Blockchain: The Game Changer

Introduction

Why did the first industrial revolution occur? What led man to the fourth Industrial Revolution? What causes a change in civilization? It is just “Necessity.” Necessities of life led man to innovation and to bring ease in our lives we started technological revolutions where one or more technologies are replaced by other technologies. But at every phase, two questions raise trust and security. At first, everything shows promising and promises are broken. Why is that? This may be because there is no shared responsibility, no distribution of power, no or less transparency, flaws in technological enhancement, lack of foresight, and lack of precision or vision. These factors contributed to making technologies vulnerable. Today our day-to-day lives, businesses, and every field in the world rely on digital technologies. That’s why *trust and security* have become the first priorities of today’s world. So we change current technologies and research for better alternatives, that’s where Blockchain comes into play. Before blockchain *trust, security, privacy, and transparency* are put under negotiations, but now all these features are equipped in Blockchain as one. It is implemented in a distributed fashion that creates a strong base of trust. By utilizing state-of-art cryptography security is enhanced. We also achieve privacy and transparency depending on what type of Blockchain we use a public or private blockchain. In public Blockchain all users are anonymous or unknown and transactions are transparent, which means anyone can audit transactions. In private blockchain, only allowed personnel can transact and audit the ledger. That’s why it has become the game changer. Blockchain is a disruptive technology it’s the modern Enigma.

Brief History

The core ideas behind blockchain technology emerged from the late 1980s and early 1990s. In the paper called The “Part-time Parliament” by Leslie Lamport describes a consensus model for agreeing on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a pair of physicists, Stuart Haber and W Scott Stornetta, published a paper to outline the use of a chain of cryptographically secured blocks to preserve the integrity of past information and protect it.

These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer to Peer Electronic Cash System.

“Bitcoin is not Blockchain. “

Bitcoin is electronic cash or cryptocurrency, Blockchain tracks the bitcoin.

Hence, Bitcoin blockchain. There are other types of blockchains implemented in the space.

Bitcoin comes up with the idea to prevent double-spending.

Even bitcoin also not a new concept, before bitcoin Cryptocurrencies like DIGICASH, BIT GOLD, and HASHCASH has been proposed and no one really paid any attention. But after the 2008 financial crises, a white paper gained public attention which is published by a shadow with the pseudonymous name Satoshi Nakamoto.

No other cryptocurrencies survived, but Bitcoin did. Just because of Blockchain. Bitcoin was just the first of many blockchain applications.

Here are few assumptions about the identity of Satoshi Nakamoto

* There is a legion called cyberpunks; some of them proposed the ideas of decentralized electronic cash systems. Some assume Satoshi had to be a Cypherpunks. Because people like Nick Zabo talked about bit gold, David charm about DigiCash and Wei Dei talked about E-Money.
* Some news articles assume that Satoshi Nakamoto’s Real Identity is probably known by US Intelligence Agencies. Because the NSA then took bulk emails and texts collected from their mass surveillance efforts. They have huge data so they can easily determine the authorship of any email through the use of their various sources, methods, and resources.

Definition

There is a hype around the use of blockchain technology, yet the technology is not well understood. Since there is no fixed definition of blockchain, everyone gives their own definition as per their understanding. Even the creator of the blockchain didn’t give any definition, so I took the liberty of giving my own definition as follows:

Blockchain is an *immutable* *distributed digital ledger* that records transactions and organized on a *decentralized* *peer-to-peer network*, which enables nodes to collaborate and coordinate in a *rational decision-making* process.

