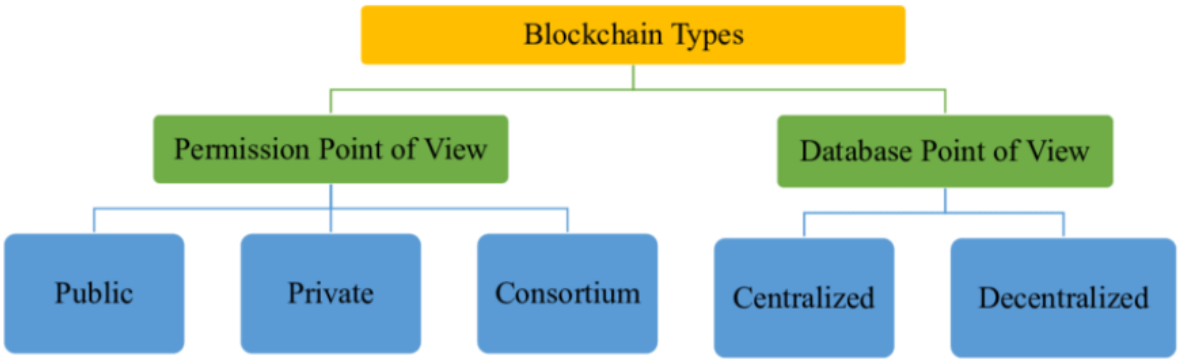
Types of Blockchain



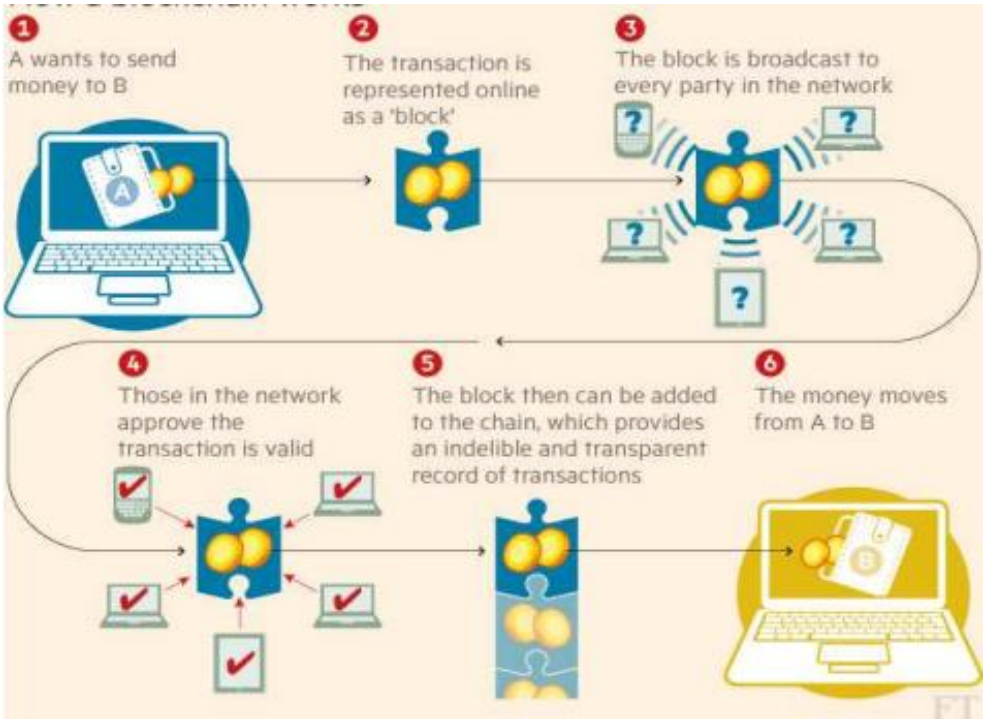
Use-case of Public Blockchain: Bitcoin

A Case Study on Bitcoin

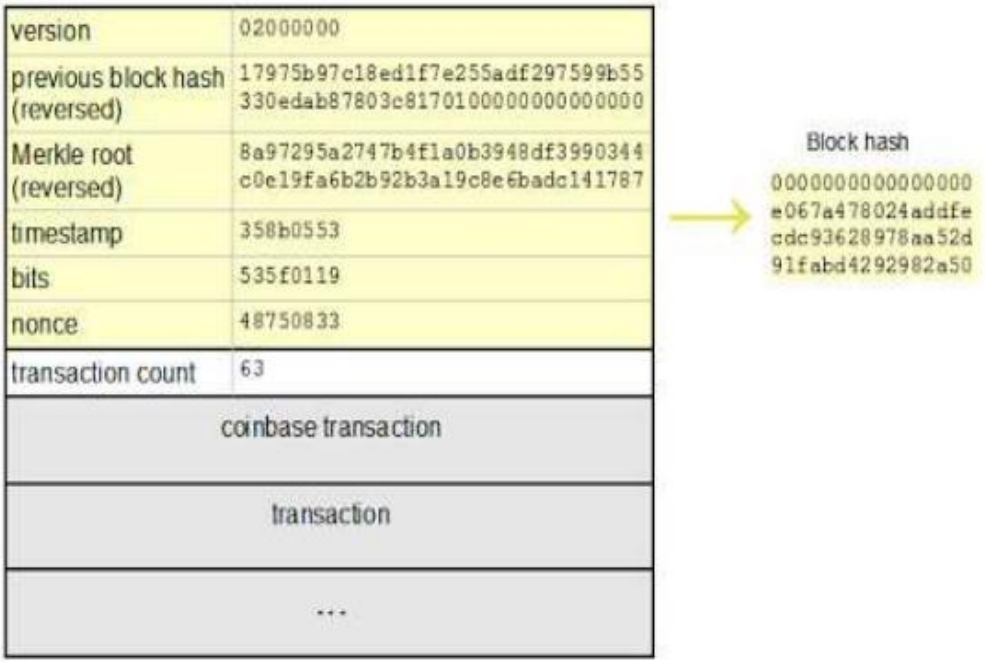
Introduction

Bitcoin (BTC) is a digital currency or cryptocurrency; this type of currency is used to distribute to others electronically. Bit coin is a decentralized peer-to-peer network. No single institution or person controls it. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through financial institution. Bitcoin was shaped by Satoshi Nakamoto, who published the invention and later it was implemented as open-source code. Bitcoin is a network practice that enables folks to transfer assets rights on account units called "bitcoins", created in limited quantity. When a person sends a few bitcoins to another individual, this information is broadcast to the peer-to-peer Bitcoin network. Bitcoins don't exist physically and are merely a sequence of virtual data. It can be exchanged for genuine money though, and are largely permissible in most countries around the world. There's no central authority for Bitcoins, similar to a central bank which controls currencies. Instead, programmers solve complex puzzles to endorse Bitcoin transactions and get Bitcoins as a reward. This activity is called Bitcoin mining, and with some knowledge of encoding codes and dollops of desire for capital, anybody can get cracking.

Bitcoin Blockchain Working

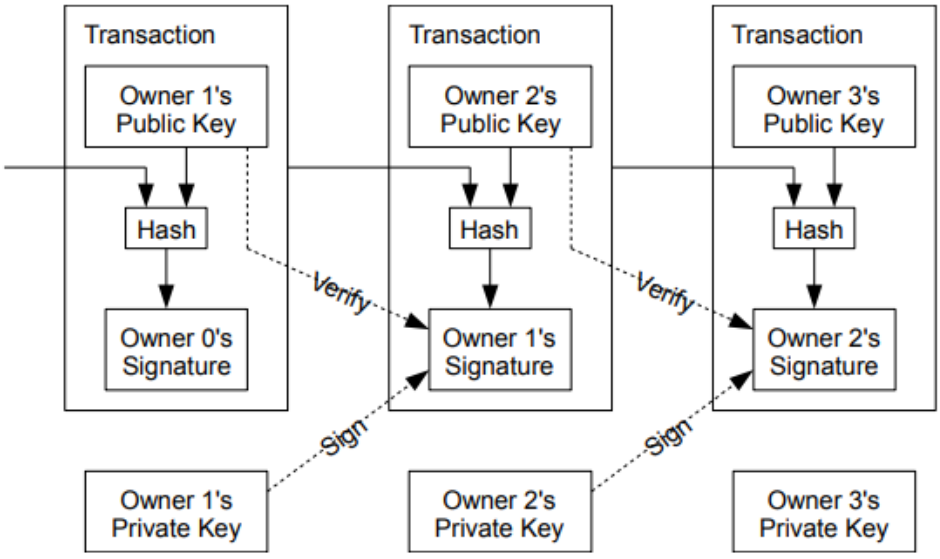


Mining requires a task that is very tricky to perform, but easy to verify. Bitcoin mining uses cryptography, with a hash function called double SHA-256. A hash takes a portion of data as input and shrinks it down into a smaller hash value (in this case 256 bits). With a cryptographic hash, there's no way to get a hash value you want without trying a whole lot of inputs. But once you find an input that gives the value you want, it's easy for anyone to authenticate the hash. Thus, cryptographic