Introduction

Blockchain technology is one of the most prominent emerging technologies in the 21st century. Blockchain is at the core implementation of any digital currency like BITCOIN , ETHEREUM . The potential of blockchain is not just limited to digital currency, it can be used any field of science. This is due to the features it provides. By definition blockchain is as shared and open ledger that keeps a record of the transactions and cannot be modified. To define in simple words blockchain is a chain of blocks where each block contains a set of transactions. Each block is connected to its neighboring block by the hash of the respective preceding block.

The very existence of the blockchain technology is to remove the dependency of centralized systems and maintain an open ledger of transactions being executed. The concept of open ledger is to maintain the peer to peer relationship between the parties involved in the transaction with no trusted third party.

A distributed ledger can be defined as a database that is consensually shared and synchronized across network spread across multiple sites, institutions or geographies. It allows transactions to be public and thereby making a cyber attack more difficult. The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it. Further, any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes.

**Distributed Ledger Technology (DLT):**

DLT is based on the peer-to-peer (P2P) technologies at its core. The P2P technology is the base of the internet and its applications such as email, sharing music or other media files, and internet telephony are driven by the same technology. However, the internet-based transfers of asset ownership have long been elusive, as this requires ensuring that an asset is only transferred by its true owner and ensuring that the asset cannot be transferred more than once, i.e. no double-spend. The asset in question could be anything of value.

A paper written by Satoshi Nakamoto named “Bitcoin: A peer to peer Electronic Cash Systems ” in 2008 proposed a novel approach of transferring “funds” in the form of “Bitcoin” in a P2P manner. The underlying technology for Bitcoin outlined in Nakamoto’s paper was termed as Blockchain, which refers to a particular way of organizing and storing information and transactions. Subsequently, other ways of organizing information and transactions for asset transfers in a P2P manner were devised which lead to term “Distributed Ledger Technology” (DLT) to refer to the broader category of technologies.

Presently the state art of distributed ledger technology has become an emerging research area both in academia and industry. These have to lead to the development of multiple DLT platforms. Some of them are Bitcoin, Ethereum, Hyperledger Fabric, Corda, etc. Though these platforms comes in different flavors, addresses this concerns of distributed system, the main aim of all the platforms is one. That is to provide peer to peer transfer of assets without central trusted system. Some of the DLT platforms are discussed in detail in the report.

The sections in the report are structured as Section 2 provide the necessity of distributed systems, Section 3 – Promises of Blockchain technology/DLT ,Section 4 - analysis of existing distributed ledger technologies, Section 5 - proposed framework and compare with the current centralized system and existing DLTs.

Central Systems and Requirements

A ledger by definition it is a book of record keeping all the financial transactions of the organization. Since ancient times, ledgers have been at the heart of economic transactions to record contracts, payments, buy-sell deals or movement of assets or property.

The journey which began with recording on clay tablets or papyrus, made a big leap with the invention of paper. Over the last couple of decades, computers provided the process of record keeping and ledger maintenance great convenience and speed. Today, with innovation, the information stored on computers is moving towards much higher forms which is cryptographically secured, fast and decentralized.

In modern days computerized ledger came into existence and the general ledger works as a central repository for accounting data transferred from all sub ledgers cash management, fixed assets, purchasing and projects. The general ledger is the backbone of any accounting system which holds financial and non-financial data for an organization. The collection of all accounts is known as the general ledger. In a manual or non-computerized system this may be a large book. Each account in the general ledger consists of one or more pages.

**Central System:**

To create and manage the central ledger the parties involved in the transaction has to trust a central party. Thus making the central trusted party as more powerful in the sense of access to data and execution of the transaction.

In the current system of banking, a client has to put his trust on the bank which is the trusted third party to execute a simple funds transfer. For example a fund transfer in the central system is explained as in the below figure.

Funds Transfer Transaction

Steps Involved:

1. Sender initiates the transaction “Send $100 to receiver” by sending the request to his/her Sender bank
2. Sender bank on receiving the request for initiation of the fund -transfer and transfers the request to the central bank only after verifying the necessary conditions.
3. The central banks upon receiving the request from bank1, executes the request and sends the response to the sender bank and also to the receivers bank
4. Receivers bank on receiving the message from central bank updates the account of the receiver, to reflect the current updated balance.

Some of the observations

1. Each transaction is broken in to multiple hops which are independent of the result of prior hop.
2. Sender is not aware of the processing being careered out by the banks.
3. Reconciliation issues which could be due any software issues

Though the central systems have been over for a long time in the systems they still have some issues which need to be addressed.

