BLOCK CHAIN

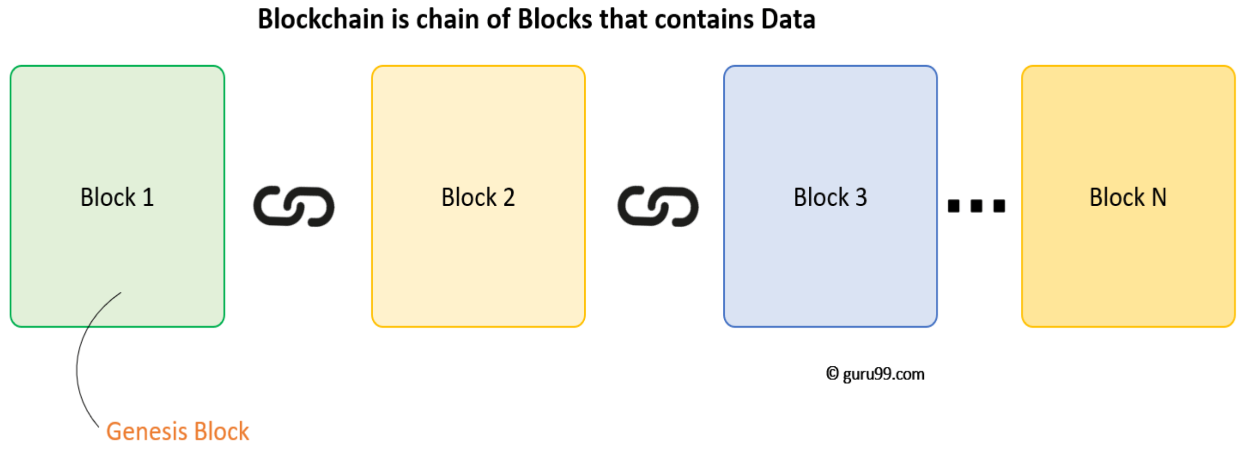
The term blockchain was first described back in 1991. A group of researchers wanted to create a tool to timestamp digital documents so that they could not be backdated or changed. Further, the technique was adapted and reinvented by Satoshi Nakamoto. In 2008, Nakamoto created the first cryptocurrency, the blockchain-based project called Bitcoin.

In general, blockchain technology has the core characteristics of decentralization, accountability, and security. This technique can improve operational efficiency and save costs significantly

a blockchain is a chain of blocks which contain specific information (database), but in a secure and genuine way that is grouped together in a network (peer-to-peer). In other words, blockchain is a combination of computers linked to each other instead of a central server, meaning that the whole network is decentralized.

Eg: The blockchain concept can be compared to work done with Google Docs. You may recall the days of tossing over doc. documents and waiting for other participants to make necessary edits. These days, with the help of Google Docs, it is possible to work on the same document simultaneously.

Block



A Blockchain is a chain of blocks which contain information. The data which is stored inside a block depends on the type of blockchain.

The blockchain data structure is explained as a back-linked record of blocks of transactions, which is ordered. It can be saved as a file or in a plain database. Each block can be recognized by a hash, created utilizing the SHA256 cryptographic hash algorithm on the header of the block. Each block mentions a former block, also identified as the parent block, in the "previous block hash" field, in the block header. Let's first look at each term more closely.

Index – This term symbolizes the location of the block inside the blockchain. The first block is indexed '0', the next '1', and so on.

Hash – Hash is the function which facilitates the rapid classification of data in the dataset

Previous hash – Each and every block in blockchain data structure, is associated with its ancestors. This characteristic adds to its immutability as a variety in the order of blocks.

numTx – This wares a tally of the number of transaction enumerated in the block.

Timestamp – It saves the time aspects of when the block was built.

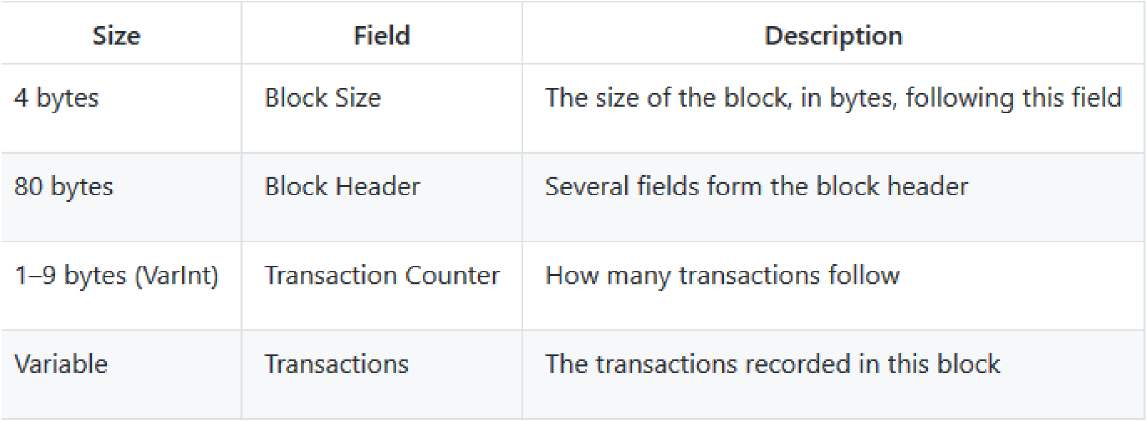
Nonce – It saves the integer (32 or 64bits) that are utilized in the mining method.

Transaction – This is a different track saved as arrays in the frame of the block. They save the specific version of a transaction executed so far in the block.

Merkel Tree– A Merkle tree, also perceived as a binary hash tree, is a data structure utilized for efficiently compiling and validating the uprightness of large sets of data.

What is a Block?

A block is a package data structure. According to Bitcoin Book, a block is a container data structure that clusters transactions for incorporation in the public ledger known as the blockchain.



