Fundamentals of Blockchain Technology Explained

Prabhu R Chennupati | Enterprise Consulting Architect | Mastech InfoTrellis

Overview

With the evolution of Blockchain in the last decade and its prominence in various applications, there has been a need to understand its concepts. This paper covers the fundamentals of Blockchain, its prominent use cases, and how "decentralization" to its core helps challenge all things we know today.

What is a Blockchain?

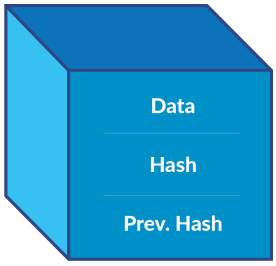
Blockchain is a collection of records linked to each other, strongly resistant to alterations, protected using cryptography with a foundation of distributed processing and persistence.

Block

A Block is a collection of data and a unique alpha-numeric value generated using the data called Hash. It also contains the Hash of the previous Block.

Data

The data inside a Block is dependent on the application, and it could be anything based on the use case.



Hash

It's a code generated based on the data in the Block. It is always unique, even though the data could still be the same.

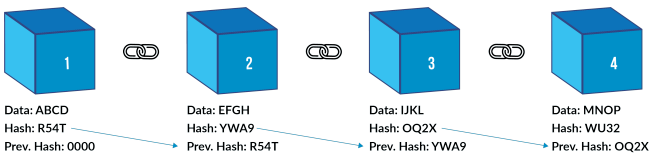
Previous Hash

It's the Hash code of the previous Block. This is how a chain of Blocks is created in a Blockchain.

Each Block contains a Hash of the previous Block to make it a chain of Blocks. This 'Previous Hash' helps to navigate the entire chain and makes it hard to tamper with data of any Block.

Contents

The first Block in the Blockchain won't have a Previous Hash populated, and it's called a Genesis Block.



Understanding Blockchain

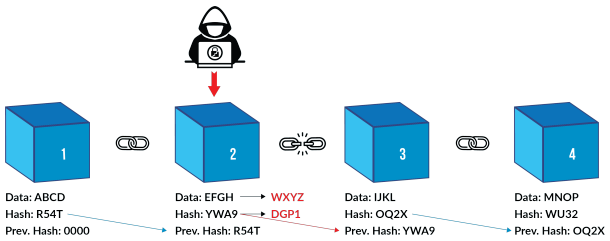
Immutable

Once a Block is written, it's immutable, meaning it cannot be altered. If any malicious actor alters a Block, its Hash changes which is already recorded in the next chained Block.

For instance, if a malicious actor tries to make a change to the data on Block #2, its corresponding Hash value needs to be regenerated. If a Hash value is regenerated for Block #2, the Previous Hash in Block #3 gets delinked, hence breaking the chain.

So theoretically, if someone changes a Block, the entire chain must be changed, which requires heavy processing power.

With today's ever-growing capacity of processing power, it could theoretically still be possible to change the entire chain. To avoid that, any change to the Block must go through something called the Consensus model.

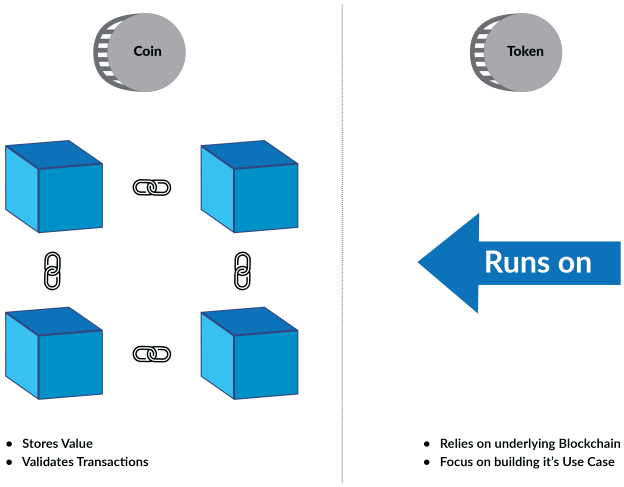


Consensus

A Block can be added to the chain by a technique called the Consensus model. The processing nodes which are distributed across, must reach a consensus before adding a new Block to the chain by solving a complex problem presented to them.

This is a topic of its own and will be covered in a follow-up paper.

Coins & Tokens



Blockchain Networks run on thousands of computers, and to motivate people to run them, an incentive is needed. This incentive is the cryptocurrency in the form of Coin or Token.

