**Introduction**

* In real word there is so many places where under corruptions are made and that record entry was stored in any one of database. But we don’t have access of that database and there is always be a chance that database admin will made changes at any time in database, for this type of data tempering and less accurate data problems resolve by blockchain
* A blockchain is a distributed, peer-to-peer database that hosts a continuously growing number of transactions. Each transaction, referred to as a “**block**,” is secured through cryptography, timestamped, and validated by every authorized member of the database using consensus algorithms (i.e., a set of rules). A transaction that is not validated by all members of the database is not added to the database.
* Every transaction is attached to the previous transaction in sequential order, creating a chain of transactions (or blocks). A transaction cannot be deleted or edited, thereby creating an immutable audit trial. A transaction can only be changed by adding another transaction to the chain.
* Blockchain was first proposed as a research project in **1991**, the blockchain concept predated its first widespread application in use: Bitcoin, in 2009.



* **[Figure 1.1 Satoshi Nakamoto]**
* The blockchain was popularized by a person (or group of people) using the name in **2008** to **Satoshi Nakamoto** serve as the public transaction ledger of the **Cryptocurrency Bitcoin** based on work by Stuart Haber, **W. Scott Stornetta, and Dave Bayer**.
* The identity of Satoshi Nakamoto remains unknown to date. The implementation of the blockchain within bitcoin made it the first digital currency to solve the Double-spending spending problem without the need of a trusted authority or central server.
* Bitcoin's **Genesis Block** was the first instance of a proof-of-work blockchain system and is the template for all other blocks in its blockchain. In 2009, Bitcoin's pseudonymous developer, Satoshi Nakamoto, created the Genesis Block, which launched the cryptocurrency boom that is ongoing today

**How does blockchain is works?**

**A picture containing logo

Description automatically generated** **Icon

Description automatically generated** A picture containing rectangle

Description automatically generated Text, letter

Description automatically generated

**Entry**

**Ledger Book**

* **[Figure 2.1 Tradition ledger book in shop]**
* In above figure we can see that how tradition way ledger book is maintained. There is shop from a person purchase a product and that person purchase amount is 200 rupees. A shopkeeper made 200 rupees entry in ledger book. A person decides with shopkeeper that he will pay his purchase amount after 2 days later. Now there is chance that a shopkeeper tempered in ledge book and person have to pay a more rupees than actual amount. That means in maintaining a book or database entry there is change that data are tempered.
* A blockchain is a mechanism with help of we can ensure that our data will not be changed. The immutable ledger and proof of work property make blockchain unchanged. There is next to impossible to do changes in blockchain. Blockchain is a distributed immutable ledger which is completely **transparent**.

Icon

Description automatically generated Icon

Description automatically generated Icon

Description automatically generated

* **[Figure 2.2 How Blockchain are store]**
* **A Genesis Block is the name given to the first block a cryptocurrency, such as Bitcoin, ever mined**. A blockchain consists of a series of so-called blocks that are used to store information related to transactions that occur on a blockchain network.
* A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as bitcoin for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.
* One key difference between a typical database and a blockchain is how the data is structured. A blockchain collects information together in groups, known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled.
* A database usually structures its data into tables, whereas a blockchain, like its name implies, structures its data into chunks (blocks) that are strung together. This data structure inherently makes an irreversible time line of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this time line. Each block in the chain is given an exact time stamp when it is added to the chain.

**Why Blockchain?**

* **Because Blockchain is a disruptive technology.**

**A picture containing transport

Description automatically generated**

**A picture containing icon

Description automatically generated**

**[Figure 2.2 Disruptive flow of hoarse drawn to car]**

* There is one question why we have to use block chain technology in our application that answer is **disruptive technology.**
* There is one question that, what is **Disruptive Technology.**

**🡺** in above figure we can see that in traditional way we have a hoarse drawn vehicle for go to one place to another. After a time is passed then car invention is made and with time hoarse drawn vehicle is not used too much and at the end the hoarse drawn vehicle way for travel is stopped. From hoarse drawn vehicle to modern cars switch of travel is known as **Disruptive of travel.**