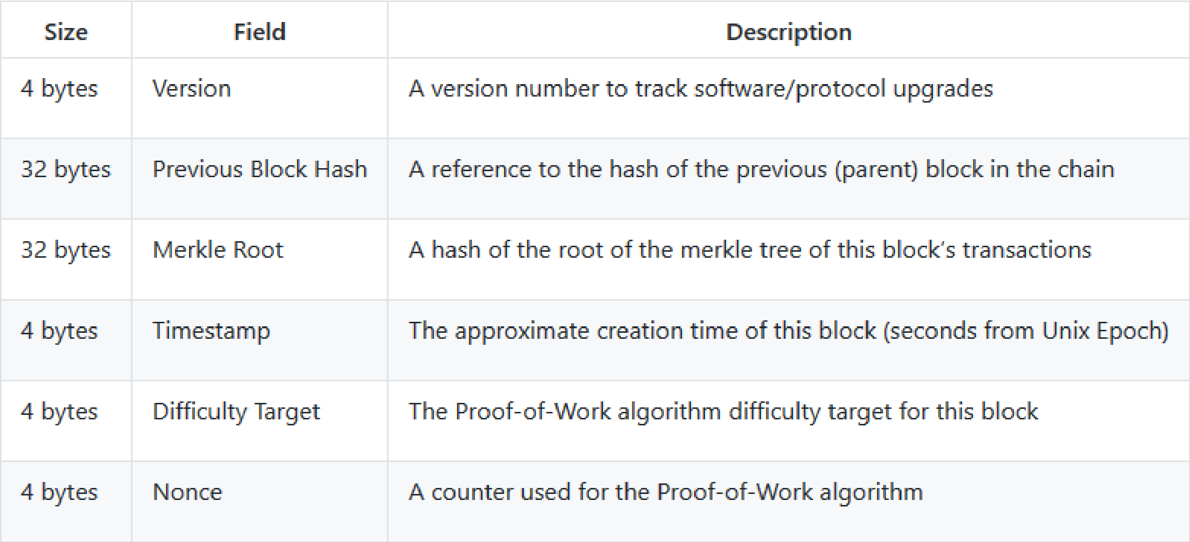
Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1–9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Block details

The block is composed of a header which includes metadata, accompanied by a lengthy record of transactions that advance its size. The block header is 80 bytes and the common transaction is at least 400 bytes. The common block includes more than 1900 transactions. A complete block, with all transactions, is almost 10,000 times greater than the block header.

What is the Block Header?

The block header is made up of metadata (Data about data).



Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

The Block Header Details

The first part: There is a citation to a former block hash, which joins this block to the earlier block in the blockchain.

The second part: In this, metadata such as timestamp, and nonce correlate to the mining race.

The third part: In this metadata is the Merkle tree root. This tree root is a data structure which is utilized to efficiently compile all the transactions in the block.

The Block Identifiers

There are two ways the blocks can be identified. These are cryptographic hash and block height.

The primitive identifier of a block is its cryptographic hash. It is also known as a digital fingerprint which is built by hashing the block header twice through the SHA256 algorithm. The resulting 32-byte hash is described as the block hash but is more precisely the block header hash, because is utilized to calculate it. For example, 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f is the block hash of the first bitcoin block ever created. The block hash recognizes a block and can be autonomously determined by any node by directly hashing the block header.

Another way to recognize a block is by its location in the blockchain. This is described as the block height. The first block created is at block height 0 (zero) and is the same block that was earlier cited by the next block hash is 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.

What is the Genesis Block?

The first block in the blockchain is known as the genesis block. This was built in the year 2009. It is the universal parent of all the blocks in the blockchain. In other words, if people begin at any block and watch the chain counter clockwise then they will ultimately come at the genesis block.

Every node perpetually begins with a blockchain of at least one block because the genesis block cannot be modified. Every node always recognizes the genesis block's hash and structure. It also recognizes its fixed time when it was created and even its single transaction. Thus, every node has the starting point for the blockchain, a secure "root" from which to build a trusted blockchain.

Blockchain technology is a unique invention that has caused the much-required security and protection in the cyber world.

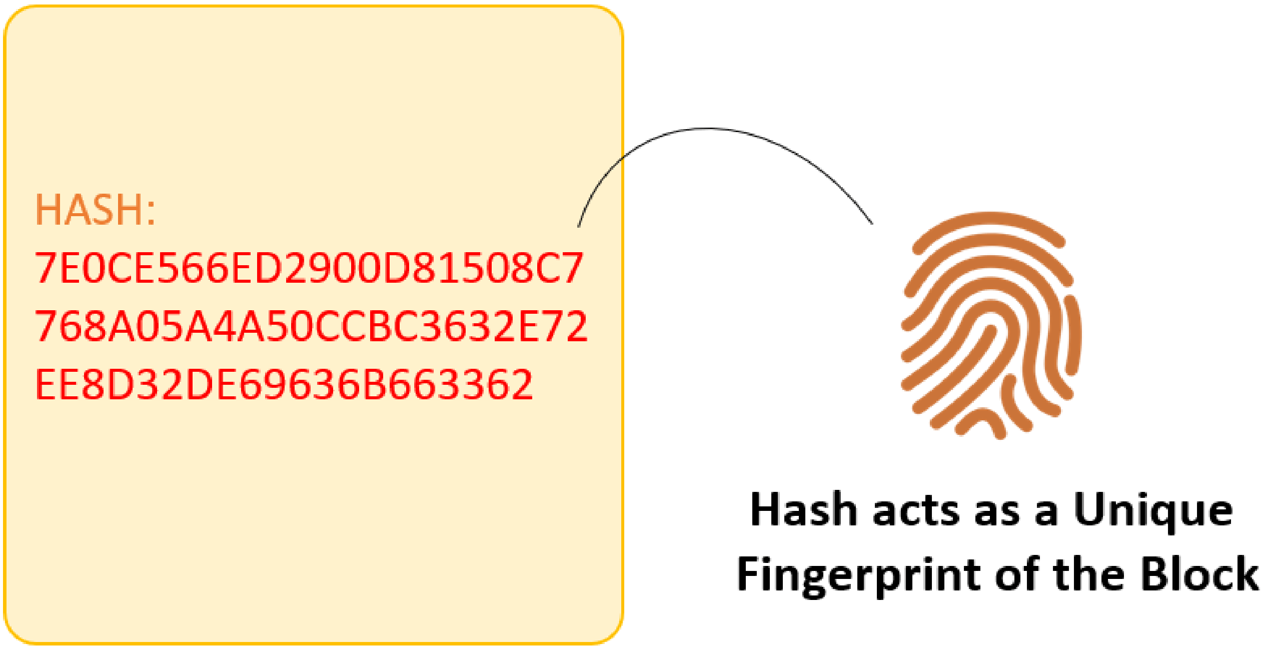
What is hashing?

When a transaction has been verified and needs to be added to a block in a chain, it will be put through a hash algorithm to convert it into set of unique numbers and letters, similar to what would be created by a random password generator. Then two transaction hashes will be combined, and put through the hash algorithm to produce another unique hash. This process of combining multiple transactions into new hashes continues until finally there remains just one hash – the 'root' hash of several transactions.

