International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online))Volume 7, Issue 6, June 2018)

BlockChain Technology and its Applications

Pradeep Yadav[1], **Seema Yadav**[2]

[1]*Department of Information Technology and Communication, Jaipur*
[2]*Jaipur Engineering College and Research Centre, Jaipur*

***Abstract*— A blockchain is basically a distributed database of records or open record all things considered or advanced occasions that have been executed and shared among taking an interest parties. A blockchain originally block chain is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block,a timestamp, and transaction data. Every exchange in the open record is checked by accord of a lion's share of the members in the framework. What's more, once entered, data can never be deleted. The blockchain contains a certain and obvious record of each and every exchange at any point made. Bitcoin, the decentralized companion -to -peer computerized cash, is the most mainstream precedent that utilizes blockchain innovation. The advanced cash bitcoin itself is very disputable however the basic blockchain innovation has worked faultlessly and discovered wide scope of uses in both money related and non-financial world. The primary speculation is that the blockchain builds up an arrangement of making a distributed accord in the computerized online world. This enables taking an interest elements to know for sure that a computerized occasion occurred by making an undeniable record in an open record. It opens the entryway for building up a fair open and adaptable computerized economy from an incorporated one. There are gigantic open doors in this troublesome innovation and insurgency in this space has recently started. This white paper depicts blockchain innovation and some convincing explicit applications in both budgetary and non-financial segment. We at that point take a gander at the difficulties ahead and business openings in this basic innovation that is good to go to alter our computerized world.**

Keywords—Blockchain, Blockchain applications, Blockchain technology,

INTRODUCTION

Cloud A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made.

To use a basic analogy, it is easy to steal a cookie from a cookie jar, kept in a secluded place than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people. Bitcoin is the most popular example that is intrinsically tied to blockchain technology. It is also the most controversial one since it helps to enable a multibillion-dollar global market of anonymous transactions without any governmental control. Hence it has to deal with a number of regulatory issues involving national governments and financial institutions. However, Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications. Last year, Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the blockchain distributed consensus modelas the most important invention since the Internet itself. Johann Palychata from BNP Paribas wrote in the Quintessence magazine that bitcoin's blockchain, the software that allows the digital currency to function should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond. Current digital economy is based on the reliance on a certain trusted authority. Our all online transactions rely on trusting someone to tell us the truth—it can be an email service provider telling us that our email has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; or it can be a social network such as Facebook telling us that our posts regarding our life events have been shared only with our friends or it can be a bank telling us that our money has been delivered reliably to our dear ones in a remote country. The fact is that we live our life precariously in the digital world by relying on a third entity for the security and privacy of our digital assets. The fact remains that these third party sources can be hacked, manipulated or compromised. This is where the blockchain technology comes handy.

It has the potential to revolutionize the digital world by enabling a distributed consensus where each and every online transaction, past and present, involving digital assets can be verified at any time in the future. It does this without compromising the privacy of the digital assets and parties involved. The distributed consensus and anonymity are two important characteristics of blockchain technology. The advantages of Blockchain technology outweigh the regulatory issues and technical challenges. One key emerging use case of blockchain technology involves "smart contracts". Smart contracts are basically computer programs that can automatically execute the terms of a contract. When a pre-configured condition in a smart contract among participating entities is met then the parties involved in a contractual agreement can be automatically made payments as per the contract in a transparent manner. Smart Propertyis another related concept which is regarding controlling the ownership of a property or asset via blockchain using Smart Contracts. The property can be physical such as car, house, smartphone etc. or it can be non-physical such as shares of a company. It should be noted here that even Bitcoin is not really a currency--Bitcoin is all about controlling the ownership of money. Blockchain technology is finding applications in wide range of areas—both financial and non-financial. Financial institutions and banks no longer see blockchain technology as threat to traditional business models. The world's biggest banks are in fact looking for opportunities in this area by doing research on innovative blockchain applications. In a recent interview Rain Lohmus of Estonia's LHV bank told that they found Blockchain to be the most tested and secure for some banking and finance related applications. Non-Financial applications opportunities are also endless. We can envision putting proof of existence of all legal documents, health records, and loyalty payments in the music industry, notary, private securities and marriage licenses in the blockchain. By storing the fingerprint of the digital asset instead of storing the digital asset itself, the anonymity or privacy objective can be achieved. In this report, we focus on the disruption that every industry in today's digital economy is facing today due to the emergence of blockchain technology.

Blockchain technology has potential to become the new engine of growth in digital economy where we are increasingly using Internet to conduct digital commerce and share our personal data and life events. There are tremendous opportunities in this space and the revolution in this space has just begun. In this report we focus on few key applications of Blockchain technology in the area of Notary, Insurance, private securities and few other interesting non-financial applications.

