[NC-Rase 18]
DOI: 10.5281/zenodo.1485382

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

REVIEW PAPER ON BLOCKCHAIN TECHNOLOGY

D. P. Patil*[1] , Yasha Soni[2], Anand Rathi[3], Prashansa Lahane[4] & Kanchan Ingle[5]
[1]Assistant Professor, Department of Computer Science and Engineering
MGI-COET, Shegaon-444203 (MH.), India

ABSTRACT

It is blockchain, the technology behind digital currencies like bitcoin, and behind global, decentralized, secure solutions for doing trusted transactions - not only money transfers, but any digital asset. Blockchain is a huge global distributed but shared ledger, running on millions of devices and open to everyone. Digital assets including - money, music, houses, deeds, art, intellectual property, scientific discoveries, and even votes – are intended to be stored and transferred securely and privately with having blockchain technology working in as the nerve of corresponding systems. Blockchain technology provide cost effective source for transferring all sorts of assets, while making these transactions much faster and more secure. Just like, Wikipedia entries are not the product of a single publisher, with a blockchain, many people can contribute to writing entries into a record of information. No one person controls the information. Blockchain provide assuring enhanced security and (in some implementations, non-traceable) privacy for diverse applications in many other domains – including in the Internet of Things eco-system, cyber security, preserving digital identity. Various consensus algorithms, a cryptographic puzzle, are helpful in ensuring blockchain security by maintaining and verifying a digital ledger of transactions, which is considered to be incorruptible.

I. INTRODUCTION

A blockchain is an electronic ledger of digital records, events, or transactions that are cryptographically hashed, authenticated, and maintained through a “distributed” or “shared” network of participants using a group consensus protocol. Consider a checkbook of an individual. It is the record of entry indicating details of each transaction i.e. withdrawal, deposit, recipient and sender information, amount of transaction and date etc. Blockchain is same as a checkbook; a complete listing of each and every transaction. But the key difference between both of them is, the blockchain is distributed in a peer to peer network across all of the nodes for validating transactions with the help of consensus protocol. Also adding a block to the chain requires the approval n majority from the nodes in a network, thus making reflective changes completely impossible.

In a distributed ledger each node can independently hold and update a database in a network. There is no intervention of central authority in communication of records to various nodes. That is, every single node on the network processes every transaction, coming to its own conclusions and then voting on those conclusions to make certain the majority agree with the conclusions. And with mutual agreement the distributed ledger is updated, and all nodes maintain their own identical copy of the ledger. Since blockchain technology’s ability to eliminate the need for third party intervention in transactions, it allows payment to be finished without any bank or any intermediary. Various financial services such as digital assets, remittance and online payment can implement blockchain in their services. Additionally, it can also be applied into other fields including smart contracts, public services, Internet of Things (IoT), reputation systems and security services. To promote online transaction of digital assets, blockchain technology can help to create system based on cryptographic proof. Thereby helps provoking any two wiling parties to transact without any other trusted body.

Blockchain technology has the ability to create organizations based on DOs (Decentralized Organizations) and DAOs (Decentralized Autonomous Organizations). This change the way people arranges their affairs. With such ideology, organizations can re-implement traditional industrial governance by operating organizations autonomously without human involvement; maintaining the flexibility and scale of informal online groups. The organizations can own, trade and interact with other organizations without thinking of traditional notions of responsibility or legal personality.

II. LITERATURE REVIEW

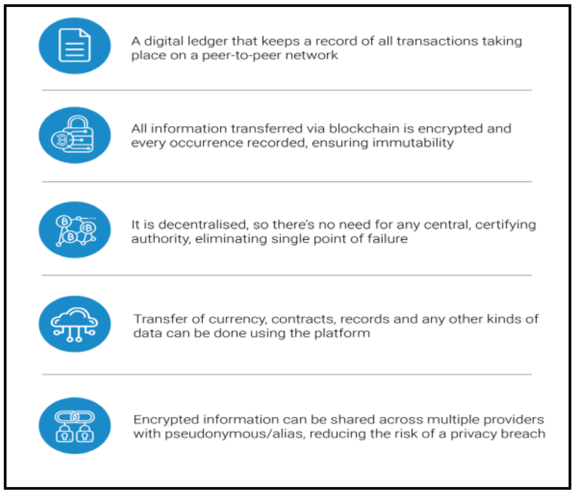
On a certain trusted authority Current digital economy is based on. Our all online transactions rely on trusting someone to tell us the truth—it can be an email service provider telling us that our email has been delivered; or it can be a social network such as bank telling us that our money has been delivered reliably to our dear ones in a remote country[3]. The fact is that we live our life perilously 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[1]. This is where the blockchain technology comes ready to hand. It has the prospective to transfigure the digital world by enabling a distributed consensus where each and every online transaction, past and present, including digital assets can be verified at any time in the future.

