ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 6 , June 2019

Blockchain Technology

Naseema Shaik, Mai Mohammed thabt Al-shahrani, Raghad Saeed Abdullah al mater, Hebah Ayad Ahmad Bjad

Lecturer, King Khalid University, Abha, Kingdom of Saudi Arabia
Student, King Khalid University, Abha, Kingdom of Saudi Arabia
Student, King Khalid University, Abha, Kingdom of Saudi Arabia
Student, King Khalid University, Abha, Kingdom of Saudi Arabia

ABSTRACT: Blockchain is a decentralized and distributed log of records, where, blocks containing a set of transactions are chained together by cryptographic hash value. Transactions originating from a node are validated by participating nodes and a set of transactions are added into a block by a “mining” node. Any mining node with sufficient compute power that solves a cryptographic problem can generate and broadcast a new block containing the set of validated transactions. Blockchain is a technology that allows data to be stored and exchanged on a peer-to-peer1 (P2P) basis. Structurally, blockchain data can be consulted, shared and secured thanks to consensus-based algorithms2. It is used in a decentralised manner and removes the need for intermediaries, or "trusted third parties". In this paper we are discussed on Blochckain technology instead of digital currency.

KEYWORDS: Blockchain, P2P, Cryptography, Hash key

I.INTRODUCTION

Blockchain was initially designed for P2P money only. But it soon showed the potential to be used for any kind of P2P value transaction on top of the Internet. Blockchain is a distributed, shared, trusted, public ledger of transactions, that everyone can check but which no single user controls. It is a distributed database that maintains a continuously growing list of transaction data records, cryptographically secured from tampering and revision. A Blockchain protocol operates on top of the Internet, on a P2P Network of computers that all run the protocol and hold an identical copy of the ledger of transactions, enabling P2P value transactions without a middleman though machine consensus. Blockchain itself a file - a shared and public ledger of transactions that records all transactions from the first block until today. The ledger is built using a linked list, or chain of blocks, where each block contains a certain number of transactions that were validated by the network in a given time span. The crypto-economic rulesets of the blockchain protocol regulate the behavioural rulesets and incentive mechanism of all stakeholders in the network[2]. This ledger runs on a Peer-to-Peer (P2P) network of computers. Distributed consensus based on economic incentive mechanisms combined with cryptography allows for secure P2P validation of transactions, thus bypassing the need for traditional trusted third parties.

Blockchain is a technology that allows data to be stored and exchanged on a peer-to-peer (P2P) basis. Structurally, blockchain data can be consulted, shared and secured thanks to consensus-based algorithms [4]. It is used in a decentralised manner and removes the need for intermediaries, or "trusted third parties". Blockchain emerged from the combination of two concepts:

1. Asymmetrical cryptography, which allows the use of a paired public and private key system.
2. Distributed IT architecture (especially P2P).

Asymmetrical cryptography enables users who do not know each other to exchange encrypted information. The system is based on a public key that can be made available to all, and allows encrypted data to be sent to a third party. The third party accesses the encrypted data via a paired private key[1]. The public key is similar to a bank account number, which can be provided to anyone. The private key, which remains secret, acts as the password to the same bank account. A distributed system is a series of independent computers such as nodes that connect to a network and can communicate with each other[3]. It is similar to the Internet, which also has no central node. Downtime for one server does not affect the other users. The blockchain network is a P2P distributed system. Information is shared among the different users.

II. HISTORY

Both blockchain and Bitcoin are a creation of ‘Satoshi Nakamoto’. Until now it is unclear who this is, it could theoretically even be a group of people. He himself claimed to be a man living in Japan, born on 5 April 1975. However, there is still some doubt and quite some names have already passed as possible real identities[3]. We can’t discuss the history of blockchain technology without first starting with a discussion about Bitcoin. Shortly after Nakamoto’s whitepaper was released, Bitcoin was offered up to the open source community in 2009. Blockchain provided the answer to digital trust because it records important information in a public space and doesn’t allow anyone to remove it. It’s transparent, time-stamped and decentralized[5]. Ever since it has been of interest to an increasing number of people. Currently a momentum around blockchain has been formed now the ’big four’ are investing in it. Blockchain is going to be of growing importance in the future. Dubai is even planning on being ”the first blockchain powered government in the world by 2020”[2].

III. BUILDING BLOCKS OF BLOCKCHAIN

There are three important aspects to be addressed in a Blockchain design.

1. Time stamping: When the transactions are chronologically ordered and a single history is agreed by majority of nodes, the double spending problem can be solved by always considering the first transaction from the sender as valid for the same funds[6]. Time stamping is achieved by collecting the pending transactions into a block and calculating the block hash. It can be proved that the transaction existed at the time of the block creation since it is hashed into the block. Granularity of this is time to generate a new block which is ~10 minutes in Bitcoin.
2. Consensus: New blocks are created & broadcast by mining nodes, each not being identical and arrive in different order at different nodes. It becomes a necessity for all the nodes to agree on a single version of block, thereby a consensus that is needed[7]. A distributed consensus (in a trust-less environment) must decide on which block out of several variants generated by multiple nodes would be added to the blockchain.
3. Data Security & Integrity: A malicious node cannot create fake transactions since private keys are used to sign the transaction. However, it can generate its own double spend transactions, one paying to a vendor and another paying back itself. While transaction ordering takes care to include only the first transaction, if the malicious node is able to generate blocks easily and deterministically, it can create new block with the transaction paying back itself. When this block is accepted by other nodes, the malicious transaction gets through.

