Block Chain: An Emerging Technology Routing to a New Internet Expedition

Husneara Sheikh[1] Rahima Meer Azmathullah[2] Faiza Rizwan[3]
[1,2,3]Prince Sattam Bin Abdalaziz University, Wadi Addawasir, Riyadh, Saudi Arabia

Abstract— This paper is proposed to build awareness about block chain technology, describing the evolution of digital currency in past and the present situation. This paper will also help to know about the rising resources of Bitcoin and other crypto-currencies that exist because of block chain. Block chain is the secured distributed ledger that no threat of information being modified as there is no central place hacker can break it. This paper provides an introduction of block chain technology, their operations, architecture and security. We will also discuss about the hypothesis and challenges come across.

Key words: Block Chain, Decentralization, Consensus, Proof-of-Work, Hashing

I. INTRODUCTION

The blockchain is an undeniably creative innovation. It is a tamper-evident, shared digital ledger that records transactions in a public or private peer-to-peer network. A distributed ledger is a database that is shared, replicated and synchronized. It records the transactions, such as the exchange of assets or data, among the participants in the network. No central authority or third-party mediator, such as a financial institution or clearing house, is involved. The information is not existed for hacker to corrupt. Blockchain technology created the backbone of a new internet by allocating digital information to be distributed. Information held on a blockchain exists as a shared and repetitively reconciled database.

Blockchain is not only for the financial sectors but also for almost any platform or product that requires reliability, such as keyless authentication. It is a distributed database that maintains a growing list of ordered records, called blocks. Each block has a timestamp and a link to a previous block. This makes blockchains exceptional for recording events like medical records, transactions, identity management, proving provenance etc.

Here, the Merkle tree approach allows for a hashing mechanism to provide efficient and secure verification of large amounts of data. This information is then used by Bitcoin to enforce their transactional checks. This technology proposes a lot of potentially disruptive control where companies are already in the race for different product offerings. “Blockchain will be the major technology of the next generation for its business application, it’s the latest internet.”

II. ORIGIN OF BLOCKCHAIN

The first well-known example of blockchain technology was outlined in a November 2008 whitepaper titled ‘Bitcoin’, the first cryptocurrency. Crypto-currencies are digital currencies protected through cryptography. Bitcoin has helped to evolve a major role in the development of blockchain technology, which describes a class of technology which goes far beyond bitcoin. This concept was commenced in 2008 by Satoshi Nakamoto, and implemented in 2009 as part of the digital bitcoin currency.

Earlier, the digital transactions were extremely complex. The process requires expectation against the threat of cyber-attacks. The intermediaries do not always manage our funds consistently to keep these records on a central ledger targeting for cyber-criminals.

Blockchains are secured databases and was first developed to process crypto-currency transactions between two parties on a decentralized network. It worked as the public ledger for all bitcoin transactions, which makes blockchains exceptional for medical records, financial transactions, and identity management sectors.

III. HOW DOES A BLOCKCHAIN WORK?

A. *Technologies used in Blockchain*

There are three primary technologies that create a blockchain:

1) Private Key cryptography,
2) A distributed network with a shared ledger and,
3) A motivation to check the network's transactions, record-keeping and security.

Private Key Cryptography	P2P Network	Blockchain's Protocol
Identity	System of Record	Platform

Table 1:

Private Key cryptography completes authentication requirements. Authentication and authorization are the key factors of a distributed peer-to-peer network. This network uses protocol for authorized transactions. They are also essential for digital transactions, which establish the configuration of blockchain technology. These technologies work together to secure digital transactions.

B. *Cryptographic keys*

The main purpose of blockchain technology is to create a secure digital identity reference based on private and public cryptographic keys. These keys collectively solve the purpose of digital signature. For instance, when sender and receiver carry out transactions over the internet, both of them holds a private key and, a public key as digital signature and the transaction is done over peer-to-peer network of devices (called miners) that is equipped with blockchain security. Miners assure each party is approved for every transaction, which are uniquely and accurately updated by blockchain. This process is called “Proof of Work.”

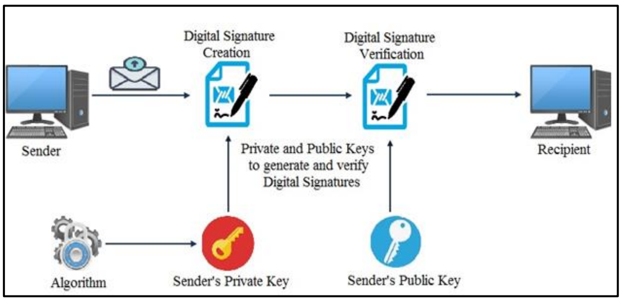
Digital Signature Creation
Digital Signature Verification
Sender
Recipient
Private and Public Keys to generate and verify Digital Signatures
Algorithm
Sender's Private Key
Sender's Public Key

Fig. 1: Digital Signature

C. *Identity*

Identity initiates with its distributed network and record system. Network size is vital for the security, where digital interactions are made with the combination of cryptographic keys. A block, which consist a digital signature, timestamp and relevant information, is then broadcast to all nodes in the network. Authentication needs to work out with the approved transaction and authorization. The main purpose of the protocol is to hide to work with different transactions altogether with all the nodes in the network, which maintains the history of transactions.