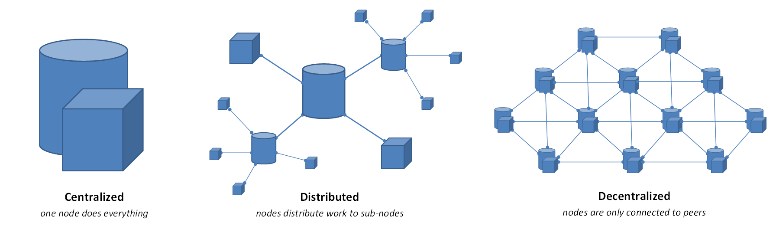
Explanation

Blockchain technology combines cryptographic primitives and record keeping concepts. It merges existing, proven concepts into a single solution. By examining each component individually, it can be simplified. Let’s discuss one by one.

Peer-to-peer network (P2P)

Two or more computer systems are connected to each other without any central server with equal privileges, and equal power is called a Peer-to-peer network. In a P2P network, each computer system or each participant in the network is a node. We use the term peer to refer to a node in the P2P network. These nodes can share or exchange resources through communication channels like cables or wireless networks. In P2P network information shared among nodes directly.

Before understanding what is distributed network means, let’s try to understand decentralization and centralization.



**Centralized networks** are controlled by a single entity where all resources are concentrated on a central or single location. They follow a client/server architecture where all clients communicate with a single central server. Centralized systems are unstable and vulnerable means if you want to create chaos, you surely know where to attack. An example of a centralized entity is Wikipedia.

**Decentralization** is one of the most frequently used terms to represent blockchain. Decentralization is the distribution of power, functionality, and resources that are dispersing away from a central authority or location. By the above definition is blockchain a decentralized network? Mostly yes, slightly no. Here is why. Let's see Vitalik Buterin, the Co-founder of ethereum explanation of decentralization:

There are three types of decentralization:

*Architectural decentralization*: How many physical computers in a network

*Political decentralization*: How many individuals or organizations control these computers?

*Logical decentralization*: Do the data structures and interfaces of the systems present and maintain like a single monolithic object or a swarm? Means if we cut the system in half including both providers and users, will both halves to continue as fully operate as independent units?

Blockchains are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure) but they are logically centralized (there is one commonly agreed state and system behaves like a single computer)

How blockchain is logically centralized consider this: All nodes in a blockchain runs the same client software turns out to have a bug now the whole system is bugged

Cloud technologies are decentralized then how blockchain is different from other decentralized technologies? It’s simple, the cloud technology is architecturally decentralized but controlled by a single entity means it is politically centralized.

By considering the above scenario, political and architectural decentralization are considered as the main factors of Blockchain it justifies our definition.

Decentralization is a subset of distributed architecture.

**A distributed network** is an extension of decentralization. It avoids the centralization meaning everyone gets access, and everyone gets the same access. The distributed network removed the need for third parties. End-user controls digital assets in a distributed architecture

A ledger in which transactions have been recorded as they occurred. A document that can serve as legal evidence of a transaction. Databases also keep track of transactions, so how blockchain is different from traditional databases? With traditional databases, we can perform CURD (Create, Update, Read and Delete) operations on records, but in blockchain, we can only create and read transactions or records.

**Distributed Ledger Technology (DLT)**

A distributed ledger is a database that exists on all peers in the network. Every node will have an exact copy of what other nodes have. With this facility, every node can process, validate the transactions independently. Blockchain uses this distributed ledger technology to promote transparency and give control of all its information and transactions to the user.

Records or transactions are only ever stored in the ledger when the consensus has been reached by the parties involved.

Immutability: Cryptography is the key

Cryptography is the process of converting the plaintext into the cipher text (unusual text)

Plain text + (Key /algorithm) = cipher text

A hash function is a digital mechanism that is used to compress data onto a specific format of a specific length.

Hash (message) = message digest

A specific cryptographic hash function used in many blockchain implementations is the Secure Hash Algorithm (SHA) with an output size of 256 bits (SHA-256) a 64 character Hexadecimal string.

SHA256 (Hello, World) = 0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Sha-0, SHA-1, SHA-2, and MD5 (Message Digest) are some hash functions.