**Issues:**

1. Single point of Failure
2. Fault Tolerance
3. Scalability
4. Reconciliation Overhead.

**Single point of Failure:**

A single point of failure (SPOF) is a potential risk posed by a flaw in the design, implementation or configuration of a circuit or system in which one fault or malfunction causes an entire system to stop operating. In a data center environment, a single point of failure can compromise the availability of the system or the entire data center depending on the location and interdependencies involved in the failure.

For example consider a data center where a single server runs a single application. The underlying server hardware would present a single point of failure for the application’s availability. If the server failed, the application would become unstable or crash entirely. Preventing users from accessing the application, and possibly resulting in some of data loss. In normal practice use of a backup server would suffice but poses the same challenge to the second server too.

**Fault Tolerance:**

Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of some (or one or more faults within) of its components. If the operating quality for a system decreases, the decrease will be proportional to the severity of the failure. Compared to a native designed system in which even a small failure can cause total breakdown (SPOF). Fault tolerance is particularly sought after in high-availability or life-critical systems.

Currently the fault tolerance of the system is being addressed by technique redundancy or replication.

**Redundancy/ Replication:**

Redundancy is the provision of functional capabilities that would be unnecessary in a fault-free environment. This can consist of backup components that automatically "kick in" if one component fails. Two kinds of redundancy are possible space redundancy and time redundancy. Space redundancy provides additional components, functions, or data items that are unnecessary for fault-free operation. In time redundancy the computation or data transmission is repeated and the result is compared to a stored copy of the previous result.

But considering the state of art of fault tolerance research there current fault tolerant mechanisms are not the best to rely on . Techniques like state machine replication in a distributed environment can guarantee better fault tolerant systems.

**Scalability:**

Scalability is the capability of a system, network, or process to handle a growing amount of work, or its potential to be enlarged to accommodate that growth. For example, a system is considered scalable if it is capable of increasing its total output under an increased load when resources are added. It is a highly significant issue in electronics systems, databases, routers, and networking. A system, whose performance improves after adding hardware, proportionally to the capacity added, is said to be a ***scalable system***.

With the centralized system in place the scalability it is always a property to be addressed keeping different constraints. Presently scalability is viewed by the number of user requests, flavors of implementation and hardware. It is very hard to scale the present system as the scaling needs all the data, state of the machine and capacity of the system needed to be changed.

**Reconciliation Overhead:**

Reconciliation is an accounting process that uses two sets of records to ensure figures are correct and in agreement. It confirms whether the money leaving an account matches the amount that's been spent, and making sure the two are balanced at the end of the recording period. The purpose of reconciliation is to provide consistency and accuracy in financial accounts. Reconciliation is particularly useful for explaining the difference between two financial records or account balances. Some differences may be acceptable due to the timing of payments and deposits.

**General causes of reconciliation:**

With centralized system it could be taken granted that the general ledger will be maintained and updated by the central systems. But in practical scenarios this is not the case with businesses. There could be various reasons where the client could expect different values in their accounts than displayed. Some are discussed as below with banking sector as example.

1. Interpretation of calculation:

In general businesses are carried on by performing multiple transactions ie., exchange of information, money or services. This expects the both the parties should have understood the business processes and their calculations. This can happen in one of two ways. You might make an error when you’re recording a transaction in your general ledger. This can be as simple as transposing two numbers or recording a transaction twice, or be more serious, such as forgetting a transaction. The other way math errors occur is when both the ledger and bank statement match, but you make a mistake during your comparisons.

1. Electronic Fees:

With more and more businesses using electronic transactions, the different fees charged can cause confusion. A simple case might be like a credit card payment for $250 and record that as a $250 credit in your ledger. However, in bank statement might show the credit card processor has taken a percentage of that $250, depending on your arrangement, and deposited less than $250 into the account. There could be monthly shopping cart, secure gateway and card processing fees, one or more of which differ each month. If the interest earned on the bank account balance, the statement would have shown after a cumulative amount earned which could lead to confusion.

1. Potential Fraud:

Another reason a bank reconciliation statement might show a difference is because a stolen or lost card/credential. A person making general ledger entries might record cash transactions in your general ledger, but not deposit the money. This might be a one-time event, or occur on a daily or weekly basis, with the person recording the fraudulent entries. To protect from such kind of frauds, checking the bank balance electronically on a regular basis, ideally daily.