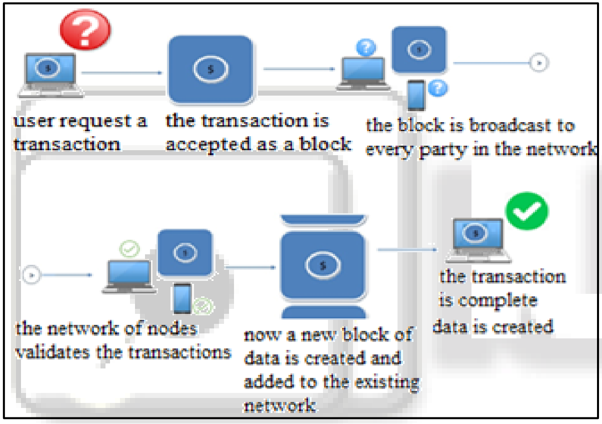
user request a transaction
the transaction is accepted as a block
the block is broadcast to every party in the network
the network of nodes validates the transactions
now a new block of data is created and added to the existing network
the transaction is complete
data is created

Fig. 2: Step-by-Step of Block Chain Technology

D. *Security*

Blockchain technology is data storage and possesses the following qualities:

1) It is a series of blocks that are linked with each other by reference.
2) Each block possessed with data record or transactions
3) Each block contains new and multiple transactions.
4) The blocks are unchangeable and references to the previous block, which develops a link between them.

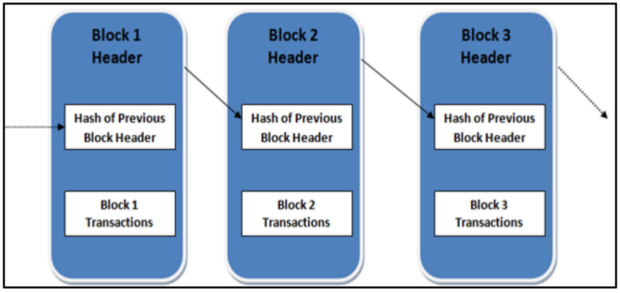

Fig. 3: Simplified Block Chain

E. *Decentralized*

The block chain is stored on multiple nodes to provide maximum data security from being manipulated.

The blockchain networks works like servers so that every node on a network can store complete or half of the blockchain.

F. *Consensus*

The blockchain network also holds a property called consensus. It means that the blockchain network must support any kind of amendments required or done to the blockchain and miners (also known as nodes) are rewarded for verifying the information. Individual blocks cannot be changed in blockchain, what can be done is to only create new blocks and this process of consensus referred to as Proof of Work (PoW).

G. *Proof of work*

1) Nodes validate transactions with other nodes on the network and submit transactions to the network.
2) These transactions exist in a "pool" of transactional data.
3) Miners (Special nodes) create a block containing the pool of proven transactional data while solving complex computer problem.
4) While creating the block, nodes validating new blocks must adhere to the blockchain protocol (rules).

There is a lot of work required for adding data to the blockchain, without any failure. It also ensures that the data cannot be tampered and enhance its security as the network increases.

H. *Hashing & Security*

The following point shows that the blockchain network would not allow any alteration to its transactional data:

1) Each block references the previous block on the network. It doesn't mean that one can simply create new blocks with references to previous blocks.
2) A block stores an address to the previous block and hash (a compressed version) of the data in the previous block. This makes it more secure.

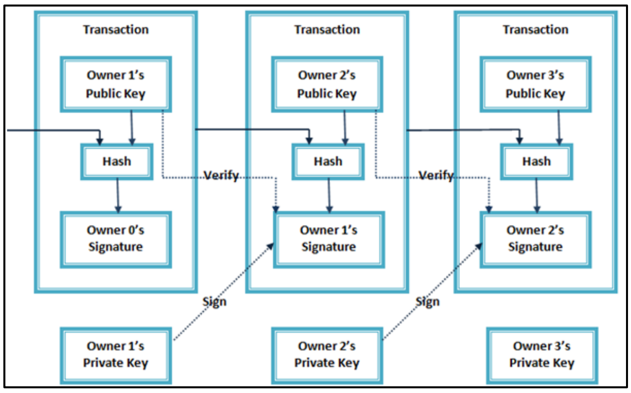

Fig. 4: Hash & Security of Block Chain

Above diagram shows, the "hash" of Block 2 is contained within Block 3. If the contents of Block 2 is changed then the hash of Block 2 would change, which is stored in Block 3, as would Block 3's hash, and so on. The network will not accept this change as every consequent block in the chain would no longer be linked to break the chain.

