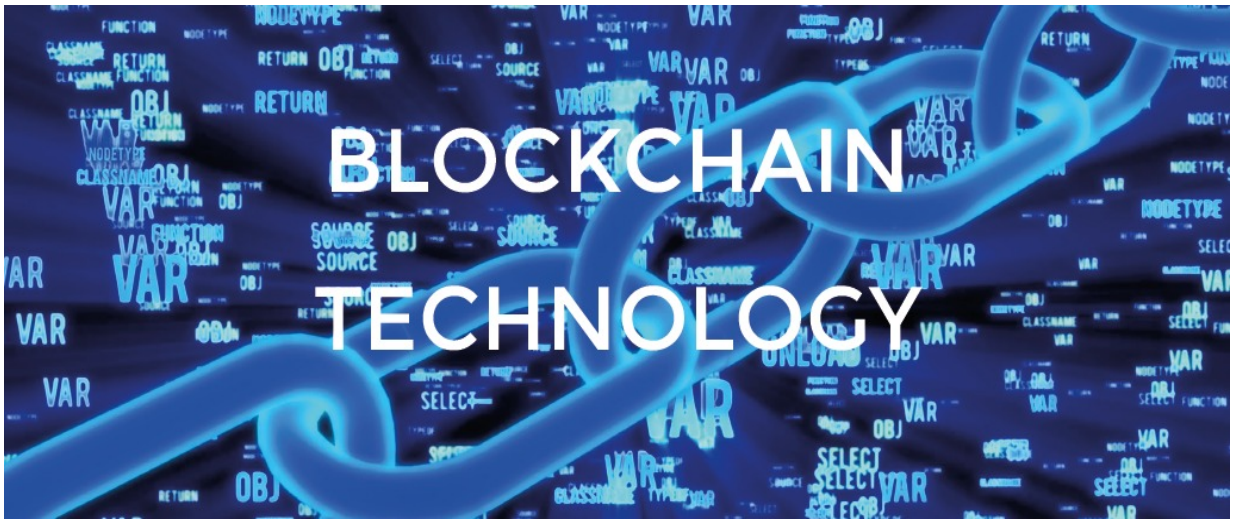
BUSINESS INFORMATION TECHNOLOGY

NewsLetter



What is Blockchain?

A **blockchain**, is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

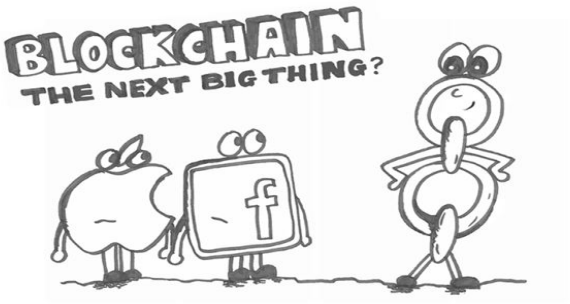
Blockchains are secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. This makes blockchains potentially suitable for the recording of events, medical records, and other records management activities, such as identity management, transaction processing, documenting provenance, food traceability or voting.

Blockchain was invented by Satoshi Nakamoto in 2008 for use in the cryptocurrency bitcoin, as its public transaction ledger. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has been the inspiration for other applications.

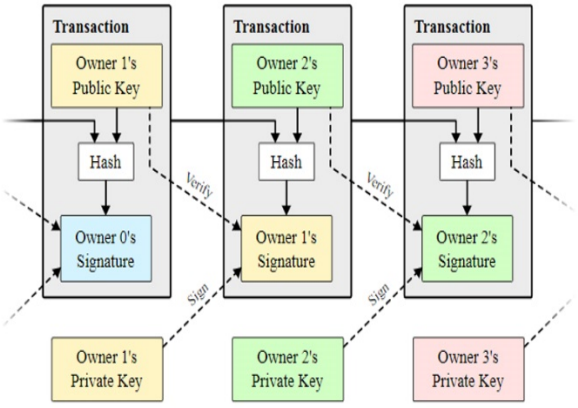
Purpose

Blockchain technology can be integrated into multiple areas. The primary use of blockchain today is as a distributed ledger

for cryptocurrencies, most notably bitcoin. While a few central banks, in countries such as India, China, UnitedStates, Sweden, Singapore, SouthAfrica and the United Kingdom are studying issuance of a Central Bank Issued Cryptocurrency (CICC)



Blockchain technology has a large potential to transform business operating models in the long term. Blockchain distributed ledger technology is more a foundational technology—with the potential to create new foundations for global economic and social systems—than a disruptive technology, which typically "attack a traditional business model with a lower-cost solution and overtake incumbent firms quickly". Even so, there are a few operational products maturing from proof of concept by late 2016. The use of blockchains promises to bring significant efficiencies to global supply chains, financial transactions, asset ledgers and decentralized social networking.



Inside a Block

On a very basic level, every block in a Blockchain comprises of three core elements:

The **'Data'** inside each block depends on the purpose for which the technology is being used. For instance, in a Bitcoin blockchain, the blocks contain the sender's ID, the receiver's ID as well as the amount of Bitcoins being transferred.

The **'Hash'** of a block can be considered as its digital signature. Each block in a blockchain contains a unique hash and can be compared to a fingerprint. If a hash of a block is changed, the block no-longer remains its original self.

The **hash of the previous block** is what forms the chain between these blocks. It acts as a valid proof of concept for the further blocks to act upon and is the primary security measure of a Blockchain against tampering.

How is it secure?

The blocks are linked in a chain. This is done by each of the block building on the hash of the previous block. Now if in case the hash of any block is changed in a Blockchain, The consecutive blocks no longer recognize it as a valid element. This in-turn renders the entire chain useless, Thus not validating any sort of tampering with any block. This is one security

measure that a block chain provides. In case any tampering has to be made valid, The distributor will have to rework the hashes of the entire following blockchain.
In addition to this, Blockchains use a 'Proof of Work' concept to increase the security. A 'Proof of Work' can be equated to the processing time taken by a computer. This essentially slows down the creation of a new block in a Blockchain. In a Bitcoin Blockchain, for instance, it takes around 10 minutes to create a new block. So to alter an entire Blockchain, one will have to spend ten minutes on each block of a Blockchain, making the process impossible.

These measures, however, do not guarantee that the value of a block cannot be changed. So there is one final security measure that Blockchains use. As discussed before, Blockchains use a 'distributed ledger', also known as a Peer-to-Peer network. This means that even if one manages to alter one particular copy of a Blockchain by adding a defected block, the altered block will still not be
accepted into the system. This is simply because the altered block will not match with the copies that others have in a system and hence will be discarded. In order for a block to be accepted into the system, it has to pass a Consensus, meaning, it has to be validated by more than 50 percent of the network. This makes the alteration of any Blockchain almost impossible.

Looking ahead

Going by recent trends and gaining popularity, it can be said with certainty that the future of blockchain is very bright when it comes to India. Everyday more and more organisations and individuals are finding an interest in this new technology, touted as the next big thing after the internet.

Blockchain, the technology behind cryptocurrencies like bitcoin, Ethereum etc- is nothing but a shared ledger/database, in which data once stored cannot be deleted or tampered with. It has no single point of failure and is stored on various nodes over the network, thereby making sure no one has complete control on it.
There are a number of start-ups which are working in the blockchain. Various big companies like Infosys, Kotak etc have shown immense interest in blockchain. Also, a number of start-ups are working in the blockchain space, using the technology.

Seeing the genuine interest in this technology by such multi-billion-dollar organisations and at the same time seeing multiple start-ups sprouting up from the Indian region the future of blockchain in India is quite bright.