The main difference between cryptography and hashing is length and size. In cryptography, we need to convert the whole file into a cipher format, meaning the greater the length, the greater the size. Hashing in another hand no matter the file size or length the output is fixed length

The hash function is one-way, it is computationally infeasible to compute the correct input value given some output value (e.g., given a digest, find x such that hash (x) = digest).

Hash functions are collision resistant means it is computationally infusible to produce hash (x) = hash (y)

In the blockchain network, we use cryptographic hash functions to

* Securing the block data
* Securing the block header
* Creating unique identifiers

There are two types Cryptographic models to understand. One is Asymmetric-key cryptography and symmetric-key cryptography.

Blockchain uses Asymmetric-key cryptography.

**Asymmetric-key cryptography** also known as public key cryptography uses a pair of keys: a public key and a private key that are mathematically related to each other. The public key is made public without reducing the security of the process, but the private key must remain secret.

One can encrypt with a private key and then decrypt with the public key. Alternately, one can encrypt with a public key and then decrypt with a private key.

Asymmetric-key cryptography enables a trust relationship between users who do not know or trust one another, by providing a mechanism to verify the integrity and authenticity of transactions while at the same time allowing transactions to remain public.

The transactions are digitally signed this means that a private key is used to encrypt a transaction such that anyone with the public key can decrypt it. Since the public key is freely available, encrypting the transaction with the private key proves that the signer of the transaction has access to the private key.

**RSA** is one of the popular asymmetric algorithms developed by Ron Rivest, Adi Shamir and Leonard Adleman. This crypto system was patented in 1983 and was released to the public domain by RSA Security in the year 2000. The key generation process depends on choosing two unique, random, and usually very large prime numbers.

**Digital Signature Algorithm or DSA** is another example of an asymmetric encryption system, though it’s used for signing and verifying data. It is developed by US Government. Similar to RSA, the specification covers the key generation process along with the signing and verifying data using the key pairs.

**Symmetric-key cryptography** in which a single secret key is used to both encrypt and decrypt. With symmetric-key cryptography, users must already have a trust.

The relationship established with one another to exchange the pre-shared key.

In Bitcoin Blockchain public key hash is the address of the user. Each blockchain implementation may implement a different method to derive an address.

**DES or Data Encryption Standard** is one of the most widely used encryption algorithms. DES was designed in the 1970s by IBM.

AES, IDEA, RC4, and RC5 are some other symmetric algorithms.

Markel Tree

A data structure where the data is hashed and combined until there is a singular root hash that represents the entire structure is represented as Markel Tree.

Root Hash (ABCDE)

A block header comprises two main hash values the previous hash and the root hash of transactions included in the current block. All these transactions are present as block data.

Transaction D

Transaction D

Transaction C

Transaction B

Transaction A

Hash E

Hash D

Hash C

Hash B

Hash A

Hash DE

Hash ABC

Each transaction has from, to, and value details, first we hash each transaction then all those hashes split into parts and generate new hashes until it becomes single hash

A transaction represents an interaction between two parties

Instead of adding every transaction into the block header, we add the root hash that was generated from the child hashes.

Wallet

Software that is used to store public keys, private keys, and associated addresses can be referred to as a wallet. It may also perform other functions, such as calculating the total number of digital assets of a user.

Blocks

Blockchain network users submit candidate transactions to the blockchain network via software (desktop applications, smartphone applications, digital wallets, web services, etc.). The software sends these transactions to a node or nodes within the blockchain network. The chosen nodes may be non-publishing full nodes as well as publishing nodes. The submitted transactions are then propagated to the other nodes in the network, but this by itself does not place the transaction in the blockchain. For many blockchain implementations, once a pending transaction has been distributed among nodes, it must then wait in a queue until it is added to the blockchain by a publishing node.

