2018 International Conference on Computing, Power and Communication Technologies (GUCON)
Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018

A Future's Dominant Technology Blockchain: Digital Transformation

Dr Kavita Saini
Galgotia's University
Science and Engineering Greater Noida, India
kavita@galgotiasuniversity.edu.in

***Abstract*—The increase use of the Internet and digital currency by layman around has given direction to many researchers to evaluate its effectiveness and applications. The blockchain's effectiveness includes the increased security, transparency, cost reduction, of various transactions taking place in real life.**

The paper discuss about the emerging technology blockchain. Blockchain a cryptographically secure digital currency and can perhaps transform how the world works. The paper discuss about the challenges and how digital transformation is taking place. Paper also discuss about the future scope of Blockchain.

Keywords— Blockchain, Bitcoin, Digital Currency, Digital money, Cryptocurrency, digital ledger, secure money

I. INTRODUCTION

The adaptation of digital technology for implementing policies and schemes are highly considerable. But on the other hand the disruptive force are motivational force to change the current digital technology.

Data, transactions and records protects assets and sets organizational boundaries. Digital data set up and corroborate identities and chronicle events of any organization and works as a guided managerial[1]. These critical digital transformations yet have not kept appropriately with economists.

The corporate, insurance, banking and other financial and non –financial service sector institutions are also undergoing massive digital transformation. A new disruptive force of digital technology is changing the business models and increasingly becoming a crucial factor around the world [2].

In a digital world, the way we regulate and maintain administrative control has to change. The solution of this issue is Blockchain. This technology guarantees to take care of such issues. The Blockchain technology is an open, distributed ledger that can record exchanges between two parties productively and in a certain and long lasting way[7]. The ledger itself can also be programmed to trigger transactions automatically. The innovation at the core of Blockchain is bitcoin and other crypto currencies.

II. BACKGROUND

Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency. The attention in Blockchain technology is growing day by day as it provides security, anonymity and data integrity without involvement of third party organization. As in traditional transactions most of the transactions are taking place with the help of third party and those third party get paid by the entities involved in that transaction. Blockchain is one of the out of the ordinary and research areas from the perspective of technical limitations and challenges. [5]

In traditional currency transactions among entities often centralized and controlled by a third party entity and all information are controlled by third party entity. [6] [5]

Blockchain technology has been developed to solve this issue.

The objective of Blockchain platform is to store all the transactions in decentralized database along with a very strong consistency support to it. It this decentralized database each entity maintains its own local copy of global data sheet. As this platform encourages only local copy of global data sheet, this platform ensures that each local copy is identical to other local copies and also updated based on the global information. All these local copies are collectively called "Public Ledger". Here a database of historical information of various transactions performed, is available to each entity involved as a stake holder. The historical may be used in future to perform any other transaction [6].

This technology ensures the elimination of the double spend problem with the help of public-key cryptography where each agent is assigned a private key. This private key is kept secret like a password and a public key is shared with all other agents. [7].

III. BLOCKCHAIN'S POTENTIAL

With Blockchain, one can envision a world in which contracts are embedded in digital code and stored in transparent, shared databases. The data is stored in such a way where it is completely shielded from deletion, altering, and any modification.

In this world each agreement, procedure, assignment, and each payment would have a computerized record and signature that could be distinguished, identified, validated, and stored and shared. Delegates like legal advisors, specialists, and brokers may never again be fundamental[4].

lawyers, brokers, bankers and other Intermediaries might no longer be necessary as individuals, organizations, machines, and algorithms would freely transact and interact with one another with little friction. With the immense potential of the Blockchain, individuals, organizations, machines, and algorithms would freely transact and interact with one another.

The Blockchain technology has potential to transform the way we are doing business and govern the organization[3]. That is because the Blockchain is not a "disruptive" technology, which can attack a traditional business model

with a lower-cost solution and overtake incumbent firms quickly, rather it is a *foundational* and revolutionary technology that has the potential to create new foundations for the economic and social systems[4][5]. Blockchain could transaction's cost and reshape the economy. It is necessity to prepared for the Blockchain's promise to become a new development environment. Blockchain technology is suitable to all the industries where data is shared across multiple entities.

