ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

An Overview of Blockchain Architecture and it's Applications

Sanjana Panicker [1], Vaishnavi Patil [2], Divya Kulkarni [3]

B. E Student, Department of Computer Engineering, Fr. Conceicao Rodrigues Institute of Technology, Navi Mumbai, Maharashtra, India [1,2,3]

ABSTRACT: The Blockchain technology is a newly developed computing paradigm that is responsible for developing a next step in the decentralized approach for creating applications.Blockchain involving records of ledger is a prime component in digital currency called bitcoin and its database interrelates trusted computing,decentralized consensus and smart contracts to empower users with high quality data.This paper aims at evaluating the distributed nature of the blockchain architecture and how it is a better solution, majorly explaining its working incorporating various real world applications that it possesses and a look into its pros and cons.

KEYWORDS: Blockchain, Bitcoin, Trusted Computing, Decentralized consensus, Smart contracts.

I. WHAT IS BLOCKCHAIN ARCHITECTURE?

A blockchain is basically a distributed data structure. It creates a digital ledger of transactions and thereby allowing to share it among a distributed network of computers and it also maintains a continuously-growing list of records called generally called "blocks" which are secured from tampering and revision.A blockchain implementation comprises of two kinds of records: blocks and transactions.In each block contains a timestamp and a link to a previous block is provided by the secure hash algorithm. The prime advantage is that it uses cryptography which allows different users to modify the transactions on a secured network each one accessing their node of data.If majority of nodes agree that the transaction performed looks valid, identifying information which matches the blockchain's history and thus a new block is added to the chain. Blockchain configurations are divided depending on the type and size of the network and then majorly by the use case of a particular company. The two types of blockchains are public and private. [1]

Ledgers are public if:

1. Anyone can write data, without permission granted by another authority.
2.Anyone can read data, without permission granted by another authority

For example, bitcoin is designed as a 'anyone-can-write' blockchain, where participants can add to the ledger without needing approval, there is no superior authority to decide, and it imbues a defense mechanisms against attacks.As a result there is an increased cost and complexity in implementing this blockchain.

In Private blockchain network the participants are known and trusted and there is a level of confidentiality.
For example, in a conglomerate, many of the mechanisms aren't needed or they are replaced with legal binding contracts making everyone whoever has signed the contract to abide to these rules. It rapidly changes the technical decisions used to build the solution. [2]

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Why use Blockchain?

The major question that arises is to why use blockchain when already the market has flourishing plethora of other databases.What substantial importance it holds against the competing products.For this let's understand the problem with the existing systems.

They could be summed up as follows:

(i) Difficult to monitor and evaluate asset ownership and its transfer in a trusted business network.
(ii) Inefficient, expensive, vulnerable: All these factors extremely hinder the performance and thereby destroying the progress.