A block contains a block header and block data. The block header contains metadata for this block. The block data contains a list of validated and authentic transactions that have been submitted to the blockchain network. Validity and authenticity is ensured by checking that the transaction is correctly formatted and that the providers of digital assets in each transaction have each cryptographically signed the transaction. This verifies that the providers of digital assets for a transaction had access to the private key which could sign over the available digital assets.

**Genesis Block** is the first block a blockchain network; it records the initial state of the system.

Transactions are added to the blockchain when a publishing node publishes a block.

Anatomy of blocks

A block contains a block header and block data

Block Height

Nonce

Current Block Hash

Previous Hash

Time stamp

Root Hash

Markel Tree

Value

To

From

Block header contains

* The block number, also known as block height
* The previous block header’s hash value except genesis block
* A hash representation of the block data in Markel tree way
* A timestamp
* The size of the block
* The nonce value ( in a mining blockchain networks to achieve proof-of-work)

Block Data

* A list of transactions
* Other data may present like ledger events

Chaining the Blocks

Blocks are chained together to each block containing the hash digest of the previous block’s header, thus forming the blockchain. If we try to change a single transaction, then the root hash will change so the entire block. Then, every subsequent block’s hash will change in the result that the chain will break. This facility made the blockchain becomes tamper proof

Block Height: 27

Previous Hash

Current Block Hash

Timestamp

Block Size

Block Height: 26

Previous Hash

Current Block Hash

Timestamp

Block Size

Block Height: 25

Previous Hash

Current Block Hash

Timestamp

Block Size

However when blockchain is distributed architecture and every node participating in mining blocks with PoW then how the blockchain gets aligned? This is solved with the “longest chain rules”.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. Most blockchain networks use the strategy of adopting the longest chain as truth when there are multiple competing chains. If two chains are competing, each includes their own unique sequence of tail blocks, whichever is longer will be adopted.

However, this does not mean that the transactions within the replaced blocks are lost, rather they may have been included in a different block or returned to the pending transaction pool.

Consensus Mechanism

Blockchain works as a pear-to-pear network and the ledger is distributed then how do you actually make those ledgers work together? How do you keep their information and alignment? And peers in the networks makes decision?

We can solve these problems with a consensus mechanism. It is a process used to achieve agreement on a single data value or a state of a network among distributed processes or multi-agent systems.

Different blockchain’s using different types of consensus algorithms

Byzantine Fault Tolerance

Achieving Byzantine Fault Tolerance is one of the most difficult challenges addressed by blockchain technology.

**Byzantine Generals Problem** describes a scenario where two generals are attacking a common enemy. They surrounded the city from both sides but each general’s army on its own is not enough to defeat the enemy army successfully. Thus they need to cooperate and attack at the same time.

 In order for them to communicate and decide on a time, General 1 has to send a messenger across the enemy’s camp that will deliver the time of the attack to General 2. However, there is a possibility that the messenger will get captured by the enemies and thus the message won’t be delivered. This will result in General 1 attacking while General 2 and his army hold their grounds.

Even if the first message goes through, General 2 has to acknowledge that he received the message, so he sends a messenger back, thus repeating the previous scenario where the messenger can get caught. This extends to infinite ACK’s and thus the generals are unable to reach an agreement.

This is a loop in its physical nature and complexity.

How it is related to blockchain?

Blockchains are decentralized ledgers which, by definition, are not controlled by a central authority. Due to the value stored in these ledgers, bad actors have huge economic incentives to try and cause faults. That said, Byzantine Fault Tolerance, and thus a solution to the Byzantine Generals’ Problem for blockchains is much needed.

The big breakthrough when Bitcoin was invented, was the use of Proof-of-Work as a probabilistic solution to the Byzantine Generals Problem.

Proof-of-work (PoW)

A key aspect of blockchain technology is determining which user publishes the next block in permission less blockchain networks. This is solved through implementing one of many possible consensus models proof-of-work.

Put it simply, for permission less blockchain networks there are many publishing nodes competing at the same time to publish the next block and get rewards.