With a wide variety of cryptoassets and Blockchains coming up for various requirements, the need for interoperability of Blockchains is gaining momentum, and platforms like Cosmos, Polkadot and Microsoft's COCO framework are working to allow different Blockchain protocols to integrate and collaborate, enabling enterprises across segments to leverage the power of distributed ledger technologies[2]. Governments across the world and leading technology companies are collaborating to leverage the power of Blockchain to improve transparency and efficiencies, and increase speed of transactions and productivity. Globally, Blockchain is gaining significant traction, and the economic gains that are projected from the adoption of Blockchain technology are deemed enormous as per Keynote Strategy Research. [2] In India, even though the government's attitude towards cryptocurrencies is lukewarm at best, the same definitely doesn't extend to Blockchain technology.

III. OVERVIEW

1. Electronic register of Blockchain

A register of records or other transactions is simply a checklist of every transaction that has been recorded by the system. The blockchain is a continually-increasing digital register of transactions. Each set of transactions (the number of which is prescribed by the protocol) is considered a block in the chain, and the register as a whole is the blockchain.[4]



A digital ledger that keeps a record of all transactions taking place on a peer-to-peer network

All information transferred via blockchain is encrypted and every occurrence recorded, ensuring immutability

It is decentralised, so there's no need for any central, certifying authority, eliminating single point of failure

Transfer of currency, contracts, records and any other kinds of data can be done using the platform

Encrypted information can be shared across multiple providers with pseudonymous/alias, reducing the risk of a privacy breach

Figure1:Simple Blockchain representation

2. Encrypting data

Hash function: Blockchain technology typically uses the encryption method known as cryptographic hashing. When a transaction is agree, the contents of that transaction plus a few key pieces of metadataare encrypted using a mathematical algorithm. The output is known as a hash; a short digest of the data. Furthermore, since the hash is purely a short digest of the original, it is not possible to decrypt a hashmaintained in the blockchain and produce the original document, but it is possible to use the hashto validate a copy of a transaction or document keep outside of the blockchain.[5] It rapidly becomes impractical or impossible to maintain the entire ledger if every encrypted document is fully registered, and the computing costs to decrypt entire transactions would be very large.[4]

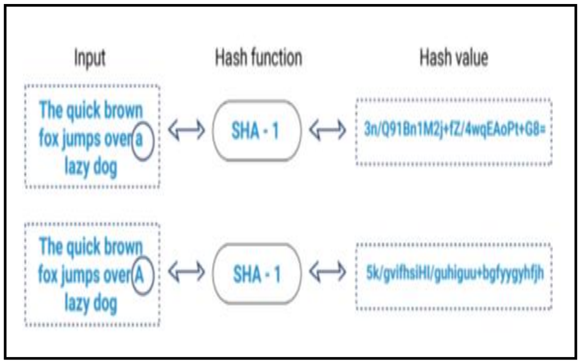

Input
Hash function
Hash value
The quick brown fox jumps over a lazy dog
SHA - 1
3n/Q91Bn1M2j+fZ/4wqEAoPt+G8=
The quick brown fox jumps over A lazy dog
SHA - 1
5k/gvifhsiHl/guhiguu+bgfyygyhfjh

Figure2:Hash function on an input data

3. Verification of Transaction

Digital Signature: The Private Key and Public Key are used to encrypt information using mathematical algorithms, rendering decryption virtually impossible without these keys.[2] However, spoiling the result is difficult without prior mastery of its factors. Digital signatures are unique characteristics of Blockchain transactions, and provide a layer of security to carry out and approve genuine transactions. A digital signature is a mathematical scheme to show the genuineness of digital messages or documents. A valid digital signature gives the recipient reason to believe that the message was created by a known sender (authentication), and the sender cannot deny having sent the message (non-repudiation), or that the message was not altered in transit.