Blockchain, mostly known as the backbone technology behind Bitcoin, is one of the emerging technologies currently in the market attracting lot of attentions from enterprises, start-ups and media. Blockchain has the potential to transform multiple industries and make processes more democratic, secure, transparent, and efficient. Though many financial and non-financial players are excited about the potential of this technology, the question that plagues the mind of the industry leaders is how to identify a good business case for Blockchain?

IV. Principles of Blockchain Technology

There are five underlying basic principles of Blockchain echnology. These principle are Distributed Database, Peer-to-Peer Transmission, Irreversibility of Records, Peer-to-Peer Transmission, and Computational Logic. These powerful theories make this technology acceptable all around the world.

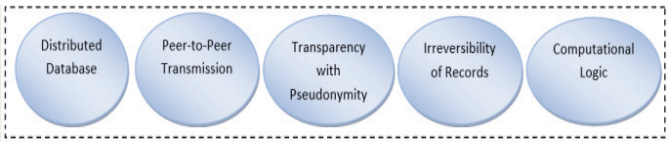

Fig. 1. Blockchain's platform

A. Distributed Database

Each entity on a Blockchain has access to the entire database and its complete history. No single entity controls the information and every entity can verify the records of its transaction partners directly, without an intermediary. Blockchain is basically an open and distributed ledger. This ledger records all the transactions between two entities efficiently and in a verifiable and permanent way[8].

: no central party for ordering or recording anything

B. Peer to Peer Transmission :

In this approach there is a software which that runs parallel to machines of all stakeholders involved in a particulay system instead of doing transaction done directly between two entities.

C. Transparency with Pseudonymity :

Each transaction is always refracted and stored to each who is the entity of that transaction. On Blockchain each participant is assigned a unique thirty plus character alphanumeric address that identifies it[4][8]. All the transactions occur between Blockchain addresses and Users may choose to remain unidentified or provide proof of their identity to others entities records cannot be altered, as they are linked to every transaction record that came before them (hence the term "chain")[8]. Number of approaches and technologies are deployed to make it sure that the changes make in the database are permanent, available to all the entities involved in the transaction and also in chronologically ordered.

D. Computational Logic

The transactions in Blockchain can be tied to computational logic as there is a digital ledger and in essence programmed. There is a wide possibility for set up rules and algorithms where these algorithms could automatically trigger transactions among various entities or nodes[8].

V. Architecture and Impact

Blockchain platform. The consensus, security and distributed replica of transaction makes this platform a transparency and robust [9]. It is a platform which is used for executing transactional services and spanned over multiple stake holders or sometimes to individuals who may not **trust** each other.

All transaction are append to shared ledger only and replicated across a network of peer nodes. Transactions are sent to public key addresses,- cryptographically generated addresses, computed by the wallet applications

This technology view not just the internal work of the organization rather keeps track of all the transactions of organization's outside entities with which organization interacts with.

With the Blockchain system digital ledger is distributed and replicated in a large number of identical databases each hosted and maintained by an interested entity. When changes are done by any of the entity in one copy of database, these changes are simultaneously update to other copies of database[6][8].

So if any transaction is being done by any of the entity records of the value and assets exchanged are permanently entered in all ledgers without intervention of third party[8].

VI. Blockchain Applicability

Ccryptographically secure Currency soon will be adopted by the central banks and going to be used widely. digital ledger technology will be launched as a Blockchain enabled ledger in future where The digital ledger will be used enhance transaction management capabilities[1].

The technology has potential to reduce the cyber risks by introducing the authentication through a visible ledger[1][9].

The technology is useful to create a secure trading environment among all involved entities, while rental agencies could use smart contracts. These agencies could allow automatic payment of rent with the assurance and confirmation through Blockchain platform. The consensus, security and distributed replica of transaction makes this platform a transparency and robust [9].

VII. Types of Blockchain

All Blockchain can be classified into three categories: Public, Permissioned, and Private.

A. *Public Blockchain :*

It is entirely decentralized and Transparent where anyone entity can read, send transactions and participate in the consensus process. A public Blockchain can be written or read by any entity with the proofs .