**Validity**: In blockchainin vast majority of created blocks are invalid so, we can think of valid block as “special” .Block validity is something defined by a blockchain protocol.

**Nonce** is a random numeric value that the only data we can change in the block to change the blocks hash to achieve PoW.

**Mining and Miners**:

We can refer miners as accountants because they record transactions into ledger.

The process of recording these transactions into blockchain is mining. So let’s see how it works

Blockchains have an arbitrary “difficulty setting”, managed by their protocol, which changes how hard it is to mine a block. This is where all the value comes from. If anyone could just create blocks and throw them on the chain, there would be no value there, and networks would never agree on which blocks should go on the chain.

Having created a block means you must have done a bunch of work. That’s what proof-of-work means. First, we hash the whole block and check if these blocks hash less than the difficulty threshold. The greater the difficulty, the lower the hash output would have to be for the block to be valid. Since hashes are effectively random hash functions, outputs are unpredictable. We can only change the nonce value and see if we happen to get a valid hash and do it repeatedly.

Adjustment is made to the difficulty level of the puzzle, and essentially either increases or decreases the number of leading zeros required. By increasing the number of leading zeros increases the difficulty of the puzzle, because any solution must be less than the difficulty level, meaning there are fewer possible solutions. By decreasing the number of leading zeros, decreases the difficulty level, because there are more possible solutions.

As the number of publishing nodes and the availability of computing power increases over time, so the puzzle difficulty is generally increasing.

For example, in a deck there are 10 cards each has its number from 1 to 10 now we want to get a number under 5 the chances are high and easy to play, if deck has 100 cards numbered from 1 to 100 and we want to get a number under 10 is bit difficult but what if there are 100,000 cards in a deck and to get under 10 is highly difficult.

SHA256 (“blockchain data” + nonce) = Hash digest “0000008f456”

Bitcoin uses the Proof-of-work mechanism, adjusts the difficulty every 2016 blocks to influence the blocks publication to be around once every ten minutes

This process is purely based on chance. This is a computationally intensive process. There is currently no known shortcut to this process. Publishing nodes must expend computation effort, time, and resources to find the correct nonce value for the target. Due to the significant resource consumption of some proof-of-work blockchain networks, there are some alternative mechanisms proposed.

Proof-of-Stake (PoS)

Proof of stake is a different way to validate transactions, and the purpose is the same as the proof of work, but the process to reach the goal is quite different. POS is based on the idea that the more stack the user has invested in the system, the more likely they will want the system to succeed. The stake is often an amount of cryptocurrency that the blockchain network user has invested into the system (through various means) once staked, the cryptocurrency is generally no longer able to be spent.

With this consensus model, there is no need to perform resource-intensive computations. So there is no reward for block creation; instead, the reward for block publication is usually the earning of user-provided transaction fees.

random selection of staked users, multi-round voting, coin aging systems, and delegate system are few approaches for PoS. Regardless of the exact approach, users with more stake are more likely to publish new blocks. Here the choice of block publisher is a random choice, the blockchain network will look at all users with a stake and choose amongst them based on their ratio of a stake to the overall amount of cryptocurrency staked. So, if a user had 42% of the entire blockchain network stake, they would be chosen 42% of the time; those with 1 % would be chosen 1% of the time.

When the choice of block publisher is a multi-round voting system, there is added complexity. The blockchain network will select several staked users to create proposed blocks. Then all staked users will cast a vote for a proposed block. Several rounds of voting may occur before a new block is decided upon. This method allows all staked users to have a voice in the block selection process for every new block.

When the choice of block publisher is through a coin age system, staked cryptocurrency has an age property. After a certain amount of time (such as 30days) the staked cryptocurrency can count towards the owning user being selected to publish the next block. The staked cryptocurrency then has its age reset, and it cannot be used again until after the requisite time has passed.

