IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Blockchain for Trusted Future

Murali Mohan Kotha[1*]

[1] Dept. of Mathematical Sciences, Sree Vidyanikethan Degree College, Sri Venkateswara University, Tirupati, India

[*]*Corresponding Author: kotha_mm@yahoo.com, Tel.: +91-9490 264 274*

DOI: https://doi.org/10.26438/ijcse/v7i2.631634 | Available online at: www.ijcseonline.org

Accepted: 15/Feb/2019, Published: 28/Feb/2019

***Abstract*—** The third industrial revolution brought in personal computers and the Internet. Like many sectors, the financial sector was also influenced by such digitalization and the internet, which resulted in the emergence of "FinTech". The blockchain is one of the many transformative and disruptive innovations of FinTech. The blockchain, though is relatively a new technology, has the potentiality, that it can be used in various other applications. Like the internet, which influenced the world, the blockchain is also expected to transform various operating models of finance. This in turn may result in evolution of new disruptive technological innovations. In recent years, many financial/ trade institutions across the globe, have been observing very closely, the developments in blockchain technology. The way the blockchain provides the complete confidence – with consensus, disintermediation, time-stamped and immutable recording of the linked transactions' history, in a distributed network – is attracted by several businesses. The blockchain can be adapted in IPR, finance, internet of things, and in any transaction for that matter. The blockchain can address the multi-party systems' inefficiencies, resulting in benefits to all. Further, the smart contract feature is useful in complex business workflows. This paper discusses structure of blockchain, its types, features, and explores some of its applications in different fields.

***Keywords*—** Financial Technologies, FinTech, Blockchain, Disintermediation, Immutable, Openness, Industry 4.0

I. INTRODUCTION

FinTech, also known as 'financial technology,' describes the way, the new and emerging technologies try to address consumer needs, and deliver financial services through automation. Several innovations of FinTech affected traditional trading, banking, financial advice and products. Some of the FinTech innovations include – crypto currencies, blockchain – a decentralized ledger, insurtech – to simplify insurance industry; among several others. The blockchain is a fusion of several technologies - decentralization of data, trustful transactions, executing a transaction when predefined criteria are met, data security using encryption etc. Though blockchain was designed for crypto currency – bitcoin; its unique features made its adaptability in several fields.

This paper is organized as follows. Section II deals with The Structure of the Blockchain; Section III contains Evolution of blockchain platforms; Section IV discusses Types of Blockchain; Section V describes Features of blockchain; while the Section VI explores Applications of blockchain; and Section VII presents Conclusion.

II. THE STRUCTURE OF THE BLOCKCHAIN

Satoshi Nakamoto proposed blockchain mechanism, for a crypto currency called bitcoin, in the year 2008. The blockchain can be considered as an operating system, upon which many applications can run. The bitcoin is the first use case for blockchain. The figure-1 shows the relationship between blockchain and several applications.

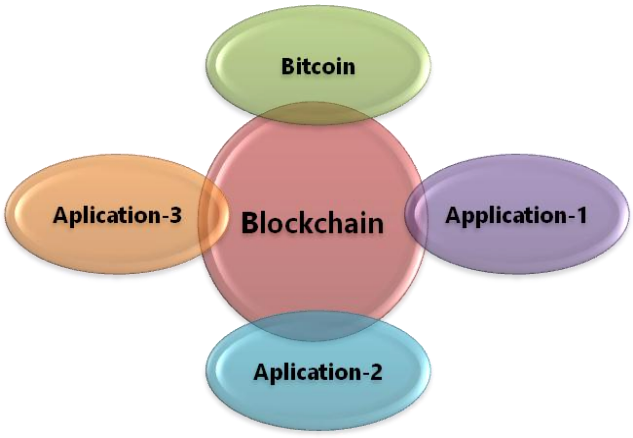

Figure-1 : The relationship between blockchain and applications.

When a new transaction occurs, all the nodes get notification about the same. Using proof-of-work mechanism, one of the miners approves it, followed by approval of all other miners. Then, the transaction gets recorded in the block. The same is

reflected in all nodes. The figure – 2, presents the same diagrammatically.

All the miners use their resources (like computing power, time, money, electricity etc.), during validation and the one who solves the puzzle first, is rewarded (with bitcoin).

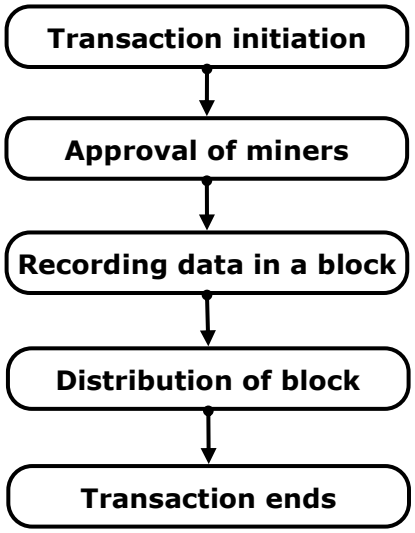

Figure – 2: Transaction process in blockchain

In blockchain, a block is the present part, which records several recent transactions. Once, the block gets completed, a new block is generated. This way, countless number of blocks exists in blockchain. Thus, a blockchain stores all transactions or events in chronological order, where all blocks are linearly connected – referred to as "Finished Transaction Blocks". It is represented as a data structure, and is distributed to all the parties, who share the network. The first block is known as the genesis block.

