanis, Michele Marchesi, Marco Ortu, Roberto Tonelli, Andrea Bracciali, and Robert Hierons. 2018. Smart contracts vulnerabilities: a call for blockchain software engineering?. In Blockchain Oriented Software Engineering (IWBOSE), 2018 International Workshop on. IEEE, 19–25.

[5] Arthur Gervais, Ghassan Karame, Srdjan Capkun, and Vedran Capkun. 2014. Is bitcoin a decentralized currency? IEEE security & privacy 12, 3 (2014), 54–60.

[6] Garrick Hileman and Michel Rauchs. 2017. Global cryptocurrency benchmarking study. Cambridge Centre for Alternative Finance (2017).

[7] Zane Hintzman. 2017. Comparing Blockchain Implementation. Technical Report. SCTE/ISBE Society of Cable Telecommunication Engineers and International Society of Broadband Experts, Exton, PA, USA.

[8] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: a technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, March 2016

[9] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, "KARMA: A secure economic framework for peer-to-peer resourse sharing," 1st Workshop on Economics of Peer-To-Peer Systems, 2003

[10] D. Malkhi and M. Reiter, "Byzantine quorum systems," Distributed Computing, vol. 11, no. 4, pp. 203-213, 1998

[11] J. Douceur, "The Sybil attack," in Proceedings of IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251-260, March 2002

[12] A. Biryukov, D. Khovratovich, "Equihash: asymmetric proof-of-work based on the generalized birthday problem," Ledger, vol. 2, pp. 1-30, April 2017

[13] Justin Sun et al. 2017. Tron Whitepaper. Technical Report. tron network, Beijing, China. https://tron.network/.

[14] Melanie Swan. 2015. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

.