When the choice of block publisher is through a delegate system, users vote for nodes to become publishing nodes–therefore creating blocks on their behalf. Blockchain network users’ voting power is tied to their stake so the larger the stake, the more weight the vote has. Nodes who receive the most votes become publishing nodes and can validate and publish blocks. Blockchain network users can also vote against an established publishing node to try to remove them from the set of publishing nodes.

The threat of losing publishing node status, and therefore rewards and reputation, is constant so publishing nodes are incentivized to not act maliciously.

Other consensus Models

**Proof of Elapsed Time**

POET is a Nakamoto-style consensus algorithm developed by Intel, and it is now the consensus model of choice for Hyperledger Sawtooth’s modular framework. It relies on a special CPU instruction set called Intel Software Guard Extensions (SGX) and prevents high resource utilization and high energy consumption.

Each publishing node requests a wait time from a secure hardware time source within their computer system. The secure hardware time source will generate a random wait time and return it to the publishing node software. The publishing node with the shortest wait time will wake up first and commits a new block to the blockchain, broadcasting the necessary information to the whole peer network; any publishing node that is still idle will stop waiting, and the entire process starts over.

**Round Robin Consensus Model**

Round Robin is a consensus model that is used by some permissioned blockchain networks. It has a long history grounded in a distributed system architecture. To handle situations where a Publishing node is not available to publish a block on its turn, these systems may include a time Limit to enable available nodes to publish blocks so that unavailable nodes will not cause a halt in block publication. This model ensures no one node creates the majority of the blocks.

Proof of Capacity, Proof of authority, and Proof of Activity are some other options.

Forking

Changes to a blockchain network’s protocol and data structures are called forks.

Performing changes and updating technology can be difficult at the best of times. For permissionless blockchain networks which are comprised of many users, distributed around the world, and governed by the consensus of the users, it becomes extremely difficult.

Forks can be divided into two categories: soft forks and hard forks. For a soft fork, changes are backwards compatible with nodes that have not been updated. For a hard fork, changes are not backwards compatible.

**Soft Forking**

A soft fork is a change to a blockchain implementation that is backward compatible. Non updated nodes can continue to transact with updated nodes. If no (or very few) nodes upgrade, then the updated rules will not be followed.

For example, a blockchain decided to reduce the size of blocks (from 1.0 MB to 0.5 MB). Updated nodes would adjust the block size and continue to transact as normal; non-updated nodes would see these blocks as valid since the change made does not violate their rules (i.e., the block size is under their maximum allowed). However, if a non-updated node were to create a block with a size greater than 0.5 MB, updated nodes would reject them as invalid.

**Hard Forking**

A hard fork is a change to a blockchain implementation that is not backwards compatible. At a given point in time (usually at a specific block number), all publishing nodes will need to switch to using the updated protocol. Additionally, all nodes will need to upgrade to the new protocol so that they do not reject the newly formatted blocks. Non-updated nodes cannot continue to transact on the updated blockchain because they are programmed to reject any block that does not follow their version of the block specification.

Security

As Blockchain is a decentralized system, it is maintained by a multiple participant on the network who are responsible for securing the data? Can we trust a bunch of strangers to take good care of the information? Well, blockchain is a system for transactions without relying on trust. It is designed to be immutable.

The records on a blockchain are secured through cryptography. Network participants have their own private keys that are assigned to the transactions they make and act as a personal digital signature. If a record is altered, the signature will become invalid and the peer network will know right away that something has happened.

However, it is possible to take control over the network with majority or at least 51% of CPU power, an attacker or group of attackers can interfere with the process of recording new blocks. They can prevent other miners from completing blocks, theoretically allowing them to monopolize the mining of new blocks and earn all the rewards.

Blockchain types

Blockchain networks can be categorized based on their permission model, which determines who can maintain them. If anyone can publish a new block, it is permission less. If only particular users can publish blocks, it is permissioned.