**Internet:**

**Blockchain:**

****

**Internet          Communication**

****

**Blockchain          Trust**

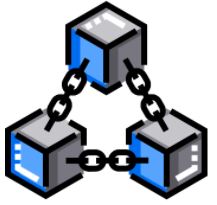
**[Figure 2.2 Disruptive flow of Internet]**

* After telephones are invented peoples are using a telephone for make calls and talks, then after many of years internet is come. People are thoughts that there is already telephone for communication that’s why internet will not has been used. But after some years Internet replace telephone communication. Now days there most of the people are use Internet for communication.
* Internet provides us a commination but not trust. Form helps of internet we can easily communicate with each other but in internet there is always chance that our data will be hacked or tempered.
* Blockchain provides trust to the users that their data will not be hacked or tempered by third party. So that Blockchain is technology is **Disruptive Technology** communication and transaction are secured and Immutable.



**[Figure 3.1 Blockchain verify Multiple transactions]**

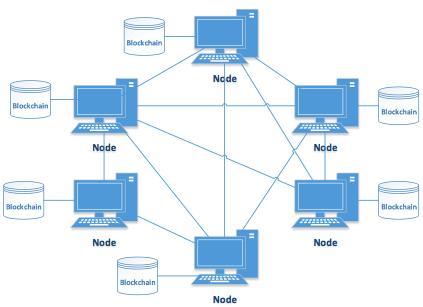
* Blockchain helps in the verification and traceability of multistep transactions needing verification and traceability. It can provide secure transactions, reduce compliance costs, and speed up data transfer processing. Blockchain technology can help contract management and audit the origin of a product. It also can be used in voting platforms and managing titles and deeds.



**[Figure 2.2 Chain of blocks]**

* Note: The data is recorded in chronological order. Also, once the data is recorded, it cannot be changed.

**Distributed P 2 P Network**

****

**[Figure 4.1 Peer-to-Peer Network]**

The underlying blockchain technology leverages the power of P2P networks and provides a shared and trusted ledger of transactions. As a distributed ledger technology, blockchain records transactions as an immutable timestamped digital block that indicates senders and receivers. No centralized authority manages the blockchain networks and only the participants can validate transactions among each other. The technology allows people and institutions to trust the output without trusting the participants. This new form of distributed data storage and management acts as a digital ledger that publicly records all transactions and activities.

Peer to peer network, commonly known as P2P is a decentralized network communications model that consists of a group of devices (nodes) that collectively store and share files where each node acts as an individual peer. In this network, P2P communication is done without any central administration or server, which means all nodes have equal power and perform the same tasks.

P2P architecture is suitable for various use cases and can be categorized into structured, unstructured, and hybrid peer-to-peer networks. The unstructured peer-to-peer networks are formed by nodes randomly from connection to each other, but they are inefficient than structured ones. In structured peer-to-peer systems, the nodes are organized, and every node can efficiently search the network for the desired data. Hybrid models are actually a combination of P2P and client-server models, and when compared to the structured and unstructured P2P systems, these networks tend to present improved overall performance.

Icon

Description automatically generated

B

A

**[Figure 4.2 Immutability maintain in each peer-to-peer network]**

* In figure 4.1 we can see that blockchain network is established between peer-to-peer and every person who in network that person has a one copy of blockchain. If any user tempered in any block than Hash of blocked is changed. And from that changed block all next blocks are becomes Invalid. When blocks are become invalid then all the person who is in network will be alerted, that there is tempering done in database. Now if majority of network are able to accept a change then and then block data will be changed.

**Hashing Algorithm**

* Hashing algorithm of blockchain is works on generating a unique has of each transaction. Whenever a new block is added in a blockchain then block contain three things.