Public Blockchain is open to all users, any one can access or write transactions but after validation only. Public Blockchain as a decentralized and secure network is helping to eliminate all the agents who are working as a middleman.Bitcoin is one of the good example of public Blockchain.

Permissioned Blockchain:

Quasi decentralized where consensus is controlled by preselected set of nodes. Where read permission is restricted to Other entities.

B. *Private Blockchain:*

Private blockchain allows only few pre-selected participants have right to use and provide consensus on the transactions. Where all the entities or participants has Read permission only and only one entity Write permissions.

VIII. Transformation of Financial Behavior:

Blockchain technology is going to dominate the future finance. It is going to help in reducing the overall cost for all market participants so is going to change the global banking [1]. Similar to the e-mail that has change the way of communication, bitcoin is going to change the way of doing payment[1].

IX. Bitcoin Developer

To become a bitcoin developer one should be aware of blockchain technology. The crypto currency which was conceptualized by the mysterious Satoshi Nakamoto, in 2009 is a decentralized digital currency and works in a peer-to peer system. Bitcoin is also a crypto currency which is utilizing the blockchain technology.

To become a bitcoin developer it is essential to know the overall functionality of blokkchain. Satoshi Nakamoto [5] elaborated that similar to linked list where each node contains data and pointer to the next node, Blockchain is also a list (chain) of blocks. Each block contains information about transaction done in this chain where no central supervision is required.

A. *Pointers*

In programming language Pointer is a variable in programming which stores the address of another variable while the normal variables stores the data directly. As Pointer stores the address of other variables hence is termed as a pointer and the capability of pointing blocks towards the current location.

B. *Linked Lists*

linked list is one of the most important data structures, where each block of data may point to another block of data and hence called a linked list. A linked list looks as shown below:

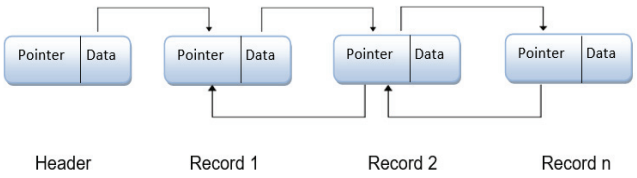

Fig. 2. Linked List

This structure of holding data and pointer may be used to store peer-to-peer transaction

It blockchain also there is a sequence of blocks. Each block contain data which is further linked to the next block. There two blocks are linked together through pointer. The pointer variable, in this case, contains the address of the next node in it and hence the connection is made. The last block has a null pointer which means that there is no further transaction in linked list chain.

And the answer for this question is the "genesis block". The first block is called the "genesis block" and its pointer lies out in the system itself.

Fig. 3. Hash Pointer

Hashing basically refers to a string input of any length that gives a fixed length output in response.

Where the hash pointer which contains previous block's hash and help maintaining the sequence of transactions . As Blockchain is a chain of various nodes or blocks where each block represents a transaction.

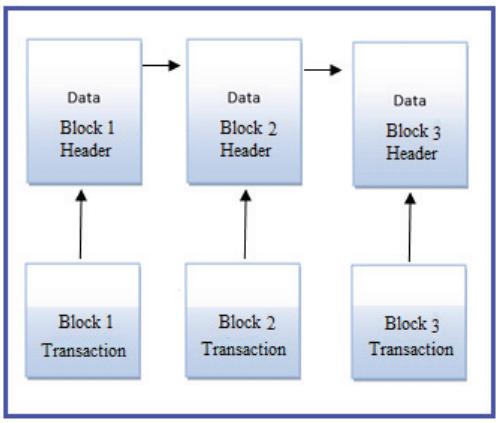

Fig. 4. Blockchain transaction Structure

So finally, a Blockchain is a linked list which contains data and a hash pointer where a hash pointer which points to its previous block or transaction. A hash pointer is similar to a pointer which not just obtain the address of the previous block rather also contains the hash of the data inside the previous block. This one small tweak, is what makes blockchains so amazingly reliable and trailblazing said Satoshi Nakamoto [5].