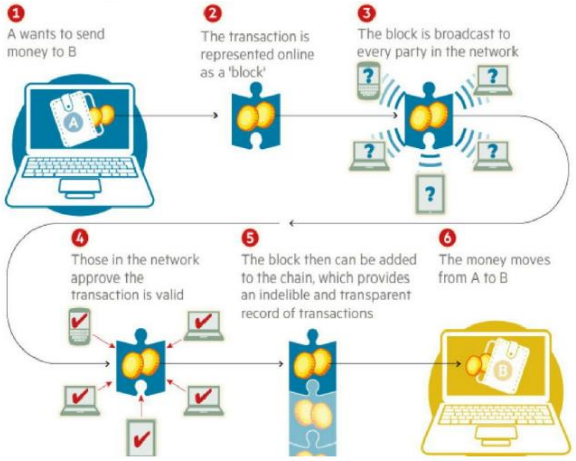
Blockchain Technology

A Blockchain allows untrusting parties with common interests to co-create a permanent, unchangeable and transparent record of exchange and processing without relying on a central authority. Bitcoin utilizes cryptographic confirmation rather than the trust in the outsider for two consenting partakers which was the case for all traditional to execute an online exchange over the Internet. Every exchange is ensured through an advanced mark. Every exchange is sent to the "public key" of the recipient carefully marked utilizing the "private key" of the sender. So as to burn through cash, proprietor of the cryptocurrency needs to demonstrate the responsibility for "private key". The element accepting the advanced money confirms the computerized mark – subsequently responsibility for "private key"- - on the exchange utilizing the "public key" of the sender.

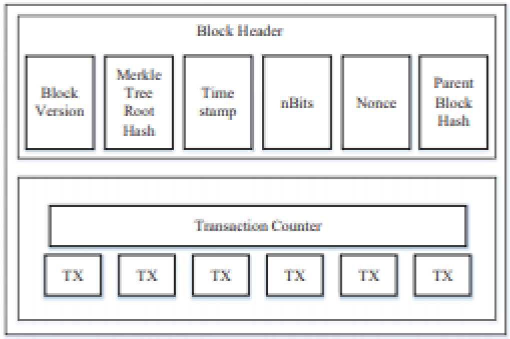
Every exchange is communicated to each hub in the Bitcoin arrange and is then recorded in a public record after check. Each and every exchange should be checked for legitimacy before it is recorded in the public record. Checking hub needs to guarantee two things before chronicle any exchange:

1. Spender claims the cryptocurrency—advanced mark confirmation on the exchange.

2. Spender has adequate cryptocurrency in his/her record: checking each exchange against sender record ("public key") in the record to ensure that he/she has adequate equalization in his/her record.


1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
?
✔

In the above diagram what is displayed as a block is actually comprises of multiple parameters. The structure of block is shown below:

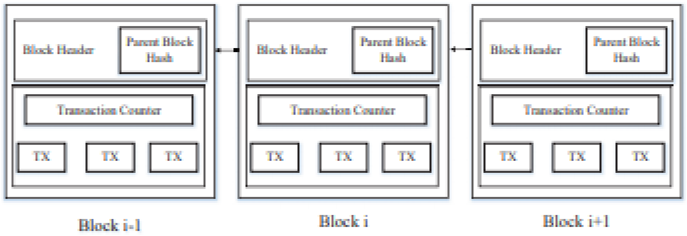


Structure of Block

Block Header

- The block number, also known as block height in some blockchain networks.
- The previous block header's hash value.
- A hash representation of the block data (different methods can be used to accomplish this, such as a generating a Merkle tree (defined in Appendix B), and storing the root hash, or by utilizing a hash of all the combined block data).
- A timestamp

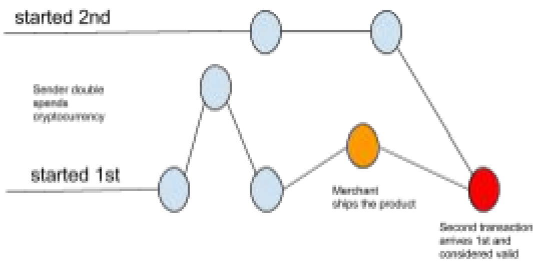
Blockchain technology works by sequence of blocks, each block is connected with other blocks as depicted in the diagram below.



Continuous sequence of blocks

Each transaction is broadcast to every node in the Bitcoin network and is then recorded in a public ledger after verification. Every single transaction needs to be verified for validity before it is recorded in the public ledger. Verifying node needs to ensure two things before recording any transaction: 1. Spender owns the cryptocurrency—digital signature verification on the transaction. 2. Spender has sufficient cryptocurrency in his/her account: checking every transaction against spender's account ("public key") in the ledger to make sure that he/she has sufficient balance in his/her account.