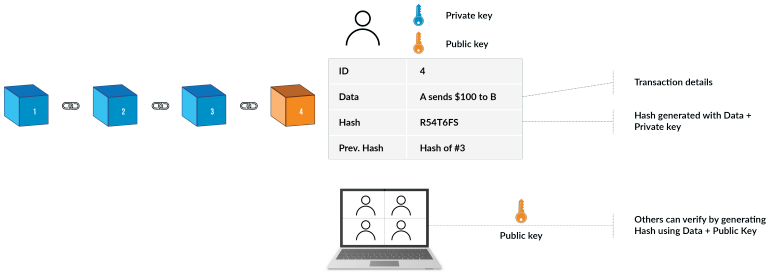
Coin: Uses its own Blockchain Network to keep track of all the data, operates independently of any other platform.

Token: Uses other Blockchain's network and infrastructure and does not worry about how it's validated on the network. The Token just runs on other Blockchain's network.

TokensTypes:

- Usage tokens: A token that is required to use a service
- Work tokens: A token that gives users the right to contribute work to a DAO and earn in exchange for their work
- Security tokens: An external, tradable asset that is a representation of value in a system

Public Key/ PrivateKey



Cryptocurrencies are built upon Public-Key Cryptography(PKC), a cryptographic system that uses pairs of keys – public keys, which are publicly known and essential for identification, and private keys, kept secret and used for authentication and encryption.

Public Key

A public key allows you to receive cryptocurrency transactions. It's a cryptographic code that's paired with a private key. While anyone can send transactions to the public key, you need the private key to "unlock" it and prove that you are the owner of the cryptocurrency received in the transaction.

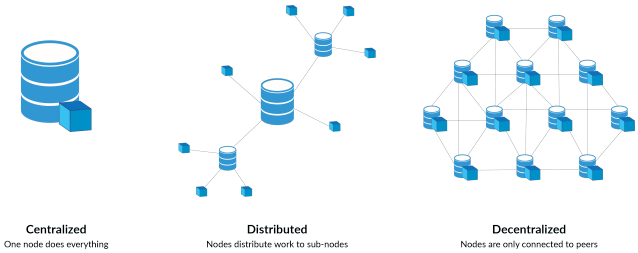
Private Key

A private key gives you the ability to prove ownership or spend the funds associated with your public address. While you can generate a public key with a private key, doing the opposite is practically impossible because of the one-way "trap-door" function. You can have any number of public keys connected to a private key.

Decentralized

Blockchain takes decentralization to an all-new level. Anything which has been centralized and managed by a central body is being re-imagined with Blockchain networks.

No single person, body, or entity owns any of the networks. Instead, everyone who is part of the network owns it – whether it is infrastructure, processing, persistence, changes to the network, or even decision making.



Infrastructure

Nodes are decentralized and not owned by an organization. Anyone who wants to make their systems contribute to the network can do so and get rewarded.

Processing

A bunch of nodes are selected by the network to process a Block. Any node from the network can be chosen to process each Block, and the selection of nodes depends on different Blockchain networks.

Persistence

Once distributed nodes process the Block, it's written to the chain and is persisted on these distributed nodes. So, no one node holds the data.

Political

Unlike traditional organizations where CEO and the executive leadership holds the decision-making power, Blockchain offers a decentralized way of making decisions called DAO –Decentralized Autonomous Organization.

Sample Use Cases

Currency

Respective central banks control fiat currencies and their value, and governments decide the volume of currencies to print. Cryptocurrencies on Blockchain networks can operate without the need for a central authority.

Voting

Voting with Blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Using Blockchain in this way would make votes nearly impossible to tamper with. The Blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election.

Property Records

In the present day, the process of recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where it is manually entered into the county's central database and public index. This process is not just costly and time-consuming, it is also prone to human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain can eliminate the need to scan documents and track physical files in a local recording office. If property ownership is stored and verified on the Blockchain, owners can trust that their deed is accurate and permanently recorded.

Supply Chain

As in the IBM Food Trust example, suppliers can use Blockchain to record the origins of their purchased materials. This would allow companies to verify the authenticity of not only their products but also common labels such as "Organic," "Local," and "Fair Trade."

