nalashaa
Healthcare Solutions

BLOCK CHAIN

REVOLUTIONIZING DATA TRANSMISSION

Data is at the core of any industry; be it healthcare, telecommunication or finance. Traditionally, organizations offering solutions for end users owned and maintained databases. For instance, in healthcare ecosystem, healthcare providers maintain most of the patient data. Having complete control over the data gives the owning organization unlimited power over it, including the ability to add data fraudulently, tamper data or reject valid changes to the data, intentionally or otherwise. In addition, the traditional way of a centralized database system is vulnerable to attacks from hackers posing major business risks to organizations that are custodians of data. The blockchain is a revolutionary technology with the potential to provide solutions to many problems including security.

nalashaa
Healthcare Solutions

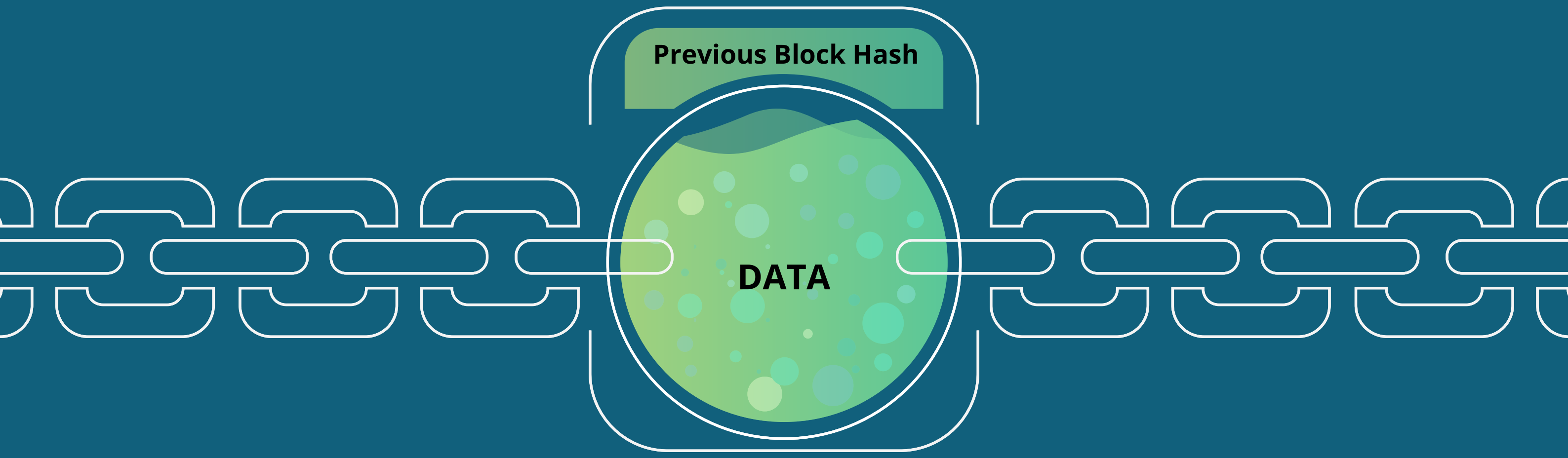
What is Blockchain?

At the very core, blockchain is a decentralized distributed system.

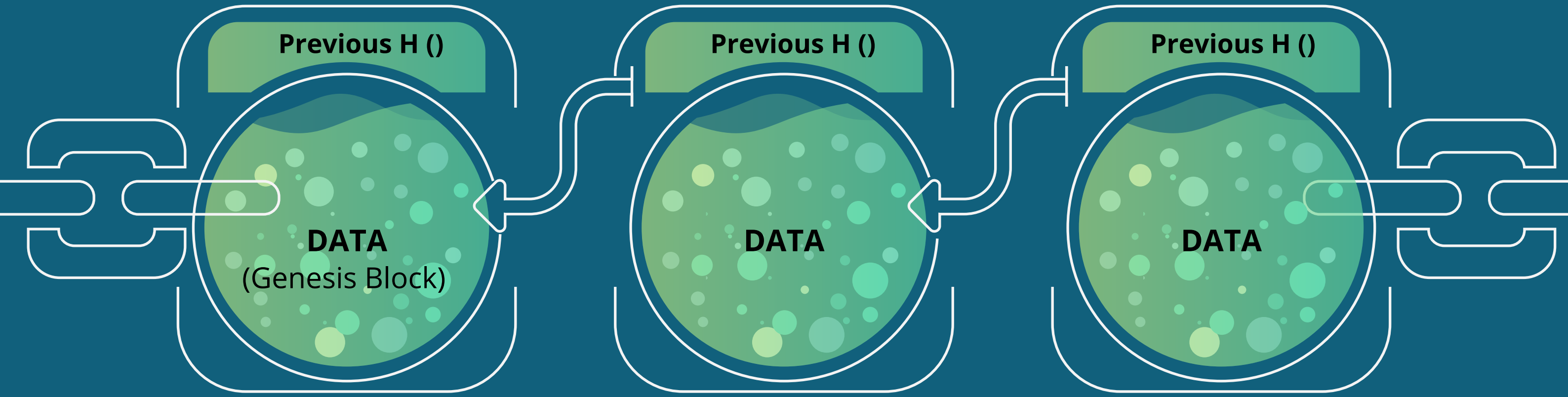
It allows participating peers to exchange data or value without the need for a centrally trusted arbitrator leading to almost immediate settlement of transactions.