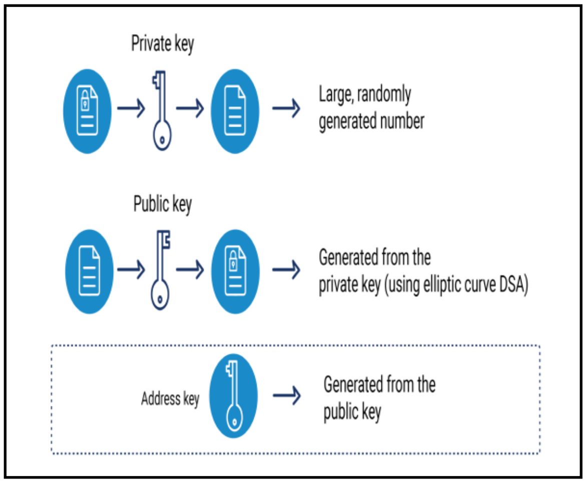

Private key
Large, randomly generated number
Public key
Generated from the private key (using elliptic curve DSA)
Address key
Generated from the public key

Figure 3:Public key and private key concept in Blockchain

A blockchain user or group of users will cryptographically hash the record of any transaction.[7] This hash is then broadcast to the network as the verification that a particular transaction has happen or event has been logged. Individual network nodes receive this broadcast and begin the process of ensuring that it is valid in confirmity with the protocol of that particular blockchain. Once a vital number of nodes agree that a set of transactions is well founded (i.e., reaching a consensus), those transactions can be added to the chain as a block, and future blocks can be built upon the information contained therein.[6]This ensures continuity of transactions and an unbroken transaction history.

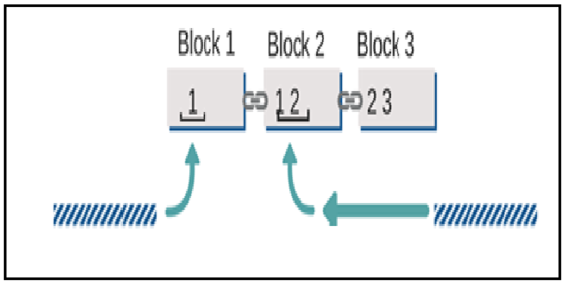


Figure 4:New blocks are added to the chain.

IV. WORKING PRINCIPLE

1. Blockchain Architecture

Blockchain is completely formed by a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. Figure illustrates an example of a block structure.

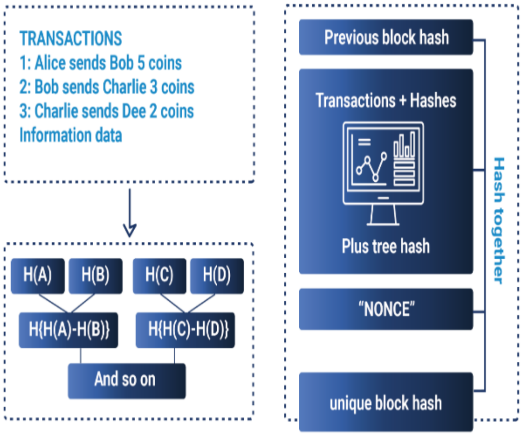


Figure 5:Block structure.

Blocks of the blockchain are data structures whose purpose is to bundle sets of transactions and be distributed to all nodes in the network. This blocks contain a block header, which is the metadata that helps verify the validity of a block.

Typical block metadata contains:

i. Version - the current version of the block structure
ii. Previous block header hash - the reference this block's parent block
iii. Merkle root hash - a cryptographic hash of all of the transactions included in this block
iv. Time - the time that this block was created
v. nBits - the current difficulty that was used to create this block
vi. Nonce ("number used once") - a random value that the creator of a block is allowed to manipulate however they so choose.

These 6 fields constitute the block header. The remaining part of a block contains transactions that the miner has chosen to include in the block that they created. Users create transactions and submit them to the network, where they sit in a pool waiting to be included in a block.