1. Data
2. Hash
3. Previous hash

* **Data:** data contain the information of transaction.
* **Hash:** hash is unique identification of current block.
* **Previous hash:** It will store it previous block hash.
* **Data are stored in blockchain in link list data structure.**

Block No.-1

Data

Hash:0000D8C42

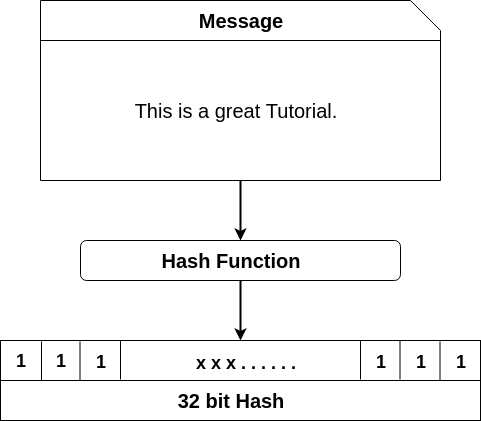
**[figure 5.1 Block] Background pattern

Description automatically generated**

Prev Hash:000000000

**[Figure 5.2 fingerprint]**

* Hash is like fingerprint, like every person to person fingerprint are unique that’s like every block to block hash is unique.
* **Hash Function**
* A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a fixed length. The fixed bit length can vary (like 32-bit or 64-bit or 128-bit or 256-bit) depending on the hash function which is being used. The fixed-length output is called a hash. This hash is also the cryptographic by product of a hash algorithm. We can understand it from the following diagram.



**[figure 5.3 Hash Function]**

**The hash algorithm has certain unique properties:**

1. It produces a unique output (or hash).
2. It is a one-way function.

* In the context of cryptocurrencies like bitcoin, the blockchain uses this cryptographic hash function's properties in its consensus mechanism. A cryptographic hash is a digest or digital fingerprints of a certain amount of data. In cryptographic hash functions, the transactions are taken as an input and run through a hashing algorithm which gives an output of a fixed size.

## SHA-256

* A Bitcoin's blockchain uses SHA-256 (Secure Hash Algorithm) hashing algorithm. In 2001, SHA-256 Hashing algorithm was developed by the National Security Agency (NSA) in the USA.
* **For example:** We have type in data section: **This is a preet**.

It will generate the corresponding Hash:

1. 759831720aa978c890b11f62ae49d2417f600f26aaa51b3291a8d21a4216582a

**Immutable ledger**

A picture containing icon

Description automatically generated Shape

Description automatically generated Icon

Description automatically generated

**Institution**

**Centralized Database**

**Maintain Register**

## [figure 6.1 Institute data storage]

## In above figure 6.1 we can see that institute data are store in central database or they can maintain a register for records entries. In central database there is chance that admin changes a data or a hacker can temper in database. Same thing in register maintains, there is chance that register is tempered by any person.

## With help of blockchain Immutable ledger feature we can make our data unchanged and reliable.

* Immutable ledger in blockchain refers to any records that have the ability to remain unchanged. It cannot be altered and hence the data cannot be changed with ease, thereby making sure that the security is quite tight. Immutability means that it is very difficult to make changes without collusion. The central idea behind the blockchain ledger is the security of data and the proof that data has not been changed or altered. Let us delve a bit deeper into the topic to understand more about blockchain immutability and the benefits it offers.

## 

## Understanding Blockchain Immutability

* Immutability is defined as the ability of a blockchain ledger to remain unchanged, unaltered, and indelible. Each of the blocks of information like facts or transaction details is carried out with the help of a cryptographic principle or a hash value. Now, this hash value has an alphanumeric string generated by each block individually. Each of the blocks contains a hash value or digital signature for itself and for the previous one as well. This, in turn, makes sure that the blocks are retroactively coupled together and unrelenting. It is this functionality of blockchain technology that makes sure no one is able to interfere with the system or change the already saved data into the block.
* In this regard, it is also quite essential to know that blockchain is distributed and decentralized in nature. Here a consensus is made among the different storing a copy of the data. It is this consensus that makes sure the originality of data is righty maintained. Immutability is undoubtedly one of the most definitive features of blockchain technology and also brings out the that can be deployed. The concept can simply redefine the entire process of auditing of data to make it much more efficient, and cost-effective, along with bringing about more trust as well as integrity into the data.

