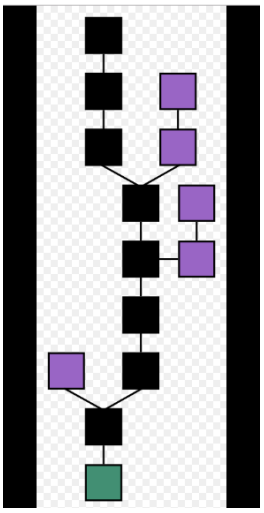
Blockchain database technology:

It is a growing list of records that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is 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 alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.



Blockchain formation. The main chain (black) consists of the longest series of blocks from the genesis block (green) to the current block. Orphan blocks (purple) exist outside of the main chain.

Blocks:

Blocks hold batches of valid transactions that are hashed and encoded into a hash tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.

Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher value can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of the history forever. Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Therefore, the probability of an entry becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low. For example, bitcoin uses a proof-of-work system, where the chain with the most cumulative proof-of-work is considered the valid one by the network. There are

a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

Decentralization:

By storing data across its peer-to-peer network, the blockchain eliminates a number of risks that come with data being held centrally. The decentralized blockchain may use ad-hoc message passing and distributed networking.

Peer-to-peer blockchain networks lack centralized points of vulnerability that computer crackers can exploit; likewise, it has no central point of failure. Blockchain security methods include the use of public-key cryptography. A *public key* (a long, random-looking string of numbers) is an address on the blockchain. Value tokens sent across the network are recorded as belonging to that address. A *private key* is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that blockchains now support. Data stored on the blockchain is generally considered incorruptible.

Every node in a decentralized system has a copy of the blockchain. Data quality is maintained by massive database replication and computational trust. No centralized "official" copy exists, and no user is "trusted" more than any other. Transactions are broadcast to the network using software. Messages are delivered on a best-effort basis. Mining nodes validate transactions, add them to the block they are building, and then broadcast the completed block to other nodes. [08] Blockchains use various time-stamping schemes, such as proof-of-work, to serialize changes. Alternative consensus methods include proof-of-stake. Growth of a decentralized blockchain is accompanied by the risk of centralization because the computer resources required to process larger amounts of data become more expensive.

How does a blockchain work?

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain.

Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

The reason why the blockchain has gained so much admiration is that:

- It is not owned by a single entity, hence it is decentralized
- The data is cryptographically stored inside
- The blockchain is immutable, so no one can tamper with the data that is inside the blockchain
- The blockchain is transparent so one can track the data if they want to

There are three pillars of blockchain

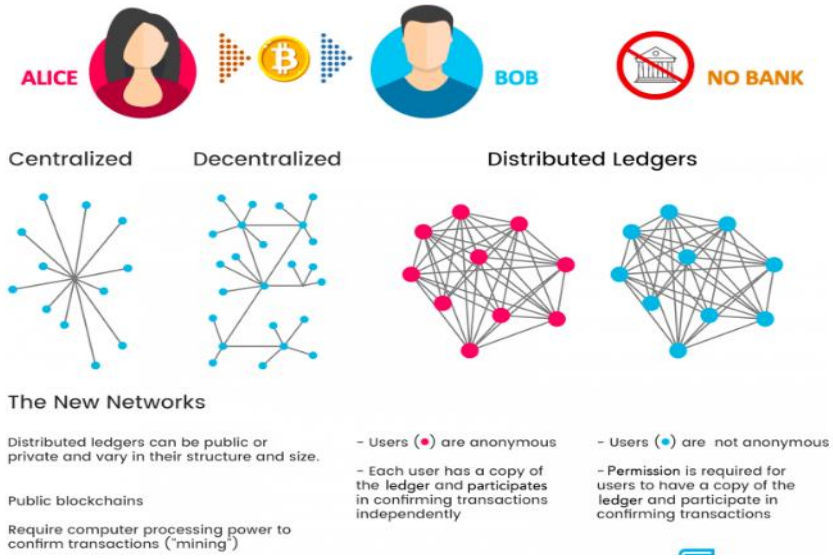
1.Decentralization

2.Transparency

3.Immutability

Decentralization:

Before Bitcoin and BitTorrent came along, we were more used to centralized services. The idea is very simple. You have a centralized entity which stored all the data and you'd have to interact solely with this entity to get whatever information you required.



Transparency:

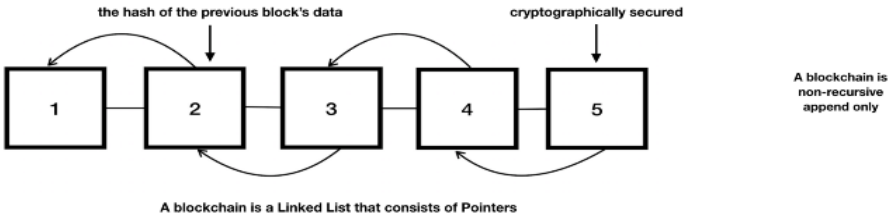
While the person's real identity is secure, you will still see all the transactions that were done by their public address. This level of transparency has never existed before within a financial system. It adds that extra, and much needed, level of accountability which is required by some of these biggest institutions.

Immutability:

Immutability, in the context of the blockchain, means that once something has been entered into the blockchain, it cannot be tampered with. Can you imagine how valuable this will be for financial institutes?

Imagine how many embezzlement cases can be nipped in the bud if people know that they can't "work the books" and fiddle around with company accounts. The reason why the blockchain gets this property is that of cryptographic hash function.

In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length. In the context of cryptocurrencies like bitcoin, the transactions are taken as an input and run through a hashing algorithm (bitcoin uses SHA-256) which gives an output of a fixed length. A blockchain stores information in uniform sized blocks. Each block contains the hashed information from the previous block to provide cryptographic security. The hashing uses SHA256 which is a one-way hash function. This hashed information is the data and digital signature from the previous block, and the hashes of previous blocks that goes all the way back to the very first block produced in the blockchain called a "genesis block". That information is run through a hash function that then points to the address of the next block. A blockchain data structure is an example of a Merkle Tree, which is used as an efficient way to verify data.



A blockchain design

Blockchain, for all its benefits, is missing the real-time analytics, native clustering, ACID transactional consistency, and the familiarity that comes along with NewSQL databases. When you can implement a NewSQL database as the support structure for blockchain, you can address the throughput, latency, and capacity concerns while also adding support for querying.

We've discussed NewSQL in the past, but it bears repeating that it balances the best of traditional operational databases with the scalability and speed of NoSQL databases. But to apply these benefits to blockchain use cases, you need the added SQL capability of recursive common table expressions (CTEs). With recursive CTEs, enterprises can establish the secure relationships within services while also meeting modern performance demands.