There is question of keeping up the request of these exchanges that are communicated to each other hub in the Bitcoin shared system. The exchanges don't come all together in which they are produced and henceforth there is requirement for a framework to ensure that twofold spending of the cryptocurrency does not happen. Taking into account that the exchanges are passed hub by hub through the Bitcoin organize, there is no certification that orders in which they are gotten at a hub are a similar request in which these exchanges were produced.


started 2nd
Sender double spends cryptocurrency
started 1st
Merchant ships the product
Second transaction arrives 1st and considered valid

This implies there is need to build up an instrument with the goal that the whole Bitcoin system can concur in regards to the request of exchanges, which is an overwhelming errand in a circulated framework.

The Bitcoin tackled this issue by an instrument that is currently known as Blockchain innovation. The Bitcoin framework orders exchanges by setting them in gatherings called blocks and afterward connecting these blocks through what is called Blockchain. The exchanges in a single blocks are considered to have occurred in the meantime. These blocks are connected to one another (like a chain) in an appropriate straight, sequential request with each square containing the hash of the previous blocks.

Applications of BlockChain

- **Private Securities**

It is over the top expensive to take an organization open. A syndicate of banks must work to endorse the arrangement and draw in speculators. The stock trades list organization shares for auxiliary market to work safely with exchanges settling and clearing in an opportune way. It is presently hypothetically workable for organizations to straightforwardly issue the offers through the blockchain. These offers would then be able to be acquired and sold in an optional market that sits over the blockchain

Mediciis being created as a securities trade that utilizes the Counterparty usage of Bitcoin 2.0. The objective here is to make a front line securities exchange. Counterparty is a convention that actualizes customary money related instruments as oneself executing keen contracts. These shrewd contracts encourage, check or uphold the arrangement of agreement and wipe out the requirement for a physical record. This dispenses with the requirement for a middle person, for example, merchant, trade or bank.

Blockstream is an open source venture with spotlight on sidechains- - interoperable blockchains- - to maintain a strategic distance from fracture, security and different issues identified with option digital forms of money. Utilizations can run from enlisting securities, for example, stocks, bonds and subordinates, to verifying bank adjusts and contracts. Coinsetter is a New York based bitcoin trade. It is taking a shot at a Project Highline, a technique for utilizing the blockchain to settle and clear monetary exchanges in T+ 10 minutes instead of the standard T+3 or T+2 days.

Augur is a decentralized expectation advertise that will enable clients to purchase and sell partakes fully expecting an occasion with the likelihood that a particular results will happen. This can likewise be utilized to make monetary and financial estimates dependent on the "astuteness of groups".

Bitshares are computerized tokens that dwell in the blockchain and reference explicit assets, for example, monetary standards or items. The Token holders may have the remarkable component of winning enthusiasm on items, for example, gold, and oil, just as dollars, euros and cash instruments.

- **Insurance**

Assets which can be exceptionally distinguished by at least one identifiers which are hard to devastate or recreate can be enrolled in blockchain. This can be utilized to check responsibility for resource and furthermore follow the exchange history. Any property (physical or advanced, for example, land, cars, physical assets, workstations, different resources) can conceivably be enrolled in blockchain and the possession, exchange history can be approved by anybody, particularly safety net providers.

Non-Financial Applications:

- Decentralized IoT

The IOT is progressively getting to be prevalent innovation in both the purchaser and the endeavor space. A dominant part of IOT stages depend on an incorporated display in which as agent or center point controls the association between gadgets, However, this methodology has turned out to be illogical for some situations in which gadgets need to trade information between themselves independently. This particular necessity has lead to endeavors towards decentralized IoT stages. The blockchain innovation encourages the usage of decentralized IoT stages, for example, verified and believed information trade just as record keeping. In such a design, the blockchain fills in as the general record, keeping a believed record of the considerable number of messages traded between savvy gadgets in a decentralized IoT topology.

- Decentralized DNS

Namecoinis is a blockchain innovation (with little varieties) that is utilized to execute decentralized adaptation of Domain Name Server (DNS) that is flexible to control. Current DNS servers are constrained by governments and vast partnerships, and could manhandle their capacity to blue pencil, capture, or keep an eye on your Internet use. Utilization of Blockchain innovation implies since DNS or phonebook of the Internet is kept up in a decentralized way and each client can have a similar telephone directory information on their PC.

- Public Key Infrastructure (PKI)

PKI innovation is generally utilized for concentrated appropriation and the board of digital certificates. Each gadget needs root authentication of the Certification Authority (CA) to confirm digital mark. While PKI have been generally conveyed and unimaginably fruitful, reliance on a CA makes adaptability an issue. The attributes of the BlockChain can help address a portion of the restrictions of the PKI by utilizing Keyless Security Infrastructure (KSI). KSI utilizes cryptographic hash work, enabling confirmation to depend just on the security of hash capacities and the accessibility of a blockchain.