X. Security Aspect

The security in the Blockchain is obtained through the pointer and hash pointer contained in each transaction block. If anyone tries to attacks any block for example block 3 and tries to change the data will not be able to change Because of the of hash functions features. If any changes are made in data of any block, will change the hash of block 2 and block 1 also, and as a result will change the entire blockchain, which is impossible. Because of this properties only blockchains is unchallengeable and achieve immutability.

XI. Transactions in Bitcoin

Unlike traditional transactions in database, Bitcoin transactions are quite different. One don't have physically Bitcoin rather need to have only proof of having Bitcoins.

A Bitcoin (BTC) transaction means transferring BTC. Each transaction in Bitcoin refers to the previous transaction done. If fact OUTPUT of previous transaction is INPUT of new transaction.

Unlike FIAT currency one don't really keep track of how and where you got that specific note from, in Bitcoin, the history of each and every single Bitcoin transaction is taken note of. During any BTC transaction between two entities Input and Output which are the two different sides of transaction.

A. Transaction Input

It is the address of Bitcoin from which any amount is sent. So for making any transaction by any entity, he/she should have Bitcoins received from various previous transactions. Each transaction is stored in history of transaction done by involved entities so every entity is required to pull Bitcoins from the following transactions. These transactions could TX (0), TX (1) and TX (2)[10]. Here all three transactions need to be added to generate new input transaction called as TX(Input) as shown in following figure:

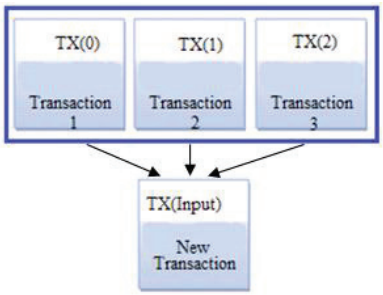

Fig. 5. Input Transaction

B. Transaction Output

Every transaction of Bitcoin generates an output. So in simple words the output is actually a Bitcoin amount available to spend by the users[10]. A pictorial representation of the output side looks like this:

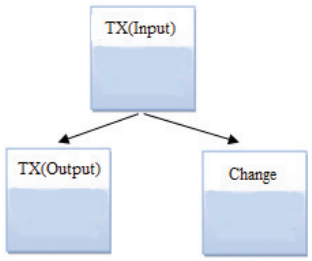

Fig. 6. Output Transaction

XII. Conclusion

The paper there is a discussion about the electronic ledger where electronic transactions are done without relying on trust.

Block chain use a framework of digital coins from digital signatures, which provides strong control to all the entities involved in transaction.

In this technology the acceptance and rejection of invalid block is done which makes it a very strong technology for future.

References

[1] https://www.shapingtomorrow.com/home/alert/665529-Future-of--Blockchain

[2] Blockchain technology in India Opportunities and challenges April, 2017 (ASSOCHAM)

[3] https://getpocket.com/explore/blockchain-technology

[4] https://www.entrepreneur.com/article/290197

[5] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (www.bitcoin.org)

[6] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander, Where Is Current Research on Blockchain Technology?—A Systematic Review, PLOS ONE, Edited by Houbing Song, vol. 11, issue 10, October 3, 2016 DOI: 10.1371/journal.pone.0163477

[7] Blockchain Works or blockchain technology : principles and applications [by Marc Pilkington]

[8] M. Iansiti, K. R. Lakhani, The Truth About Blockchain, Harvard Business Review, JANUARY–FEBRUARY 2017

[9] Barber S., Boyen X., Shi E., Uzun E. (2012) Bitter to Better — How to Make Bitcoin a Better Currency. In: Keromytis A.D. (eds) Financial Cryptography and Data Security. FC 2012. Lecture Notes in Computer Science, vol 7397. Springer, Berlin, Heidelberg DOI https://doi.org/10.1007/978-3-642-32946-3_29

[10] https://blockgeeks.com/guides/bitcoin-developer/

[11] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[12] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[13] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[14] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[15] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[16] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[17] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[18] W. Feller, "An introduction to probability theory and its applications," 1957