## How to Achieve Immutability?

* As explained above, the hash value helps in securing each block of code in a separate manner. To understand how to achieve immutability, clarification of the concept of cryptographic hashing is essential. Nowadays, the generation of a cryptographic is not quite a dreadful task. It is because of the fact that modern programming languages come with an array of hash functions. With the help of these hash functions, it is just required to pass a set of bytes and the function will be returning a checksum signature. These functions always generate a string of length of 64 characters and we would always be getting the fixed string length regardless of the size of the input, which is referred to as a digital signature.
* The digital signature points to the exact data that the users input. But hash cannot be reverse-engineered which means that the users cannot make use of this output string for the purpose of finding the input data. This, in turn, results in the immutability of the blockchain ledger. In this system, each of the transactions is verified with the help of a blockchain network. It includes blocks of information embedded with timestamps and is secured by a hashing process. It links together and incorporates the hash of the last block. This mechanism plays a major role in developing the chronological chain which helps in joining each of the blocks.
* The meta-data of the last block is always included by hashing at the time of generating a new hash for it. This, in turn, helps in creating a link between the block and the chain, thereby making it unbreakable. Once this is done, none can alter or delete the data of the block which is placed in the blockchain. It is because whenever anyone would be attempting to make a change, the modification is rejected by the subsequent block since the hash of the block would not be valid anymore.

**Smart Contract**

Text

Description automatically generated

**[figure 7.1 Smart Contract]**

* Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss.

## How smart contracts work

* Smart contracts work by following simple “if/when…then…” statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.
* Within a smart contract, there can be as many stipulations as needed to satisfy the participants that the task will be completed satisfactorily. To establish the terms, participants must determine how transactions and their data are represented on the blockchain, agree on the “if/when...then…” rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes.
* Then the smart contract can be programmed by a developer – although increasingly, organizations that use blockchain for business provide templates, web interfaces, and other online tools to simplify structuring smart contracts.

## Benefits of smart contracts

#### Speed, efficiency and accuracy

🡺Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there’s no paperwork to process and no time spent reconciling errors that often result from manually filling in documents.

#### **Trust and transparency**

🡺Because there’s no third party involved, and because encrypted records of transactions are shared across participants, there’s no need to question whether information has been altered for personal benefit.

#### **Security**

🡺Blockchain transaction records are encrypted, which makes them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.

#### **Savings**

🡺Smart contracts remove the need for intermediaries to handle transactions and, by extension, their associated time delays and fees.

**Applications of Blockchain**

A picture containing icon

Description automatically generatedIcon

Description automatically generated

* **Bitcoin**



**[figure 8.1 Bitcoin]**

Though Bitcoin is the most extensive application of blockchain, an essential thing to understand is that blockchain can be used to record any number of data points across any industry immutably. FinTech is following right behind cryptocurrencies in blockchain adoption, particularly during the compressed disruption in 2020 that is likely to continue this year. Let’s take a look at why and how other industries and applications will, and should, be next.

* **Health care**

Icon

Description automatically generated

**[figure 8.1 Health care]**

According to a Data Bridge Market Research study released in December 2020, Blockchain technology in the health care market is expected to gain market growth in the forecast period of 2021 to 2028. The market is expected to grow at a CAGR of 21.70% in the same period, perhaps even further influenced by patient demand once they realize the benefits explored below.

For healthcare, the distributed ledger methodology provides an unprecedented level of privacy and security for all stakeholders, ensuring vigorous data integrity while giving patients control over their personal data. Most healthcare organizations have yet to operationalize blockchain, but the industry understands the technology can address healthcare management's most pressing challenges. With the increased usage of medical devices and apps, blockchain could be the link that bridges the data silos this connectivity potentially creates. Patient consents, information governance, and changes from multiple sources can all be entered and verified on a secure, private ledger. Vaccination records (including the Covid 19 vaccination) will also eventually need to be verified to facilitate the safe return to workplaces, schools, and some travel.