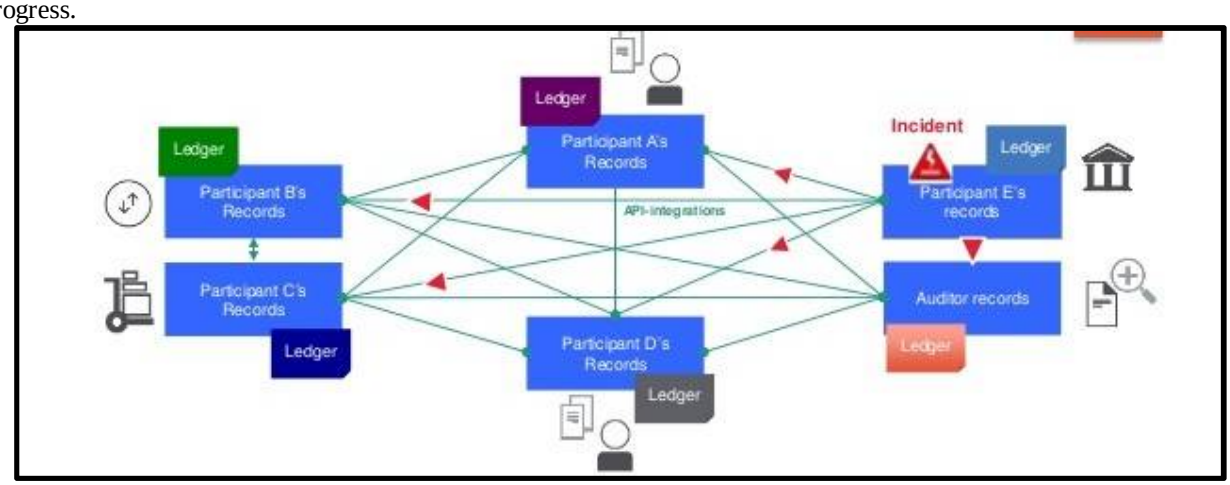

Fig 1: Problem with traditional system[3]

How will Blockchain provide the solution?

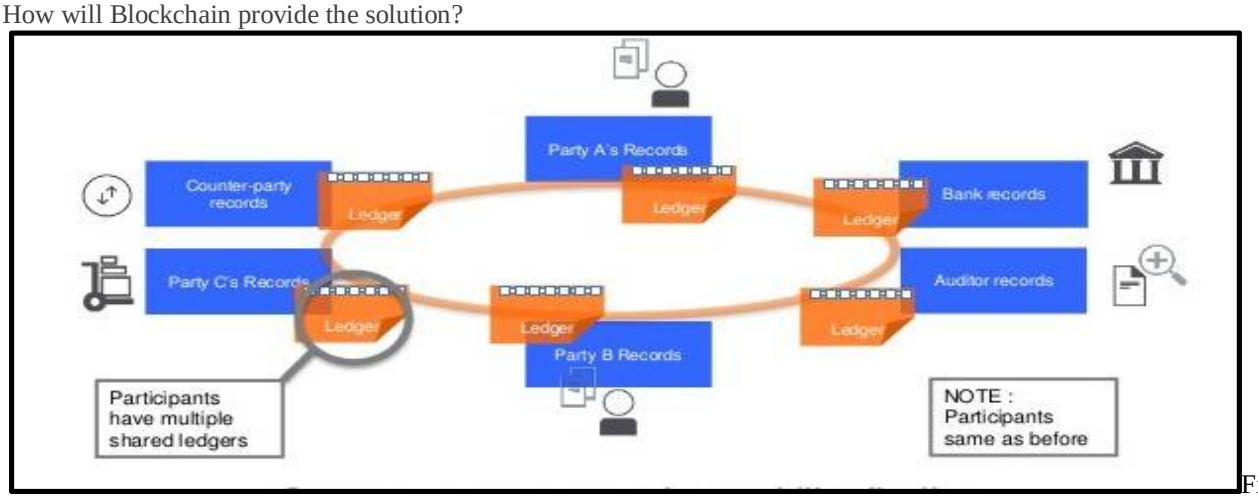

Fig 2: Blockchain's solution[3]

Blockchain unlike traditional systems is dynamic enough to become a leader in implementation in a mercurial market scenario.In a blockchain the supreme advantage it ensures is that each party has a record which is maintained in a ledger available to each one.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

It is a ledger widely passed between different users thereby creating a shared database which is replicated to these users and who can access it only after they have the access right for it.

Consensus, provenance, immutability, finality are the various aspects into which it works, making sure that all these facets work together into a reasonable amalgamation.