What makes hashes unique, and a key security feature for blockchains, is that they only work one way. While the same data will always produce the same hash of numbers and letters, it is impossible to 'un-hash', or reverse the process, using the numbers and letters to decipher the original data.

Understanding SHA256 - Hash

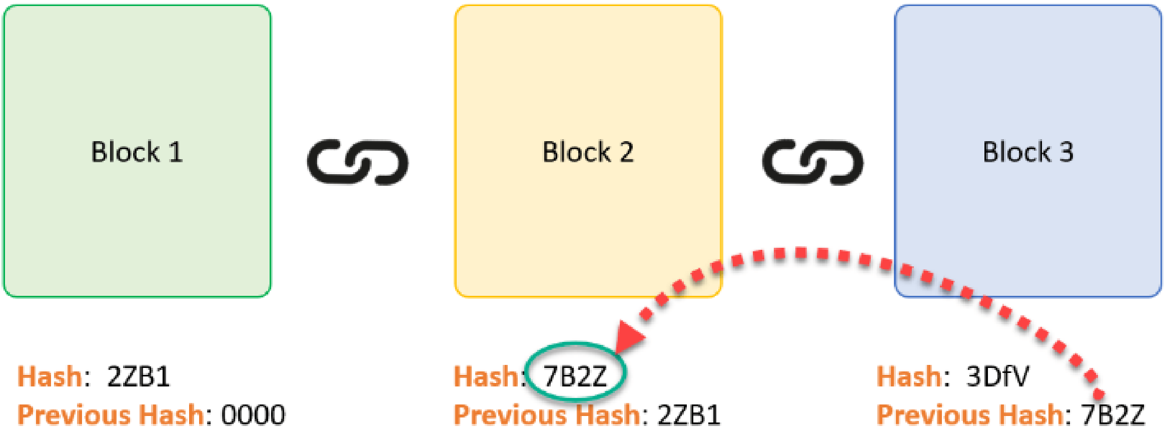
A block also has a hash. A can be understood as a fingerprint which is unique to each block. It identifies a block and all of its contents, and it's always unique, just like a fingerprint. So once a block is created, any change inside the block will cause the hash to change.



Each Block has

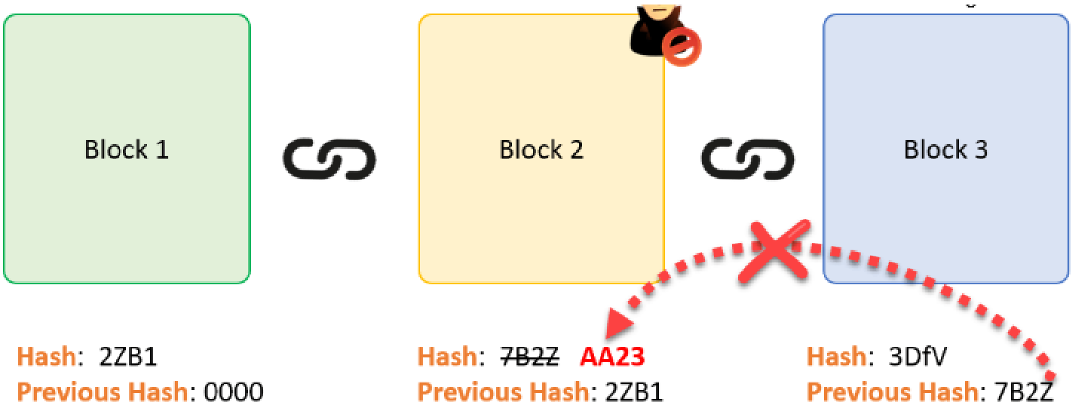
1. Data
2. Hash
3. Hash of the previous block

Consider following example, where we have a chain of 3 blocks. The 1st block has no predecessor. Hence, it does not contain has the previous block. Block 2 contains a hash of block 1. While block 3 contains Hash of block 2.



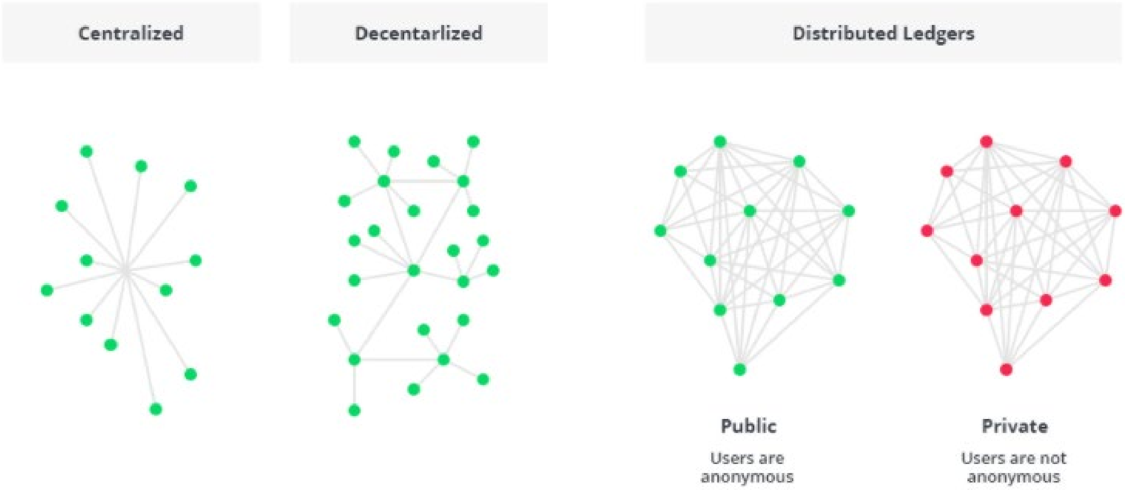
Hence, all blocks are containing hashes of previous blocks. This is the technique that makes a blockchain so secure. Let's see how it works -

Assume an attacker is able to change the data present in the Block 2. Correspondingly, the Hash of the Block also changes. But, Block 3 still contains the old Hash of the Block 2. This makes Block 3, and all succeeding blocks invalid as they do not have correct hash the previous block.



Therefore, changing a single block can quickly make all following blocks invalid.