In terms of underlying data structure, blockchain is 'append only' sequential data structure. Blocks are at the core of a blockchain system. We can think of a block as a logical grouping of transactions. These transactions can be anything from transfer of money, audit trail of activities such as patient visit to a trail of patient data in various organizations. A unique hash identifies each block in a blockchain, which is similar to a pointer in a linked list data structure. Through the hash of the previous block, each block also contains a reference to the previous block known as the parent block. In case of the blockchain, the hash pointer is different from a normal pointer. They not only point to the address of the parent block, but also have the ability to verify whether the parent block data is tampered. To generate the hash pointers, there are various cryptographic hash algorithms out of which MD5 and SHA256 are the most popular.

A typical block structure is shown below:



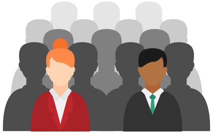
A block mainly contains transaction data and a hash pointer to the previous block on the chain except for genesis block. A chain of blocks is created by the sequence of hash pointers linking each block to its parent, going all the way back to the first block in the chain. Genesis block has no previous block as it is the first block in the chain.



One of the basic characteristics of a blockchain is that new blocks can only be appended at the end of the chain and a block can never be added to the middle of the blockchain. To change a block in the middle of a chain will require all subsequent blocks to be changed. This inherent structure of a blockchain makes it almost impossible to corrupt data on the chain. In a nutshell, a blockchain is a distributed tamperproof database, shared and maintained by multiple parties for secured sharing of records. Each record contains a timestamp and secure links to the previous record. Records can only be added to the database and never removed, with each new record cryptographically linked to all previous records in time.

Blockchain Types

Blockchain can be broadly divided into two different types:



Public blockchains

These are open blockchains where anyone can participate as a node in the decision making process. These ledgers are not owned by anyone and are known as a permission-less ledger. All users maintain a copy of the ledger on their local nodes and use a distributed consensus mechanism in order to reach a decision about the eventual state of the ledger.