1. Outstanding payments/checks

Another reason bank statements and general ledgers may not agree is because a payment recorded in the general ledger might have been a check that did not clear by the bank until after statement closing date. For example, if you pay a vendor $105.08 on March 15 and the vendor does not cash the check until March 30, your bank account probably won’t be debited $105.08 in March. Your ledger will have the $105.08 payment debit recorded in March, however. If you find your numbers are off by $105.08, you might quickly find a $105.08 transaction in your ledger, but not on your bank statement. For this reason, it’s common practice to record how transactions are paid in the general ledger.

With the above issues, it is certain that there are businesses needs much more and better systems than the current centralized system to meet their requirements.

**Business Requirements:**

Different businesses could have different requirements to be met by the underlying frameworks or systems which enable them to do business. Current centralized systems even though meet the business requirements they fall short in addressing some requirements or the current state of art of the solutions implemented could be not he right matching. Below are some of the most common requirements from the community to be met by the service/framework providers.

**Requirements:**

1. Guaranteed message delivery
2. Guaranteed on results of business processes
3. Business continuity
4. End-to-end security
5. Privacy
6. Data integrity
7. Latency
8. Asynchronous processing

**Guaranteed message delivery:**

This is most common and necessary requirement for system to provide. This is mostly related to the communication trust level provided by the service. Each business process communication depends on the delivery of the message sent. And this would not expect just only delivery but the order of message deliver. With the current implementations of message delivery systems is guaranteed that the messages from the two parties are delivered as expected.

**Guaranteed on results of business processes:**

Businesses expects for a smoother and correct processes. This could also mean the actual execution of the business agreements should be as expected. Though the requirement is on results of the business processes it is more related to the terms and conditions both the parties agreed upon but technology is the one which provides platform to execute the processes. For example the different environment of executions should results in same result of the processes.

**Business continuity:**

Business should be able to continue even with the existence of systems failures. This mostly deals with the fault tolerance provided by the systems. Presently fault tolerant systems are available in the market namely the DCDR systems. But the current implementations of the fault tolerant techniques used are not very promising.

**End-to-end security:**

The current centralized system of doing transactions was not able to provide the end-to –end security. The end-to-end security can defined as the “Only the participants should be able to view the contents of a transaction”. But in central systems / decentralized systems , a transaction is performed in multiple hops. The details of the transaction is being viewed by all the participants involved in all the hops a single transaction. Making the details not only available to participants other than the intent receiver, but also not revealing the data to the actual sender and receiver. This could be viewed as a serious issues in a business transaction as the initiator (sender) of the transaction will not be aware of the status of the transaction until he/she hears from the receiver acknowledging for that specific transaction . So there is a very much requirement of a framework which provided end-to-end security

**Privacy:**

As discussed in the above requirement each transaction in the central/decentralized systems is carried out in multiple hops. At each hop the data transmitted will be viewed and perform the necessary steps. This can also be viewed as the loss of privacy of the sender and receiver of the transaction. In business community the data shared to perform a transaction could be of highly sensitive.

With the introduction of General Data Protection Regulation (GPDR), there is a huge requirement to provide services to either businesses or to individual in a private preserving ways.

**Data integrity:**

Data integrity is the assurance that information is not corrupted and can only be accessed or modified by those authorized to do so. Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.

To maintain integrity, data must not be changed in transit and steps must be taken to ensure that data cannot be altered by an unauthorized person or program. Such measures include implementing user access controls and version controls to prevent erroneous changes or accidental deletion by authorized users. Other measures include the use of checksums and cryptographic checksums to verify integrity. Network administration measures to ensure data integrity include documenting system administration procedures, parameters and maintenance activities, and create disaster recovery plans for occurrences such as power outages, server failure or security attacks. If data become corrupted, backups or redundancies must be available to restore the affected data to its correct state.

**Latency:**

Latency by definition is the time lapse between two events. In the systems dealing with the transactions latency is defined according to the time taken to complete a transaction.

In the current systems latency is at acceptable level that is a transactions completion a very low but these are achieved with a trade-off between privacy. Since the central party cloud complete the transaction just by updating its state based in the input provided by the intermittent nodes the latency is low.

**Asynchronous processing:**

The capability of a system to perform transactions asynchronously is known as asynchronous processing. Current systems do provide asynchronous processing of each clients, but mostly depends on the hardware, network and the processing speed of the system . If there is an increase in the incoming requests asynchronous processing could be affected.

Promises of Blockchain

As discussed, blockchain “is as shared and open ledger that keeps a record of the transactions and cannot be modified ” . This is based on the properties of linked list data structure and the concept cryptography. With linked list the data in set the form of blocks(collection of data points/rows) are linked to one an another . In the header (meta data) , the hash of the most recent (latest) block is embedded. Here the hash function is used to maintain the sanctity of the data being added to in the new block.