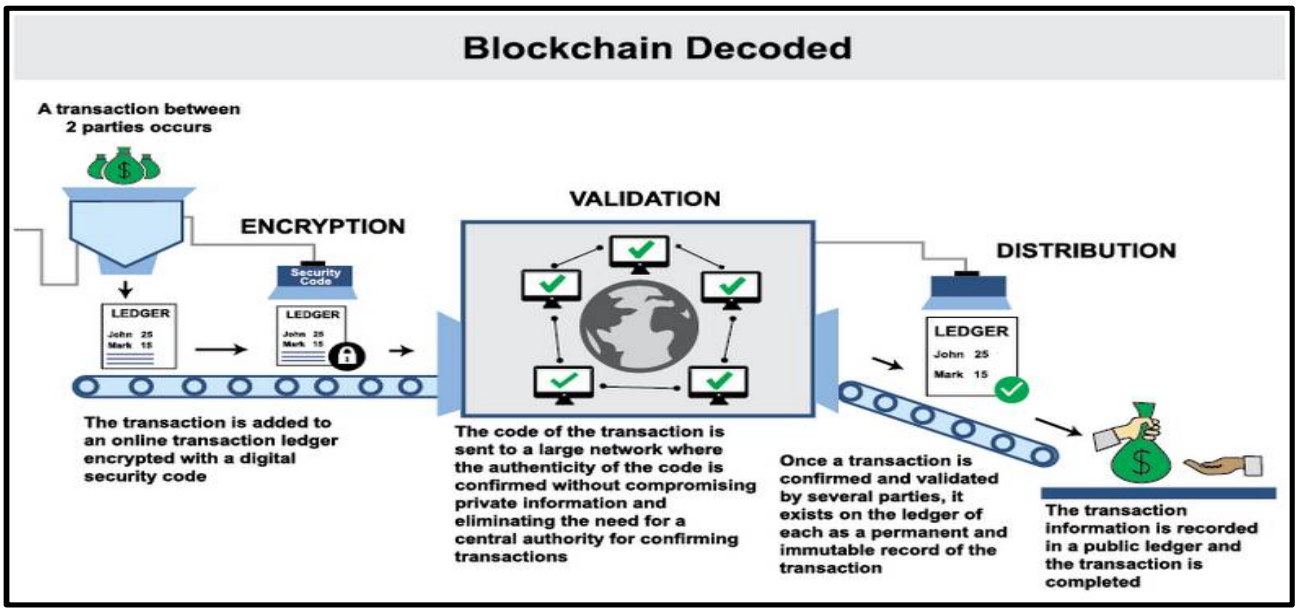

Fig 3:Anatomy of the Blockchain architecture[4]

The blockchain architecture consists of a few fundamental concepts like decentralization,digital signature,mining and data integrity.

(i) **Decentralization:** Rather than one central authority overpowering others in the ecosystem, blockchain explicitly distributes control amongst all peers in the transaction chain.

(ii) **Digital signature:** Blockchain enables an exchange of transactional value using public keys by the mechanism of a unique digital sign i.e. code for decryption known to everyone on the network and private keys known only to the owner to create ownership.

(iii) **Mining:** In a distributed system every user mines and digs deep into the data which is then evaluated according to the cryptographic rules and it also acknowledges miners for confirmation and verification of the transactions.

(iv) **Data integrity:** Complex algorithms and agreement among users ensures that transaction data, once agreed upon, cannot be tampered with and thus remains unaffected. Data stored on blockchain acts as a single version of truth for all parties involved hence reducing the risk of fraud.[4]

II. RELATED WORK

The Blockchain is a decentralized peer to peer distributed architecture.
Hence let us first see what is a peer to peer architecture, a decentralised architecture and distributed architecture.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

(i)**Peer to peer architecture:** This is a networking architecture model in which each computer or node has the same responsibilities and capabilities as the other nodes present in the network. It is a contrast from the traditional client server architecture where some nodes provide a service to the other nodes.

(ii)Distributed Architecture: Distributed architecture involves components hosted on multiple platforms and they communicate through a network comprising of a server and client, working as master and slave respectively.The introduction of blockchain into the distributed network has added to the distributed functionality not only making transactions dynamic but also providing user with a style of computing that is safer, faster and hassle free.

(iii)**Decentralized Architecture:** The key to Decentralized Architecture is the existence of multiple authority (control) domains, or agencies, participating in the application. Multiple artifacts are controlled by multiple "owners"
The parts may communicate over a network. Distributed system has parts of the system physically located in different places, but may still have one control point. Decentralized architecture mainly focuses on control problems in addition to latency and other problems. Grid computing is a "coordinated" resource sharing and computation in a decentralized environment.

III. HOW BLOCKCHAIN WORKS?

As described above the block chain is nothing but a distributed shared decentralized public ledger which is open to all. It is a data structure which is perceived to be robust and immutable.

The essence of the blockchain as showcased in it's most famous implementation to date is that the data is replicated. Every participant in the network has the same list of bitcoin txns. In a blockchain we check if the ledger is verifiable by a majority of the participants in the network. In the bitcoin network, this majority of participants is replaced by important members designated as the Validators in the networks. These validator nodes checks and then pass around the payments and the block data. This is because to maintain the essence of the blockchain philosophy, the bitcoin system aim to decentralized, thus not giving control to one single authority.