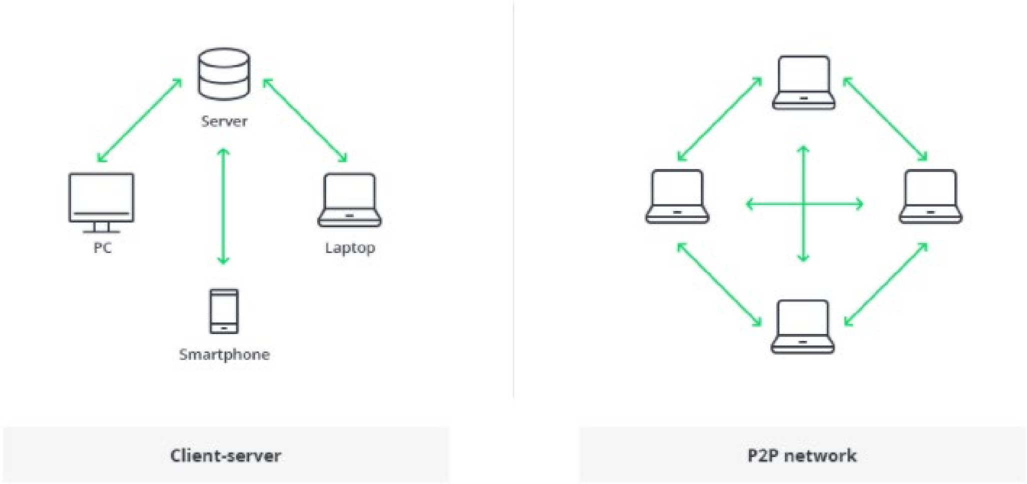
What is Blockchain Datastructure?



The blockchain technique allows digital information to be distributed, rather than copied. This distributed ledger provides transparency, trust, and data security.

Blockchain architecture is being used very broadly in the financial industry. However, these days, this technology helps create software development solutions for cryptocurrencies and record keeping, digital notary, and smart contracts.

Database vs. Blockchain Architecture



Client-Server vs P2P Network

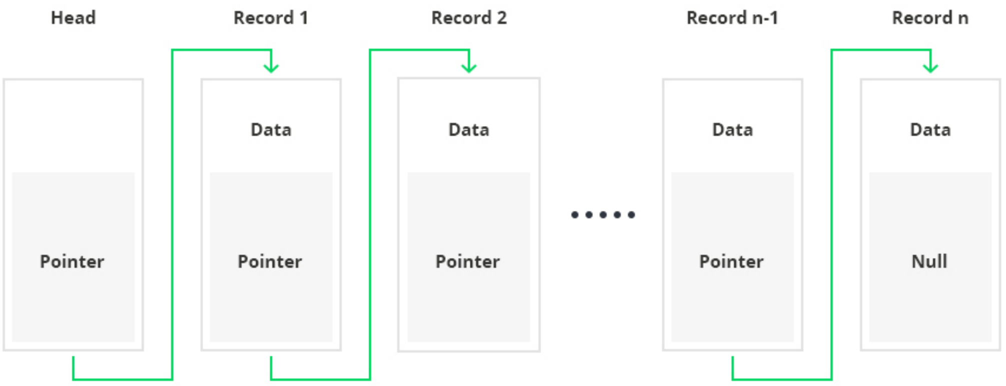
he traditional architecture of the World Wide Web uses a client-server network. In this case, the server keeps all the required information in one place so that it is easy to update, due to the server being a centralized database controlled by a number of administrators with permissions.

In the case of the distributed network of blockchain architecture, each participant within the network maintains, approves, and updates new entries. The system is controlled not only by separate individuals, but by everyone within the blockchain network. Each member ensures that all records and procedures are in order, which results in data validity and security. Thus, parties that do not necessarily trust each other are able to reach a common consensus.

To summarize things, the blockchain is a decentralized, distributed ledger (public or private) of different kinds of transactions arranged into a P2P network. This network consists of many computers, but in a way that the data cannot be altered without the consensus of the whole network (each separate computer).

The structure of blockchain technology is represented by a list of blocks with transactions in a particular order. These lists can be stored as a flat file (txt. format) or in the form of a simple database. Two vital data structures used in blockchain include:

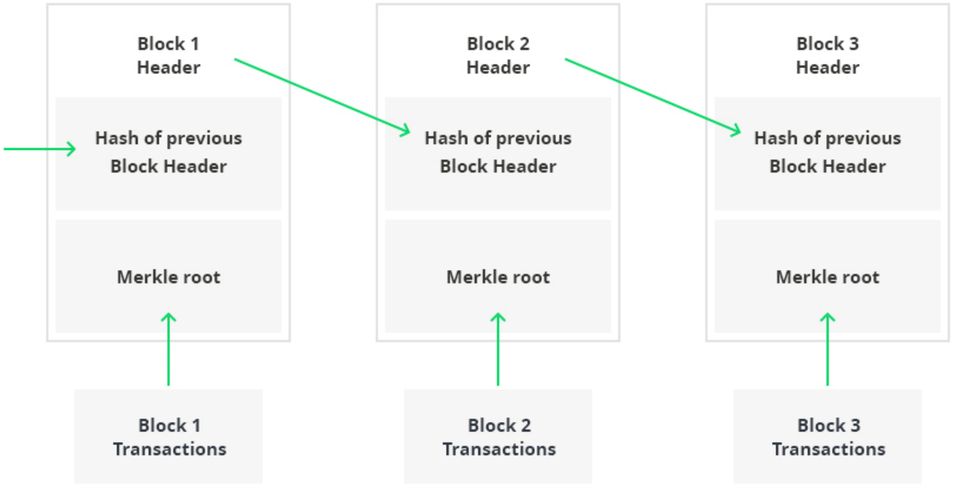
- Pointers - variables that keep information about the location of another variable. Specifically, this is pointing to the position of another variable.
- Linked lists - a sequence of blocks where each block has specific data and links to the following block with the help of a pointer.



Blockchain Hashing

Logically, the first block does not contain the pointer since this one is the first in a chain. At the same time, there is potentially going to be a final block within the blockchain database that has a pointer with no value.