2. Working

To execute an online transaction over the Internet, bitcoin uses cryptographic proof instead of the trust in the third party for two willing parties transaction. Each transaction is protected through a digital signature. For success execution of any transaction it sends to the public key of the receiver digitally signed using the private key which is send by the sender. In order to spend cryptocurrency, owner of the cryptocurrency needs to prove the ownership of the private key. The digital signature is verified every time when user receives the digital currency thus ownership of corresponding private key on the transaction using the public key of the sender. Each transaction which is made on digital currency is broadcast to every node in the bitcoin network and is then recorded in a public ledger after verification. [10] Every single transaction needs to be verified for validity before it is recorded in the public ledger.

Verifying network node needs to ensure two things before recording any transaction:

- Spender owns the cryptocurrency and each transaction is verified by digital signature.
- Spender should have 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.

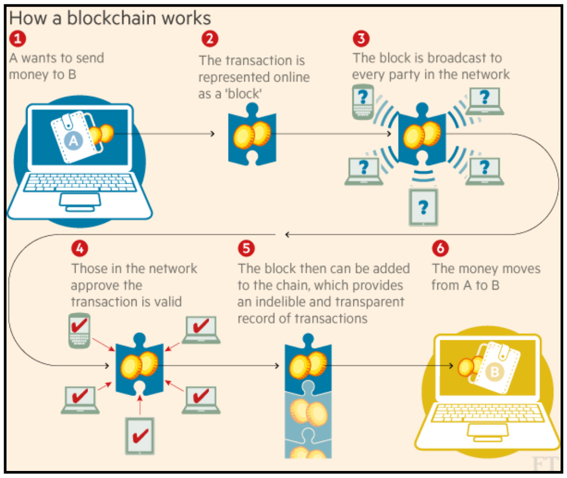

How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent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

Figure 6:Working of Blockchain.

3. Characteristics

1. **Peer to peer:** Blockchain enables peer-to-peer transactions across parties that are unknown to each other. Unlike in current methods, where trusted intermediaries or central authorities help alleviate third-party risk, peers in the Blockchain can transact through an automated programmer that guarantees correct transactions.
2. **Secure transaction:** Transactions on the Blockchain take place between parties verified and authenticated through cryptographically-secured keys, and digital signatures. Further, transactions are approved and authorized by a tested democratic process known as 'Consensus Mechanism'. [8]
3. **Decentralization:** In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Compare to the centralized mode, third party is no longer needed in blockchain.[9]Consensus algorithms in blockchain are used to maintain data consistency in distributed network.
4. **Persistency:** Transactions can be validate quickly and invalid transactions would not be admitted by honest miners. It is next to impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.[9]
5. **Auditability:** The data in blockchain is stored in the form of hashes and Merkle roots of sets of data. In case any data is changed, the hash of the data, and that of the overall set of data (stored in the form of a Merkle root or combined hash of hashes) changes. Hence, blockchain can be used to audit data to throw out any unapproved tampering.[9]

ISSN 2348 – 8034
Impact Factor- 5.070

6. **Immutable data:** The blockchain contains replicated transactional data appended to the existing database in the form of serially numbered and time stamped blocks after being approved by the constituents of the blockchain as per a standardized and fool-proof protocol. Hence, to change the data recorded in the system, one has to get approval from all parties, and even after that, the new data is recorded through approval of updating transactions. Once a transaction is approved and data recorded, it is considered immutable. All changes thus become identifiable in the form of updating transactions along with their corresponding track record. [8] This is how data in the Blockchain is considered tamper proof.

V. FUTURE SCOPE

1. Manufacturing

We discuss possible future directions with respect to three areas: stop the tendency to centralization, big data analytics and blockchain application. A lot of activity in blockchain technology is centered on financial applications, asset tracking, and supply chain. Application of a framework to identify various aspects in the manufacturing sector gives us an idea of the segments that are amenable to the application of blockchain technology. [8]

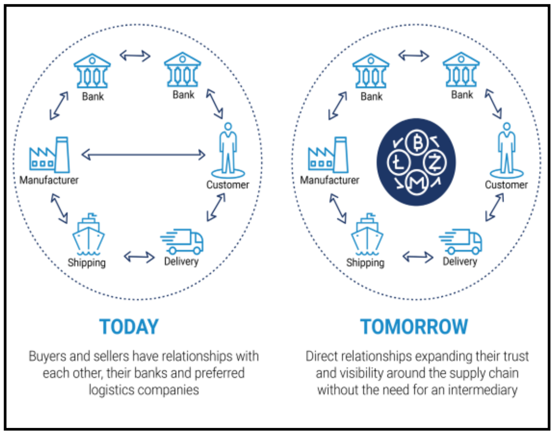

Bank
Bank
Manufacturer
Customer
Shipping
Delivery
TODAY
Buyers and sellers have relationships with each other, their banks and preferred logistics companies
Bank
Bank
Manufacturer
Customer
Shipping
Delivery
TOMORROW
Direct relationships expanding their trust and visibility around the supply chain without the need for an intermediary