The working of a blockchain be it public or private is as described below:

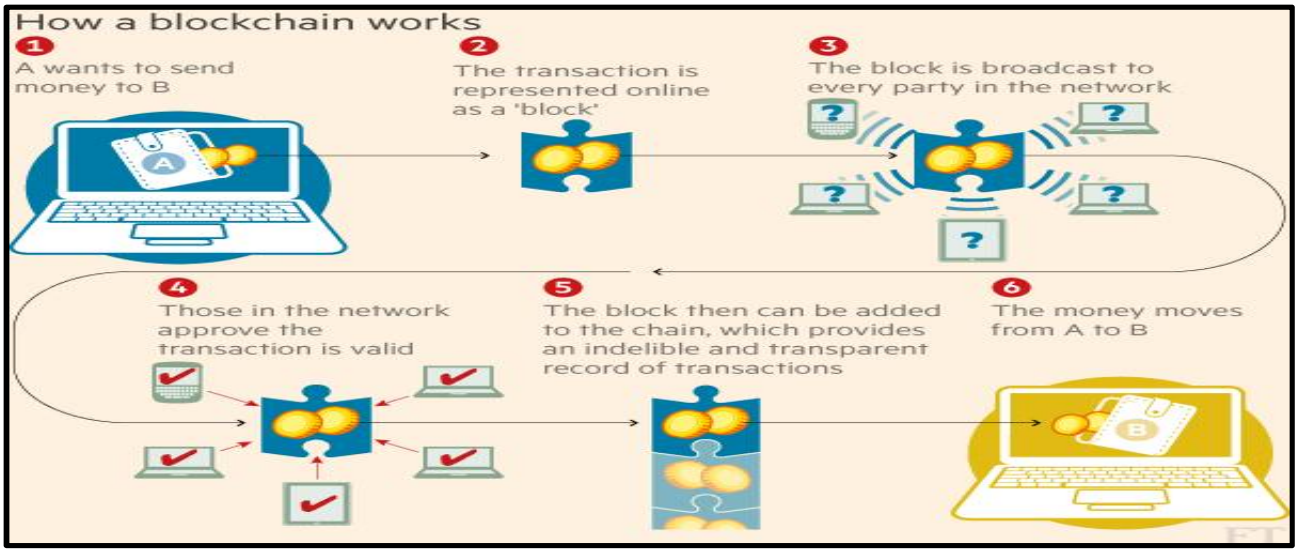

Fig 4:How a blockchain works[5]

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Let us consider 5 participants in our blockchain, A, B, C, D, E who are on a decentralized, distributed network. This blockchain example will implement the blockchain technology in the bitcoin system.

(1) A wants to send 50 bitcoins to B.
(2) This transaction of 50 bitcoins is represented online as a block.
(3)This block is then broadcasted to each and every participant in the network [C,D and E].
(4)In this example, C,D and E will serve as the validators in our network. The approve that the transaction is valid.
(5) This block containing the transaction them is added to the blockchain.
(6) The 50 bitcoins are transferred from A to B.

In Step 4, the validator, C, D and E execute cryptographic algorithms and conduct an evaluation and verification of the history of the individual blockchain under consideration. If the evaluation proves that history and the hash values are all valid, then the txn is accepted.This is known as distributed consensus.

If C,D and E for some reason cannot validate the information in the blockchain, then the data is rejected and entry for the block is denied and it is not added into the blockchain.[6]

Here, one must note that each block is like a page in a book. Just like a page contain two main characteristics, name a header containing book name/chapter name and page number, and the contents of the book which is the story, the block in the blockchain contains the header which is the hash value of the previous block and the content which is the bitcoin txn itself. [2]

So the Block 2 contains the hash value of Block 1,Block 3 contains the hash value of Block 2, Similarly Block N contains the hash value of Block N-1.
The first block is called the genesis block and it is different from the other blocks in the sense that it does not contain a hash value of another block and hence, produces an unspendable subsidy.[[7]]

The new blocks are added and linked to the older blocks of the blockchain. This chain is continuously updated so that every ledger remains the same.

