IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

The Blockchain Technology

Shiza Amreen J[1], Shailashree Mendon[2], Sujaya Nayak[3], Merlyn Melita[4]
Students, Department of Computer Science and Engineering[1,2,3]
Faculty, Department of Computer Science and Engineering[4]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India
shizaamreennrp@gmail.com[1], shailashree62@gmail.com[2], sujayanayak10@gmail.com[3], merlynmetita@aiet.org[4]

Abstract: *Today, Blockchain is a decentralized ledger of all transaction across a peer-to-peer network, technological weapon behind the success of Bitcoin, Ethereum and other various kinds of cryptocurrencies. Also the impact of blockchain technology on other existing applications and overview on the emerging blockchain technology and understanding on cryptocurrency and provide insight on blockchain and pros and cons.*

Keywords: Decentralised, Peer-to-Peer, Cryptocurrency

I. INTRODUCTION

Blockchain is a decentralized database, a chain of blocks that contain information in a systematic way, such that it becomes difficult or impossible to change, hack or cheat system. Blockchain is a set of blocks that records a information of transactions like who made the transaction to whom, the amount of trade as a digital ledger that is distributed across the network. It timer the digital document/data, making it impossible to edit or modify the information. Blockchain ensures data safety and transparency.

The main technology behind the cryptocurrency is the blockchain, which allows every client on the network to reach a consensus without trusting each other. The idea behind blockchain technology has been described since 1991 when researchers Stuart Haber and W. Scott Stornetta introduced a practical computer solution for time-stamping digital documents so that they do not may be altered or damaged.. And in 1992 Merkle tree were integrated to this system, making it more efficient by permitting several document to be collected into one block. However, this invention was never implemented, and the patent expired in 2004, four years before bitcoin was invented. Hal Finney a computer scientist in 2004 introduced the new functionality called Reusable proof of work which are also known as RPoW. The system works by receiving a non-tradable or non-fungible proof-of-work token based on Hashcash and in return generated an RSA signed token that can then be transferred from the person to someone else. The double spending problem was solved in RPow and integrity in real time In the history of cryptocurrencies, RPoW can be considered an early prototype and an important early milestone.

A individual or group using the pseudonym Satoshi Nakamo to introduced a white paper to a cryptography mailing list in late 2008 introducing a decentralized peer-to-peer electronic cash system named Bitcoin.Bitcoin was provided tracking and verifying the transactions by using by decentralized peer-to-peer protocol. Transactions are tracked and verified via a peer-to-peer system. Bitcoin can be mined by individuals to get a reward and its get validated. Bitcoin was created on January 3rd, 2009, when Satoshi Nakamoto mined the first bitcoin block, which had a reward of 50 bitcoins.

The first recipient of Bitcoin was Hal Finney, he received 10 bitcoins from Satoshi Nakamoto and the world's first Bitcoin transaction on 12 January 2009.In 2013, Vitalik Buterian, a programmer an a co-founder of Bitcoin magazine stated that Bitcoin needed a scripting language for building a decentralized applications. Vitalik developed Ethereum blockchain, which uses a functionality called smart contracts. Smart contracts are the programs they are written in some certain programming language. The application which executes in Ethereum are usually referred as Dapps(decentralized applications) and cyptocurrency of Ehereum is called Ether. In recent days blockchain technology has emerged outstandingly and its application is not only to restricted to cryptocurrencies it is used in numerous other arising domains.

II. BACKGROUND

A central part in every blockchain is the mining algorithm. Let's take one algorithm as an example. It's called Sha-256 secure hash algorithm 256 bits, it takes an input which can be anything text, number or even computer file of any length,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

the output will be of equal length called a hash. The 256 bits in machine code the input will give the same output every time it's not random but if you make a small change to the input the output will change completely its also called one-way function meaning that if you have the output you can't calculate what the input was you can only guess what the input was and the odds of guessing that right is one in 2 to the power of 256 which is pretty much impossible in other words it's secure.