Private blockchains

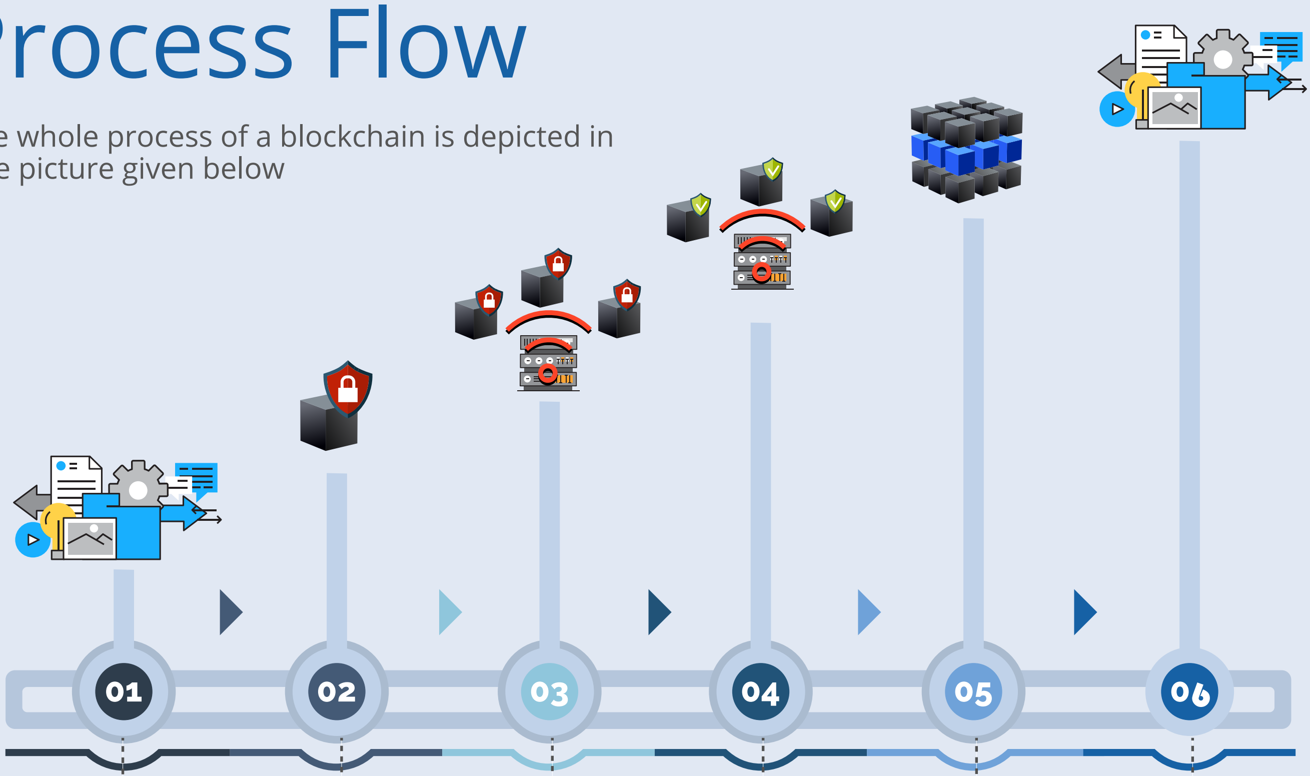
These blockchains are private and are controlled by a consortium or organizations that have decided to share the ledger among themselves. Anyone wanting to join the blockchain requires permission from the consortium or organization to join the blockchain.

nalashaa
Healthcare Solutions

Blockchain Process Flow

nalashaa
Healthcare Solutions

The whole process of a blockchain is depicted in the picture given below



01 Sender creates a new transaction message including recepient details, transaction value.

02 A node validates the transaction by authenticating the digital signature and adds the transaction to a pool of pending transactions.

03 This transaction along with other pending transactions is broadcasted on the blockchain network.

04 Nodes in the network validate the block. This step can be considered as finding a key to unlock the transaction.

05 Once the validation process completes, the block is added to the chain and becomes available for all the nodes in the network.

06 The transaction is complete and purpose of the transaction is achieved.

Blockchain Characteristics

Distributed consensus

The consensus mechanism ensures that the data on the blockchain is incorruptible by distributed consensus among the stakeholders, without the need for a central authority.

Transaction verification

Any transactions posted from nodes on the blockchain are verified based on a set of predetermined rules and only valid transactions are selected for inclusion in a block.

Smart Contracts

Smart contract ensures the accuracy of the data outcome by defining a set of conditions in a blockchain network where all the computers on the network execute the program upon meeting the required conditions.

Security

Blockchain ensures the integrity and availability of data by using proven cryptographic technology. This makes it impossible for one party to manipulate previous records without breaking the overall consistency of the database.

Immutability

Records once added onto the blockchain are immutable, as even the possibility of rolling back the changes will require an unaffordable amount of computing resources.

Challenges in blockchain

Despite the large number of industries that the blockchain is impacting, there are also concerns regarding the technology that is still preventing its widespread adoption.

1 Scalability

Scaling of a blockchain system poses serious challenges to widespread adoption of the technology. As a result of numerous researches to make blockchain system scalable, many approaches are proposed.

Proof of Stake algorithm

Using Proof of Stake algorithm instead of using Proof of Work proved to be fundamentally faster. Through Proof of Stake algorithm, cryptocurrency blockchain network aims to achieve distributed consensus.

Increasing the block size

The size of the block can be increased to hold more transactions, which enables faster confirmation of transactions. In Bitcoin, the block size is hardcoded to be 1 MB, which allows it to process only about three to seven transactions per second.

Sharding

In this method, tasks are split up into multiple chunks. This allows different nodes to process different chunks of tasks resulting in improved throughput and reduced storage requirements. In blockchains, the state of the network is partitioned into multiple shards.

2 Privacy

Though Blockchain is transparent in nature, for industries such as healthcare and finance, the privacy of user data is of paramount importance. Some of the popular techniques to achieve privacy in blockchain system are:

Indistinguishability obfuscation (IO):

This obfuscation technique will turn smart contracts into a black box. This mechanism obfuscates program code by mixing it with random elements. The desired outcome is produced only if the program run as intended.