The presence of this hash value is what makes the blockchain robust. If say Block 3 is to be modified, then the hash values in all of it's subsequent blocks (Block 4, Block 5….. Block N) is also modified, thus giving rise to a regenerated blockchain. This decentralized, transparent mechanism makes the blockchain secure, robust and free from damage. The validators and the generators add to the blockchain only if they verify that it is the latest block in the longest valid change. Another point to be noted here is that in a blockchain, the length of the blockchain is not the number of blocks but the combined difficulty of the blocks.

A blockchain is said to be valid:

(1) All the blocks in the blockchain are valid.
(2) All the transaction contained in the blocks are valid.
(3) If the blockchain starts with the genesis block.

IV. APPLICATIONS OF BLOCKCHAIN

The applications of the Blockchain technology can be broadly classified into two:
(1)Financial: The single biggest financial use of blockchain is the Bitcoin technology.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

This has now led to a monumental shift in the banking industry as well. Banks across the world are now experimenting with Blockchain. Big names like

- Goldman Sachs
- Barclays
- Citibank
- Rabobank
- ABN Amro
- ING Bank
- BNP Paribas

are experimenting with Blockchain.

In India, ICICI Bank has already carried out two transactions using blockchain technology. Kotak Mahindra Bank and Axis Bank too have started carrying out pilot transactions and they have been experimenting use of blockchain in various business segments. Kotak Mahindra Bank has claimed that the use of Blockchain can reduce the cross border remittances from two days to a few minutes. [8]
Another interesting use of Blockchain is being done in the insurance industry. The insurance industry now helps the clients and customers reduce the risk of cyber crime. It is also reducing the time for claims reporting and processing.[9]
The other financial use cases of Blockchain have been documented in the diagram given and they include uses in sectors like trading platforms, P2P transfers and currency exchange and remittances.

Fig5: Financial Use Cases[4]

(2)**Non-Financial:** The non financial uses of Blockchain are vast and many. A very interesting use is in energy distribution and in the solar energy market. The company LO3 has conducted an experiment wherein a New York resident could generate solar power and distribute a certificate for the generated solar power to his neighbour.

In association with ConsenSys, they have created the Transactive Grids where with the help of smart contracts energy is traded between participants who need and who have it. [9]
Some of the interesting uses in different fields along with use cases is given below:

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

(a) **Social Media:** Blockchain is being used in social media by rewarding users for their posts with financial incentives in applications like Steemit.

(b) **Opinion Voicing Platforms:** In websites like Glassdoor where there are users who post reviews and opinions, there is always a danger of forced authenticity giving rise to fake reviews thereby invalidating the genuineness of the website. Blockchain removes this forced authenticity and ensures legitimacy of the users.

(c) **Cloud Storage:** Storj is a blockchain enabled, end to end, distributed cloud storage platform which is used to store data. HyperLedger by IBM is another cloud storage application of Blockchain.

(d) **InternetOfThings:** Blockchain is being used in IoT in different applications like Cryptotronix which uses embedded cryptographic hardware and TilePay which enables data access on IoT devices.

(e) **Art and Ownership:** The company Deloitte has demonstrated use cases for the art industry. It has created an application which is used to track the authenticity, history of ownership and use of that work for a art artifact.