Below are some of the benefits provided by the blockchain technologies.

1. Immutability
2. Transparency
3. Business Continuity
4. Privacy
5. Disintermediation
6. Consensus
7. Trust
8. Smart Contracts

Immutability:

Immutability can be defined as the property of an object of not being able to change its structure due to changes in its environment or external factors. It is difficult to obtain the perfect immutability in the current systems or in the blockchain technologies.

The immutability definition is slightly modified in the blockchain technology and defined as the data in blockchain is hard to modify and easy to verify. This means the data in the blockchain is made to be very hard to modify . This is due to the process involved in the creation of blocks and making the blockchain as append only. Append only constraint makes the participants of the blockchain to only append a new block and cannot modify the existing block.

Blockchain provides the benefit of easy to verify to check if the block is modified (incase). With the hash of each preceding block embedded in new block’s headers provides an easy technique to verify the sanctity of a block. In this way the data added to the blockchain can be considered near to immutable object.

**Transparency:**

Transparency can be defined as a property where all the parties getting involved in the transaction knows exactly what actions are being taken on what data. In public or private blockchain technologies, all the transactions performed are added to the blockchain/ledger. As the ledger is accessible by all the participants (private) transparency could be achieved. By making the ledger available on the network that is by broadcasting, the risk of cyber attacks can also be reduced.

**Business Continuity:**

Businesses are purely based on the service provided by them to its client. This makes the availability of business as one of the top requirements for any business. No matter what are the faults in the system, the system is expected to support the business continuity. Present centralized systems are prone to single point failures. Though they provide the fault torrent systems , the implementation of those software could pose some unexpected challenges like “synchronization of data” at the time of fallback .

In blockchain, data is available to each and every participant; this reduces the effort of synchronization of data at fallback time. And the systems in the blockchain are connected, so single server failures cannot affect the continuity of the service.

**Privacy:**

Privacy of the data being shared between the parties of the each transaction is a very important feature for any system. In public blockchain all the data is shared to all the members of a network. But as businesses cannot be performed on such a public platforms , private blockchain have been introduced where data being shared can be restricted to be viewed by only some participants. Platforms like hyperledger frabic , Multichain ,Quorum and Corda provide high level of privacy making suitable for businesses.

**Disintermediation**

Disintermediation is the removal of intermediaries in any transaction based systems, or cutting out the middleman in connection with a transaction or a series of transactions**.** Blockchain technologies provide a system with no intermediary to carry out transactions. Here any valid member can initiate a transaction with any member without any intermediary. Each transaction can be verified as valid or invalid transaction by all the participants based on the information in the blockchain. Thus removing the intermediaries to carry out the transaction.

**Consensus**

A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems. It is useful in record-keeping, among other things.

In any centralized system, like a database holding key information about all the transactions, a central administrator has the authority to maintain and update the database. The task of making any updates - like adding/deleting/updating is performed by a central authority who remains the sole in-charge of maintaining genuine records.

Public/private blockchains that operate as decentralized, self-regulating systems work on a global scale without any single authority. They involve contributions from hundreds of thousands of participants who work on verification and authentication of transactions occurring on the blockchain.

In such a dynamically changing status of the blockchain, these publicly shared ledgers need an efficient, fair, real-time, functional, reliable, and secure mechanism to ensure that all the transactions occurring on the network are genuine and all participants agree on a consensus on the status of the ledger. This all important task is performed by the consensus mechanism,

which is a set of rules that decides on the contributions by the various participants of the blockchain.

**Trust**

The problem blockchain is trying to solve is how to run a trusted system with trustless people. With just immutability property of blockchain alone trusted systems cannot be produced . It has to decouple from the operating team(human interference).

Blockchain and DLT ( Distributed Ledger Technology) together eliminate the vulnerability of human interference, as a system built with both technologies can operate without having to trust system administrators. There is also no hierarchy of users in a DLT system, no super-administrators or privileged accounts that can delete transactions in the system. Each transaction must be endorsed by other users.

**Smart Contracts**

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.

Smart contracts allow the performance of credible transactions without third parties. Contents of smart contracts claim that many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing, or both. The aim of smart contracts is to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting.

With all the assurances provided by smart contracts , the execution environment should also be trusted . Though the smart contracts assure the business processes execution, the environment where these are executed will also affect the result of the smart contracts. So there should be an agreement on the execution environment of these smart.