Figure 7:Manufacturing with Blockchain technology

2. Energy Trading

Energy trading is another opportunity that is increasingly being evaluated for blockchain adoption. Smart contracts help trade any excess energy from producers, and can provide for listing, discovery, trading, and settlement of all transactions pertaining to energy trading among the generators and users. [8]

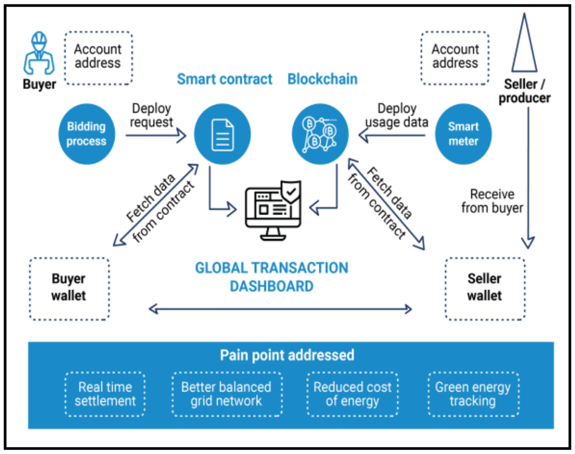


Figure 8:Blockchain based energy exchange

3. Cyber Security

Hackers use several techniques to incite an attack, like, sending thousands of junk requests to a website, increasing traffic until the site can no longer bear the coming requests and crashes. Current hurdle in preventing DDoS attacks come from the Domain Name System (DNS). As DNS is partially decentralized one-to-one mapping of IP addresses to domain names.

Implementing bockchain technology would fully decentralize DNS, distributing the contents to a large number of nodes and making it nearly impossible for hackers to attack. Domain editing rights would only be granted to those who need them and no other user could make changes, significantly reducing the risk of data being accessed or changed by unauthorized parties. BY using blockchain technology to protect data, a system can ensure that it's invulnerable to hackers, unless every single node is simultaneously wiped clean. [11]

4. Supply Chain

Blockchain can enable direct interaction among various parties in a supply chain, establishing programmer-driven trust and eliminating intermediaries. One example could be the tracking of refrigerated goods by recording the temperature across the value chain with the help of IOT devices. Further, the movement of goods from the manufacturer to the end consumer, along with the various parameters associated with the goods, can be tracked on a live basis with IOT sensors and devices tagged to the goods. [1] This will further help in the elimination of fake products as their ownership can be traced. An example use case is depicted below:

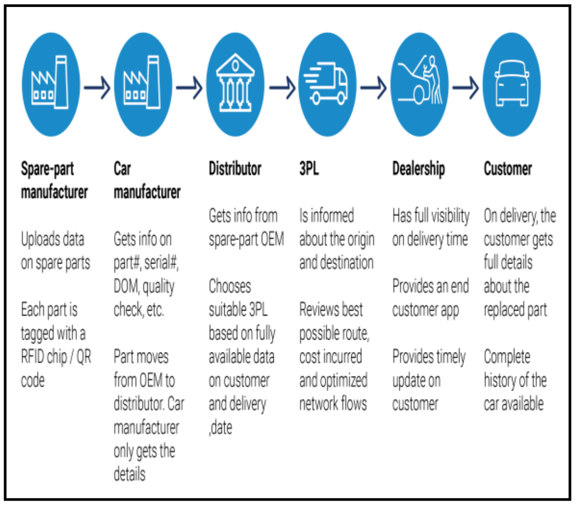

Spare-part manufacturer
Uploads data on spare parts
Each part is tagged with a RFID chip / QR code
Car manufacturer
Gets info on part#, serial#, DOM, quality check, etc.
Part moves from OEM to distributor. Car manufacturer only gets the details
Distributor
Gets info from spare-part OEM
Chooses suitable 3PL based on fully available data on customer and delivery ,date
3PL
Is informed about the origin and destination
Reviews best possible route, cost incurred and optimized network flows
Dealership
Has full visibility on delivery time
Provides an end customer app
Provides timely update on customer
Customer
On delivery, the customer gets full details about the replaced part
Complete history of the car available