Basically, the following blockchain sequence diagram is a connected list of records:

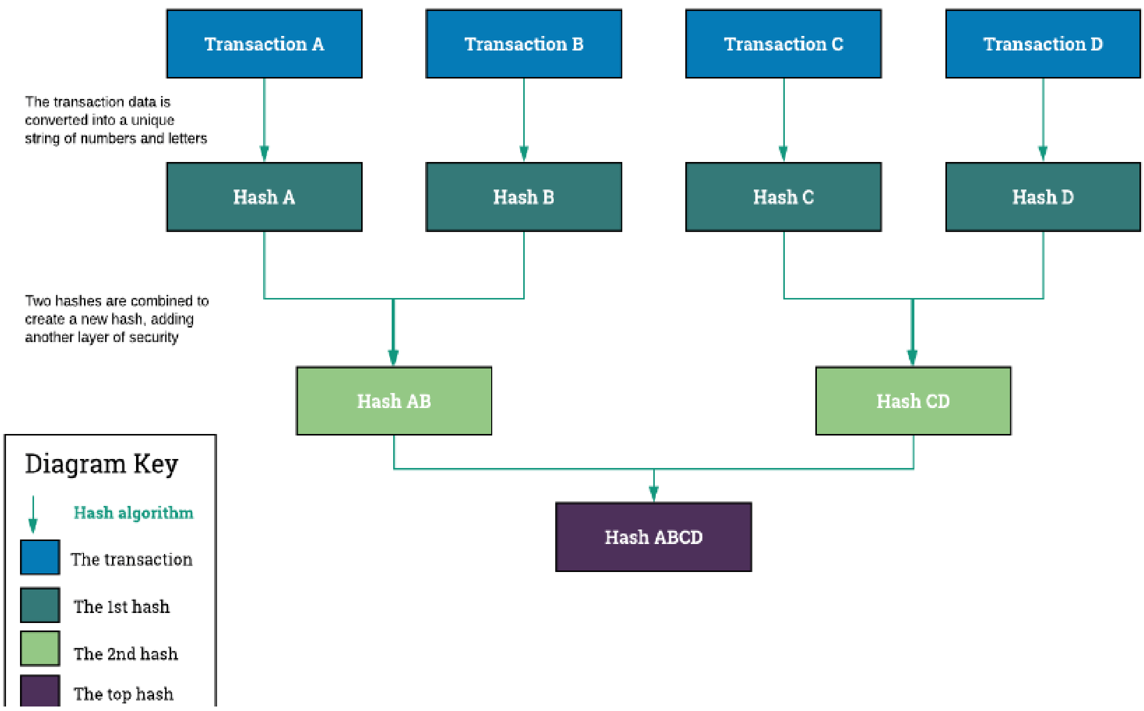


Blockchain Structure

What is a Merkle Tree?

If the hashing process is repeated with exactly the same transactions, exactly the same hashes will be created. This allows anyone using the blockchain to check that the data has not been tampered with, because ANY change in any part of the data will result in a completely different hash, affecting every iteration of hashes all the way to the root. This is known as a Merkle Tree.

A Simplified Merkle Tree diagram



Merkle Trees serve the purpose of significantly reducing the amount of data required to be stored and transmitted or broadcast over the network by summarising sets of hashed transactions into a single root hash. As each transaction is hashed, then combined and hashed again, the final root hash will still be a standard size.

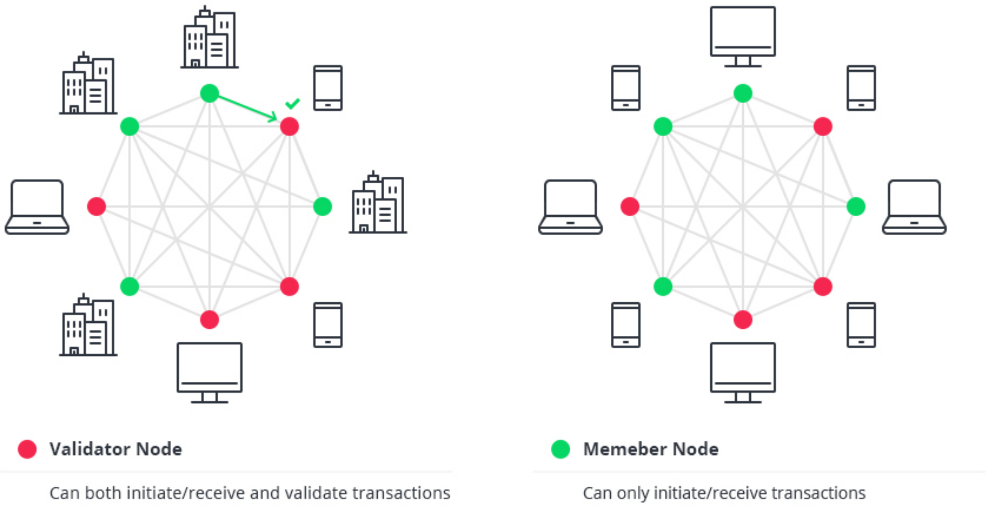
BLOCK CHAIN ARCHITECTURE

Blockchain architecture can serve the following purposes for organizations and enterprises:

- Cost reduction - lots of money is spent on sustaining centrally held databases (e.g. banks, governmental institutions) by keeping data current secure from cyber crimes and other corrupt intentions.

- History of data - within a blockchain structure, it is possible to check the history of any transaction at any moment in time. This is a ever-growing archive, while a centralized database is more of a snapshot of information at a specific point.
- Data validity & security - once entered, the data is hard to tamper with due to the blockchain's nature. It takes time to proceed with record validation, since the process occurs in each independent network rather than via compound processing power. This means that the system sacrifices performance speed, but instead guarantees high data security and validity.

Types of Blockchain Architecture Explained



● Validator Node
Can both initiate/receive and validate transactions
● Memeber Node
Can only initiate/receive transactions

Nodes in Public vs. Private Blockchains

All blockchain structures fall into three categories:

- Public blockchain architecture

A public blockchain architecture means that the data and access to the system is available to anyone who is willing to participate (e.g. Bitcoin, Ethereum, and Litecoin blockchain systems are public).