Homomorphic encryption

The data stored on the blockchain can be encrypted using homomorphic encryption and computations can be performed on that data without the need for decryption, providing privacy service on the blockchains.

Zero Knowledge Proofs (ZKPs):

This mechanism proves the validity of an assertion without revealing any information about the assertion. Zero-knowledge property ensures the confidentiality of the assertion except whether it is true or false.

3 Resource Intensiveness

When transactions are posted to the blockchain, all nodes on the network are involved in verifying and recording them. With blockchain technology, multiple transactions are grouped into boxes with a virtual padlock called blocks. Once the nodes in the blockchain network find the key for the block, it opens and the transactions are verified. The whole mechanism requires a considerable amount of computational power based on the size of blockchain.

4 Standardization

The absence of an elaborate standard protocol for blockchain technology is a hindrance while integrating blockchain technology with existing systems. This results in lack of communication between even two blockchain networks. A certain amount of standardization is needed to help improve interoperability, adaptability, and integration aspects of blockchain technology.

5 Premature

Blockchain is still a premature technology and there are not many enterprise blockchain applications barring a few digital currencies available in the market. The technology itself has created a lot of buzzes and people from different industries, be it healthcare or finance or insurance etc. are taking note of it. Many resources are being devoted to PoCs and exploring the value based application of the technology.

6 Regulation

Another major challenge in the adoption of blockchain technology is there is the absence of a regulatory body. Now developers and companies working on blockchain solutions have started actively engage policymakers in order to ensure proper regulation and soon we will have global central authority for blockchain regulation and legislation.

7 Consensus

There are many algorithms to achieve consensus in blockchain such as Proof of Work (Pow), Proof of Stake, proof of elapsed time, proof of importance, delegated proof of stake, deposit based consensus etc. Proof of work is a proven and one of the most successful mechanisms to reach consensus in a public blockchain. In this mechanism, the network challenges every machine on the network that stores a copy of the ledger to solve a complex puzzle based on its version of the ledger. The puzzle could be a complex algorithm to verifying a new transaction on the chain. For this, machines with identical copies of the ledger function together. Winner of the puzzle is the team that solves the puzzle first. To represent the latest ledger their version of ledger is considered. All the other nodes update their ledger to match that of the winning team.