Let's take one scenario of how blockchain works with simple example of transaction, here we have two parties named 'A' and 'B'. Let's assume user 'A' has 3 bitcoins and user 'B' has 2 bitcoins. Now the user 'A' wants to send the Bitcoins to user 'B'. The user 'A' has to initiate the transaction to construct the transaction record that contains the information about transaction and that was signed with user 'A's signing key and that actually contained user 'A's public verification key and 'B's public verification key as well. And that transaction information is basically broadcast out to the entire Bitcoin ecosystem to all the nodes in the peer-to-peer network. And the several nodes in the Bitcoin system that are going to receive this information about this transaction and they also get the information about the transactions that are taking place around the same time. These nodes are going to incorporate this transaction record into a ledger of all transactions that have ever taken place in the Bitcoin system. And their main aim is to collate these transaction into a transaction block. And they are going to basically hash the transactions in pairs usually a tree like structure to get a single digest value. This digest effectively encodes all of the transaction that are received before by these individual nodes. This digest is basically going to combine with hash of transaction block that was already exist in the network. The last block is combined with the most recent block. And we are basically end up with the sequence of number and convert that sequence of number into a challenge in a proof of work protocol. Let's assume proof of work is eventually found, the Bitcoin miner will announce the results to the overall peer-to-peer network

III. BLOCKCHAIN AND CRYPTOCURRENCY

A cryptocurrency is a digital asset with a primary function to work as a medium of exchange value within peer-to-peer economic system that uses cryptography to verify and secure a transaction and control creation of additional units. One of the main feature of the cryptocurrency is its decentralized and cryptocurrencies are highly secure and scalable. The cryptocurrency transaction charges are very less comparatively.

However, Private companies and foundations, on the other hand, administer and develop several cryptocurrencies. A technology known as Blockchain is at the root of most cryptocurrencies. In 2009 , Satoshi Nakomoto created the first cryptocurrency known as Bitcoin. Not only Bitcoin these days thousand other cryptocurrencies are also available in the market such as Ethereum, Litecoin ,Monero etc.

Bitcoin and Ethereum netwroks Ether are most widely used cryprocurrencies. Both of them are deployed using blockchain technology and both make use of proof of work and a mathematical computation. The only different is Bitcoin act as a digital currency and Ethereum is used for building the dApps.

3.1 Advantages of Blockchain

Crypto currency is decentralized where every transaction is recorded on same ledger everyone has their own copies of same ledger who is part of the network. Crypto currency is a open traceable transaction where is no need of paper work and documentation. Block chain is secure because it has encryption features and where transaction will be done instantly and transparently because ledgers will be updated automatically and authentication and transaction is verified by participants itself.

3.2 Disadvantages of Blockchain

Crypto currency transaction are stable because of privacy and security therefore it is difficult for the government to trace each user by their data. Bitcoin may be used as mode of exchanging money for illegal activities. It is volatility while investing money in crypto currency comes with potential of high returns because of valve of these coins can change widely in short period. It may cause data loss results in financial loss as if user loss private key to the wallet it remains locked and not accessible coins. No cancellation policy if a dispute occurs and in case user sends the coins mistakenly to the wrong wallet address we can't get back the coins.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

IV. CONCLUSION

The quick, practical overview of the basic concepts of how blockchains work and its applications. Given that background, the paper has suggested that there may even be transformational for the future applications, that are very applicable to the industry. However, the benefit of blockchains to those use cases must be carefully considered because blockchains can be inefficient and/or expensive. Where blockchains seem to fit well for industrial and applications, we may find that public or otherwise commercially-enabled chains.

REFERENCES

[1]. Lisa Morhaim, Blockchain and cryptocurrencies technologies and network structures applications, implication and beyond.
[2]. Knoll, J. Meinkoehn, Data fusion using large multi-agent networks: an analysis of network structure and performance, In: Pro] Jameela Al-Jaroodi and Nader Mohamed. Blockchain in industries: A survey. IEEE Access,
[3]. Martin Garriga ,AlanDerenzis, Maximilliano Arias, Blockchain and cryptocurrency : A framework of the main Architectural Drivers.
[4]. Brian A Scriber. 2018. A Framework for Determining BlockchainApplicability. IEEE Software 35, 4 (2018).
[5]. Arthur Gervais, Ghassan Karame, SrdjanCapkun, and VedranCapkun. 2014. Is bitcoin a decentralized currency? IEEE security & privacy 12, 3 (2014).
[6]. Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).
[7]. M. Marchesi, "'Why blockchain is important for programming designers, and why programming building is crucial for blockchain programming (Keynote),"' 2018 International Workshop on