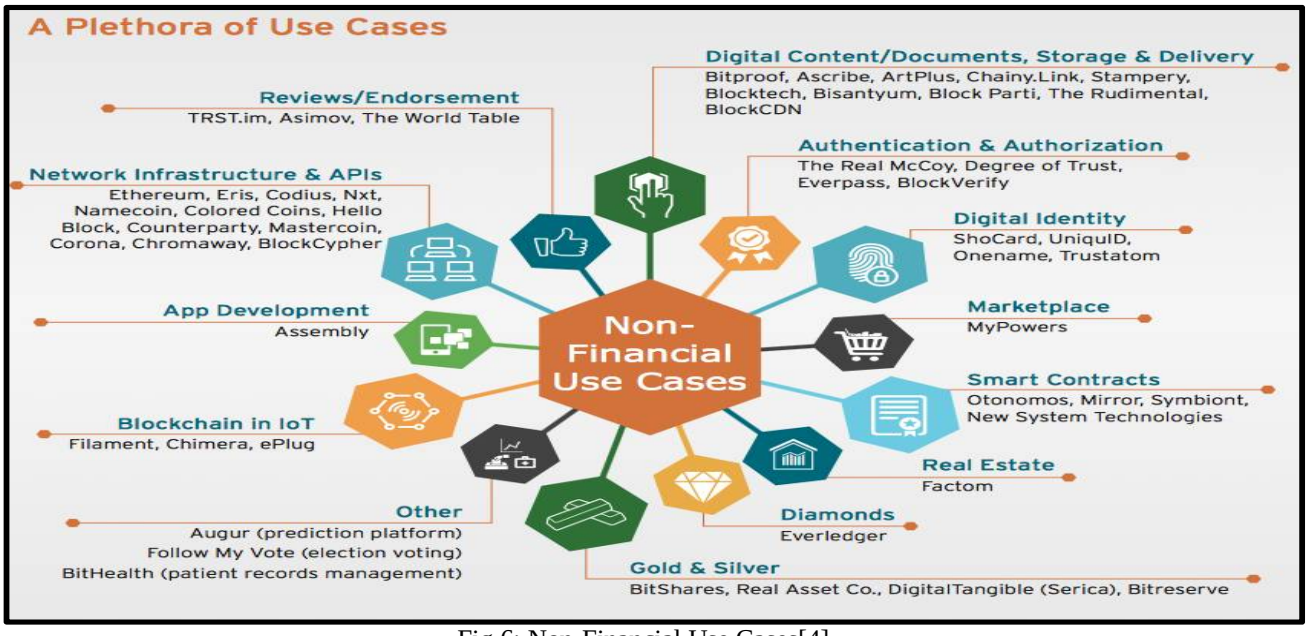

Fig 6: Non-Financial Use Cases[4]

The other non financial use cases of Blockchain have been given in the figure above.

V. ADVANTAGES OF BLOCKCHAIN

There are various advantages of Blockchain in many different fields.

(a) **Disintermediation:** Any two parties can make an exchange without any intermediation of a third party. Thus, the parties which are communicating with each other will not face any interference from a third party. This helps in reducing, sometimes even eliminating counterparty risks. [10]

(b) **Freedom in payment:** With blockchain comes freedom in payment. Using bitcoin it is possible to send and receive

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

money anywhere and anytime. Therefore, blockchain works very conveniently according to the user's wish. You do not have to worry about the bank holidays, the receiver's destination or any other such hurdles which normally occur while transferring money.

(c) **Decentralization and user empowerment:** Blockchain technology discards the need of any third-party or central authority of peer-to-peer transactions. Users are in full control of all their information and transactions. Thus, blockchain technology ensures user empowerment. The user is able to see all the transfers made, and if any one goes wrong, the user knows exactly where his money is.

Due to the decentralized network, there is no central point of failure in blockchain. Thus, failure of any one site will not affect the entire network. This leads to decreased number of malicious attacks.

(d) **Control and Security:** Blockchain allows users to be in full control of their information and transactions which leads to a safe and secure network.
Merchants cannot charge extra fees on an anything without their concern. They must first confirm with the customers and ask for their approval before making any changes.

Since all the personal information of users is kept hidden from other unauthorized users, blockchain protects against identity theft. Also, bitcoin can be backed up and encrypted to ensure the safety of your money. As a public ledger system, blockchain records and validates each and every transaction made, which makes it safe and reliable. Apart from that, all the transactions made are authorized by miners, which make them immutable and prevent various hacking threats. [11]

(e) **High Quality data:** The data in blockchain is of high quality, i.e. it is complete, correct, accurate and available to the users whenever they need it.

(f) **Speeding transactions:** Sometimes bank transactions take a lot of time(days or even months) for completion of the transactions successfully and for the final settlement. Blockchain transactions can help reduce transaction time to minutes by processing the transactions on a regular daily basis.

(g) **Transparency:** The changes done in the transactions are able to be viewed publicly by all users, thus creating a level of complete transparency. Moreover all changes that are made in the transactions are immutable, i.e the changes cannot be altered or deleted. Thus, the user does not have to worry about the integrity of his transactions.