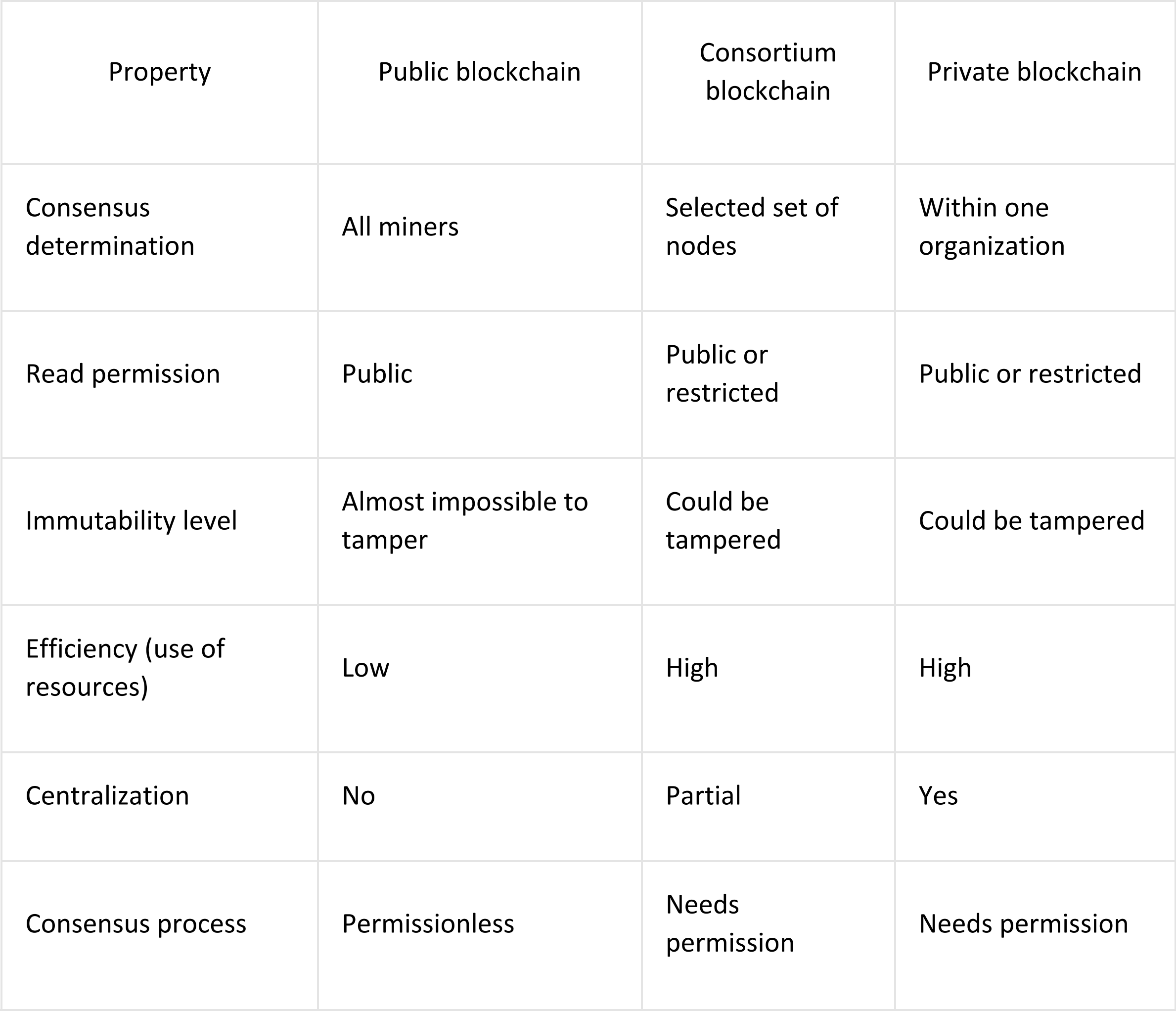
- Private blockchain architecture

As opposed to public blockchain architecture, the private system is controlled only by users from a specific organization or authorized users who have an invitation for participation.

- Consortium blockchain architecture

This blockchain structure can consist of a few organizations. In a consortium, procedures are set up and controlled by the preliminary assigned users.

The following table provides a detailed comparison among these three blockchain systems:



Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	Within one organization
Read permission	Public	Public or restricted	Public or restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Efficiency (use of resources)	Low	High	High
Centralization	No	Partial	Yes
Consensus process	Permissionless	Needs permission	Needs permission

As mentioned, blockchain is a distributed journal where all parties hold a local copy. However, based on the type of blockchain structure and its context, the system can be more centralized or decentralized. This simply refers to the blockchain architecture design and who controls the ledger.

A private blockchain is considered more centralized since it is controlled by a particular group with increased privacy. On the contrary, a public blockchain is open-ended and thus decentralized.

In a public blockchain, all records are visible to the public and anyone could take part in the agreement process. On the other hand, this is less efficient since it takes a considerable amount of time to accept each new record into the blockchain architecture.

In terms of efficiency, the time for each transaction in a public blockchain is less eco-friendly since it requires a huge amount of computation power compared to private blockchain architecture.

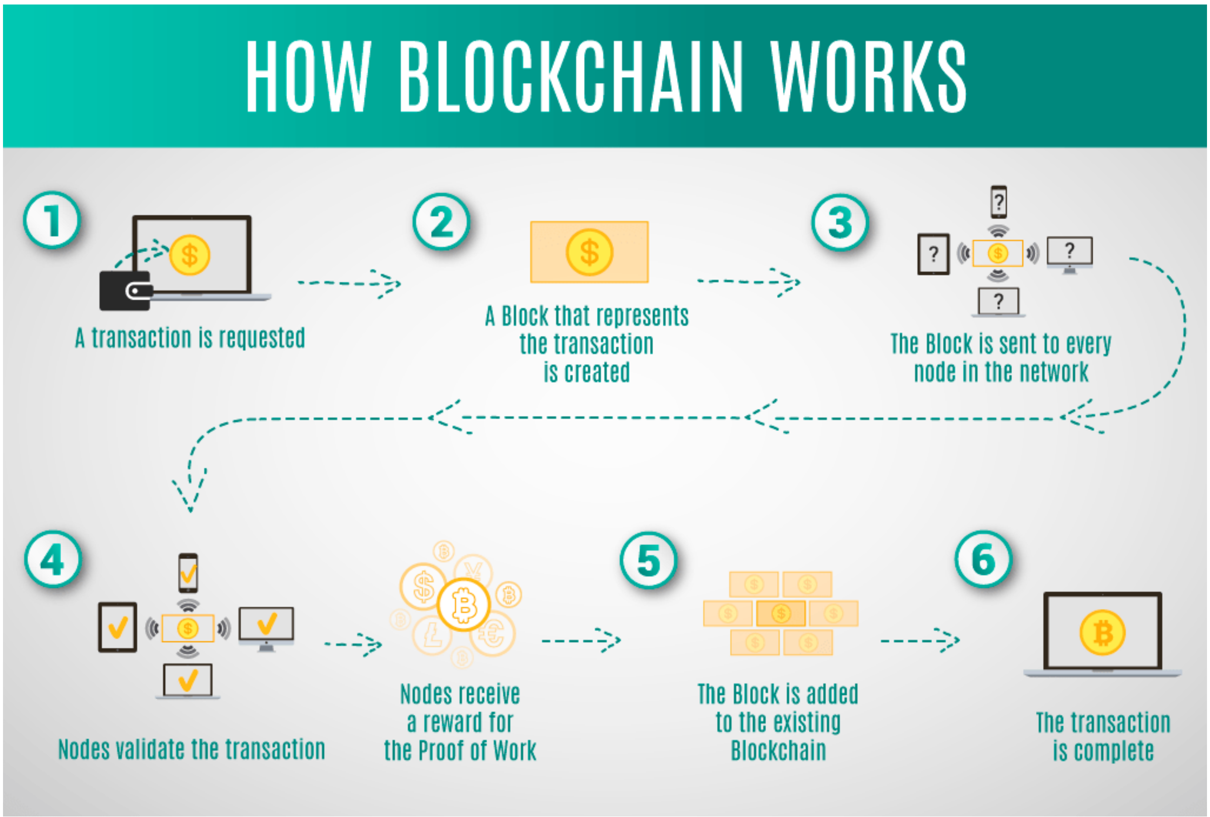
Core Components of Blockchain Architecture: How Does It Work