IV. WORKING OF BLOCKCHAIN

Let us understand the working of Blockchain by going through how Bitcoin works since they both are linked intrinsically. In general, Blockchain technology is applicable to any digital asset transaction carried online.

The present-day internet commerce is exclusively tied to third-party financial institutions who validate and safeguard transactions[8]. A certain fraud is predictable in online transactions leading to high transaction costs.

On the other hand, Bitcoin uses cryptographic validation instead of third-party trust for carrying online transactions. Each transaction is protected through a digital signature. Every transaction is sent to the “public key” of the receiver signed using “private key” of the sender. In order to spend the cryptocurrency, an owner must prove his ownership of the private key. The owner of organization verifies this digital sign on the transaction using the public key.

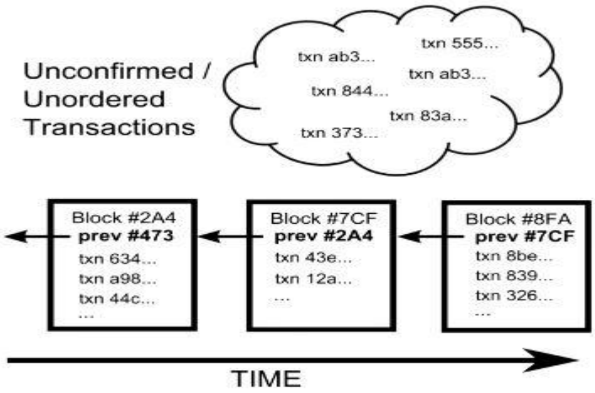

Fig.1: Blockchain unconfirmed Transactions

Each transaction is broadcast to every node of the network and finally saved in the public ledger after verification. Every transaction is verified before entering it into the Public Ledger. Each node ensures two things before recording any transaction:

1. Ownership of crypto currency by the sender (digital sign on private key).

2. Ensure spender has enough crypto currency in the account; estimating every transaction made from his account.

3. Now, arises the question of maintaining the order of transactions that are broadcast to each node in Bitcoin peer-to-peer technology. The transactions might not proceed in the same order as they are when generated. Hence, there arrives the need for a system which eliminates double spending of cryptocurrency.

4. In order to eradicate the problem, a mechanism has been developed wherein the entire Bitcoin network agrees regarding the order of transactions in a distributed system.

The bitcoins order themselves in the form of blocks, which link among themselves in a chronological order to form what is called "Blockchain". Each block holds transactions at a time. Every block carries the hash of the previous block[9]. "There can be multiple blocks in the line, then How does the network decide which block is next in the line?". Bitcoin will solve this problem as well. It introduces a mathematical puzzle. Each block comes in the line only when it answers this special mathematical problem. This whole process is termed as "Proof of Work". The nodes donating their complexity in solving puzzles and finding the results are termed as "miner nodes" and are financially awarded for their efforts.

This problem is not something trivial, its toughness can be adjusted owing the result is solvable within just 10 minutes for each node. There is very less probability of inaccuracy. The math involved is a bit difficult ensuring the stability of Blockchain. The network accepts and validates only the longest blockchain[10]. Hence, it is very difficult for an attacker to introduce a fraudulent blockchain which not only solves mathematical puzzles but also race against good nodes and generate the valid subsequent blocks. This job is made even more difficult since blockchains are linked together cryptographically.

V. CONCLUSION

This paper we sets out to provide a general explanation of blockchain. Blockchain truly is a mechanism to bring everyone to the highest degree of accountability. No more missed transactions, human or machine errors, or even an exchange that was not done with the consent of the parties involved. Above anything else, the most critical area where Blockchain helps is to guarantee the validity of a transaction by recording it not only on a main register but a connected distributed system of registers, all of which are connected through a secure validation mechanism. Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability.

REFERENCES

[1] Arnold, M. (2017). Blockchain-related job adverts surge. Financial Times. Online at ttps://www.ft.com/content/e49e5310-4923-11e7-919a-1e14ce4af89b.

[2] NIKHIL LOHADE, ’Dubai Aims to Be a City Build on Blockchain’, 24-4-2017 https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080? prclt=DyD2kRRG

[3] Satoshi Nakamoto, the creator(s) of bitcoin https://en.wikipedia.org/wiki/SatoshiNakamoto.

[4] Holotiuk, F., Pisani, F., & Moormann, J. (2017). The impact of blockchain technology on business models in the payments industry. 13th International conference on Wirtschaftsinformatik.

[5] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Online at https://bitcoin.org/bitcoin.pdf.

[6] Konstantopoulos, G. (2017). Million-User DApps on Ethereum: An Introduction to Application-Specific Sidechains. Loom Network Journal: Blockchain research, outreach, and tutorials.

[7] White, G. R. (2017). Future applications of blockchain in business and management: A Delphi study. Strategic Change, 26(5), 439-451.

[8] Smolenski, N. (2017). Blockchain in Government. Learning Machine. Online at http://www.learningmachine.com/wp-content/uploads/2017/07/Blockchain-in-Government-2017-Q3.pdf.

[9] S. Billah, “One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner,” 2015.

[10] D. Mazieres, “The stellar consensus protocol: A federated model forinternet-level consensus,”Stellar Development Foundation, 2015.