With the blockchain technology, all the completed transactions is publicly visible, however personal and confidential information of the user is hidden. Therefore although the system is transparent, the user need not worry about the security, accessibility and integrity of his confidential information. The user's public address is what is visible publicly, his personal information is not tied to see.
For example, the transaction can be verified anytime in the Bitcoin block chain. The Bitcoin protocol cannot be manipulated by any person or organisation due to Bitcoin being cryptographically secure. Users can trust that transactions will be executed exactly as per the protocols. [11]

(h**) Reduced transaction costs:** Since a lot of overhead costs is reduced by eliminating third party intermediations, the overall transaction costs are also reduced.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

VI. DISADVANTAGES OF BLOCKCHAIN

While there are many advantages of using blockchain technology, we can also face some challenges while using it.

(a) **Lack of awareness:** Many people are still unaware of Blockchain technology and its applications. People first need to be made aware and educated about Blockchain, and they should be able to apply it to their lives. Since there is very less awareness about Blockchain, it is not able to be used by many people. This awareness can be spread using networking. {D2]
For wide application of Blockchain we should be able to resolve challenges such as transaction speed, verification process and data limits.

(b) **High standards of technology:** We need to set high standards for the security, robustness and performance of blockchains. This can be done by integrating blockchain with other non-blockchain systems. [12]

(c) **Managing risks of transition:** The solutions offered by Blockchain applications require significant changes to or replacement of existing systems. In order to make the switch companies must make a strategy for this transition to occur..

(d) **Upgrading of regulation and legislation:**There are many already existing and regulating modern currencies that have already been created. Because of this blockchain faces a hurdle in widespread approval and adoption by pre-existing financial institutes. New regulatory principles need to be included in order to make blockchain technology an integral part of the market. [10]

(e) **High Initial capital cost:** Although Blockchain reduces transactional costs, the high initial capital costs are deterrent.

(f) **Control, security and privacy** There are still cyber security concerns associated with blockchains that need to be addressed despite strong encryption. The users should be made aware of this problem before they trust their confidential information to a blockchain solution. [10]

(g) **Large energy consumption:** The blockchain technology uses substantial amounts of computer power.

VII. SOLUTIONS FROM BLOCKCHAIN

Financial institutes can build a shared ledger using blockchain technology., which is managed by trusted processing nodes. We can use digital signatures, financial intermediaries we can update a ledger to complete a business transaction. This shared ledger needs to be protected by some kind of encryption in order to protect the confidentiality and integrity.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

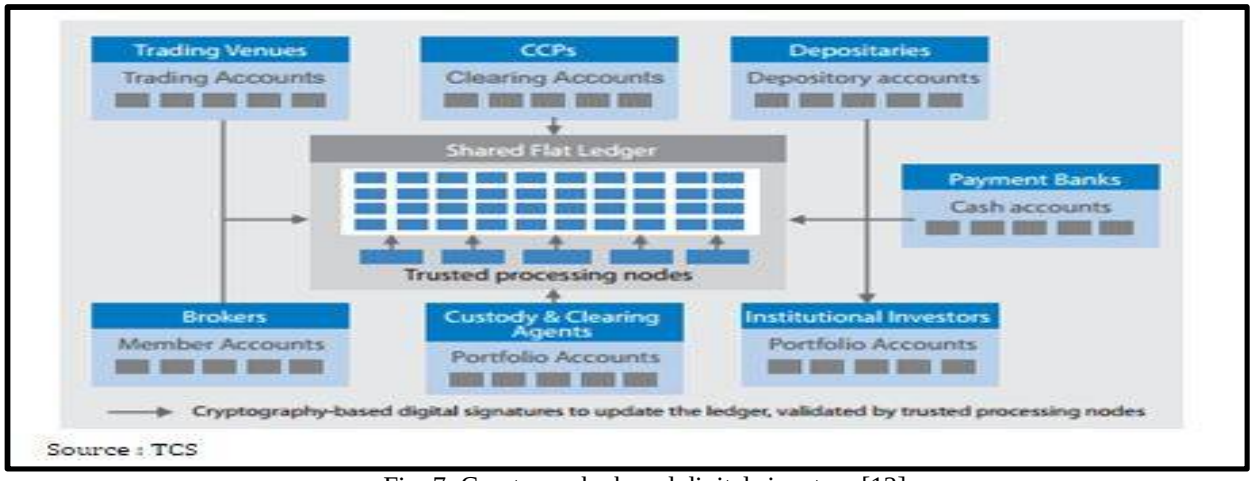

Fig. 7: Cryptography based digital signature [12]