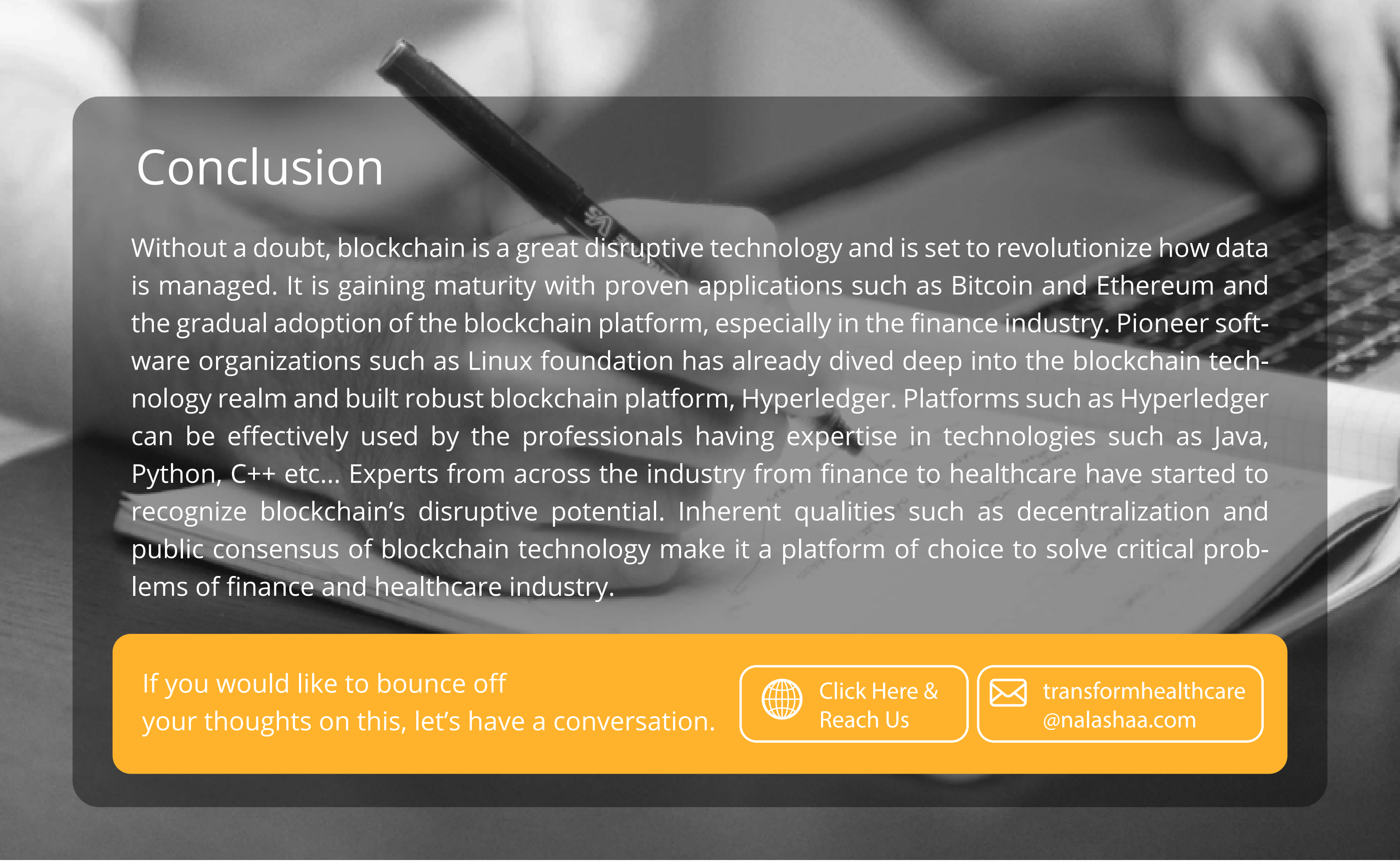
Popular frameworks in existence today

There are many blockchain frameworks available today such as:

- Open-chain
- Quorum
- Stellar
- Ethereum
- Hydrachain
- Hpperledger Fabric
- Corda
- Domus Tower Blockchain
- Elements Blockchain Platform
- Hyperledger Iroha
- Hyperledger Sawtooth Lake
- Symbiont Assembly

Below table shows a comparison of three of the most popular blockchain frameworks on basic characteristics that must be considered while deciding on a specific blockchain framework to use:

Characteristics	Hyperledger Fabric	Ethereum	Multichain
Popularity	Very popular	Very popular	Not very popular
Activity	Actively developed and supported by industry leading foundation Linux	Very popular	Not very popular
Type of Network	Both permissioned and permission less, Public, private	Permission less, Public	Permissioned, Private
Platform	Modular Blockchain	Generic Blockchain	Generic Blockchain
Supported language	Java, Python, Go	Python, Go, C++	Python, C#, JavaScript, PHP, Ruby
Smart Contract	Yes	Yes	Yes
Consensus Mechanism	Supports multiple consensus mechanism	Proof-of-Work (PoW)	Practical Byzantine Fault Tolerance
Consensus Level	Transaction level	Ledger level	Ledger
Governing Organization	Linux Foundation	Ethereum Developers	Coin Sciences
Pricing	Open Source	Open Source	Open Source



Conclusion

Without a doubt, blockchain is a great disruptive technology and is set to revolutionize how data is managed. It is gaining maturity with proven applications such as Bitcoin and Ethereum and the gradual adoption of the blockchain platform, especially in the finance industry. Pioneer software organizations such as Linux foundation has already dived deep into the blockchain technology realm and built robust blockchain platform, Hyperledger. Platforms such as Hyperledger can be effectively used by the professionals having expertise in technologies such as Java, Python, C++ etc... Experts from across the industry from finance to healthcare have started to recognize blockchain's disruptive potential. Inherent qualities such as decentralization and public consensus of blockchain technology make it a platform of choice to solve critical problems of finance and healthcare industry.

If you would like to bounce off
your thoughts on this, let's have a conversation.

🌐 Click Here & Reach Us

✉ transformhealthcare@nalashaa.com

About the Author:

Santosh Kumar

Santosh is a professional with more than a decade experience in architecture, design and, delivery of enterprise software applications. He has vast experience of designing and developing multi-tier highly scalable enterprise systems. He is also an expert in end-to-end architecture and design of mission critical high volume and high availability software systems using the latest technology. Santosh aims at using technology to provide innovative solutions for various challenges in health-care industry.

About Us

Nalashaa believes in simple solutions to derive meaningful insights and in exceeding your expectations. Our clarity of thought has earned us many laurels in this fast paced world where healthcare technology advancements are rolling out continuously.

nalashaa
Healthcare Solutions

Reach Us:

555 US Highway 1 South,
Suite 170, Iselin, NJ 08830, USA

☎ 732-602-2560 X 200

🌐 www.nalashaahealth.com