- Decentralized Storage

Storj gives a blockchain based shared peer-to-peer distributed storage stage that enables clients to exchange and share information without depending on an outsider information supplier. This enables individuals to share unused web data transfer capacity and extra circle space in their individualized computing gadgets to those hoping to store substantial documents as an end-result of bitcoin based micropayments.

- Decentralized proof of existence of documents

Validating the existence of signed documents is of extreme importance in any legal solution. Traditional document validation models mostly rely on central authorities for the purpose of storing and validating. By blockchain provision a user can store the signature and timestamp associated. By leveraging the blockchain, a user can simply store the signature and timestamp associated with a legal document in the blockchain and validate it anytime using native blockchain mechanisms. Proof of Existence is a straightforward administration that enables one to secretly and safely store online proof of existence of any archive. This administration essentially stores the cryptographic condensation of the document, connected to the time in which a client presents his/her record. It is to be noted here that cryptographic overview or unique mark - not the real record is put away in blockchain, so client need not be stressed over the protection angle.

- Blockchain in the Music Industry

The procedure by which music royalties are resolved has dependably been tangled one, however the ascent of the Internet has made it considerably increasingly complex offering ascend to the interest of straightforwardness in the eminence installments by craftsmen and songwriters.This is the place the blockchain can assume a job by keeping up a far reaching, exact circulated database of music rights proprietorship data in a public record.

Notwithstanding rights proprietorship data, the eminence split for each work, as controlled by "brilliant contracts" could be added to the database. The "keen contracts" would characterize connections between various partners (addresses) and computerize their communications

- Healthcare

Blockchain Technology can possibly upset the social insurance industry's brought together tasks, opening the entryway for upgraded business and administration conveyance. The Distributed Ledger Technology (DLT) is an advancement fruitful with the likelihood of improved straightforwardness, security, and productivity. Shrewd contracts on the blockchain work naturally without outsider staff expected to confirm archives or explicit advances utilizing pen-and-paper forms. With mechanization comes a decrease in the famous organization that right now obstructs patients accepting the most ideal consideration.

- Contracts

Blockchain innovation gives the perfect motor to control digital characters. While digital personalities are developing as an unavoidable piece of our associated world, how we secure our online data is going under extreme examination. Blockchains based personality frameworks can furnish an answer for this issue with solidified cryptography and circulated records.

- Real Estate, Supply Chain and many others.

Conclusion:

To Conclude up, Blockchain is the innovation spine of Bitcoin. The conveyed record usefulness combined with security of BlockChain, makes it extremely appealing innovation to unravel the current Financial just as non-financial business issues. There is huge enthusiasm for BlockChain based business applications and henceforth various Start-ups chipping away at them. The selection certainly faces solid headwind as portrayed previously. The expansive Financial establishments like Visa, Mastercard, Banks, NASDAQ, and so on., are putting resources into investigating utilization of current plans of action on BlockChain. Actually, some of them are looking for the new plans of action in the realm of BlockChain. Some might want to remain on the ball regarding changed administrative conditions of BlockChain. To finish up, we imagine BlockChain to experience moderate selection because of the dangers related. The greater part of the Startups will fall flat with couple of victors. We must see great success and scope of Blockchain in coming years.

References

[1] Michael Crosby, Google Nachiappan, Yahoo Pradhan Pattanayak,Yahoo Sanjeev Verma, Samsung Research America Vignesh Kalyanaraman,Fairchild Semiconductor BlockChain Technology October 2015

[2] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, An Overview of Blockchain Technology, IEEE 2017 ICC

[3] “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,” 2016. [Online]. Available: http://www.coindesk.com/ state-of-blockchain-q1-2016/

[4] G. Foroglou and A.-L. Tsilidou, “Further applications of the blockchain,” 2015

[5] V. Buterin, “A next-generation smart contract and decentralized application platform,” white paper, 2014.

[6] J. Barcelo, “User privacy in the public bitcoin blockchain,” 2014

[7] Supriya Thakur Aras and Vrushali Kulkarni, “Blockchain and Its Applications – A Detailed Survey” Dec 2017

[8] Pilkington Mark. 2016 Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations, Social Science Research Network

[9] Peters G.W. Panayi E. 2016. Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money , Banking Beyond Banks and Money, Springer Sep 2016, pp. 239-278

[10] Satoshi Nakamoto. 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, [Online] http://www.bitcoin.org

[11] Buterin, Vitalik. 2015, On Public and Private Blockchains. [Online] https://blog.ethereum.org/2015/08/07/on-public-andprivate-blockchains/

[12] Xu et al. 2017. A Taxonomy of Blockchain-Based Systems for Architecture Design. 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3-7 April 2017