Every block consists of four components –

1. The data component – consists of transaction details like sender (origin), receiver (destination), the value of transaction, etc.
2. The previous hash – that points to previous block.
3. The nonce – a number, which is used for generating block hash.
4. The block hash – the digital finger print generated using SHA256 algorithm

The nonce is random number used to generate block hash. Hashing is a process, in which a string of any length is taken as input, which gives out an output of a fixed length. In blockchain, SHA-256 (Secure Hashing Algorithm 256) is used, which generates a hash of 256-bit length.

III. EVOLUTION OF BLOCKCHAIN TECHNOLOGY PLATFORMS

There are four versions in the evolution of blockchain technology.

A. Blockchain 1.0 : Currency

The very first application or use case of blockchain was bitcoin – one of the crypto currencies. The bitcoin was considered as the "Cash for the Internet". Such crypto currency was used in applications such as transferring the money, remittances etc.

B. Blockchain 2.0 : Smart Contracts

The smart contracts are autonomous computer programs, whose size is small, and reside in blockchain. They get executed automatically, when a predefined set of conditions are fulfilled. It is really impossible to hack or tamper smart contracts. Hence, the smart contracts reduce the cost of transaction verification, arbitration and even prevent fraud; which results in transparency.

C. Blockchain 3.0 : DApps

The DApps are known as Decentralized Applications. The backend code of DApps runs on a decentralized peer-to-peer network, a blockchain. The frontend of DApps/ user interfaces can make a call to its backend. However, such frontend should be hosted on decentralized storages.

D. Blockchain 4.0 : Adaptability of Blockchain in Industry 4.0

Blockchain 4.0 indicates using Blockchain 3.0 in everyday business scenarios. It should even satisfy the needs of Industry 4.0.

IV. TYPES OF BLOCKCHAIN

There are three types of blockchain networks:

A. Public Blockchains

The public blockchains do not have single owner. They are visible to everyone and any one can participate in it. It is like a blockchain that is "by the people, for the people and of the people". These types of networks offer incentives for those who secure them.

Ex. Crypto Currencies

B. Private Blockchains

A private blockchain is a private property of an individual or an organization. One can join the network, with an invitation of the administrator.

Ex. Blockchains of banks, insurance companies

C. Consortium or Federated Blockchain

It is a semi-decentralized one in which, a group of individuals makes decisions in the interest of whole network. Such group is called a consortium or a federation. That's the reason why, the name consortium or federated blockchain.

V. FEATURES OF BLOCKCHAIN

The various features of blockchain include:

A. Transparent Distributed Leger

Every node in the blockchain consists of an identical copy of a transaction. All the nodes will be updated with new transaction details.

B. Data Reliability and Security

The blockchain contains updated information, at all nodes. Thus, the data reliability is achieved. Since, each transaction is stored at many places, it leads to costly redundancy.
However, such kind of storing reliable data, at several locations, is required in different applications like citizens' data, land records etc.

Further, using private-public key mechanism, all the transactions are secured. Every transaction is encrypted at origin, using private key. The public key is made available to miners, using which the miners approve the transaction. A note worthy point is – if the private key is lost, all the assets of individuals will be considered vanished.

Since, Cryptographic Hash Algorithms like SHA-256 (256 bit Secure Hash Algorithm) are used, the transactions remain unaltered.

Any intrusion into the network can be averted using blockchain. Since the miners monitor the network, the integrity of records is assured. Even if a record in a node is altered, the original data can be restored from other nodes.

C. Consensus and Trust

The blockchain eliminates the need of intermediaries. Further, each and every transaction is verified and validated by all the miners in blockchain.

There is a famous Russian proverb - "trust, but verify." The same could be applicable for blockchain. Everyone trusts the data by consensus, since identical copies exist with them. However, everyone is responsible for verifying each and every transaction.

D. Widely Adaptable

Though blockchain has evolved for bitcoin, the exclusive characteristics of blockchain make it adaptable for many applications.

A transaction can get executed automatically, when the specified criteria is met. This is achieved using a special feature known as Smart Contract. The smart contracts are small programs that reside in blockchain.
Several financial companies are planning to use blockchain technology.

E. Anonymous, Irreversible and Traceable

Every transaction is executed in an anonymous manner. Further, such transactions can never be modified or rolled back. Since, every transaction is time stamped; one can trace a transaction and in this process, may even reach the provenance.

F. Lower Transaction Charges

All the transactions happen in peer-to-peer model. The transaction charges get reduced, since there is no presence of intermediaries/ regulators/ authorities.
However, the absence of regulators and transaction anonymity may result in illegal business, which should be addressed to.