Figure 9:End to end Blockchain enabled supply chain

VI. APPLICATIONS

1. Cryptocurrencies

- **Bitcoin:** Bitcoin is a type of cryptocurrency which is a form of the electronic cash. Bitcoin is a decentralised digital currency which can be transfer from user to user on the peer to peer bitcoin network without the help of central bank or single administrator. This transfer is note down or verified on the network node with the help of cryptography and stored in a public distributed ledger called a blockchain. Bitcoin is an open source software which was developed by a group of people using name Satoshi Nakamoto. At initial stage it was developed as a reward for the process known as mining further it used in exchange of goods, products, services and with other currencies also. The bitcoin blockchain is a public ledger that records bitcoin transactions.[12] t is implemented as a chain of blocks, each block containing a hash of the previous block up to the genesis block of the chain. A network of communicating nodes running bitcoin software maintains the blockchain.[13] Transactions of the form *payer X sends Y bitcoins to payee Z* are broadcast to this network using readily available software applications.

- **Ethereum:**Ethereum is a open source software platform which works on blockchain technology that allows the user to develop and deploy decentralised applications. Like bitcoin, ethereum also work on distributed public blockchain network. Although there is a significant difference in between bitcoin and ethereum, the most important difference is that bitcoin and ethereum differs substaintly in purpose and capability. Instead of mining for bitcoin, miners work to ether in ethereum blockchain. Ether is a type of crypto token that fuels the network beyond a tradable cryptocurrency. Ethereum was introduced by a cryptocurrency researcher and programmer Vitalik buterin in late 2013. Ethereum are also used to pay for computational services and transaction fees on the ethereum network. As like with other cryptocurrencies, the validity of each ether is provided with the help of blockchain, which is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography.

2. Smart Contract

A smart contract is the application of a bloackchain technology, which is a computer protocol which verify or enforce the negotiation or performance of contract. Smart contract allows transaction without third parties. Smart contract transactions are irreversible and trackable. The term smart contract was first proposed by Nick Szabo in the year 1994. Smart contract claims that many kinds of contractual causes may be made partially or fully self executing. The main of smart contract was to provide the superior security that is to the traditional contract laws and reduce the transaction costs related to the contracting system. Various type of smart contracts are implemented by different cryptocurrencies.Byzantine fault tolerant algorithms allowed digital security through decentralization to form smart contracts.[14] Additionally, the programming languages with various degrees of Turing-completeness as a built-in feature of some blockchain make the creation of custom sophisticated logic possible.[14]smart contract in blockchain, is a code fragment that could be executed by miners automatically.

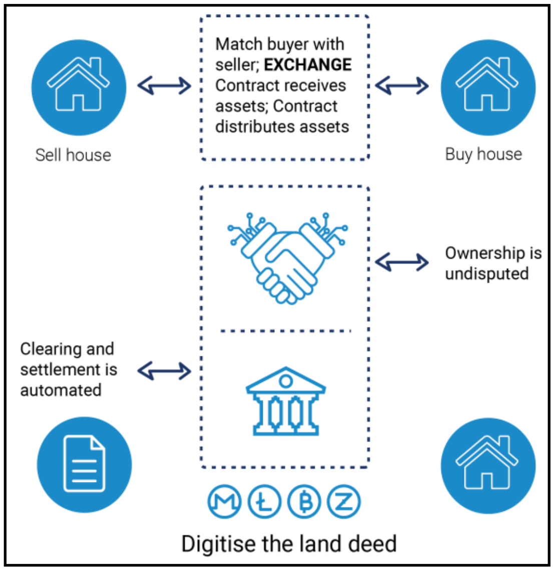

Match buyer with seller; EXCHANGE Contract receives assets; Contract distributes assets
Sell house
Buy house
Ownership is undisputed
Clearing and settlement is automated
Digitise the land deed

Figure 10:How smart contract works

VII. LIMITATIONS

1. Scalability

With the amount of transactions expanding day by day, the blockchain becomes bulky. Each node has to store all transactions to confirm them on the blockchain because they have to check if the source of the present transaction is unspent or not. Besides, due to the original restriction of block size and the time interval used to generate a new block, the Bitcoin blockchain can only exercise nearly 7 transactions per second, which cannot frealize the requirement of processing millions of transactions in real-time fashion. Meanwhile, as the capacity of blocks is very little, many small transactions might be delayed since miners prefer those transactions with high transaction fee.