There are three types of blockchains to opt from

* Public Blockchain aka Permissionless
* Private Blockchain aka Permissioned Blockchain
* Consortium Blockchain aka Hybrid blockchain

Public Blockchain

In Permissionless blockchain anyone can publish blocks and validate them any blockchain network user within a permissionless blockchain network can read and write to the ledger.

Public Blockchain is publicly accessible and has no restriction on who can participate or be a validator. In public Blockchains, no one has complete control over the network. This ensures data security and helps immutability because a single person cannot manipulate the Blockchain.

Since permissionless blockchain networks are open to all to participate, malicious users may attempt to publish blocks in a way that subverts the system. To prevent this, permissionless blockchain networks often utilize a multiparty agreement or ‘consensus’ system that requires users to expend or maintain resources when attempting to publish blocks. This prevents malicious users from easily subverting the system.

Examples: Bitcoin Blockchain, Ethereum.

Private Blockchain

Permissioned blockchain networks are ones where users publishing blocks must be authorized by some authority. Since only authorized users are maintaining the blockchain, it is possible to restrict read access and to restrict who can issue transactions.

They also use consensus models for publishing blocks, but these methods often do not require the expense or maintenance of resources.

Permissioned blockchain networks may also be used by organizations that wish to work together but may not fully trust one another. They can establish a permissioned blockchain network and invite business partners to record their transactions on a shared distributed ledger.

Example: Hyperledger Fabric

Consortium Blockchain

It is a combination between different characteristics both public and private blockchains have by design. It allows to determine what information stays private and what information is made public.

Smart Contracts

A computerized transaction protocol that executes the terms of a contract can refer to a smart contract. A smart contract is just a small pieces of logic or code that operates on a blockchain. Smart contracts eliminate the need for third parties.

Even the smart contracts are not new, the term smart contract is proposed defined by Nick Szabo in 1994.

The general objectives of smart contract design is to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.”

The smart contract is executed by nodes within the blockchain network; all nodes that execute the smart contract must derive the same results from the execution, and the results of execution are recorded on the blockchain.

This added functionality to the blockchain can referred as blockchain2.0. Because Bitcoin blockchain can only perform addition and subtraction.

Decentralized Applications (DApps)

DApps are applications that run on a P2P network of computers rather than a single computer.

DApps connect users and providers directly. There is no need for a trusted third party hosting providers like GoDaddy, Bluehost or AWS.

Popular DApps platforms are Ethereum, EOS.

Blockchain Platforms

There are nearly a dozen blockchain platforms implemented in the space. Let’s see the most popular blockchains for now.

Ethereum

Vitalik Buterin, a Russian-canadian programmer come up with an idea of executing smart contracts on blockchain. Then he teamed with Gavin Wood, Joseph Lubin, and announced Ethereum in 2014. Ethereum initially released on 2015 July.

Ethereum is an example of Blockchain 2.0 technology. Ethereum’s vision is to create a “World Computer”–a huge network of many private computers that run all future internet applications without any third parties. It is a Blockchain based distributed computing platform, and it is public and open-source.

Ethereum also has its own cryptocurrency called Ether and Ethereum keeps track the history of Ether. It can also be used to track any other assets like we can run applications on etherum commonly called as decentralized applications. All users are anonymous and is fully transparent. Here No permission is needed because third parties are no longer required.

Ethereum uses keccak-256 hash functionality to send ether to an account, you need the Keccak-256 hash of the public key of that account. Ether is a fundamental token for the operation of Ethereum, which thereby provides a public distributed ledger for transactions. It is used to pay for gas, a unit of computation used in transactions and other state transitions.

The Ethereum Virtual Machine (EVM) is the runtime environment to execute smart contracts in Ethereum. These smart contracts can be written in solidity.