Key processes involved in executing a trade such as security issuance , trading, clearing and settlement can be used to redesign and simplify using such a solution.

VIII. CONCLUSION

To conclude, Blockchain is the technology backbone of Bitcoin. The distributed ledger functionality coupled with security of BlockChain, makes it very attractive technology to solve the current Financial as well as non-financial business problems.

There is enormous interest in BlockChain based business applications and hence numerous Start-ups working on them. The adoption definitely faces strong headwind as described before. The large Financial institutions like Visa, Mastercard, Banks, NASDAQ, etc., are investing in exploring application of current business models on BlockChain. In fact, some of them are searching for the new business models in the world of BlockChain. Some would like to stay ahead of the curve in terms of transformed regulatory environments of BlockChain.

We have also seen many advantages and a few disadvantages of using BlockChain technology To conclude, we envision BlockChain to go through slow adoption due to the risks associated. Most of the Startups will fail with few winners. We should be seeing significant adoption in a decade or two. [13]

IX. ACKNOWLEDGEMENT

We sincerely appreciate the inspiration; support and guidance of all those people who have been instrumental in making this project a success. We are grateful to Mr. Mritunjay Ojha, our Cryptography and System Security professor and Mrs. Rakhi Kalantri, our Software Architecture teacher for encouraging us to broaden our horizons and read more and learn more by way of assignments which help us discover topics like these. We would also like to express our gratitude to Mrs. Kiruthika, the HOD for the Computer Department for her encouragement for the same. We would also like to extend our thanks to Mr. Achuthan Nair, for his wonderful insights and encouragement to write the article.

REFERENCES

[1] "Blockchain (Database)". *En.wikipedia.org*. N.p., 2016. Web. 14 Nov. 2016.
[2] "A Gentle Introduction To Blockchain Technology". Bits on blocks. N.p., 2016. Web. 30 Oct. 2016.
[3] *"Making Blockchain Real For Business"V2.09 19 Jan 16*
[4]Akhil Tandulwadikar, Senior Researcher, Cognizant Research Center *"Blockchain In Banking: A Measured Approach*." April 2016
[5] "Technology: Banks Seek The Key To Blockchain". Financial Times. N.p., 2016. Web. 30 Oct. 2016
[6] Hassell, Jonathan. "What Is Blockchain And How Does It Work?". CIO. N.p., 2016. Web. 12 Nov. 2016.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

[7] "Block Chain - Bitcoin Wiki". En.bitcoin.it. N.p., 2016. Web. 12 Nov. 2016.
[8] "Axis, Kotak Mahindra Banks Test Blockchain Transactions". http://www.livemint.com/. N.p., 2016. Web. 31 Oct. 2016.
[9] "Blockchain All Set To Support Insurance Banking - Finance 2.0". Finance 2.0. N.p., 2016. Web. 31 Oct. 2016.
[10] "Blockchain Technology: 9 Benefits & 7 Challenges | Deloitte". *Deloitte Nederland*. N.p., 2016. Web. 14 Nov. 2016.
[11]"What Are The Advantages And Disadvantages Of Bitcoin?". *CoinReport*. N.p., 2016. Web. 14 Nov. 2016.
[12] "Know More About Blockchain: Overview, Technology, Application Areas And Use Cases - Let's Talk Payments". *Let's Talk Payments*. N.p., 2016. Web. 14 Nov. 2016.
[13]*Michael Crosby, Google Nachiappan, Yahoo Pradhan Pattanayak,Yahoo Sanjeev Verma, Samsung Research America Vignesh Kalyanaraman, Fairchild Semiconductor "Blockchain Technology*." 1st ed. Berkeley: N.p., October 16, 2015