2. Selfish Mining

Blockchain is open to attacks of colluding selfish miners. In particular, Eyal and Sirer showed that the network is vulnerable even if only a small portion of the hashing power is used to cheat. In selfish mining strategy, selfish miners keep their mined chunks without live-streaming and the private branch would be revealed to the public only if some requirements are satisfied. As the private branch is longer than the current public chain, it would be admitted by all miners.[15] Before the private blockchain publishment, honest miners are wasting their resources on an useless branch while selfish miners are mining their private chain without competitors. Hence selfish miners tend to get more revenue. Based on selfish mining, many other criticizes have been proposed to show that blockchain is not so secure. In stubborn mining, miners could amplify its gain by non-trivially composing mining attacks with network-level eclipse attacks. The trail-stubbornness is one of the stubborn strategies that miners still mine the blocks even if the private chain is left behind. Yet in some cases, it can result in 13% gains in contrast with a non-trail-stubborn complement. This shows that there are selfish mining strategies that earn more money and are profitable for smaller miners compared to simple selfish mining. But the gains are relatively small. Furthermore, it conveys that attackers with less than 25% of the computational resources can still acquire from selfish mining. To help fix the selfish mining problem, Heilman presented an novel approach for honest miners to choose which branch to follow. With random beacons and timestamps, honest miners would select more firm blocks. However, is vulnerable to forgeable timestamps. ZeroBlock builds on the simple scheme: Each block must be generated and accepted by the network within a maximum time interval. Within ZeroBlock,selfish miners cannot achieve more than its expected reward.

3. Privacy leakage

Blockchain can maintain a certain amount of privacy through the public key and private key. Users transact with their private key and public key without any real identity submission. However, it is shown in that blockchain cannot guarantee the *transactional privacy* since the values of all transactions and balances for each public key are publicly visible. Besides, the recent study has shown that a user's Bitcoin transactions can be linked to reveal user's information. Moreover, Biryukov et al. presented a method to link user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls. In each client can be uniquely identified by a set of nodes it connects to. However, this set can be learned and used to find the dawn of a transaction.

VIII. CONCLUSION

Blockchain technology is the emerging source to access the digital currencies, decentralized transaction systems; drastically changing the manufacturing, financial, educational, governance policy etc. By fusing all of these elements with blockchain technology, the user autonomy and individual freedom can be promoted to the higher level. Iteratively constructing and experimenting with blockcain based applications the world can get connected without any need of centralized institution and get corruption free governance. Regardless of nationality, people could be granted equal access to basic digital institutions and infrastructure such as decentralized laws, markets, judiciaries, and payment systems, which can be customized to each country's, group's, and individual's needs.

REFERENCES

1. *https://bitdeal.com/themes/default/pdf/WhitePaper.pdf*
2. *https://auxledger.org/img/news/msfu9mos-Blockchain-Report.pdf*
3. *http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf*
4. *http://www.dfr.vermont.gov/sites/default/files/Blockchain%20Technology%20Report_0.pdf*
5. *https://vdocuments.site/blockchain-technology-report-draft.html*
6. *https://www.linkedin.com/pulse/block-chain-technology-brief-analysis-tejash-chokshy/*
7. *https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf*
8. *Srinivas Mahankali, "Catalysing the Growth of India's Blockchain Ecosystem", Bengaluru, Karnataka.*

9. *Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangning Chen and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus and Future Trends", 2017 IEEE 6th International Congress on Big Data, China, 2017*
10. *https://cryptovest.com/education/what-is-consensus-algorithm-in-blockchain-and-why-do-we-need-it/*
11. *https://steelkiwi.com/blog/using-blockchain-technology-to-boost-cybersecurity/*
12. *"The great chain of being sure about things". The Economist. The Economist Newspaper Limited. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 3 July 2016.*
13. *"Bitcoin: Economics, Technology, and Governance". Journal of Economic Perspectives. Retrieved 21 July 2018.*
14. *https://en.wikipedia.org/wiki/Smart_contract*
15. *https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends.*