**Enterprise Ethereum Alliance (EEA)** is formed in 2017 as a non-profit organisation. It promotes Ethereum to large corporations and connects them with Ethereum. Its vision is to create enterprise-ready solutions. It plays an important role in standardizing approaches for privacy, permissioning and providing alternative consensus algorithms to improve its usability in enterprise settings

Hyperledger

It is intended to be a platform for building cross-industry enterprise applications using blockchain technology.  It does not support any cryptocurrency.  It is permissioned blockchain which means only authorize personal can only transact or validate the transaction

Hyperledger project is started in late 2015 by Linux Foundation and supported by big industry players like IBM, Intel and more. Brian Behlendorf, the creator of the Apache web server, is the executive director of the project. Hyperledger can track any kind of assets. It is also featured with smart contracts here they called as chain code

Many frameworks and Tools are developed under the hyperledger project.

**Hyperledger Fabric** is a permissioned blockchain infrastructure. A Fabric Network comprises “peer nodes”, which execute Chaincode, access ledger data, endorse transactions and interface with applications. “Ordered nodes” which ensure the consistency of the blockchain and deliver the endorsed transactions to the peers of the network

Chain code can be written in Golang and JavaScript.

**Hyperledger Iroha** was written in C++, with an emphasis on supporting mobile applications.

**Hyperledger Sawtooth** includes a dynamic consensus feature enabling hot swapping consensus algorithms in a running network. Among the consensus options is a novel consensus protocol known as “Proof of Elapsed Time”

**Hyperledger Indy** for decentralized Identity and Hyperledger Grid are few other frameworks.

Other Blockchain Platforms

**Ripple**

The idea of Ripple is connecting payment providers, digital asset exchanges, banks, and corporate via blockchain network. It is a permissioned blockchain.

**R3 Corda**

R3 is a consortium of world’s leading financial institutions that built an open-source distributed ledger platform called Corda in 2015. Corda is a cutting-edge blockchain platform, which enables institutions to transact directly with smart contracts by removing costly frictions in business transactions. Corda does not have a cryptocurrency or built-in token and is a permissioned blockchain.

**Quorum**

It is a permissioned blockchain and founded by J.P.Morgan and is open-source. Quorum modifies the core of Ethereum to enhance confidentiality for enterprises.

**EOS** is designed for the development of DApps.

NEO, Stellar, OpenChain are some other Blockchain platforms has their unique features.

Blockchain Use Cases

The Scope of the blockchain usage is gone from cryptocurrencies to multiple domains. Blockchain does not fit everywhere.  Let’s see where blockchian fits.

Banking, Government, Educational institutions, Health care industry, Supply chain, Real Estate, IOT and data science. These are few among other industries.

Before thinking about to use Blockchain in an enterprise, consider the following questions.

* Do we need a trusted third party?
* Do we need a shared, consistent data store?
* More than one entity needs to contribute data
* Data record once written never updated or deleted
* Do we want a tamper proof log of all writes to the data store?
* If cryptographically secure system of ownership is needed
* A need for a decentralized naming service or ordered registry

If the all answers are yes, we have a blockchain use case.

Obstacles to the Adoption of Blockchain

* Performance
* Energy conceptions is high
* Security
* Scalability
* Setup Costs
* Lack of knowledge and skill set

There is a lack of education about the blockchain technology. There has been a lot of unawareness and misinformation with most people thinking the technology is limited to cryptocurrencies and the financial sector.

Conclusion and Final Thoughts

By now we may understand that we need not rely completely on centralization. Decentralization and Distributed ledger technologies have been a new approach. Blockchain gather a huge hype and there is less knowledge about disruptive technology. It eliminated or reduced the need of third parties, shown a way minimise the fraud and expenditure. It solved double spending issues identity issues. It also solved many problems that Industries like healthcare, financial sectors facing, but it cannot solve every problem. It cannot be applied universally. Like every technology blockchain also has its drawbacks like misusing its anonymity feature to behave or other purposes. The large organizations started adopting blockchain so it can create multiple Opportunities.