**International Wire Transfer**

* **Real Estate**



**[figure 8.1 Real Esate]**

The real estate industry is embracing blockchain in some exciting ways. By digitizing and tokenizing assets, applied using blockchain, investors can buy a fractional interest rather than an entire asset or portfolio, providing data security and integrity. This also provides a lower barrier to entry and increased liquidity options. Owners and tenants can use blockchain to check credit and rental history, make payments, and submit maintenance tickets. Real estate dealings have dozens of transactional touchpoints across the lifetime of a deal. By borrowing the inherent trust of blockchain, migrating the data and actions of those touchpoints to a distributed ledger, and automating the process using smart contracts, brokers and agents will save time, eliminate rework and cut costs. In a blockchain world, the Multiple Listing Service (MLS) database would provide a far more transparent ledger system for brokers and agents to see the entire transaction history of a property. At a time when daily purchases and leases are vast, this could be incredibly valuable.

* **International wire transfer**

A picture containing icon

Description automatically generated

**[figure 8.1 international wire transferS]**

However, with the advent of mobile wallets powered by blockchain technology, the way international payments are made is set to change completely. Mobile wallets are installed on mobile phones and offer a variety of functionalities, including the ability to transfer money internationally. Blockchain is how this happens. Why are the payments processed using blockchain? Blockchain is the most efficient, transparent and secure way to facilitate international payments because it is based on distributed ledger technology (DLT). According to Get Elastic, a media platform focused on commerce trends, emerging technologies and digital insights for practitioners and developers blockchain transactions are distributed, with records verified by a network of computers versus by one party or bank, and visible to all parties versus held in a central database .In an article that details [how blockchain for B2B payments works](https://www.getelastic.com/crypto-commerce-banking-on-blockchain-for-b2b-payments), transactions that take place on DLT are immutable once recorded and cannot be altered, reversed or tampered with, which makes the payment process highly secure.

For instance, blockchain business-to-business payments, which rose to $171 billion in 2019, according to Juniper Research, are predicted to exceed $4.4 trillion by 2024.The key benefits for individuals and businesses making cross-border payments on blockchain-powered mobile wallets are that costs will come down substantially, and the payment will happen far quicker than conventional bank international payments or money transfers.

Blockchain removes multiple intermediaries that participate in traditional cross-border money transfers. Money is transferred directly via blockchain from Bank A to Bank B, eliminating the need to go through two other correspondent banks and reducing the time and cost of the transaction. The cost savings a customer can make by using block chain based cross border payment solution are substantial. For instance, a customer making a remittance payment of $20 000 would incur an average cost of 7.1%, or $1 420, as calculated by the World Bank. That compares with an estimated 2%, or $400, to 3%, $600, cost of remitting the payment via a blockchain-based remittance provider.

**Advantages**

* Trust. Blockchain creates trust between different entities where trust is either nonexistent or unproven. ...
* Decentralized structure. Daniel Field. ...
* Improved security and privacy. ...
* Reduced costs. ...
* Speed. ...
* Visibility and traceability. ...
* Immutability. ...

Individual control of data

Disadvantages

**Disadvantages**

* **High implementation costs**:

Just as this technology represents low costs for users, unfortunately, it also implies high implementation costs for companies, which delays its mass adoption and implementation. Inefficiency.

* **Blockchain is not indestructible**:

Scalability remains blockchain's weakness. Blockchain entries do not last forever or are not immutable.

Conclusion

**Conclusion**

* Blockchain is **a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system**. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.
* **The Bitcoin is the first successful implementation of blockchain**. Today, the world has found applications of blockchain technology in several industries, where the trust without the involvement of a centralized authority is desired

**References**

🡺https://www.cpajournal.com/

🡺 https://www.investopedia.com/

🡺https://www.javatpoint.com/

🡺https://www.solulab.com/

Thank you…