G. Works Very Slow

The process of transaction verification and validation, recording distributing the same, in blockchain network takes longer processing time. Further, the blockchain network is getting congested due to its rising popularity.

VI. APPLICATIONS OF BLOCKCHAIN

Though relatively new technology, the blockchain technology is widely adaptable in several fields. Some of them are listed below:

A. Record Keeping

All transactions of tangible items like land, houses; and intangible items like IPR, copyrights, patents, trademarks etc. can be recorded in blockchain.

Several countries suffered loss of land records during tsunamis. Further, in many countries, the farmers do not have proper land records. Because of this, they do not get loans from banks. To overcome these problems, countries like India, have been digitalizing the agricultural land records using blockchain technology. This not only reveals who is the owner of land, but also reveals who owned it previously. This is beneficial for a society as it reduces the bureaucracy and the corruption.

The blockchain is even used for recording Intellectual Property Rights. It even helps in preventing plagiarism.
The students' data, faculty records, educational certificates, etc., are to be shared with multiple stakeholders. It is required to ensure that they are trustworthy.

The fraudulent medical practitioners can be prevented by putting all medical licenses on a blockchain.

B. Financial sector:

The blockchain is the most sought after technology in the field of finance since it provides transparency among all trading parties. Getting approvals for cross border business is really a difficult task, since different agencies require different data. The blockchain provides comprehensive data for all the parties like banks, transporters, tax departments, port authorities, insurance agencies etc.

In food-based supply chain, the traceability can be achieved from farmer to consumer. This helps in eliminating counterfeits.

C. Government:

The governments can provide a digital identity to countrymen. Such information can be made accessible to banks, educational institutions, election commission, courts, passport offices, hospitals etc.

Governments offer several benefits to people like – cooking gas subsidies, loan interest waiving, etc. The banks can transfer these amounts directly to the right beneficiaries account.

People can perform voter registration; and can even cast their vote using a computer/ laptop or even with a mobile phone. This prevents controversies, since it avoids electoral fraud.

In healthcare, the patients' data, doctors' data, diagnosis, treatment, billing – all can be maintained securely using blockchain. This ensures creating a secure system for accessing Electronic Health Records (EHRs). Using smart contracts, the medical bills payment can be done easily.

D. Internet of Things

The Internet of Things refers to a network of connected objects like structures, vehicles, or home appliances. It is expected that, by 2020 there could be 20 billion connected objects, and by 2030 the number could be more than 500 billion. Hence, several businesses want coexistence of distributed ledger (blockchain) and distributed things (IoT).

By merging both of them, a secured and verifiable data recording can be achieved. Such data can be processed by smart machines; so that the interconnected devices can interact with external world and can take decisions, without any human intervention.

VII. CONCLUSION

The internet and digitization resulted in emergence of new financial sector called the FinTech. This in turn spurred several innovations. The blockchain is one such. It is still in the phase of evolution. However, because of its disruptive and innovative features, several businesses are embracing blockchain technology. Started as the platform for a crypto currency bitcoin; emerged with smart contracts, and DApps; reached a stage of wide adaptability in several areas, including industry 4.0.

This paper explained the definition of blockchain, its structure, and types; and described its features, and explored some of its applications.

REFERENCES

[1] Zheng, Z, Xie, S., Dai, HN., Chen, X., Wang, H.: "*An overview of Blockchain Technology: Architecture, Consensus, and Future Trends*." In: 978-1-5386-1996-4/17 6th International Congress on Big Data PP557-564 IEEE (2017).

[2] M. Swan, "*Blockchain: Blueprint for a New Economy*", 1st ed. O'Reilly, February 2015.

[3] Singh, S, Singh, N.: "*Blockchain: Future of Financial and Cyber Security*". In: 978-1-5090-5256-1/16/PP463-467 IEEE (2016)

[4] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., Amaba, B.: "*Blockchain Technology Innovations*". In: 978-1-5090-1114-8/17/ Technology & Engineering Management Conference (TEMSCON) IEEE (2017)

[5] Hamida, E.B., Brousmiche, K.L., Levard, H., Thea, E.: "*Blockchain for Enterprise: Overview, Opportunities and Challenges*." In: The Thirteenth International Conference on Wireless and Mobile Communications-IEEE ICWMC (2017)

[6] IDRBT. (2017). "*Applications of blockchain technology to banking and financial sector in India*." White paper. Retrieved from http://www.idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf (last accessed on 4 January, 2019)

[7] Guo, R., Shi, H., Zhao, Q., and Zheng, D., "*Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems*." IEEE Access. 6:11676–11686, 2018.

[8] Doori A, Kanhere S, Jurdak R (2016) "*Blockchain in Internet of Things: Challenges and Solutions.*" CoRR. 1608

Author's Profile

Mr. Murali Mohan Kotha is currently working as Lecturer in Computer Science, in the Department of Mathematical Sciences, Sree Vidyanikethan Degree College, affiliated to Sri Venkateswara University of India. He has presented many research papers in several national and international conferences. His interests include – Internet of Things, Web Technologies and Programming Languages. He has 25 years of teaching experience.