Healthcare Records

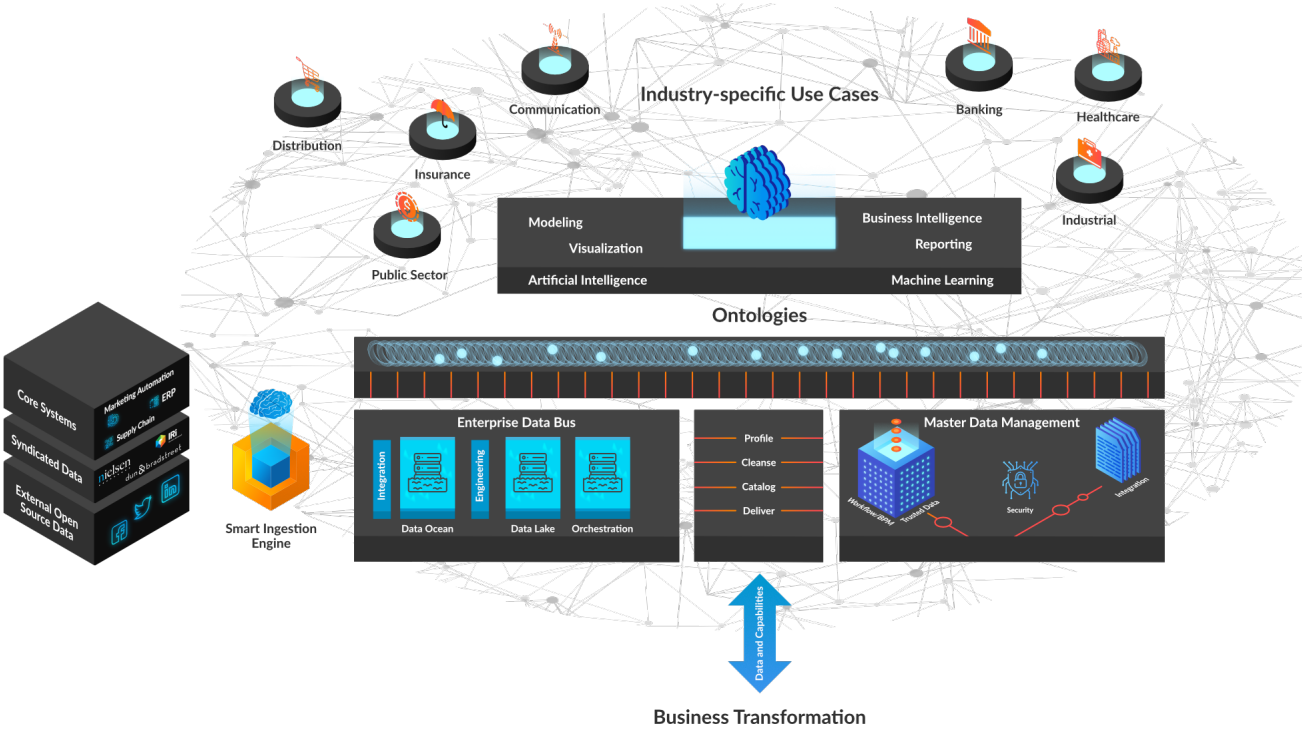
Healthcare providers can leverage Blockchain to store their patients' medical records securely. When a medical record is generated and signed, it can be written into the Blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the Blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy.

Conclusion

Blockchain is a burgeoning technology that can potentially be integrated with many business sectors and establish a highly-secure system for transacting and maintaining records. Conventional and centralized systems are being challenged with Blockchain-based applications, and large corporations are leading the research and development of such products. With an explosive rise in the popularity and consumption of cryptocurrencies, Blockchain technology is here to stay and kick-start a new revolution in the market.

We Architect Enterprise Intelligence

At Mastech InfoTrellis we work to expose the entire corpus of enterprise data and leverage it with state of the art techniques from Decision & Data Science to accelerate enterprise learning. We would love to talk with you about it.



Author

Prabhu has over 20 years of experience in various roles, including Enterprise Architecture, Data & Solution Architecture, Strategic Data & Solution Planning, and Leading Deliveries. He has been instrumental in helping CDO Organizations in Data Architecture Strategy & Roadmap for short-term and long-term goals for various clients.

About

Mastech InfoTrellis partners with enterprises to help them achieve their business objectives by leveraging the power of data to derive deep, analytical insights about their business and its operations. We accelerate business velocity, minimize costs, and drastically improve corporate resiliency through personalized, process-oriented programs, consisting of strategy, data management (including master data management), business intelligence and reporting, data engineering, predictive analytics, and advanced analytics. Part of the NYSE-listed, $193.6M, digital transformation IT services company, Mastech Digital; we drive businesses forward around the world, with offices spread across the US, Canada, India, Singapore, UK, and Ireland.