These are the core blockchain architecture components:

- Node - user or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger)
- Transaction - smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain
- Block - a data structure used for keeping a set of transactions which is distributed to all nodes in the network
- Chain - a sequence of blocks in a specific order
- Miners - specific nodes which perform the block verification process before adding anything to the blockchain structure
- Consensus (consensus protocol) - a set of rules and arrangements to carry out blockchain operations

Any new record or transaction within the blockchain implies the building of a new block. Each record is then proven and digitally signed to ensure its genuineness. Before this block is added to the network, it should be verified by the majority of nodes in the system.

The following is a blockchain architecture diagram that shows how this actually works in the form of a digital wallet.


HOW BLOCKCHAIN WORKS
1
A transaction is requested
2
A Block that represents the transaction is created
3
The Block is sent to every node in the network
4
Nodes validate the transaction
Nodes receive a reward for the Proof of Work
5
The Block is added to the existing Blockchain
6
The transaction is complete

How Blockchain Works

The blockchain technology immutable and cryptographically secure by eliminating any third-parties. It is impossible to tamper with the blockchain system; as it would be necessary to tamper with all of its blocks, recalculate the proof-of-work for each block, and also control more than 50% of all the nodes in a peer-to-peer network.

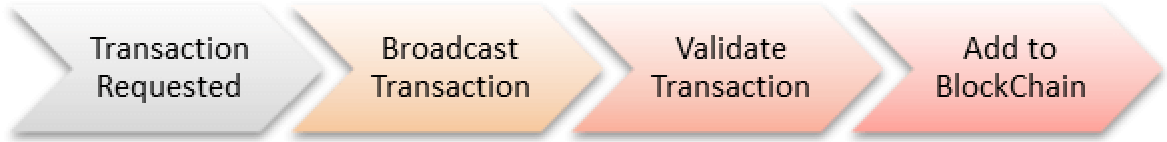
Key Characteristics of Blockchain Architecture

Blockchain architecture possesses a lot of benefits for businesses. Here are several embedded characteristics:

- Cryptography - blockchain transactions are validated and trustworthy due to the complex computations and cryptographic proof among involved parties
- Immutability - any records made in a blockchain cannot be changed or deleted
- Provenance - refers to the fact that it is possible to track the origin of every transaction inside the blockchain ledger

- Decentralization - each member of the blockchain structure has access to the whole distributed database. As opposed to the central-based system, consensus algorithm allows for control of the network
- Anonymity- each blockchain network participant has a generated address, not user identity. This keeps users' anonymity, especially in a public blockchain structure
- Transparency - the blockchain system cannot be corrupted. This is very unlikely to happen, as it requires huge computing power to overwrite the blockchain network completely

How Blockchain Transaction Works?



Blockchain Transaction Process

Step 1) Some person requests a transaction. The transaction could be involved cryptocurrency, contracts, records or other information.

Step 2) The requested transaction is broadcasted to a P2P network with the help of nodes.

Step 3) The network of nodes validates the transaction and the user's status with the help of known algorithms.

Step 4) Once the transaction is complete the new block is then added to the existing blockchain. In such a way that is permanent and unalterable.

Advantage of Blockchain?

Here, are some reasons why Blockchain technology has become so popular.

Resilience: Blockchains is often replicated architecture. The chain is still operated by most nodes in the event of a massive attack against the system.

Time reduction: In the financial industry, blockchain can play a vital role by allowing the quicker settlement of trades as it does not need a lengthy process of verification, settlement, and clearance because a single version of agreed-upon data of the share ledger is available between all stack holders.

Reliability: Blockchain certifies and verifies the identities of the interested parties. This removes double records, reducing rates and accelerates transactions.

Unchangeable transactions: By registering transactions in chronological order, Blockchain certifies the unalterability, of all operations which means when any new block has been added to the chain of ledgers, it cannot be removed or modified.

Fraud prevention: The concepts of shared information and consensus prevent possible losses due to fraud or embezzlement. In logistics-based industries, blockchain as a monitoring mechanism act to reduce costs.

Security: Attacking a traditional database is the bringing down of a specific target. With the help of Distributed Ledger Technology, each party holds a copy of the original chain, so the system remains operative, even the large number of other nodes fall.

Transparency: Changes to public blockchains are publicly viewable to everyone. This offers greater transparency, and all transactions are immutable.

Collaboration – Allows parties to transact directly with each other without the need for mediating third parties.

Decentralized: There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated, and all valid transactions are added one by one.

CONTRACT DATA

A smart contract is a self-enforcing agreement embedded in computer code managed by a blockchain. The code contains a set of rules under which the parties of that smart contract agree to interact with each other. If and when the predefined rules are met, the agreement is automatically enforced. Smart contracts provide mechanisms for efficiently managing tokenized assets and access rights between two or more parties. One can think of it like a cryptographic box that unlocks value or access, if and when specific predefined conditions are met. The underlying values and access rights they manage are stored on a blockchain, which is a transparent, shared ledger, where they are protected from deletion, tampering, and revision. Smart contracts, therefore, provide a public and verifiable way to embed governance rules and business logic in a few lines of code, which can be audited and enforced by the majority consensus of a P2P network.

How do 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 (releasing funds to the appropriate parties; registering a vehicle; sending notifications; issuing a ticket) when predetermined conditions have been met and verified. The blockchain is then updated when the transaction is completed.