I. *Public vs. Private Network*

Blockchain has two types of networks, public and private.

1) Public Networks

These networks are owned by commercial chain like some malls or community centers. The machine is visible to others or initiates any kinds of data transfer with them. This saves the machine from malicious attacks and defends it from attacks from threats over a network.

2) Private Networks

These networks are owned by an individual – usually be located in Homes and Offices. On these networks, Smachines are visible to others and even initiate a data transfer between devices on the common network.

J. Crypto-Currencies

Crypto currencies are a spotlight of blockchain technology. In case of standard databases, operated by banks, cyber security is most important to prevent hackers from infiltrating the network. Blockchain technology is more secured and decentralized. It is extremely difficult to hack, and can stay online as long as there are nodes. The possibility of blockchain being used as a ledger with fund movement because of its transaction based nature. As a result, crypto currencies have emerged as digital currencies, which are not limited by banks or regulators.

IV. Challenges & hypothesis

Hypothesis: Digital Trust is an uncertain decision between different parties. It is quite challenging to trust in the digital world to prove identity (authentication) and permissions (authorization). There is unreliability in any technological revolution. Some blockchain industry believes that blockchain has become hyped-up, whereas others believes the technology has limitations and is unsuitable for most of the digital interactions; however, it has enlightened the latest issues and exceptions of blockchain through continuous research and development.

A. Complexity

Blockchain technology has made cryptography more conventional. The highly expert industries has full of jargon, which has been made effortless through glossaries and indexes.

B. Size of Network

Blockchains, like all distributed systems, are 'antifragile', which requires a large network of users. Blockchain needs to be a robust network else it would be complicated to get its advantage. There are many controversies about fatal mistakes for the blockchain projects.

C. Human Error

The information in the blockchain database needs to be highly secured. The data stored on a blockchain is unreliable, so events need to be recorded accurately in the first place.

D. Unavoidable Security Error

It is one of the distinguished security problems in bitcoin and other blockchains transactions. Satoshi Nakamoto, when he launched bitcoin, highlighted that if more than half nodes in the network is unreliable then it is considered as '51% attack'. It has become more important to ensure that the every transaction needs to be monitored effectively.

E. Politics

Blockchain and miners helps to digitize governance models, but there are public disagreements between different community sectors. These disagreements have become difficult for the blockchain industry though majority of users have agreed to it. These controversies can be technical, nevertheless informative for new opportunities for governance experimentation that blockchain technology is bringing up.

V. Conclusion

Blockchain is emerging and new distributed database with many still-to-be-found solutions. It is essential to educate people about the nature of the technology for its better and complete utilization. It should not be assumed that all blockchain system needs bitcoin mechanisms such as proof of work. The easiest method to enlighten what it does is to split the word blockchain into two – block and chain. This technology enables distributed public ledgers that hold immutable data in a secure and encrypted way and ensure that the transactions can never be altered. Of course, there are limits to the possibilities and uses of blockchain. For instance, it is unsuitable where data has to be able to be removed. Blockchain technology has been criticized for use in illegal activities; however, the hacker could not make changes to the blockchain. It is also being criticized in complexity, network size, human error etc. Despite all the controversies, the technology represent a real opportunity to all those who are connected with the future of business. The technology is not only shifting the way we use the Internet, but it is also serving to transform the global economy.

References

[1] Sloane Brakeville, Bhargav Perepa, Blockchain basics: Introduction to distributed ledgers. 16 October 2018. https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemix-trs/

[2] Bernard Mar, A Complete Beginner's Guide to Blockchain. 24 Jan 2017. https://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain/#3af147a36e60

[3] INTRODUCTION TO BLOCKCHAIN TECHNOLOGY https://www.3pillarglobal.com/insights/introduction-to-blockchain-technology

[4] Joshua Buirski, Blockchain, Distributed Ledger, A Brief Introduction to Blockchain Technology. Jul 28, 2017. https://dt.institute/2017/07/28/a-brief-introduction-to-blockchain-technology/

[5] An Introduction to Blockchain Technology (and Crypto-currencies) https://medium.com/station-five/an-introduction-to-blockchain-technology-and-crypto-currencies-d554cf410121

[6] Nolan Bauerle, images by Maria Kuznetsov. What is Blockchain Technology? https://www.coindesk.com/information/what-is-blockchain-technology/

[7] Nolan Bauerle, images by Maria Kuznetsov. How Does lockchain Technology Work?

https://www.coindesk.com/information/how-does-blockchain-technology-work/

[8] Nolan Bauerle, What are Blockchain's Issues and Limitations? https://www.coindesk.com/information/blockchains-issues-limitations/