Let’s see how this plays out in a supply chain example. Buyer B wants to buy something from Seller A, so she puts money in an escrow account. Seller A will use Shipper C to deliver the product to Buyer B. When Buyer B receives the item, the money in escrow will be released to Seller A and Shipper C. If Buyer B doesn’t receive the shipment by Date Z, the money in escrow will be returned. When this transaction is executed, Manufacturer G is notified to create another of the items that was sold to increase supply. All this is done automatically.

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 to a blockchain platform must determine how transactions and their data are represented, agree on the rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes. It’s usually an iterative process that involves both developers and business stakeholders.

What are the benefits of smart contracts?

The benefits of smart contracts go hand-in-hand with blockchain.

Speed and accuracy: Smart contracts are digital and automated, so you won’t have to spend time processing paperwork or reconciling and correcting the errors that are often written into documents that have been filled manually. Computer code is also more exact than the legalese that traditional contracts are written in.

Trust: Smart contracts automatically execute transactions following predetermined rules, and the encrypted records of those transactions are shared across participants. Thus, nobody has to question whether information has been altered for personal benefit.

Security: Blockchain transaction records are encrypted, and that makes them very hard to hack. Because each individual record is connected to previous and subsequent records on a distributed ledger, the whole chain would need to be altered to change a single record.

Savings: Smart contracts remove the need for intermediaries because participants can trust the visible data and the technology to properly execute the transaction. There is no need for an extra person to validate and verify the terms of an agreement because it is built into the code.

Exploring a blockchain application

Car companies make leasing a vehicle look easy, but in reality, it can be quite complicated. A significant challenge faced by today's car leasing networks is that even though the physical supply chain is usually integrated, the supporting systems are often fragmented. Each party within the network maintains its own ledger, which can take days or weeks to synchronize

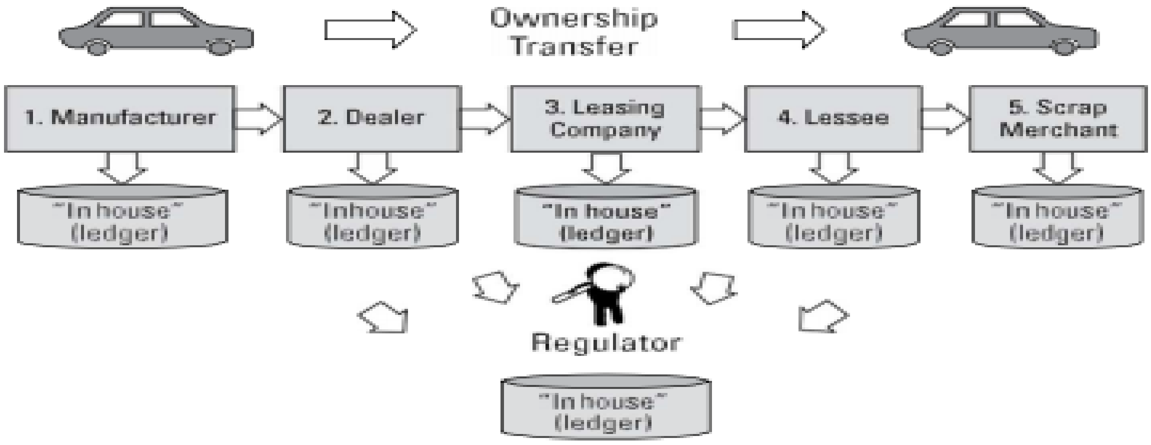


FIGURE 1-2: **Tracking vehicle ownership without blockchain.**

By using a shared ledger on a blockchain network, every participant can access, monitor, and analyze the state of the vehicle irrespective of where it is within its life cycle

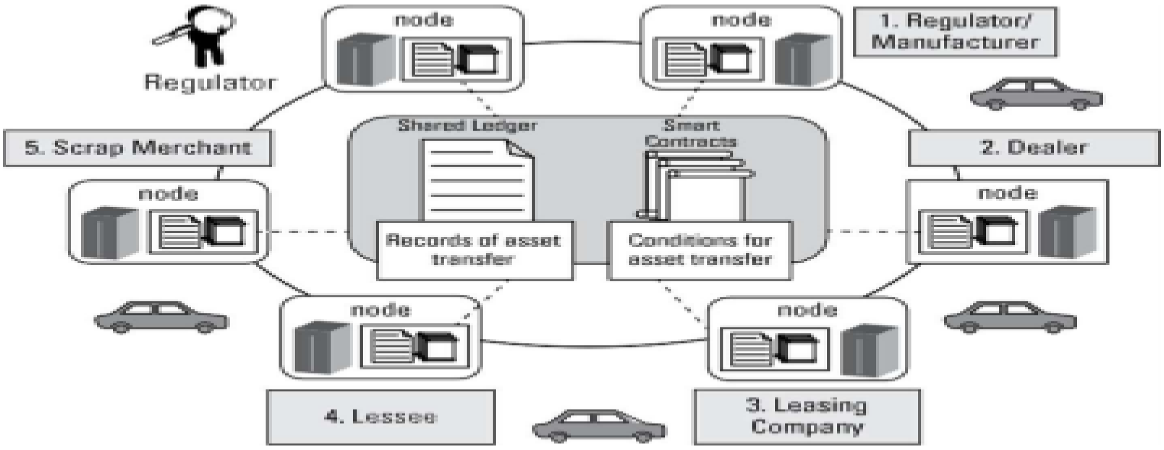


FIGURE 1-3: **Tracking vehicle ownership with blockchain.**

With blockchain, network participants can interact as follows:

With blockchain, network participants can interact as follows:

1. The government regulator creates and populates the registration for the new vehicle on the blockchain and transfers the ownership of the vehicle to the manufacturer.

2. The manufacturer adds the make, model, and vehicle identification number to the vehicle template within the parameters allowed by the smart contract (a digital agreement or set of rules that govern a transaction

3. The dealer can see the new stock availability, and ownership of the vehicle can be transferred from the manufacturer to the dealership after a smart contract is executed to validate the sale.

4. The leasing company can see the dealer's inventory. Ownership of the vehicle can be transferred from the dealer to the leasing company after a smart contract is executed to validate the transfer.

5. The lessee can see the cars available for lease and complete any form required to execute the lease agreement.

6. The leasing process continues between various lessees and the leasing company until the leasing company is ready to retire the vehicle. At this point, ownership of the asset is transferred to the scrap merchant, who, according to another smart contract, has permission to dispose of the vehicle.