hashing becomes a good way to apply the Bitcoin "proof-of-work". In more detail, to mine a block, you first collect the new transactions into a block. Then you hash the block to form a 256-bit block hash value. If the hash starts with sufficient zeros, the block has been successfully mined and is sent into the Bitcoin network and the hash becomes the identifier for the block. Most of the time the hash isn't successful, so you alter the block to some extent and try again, over and over billions of times. About each 10 minutes somebody will successfully mine a block, and the procedure starts over. The fig below shows the structure of a precise block, and how it is hashed. The yellow part is the block header, and it is followed by the transactions that go into the block. The first transaction is the special coin base transaction that grants the mining reward to the miner. The remaining transactions are normal Bitcoin transactions moving bitcoins around. If the hash of the header starts with enough zeros, the block is successfully mined. For the block below, the hash is successful: 0000000000000000e067a478024addfecdc93628978aa52d91fabd4292982a50 and the block became block #286819 in the blockchain.



Bitcoin Transaction

A Bitcoin transaction is a signed section of data that is transmitted to the network and, if valid, ends up in a block in the blockchain. The idea of a Bitcoin transaction is to transfer ownership of an amount of Bitcoin to a Bitcoin address. When you send Bitcoin, a single data structure, namely a Bitcoin transaction, is created by your wallet client and then broadcast to the network. Bitcoin nodes on the network will communicate and rebroadcast the transaction, and if the operation is valid, nodes will include it in the block they are mining. Usually, within 10-20 mins, the transaction will be included, along with other transactions, in a block in the blockchain. At this position the receiver is able to see the transaction amount in their wallet.

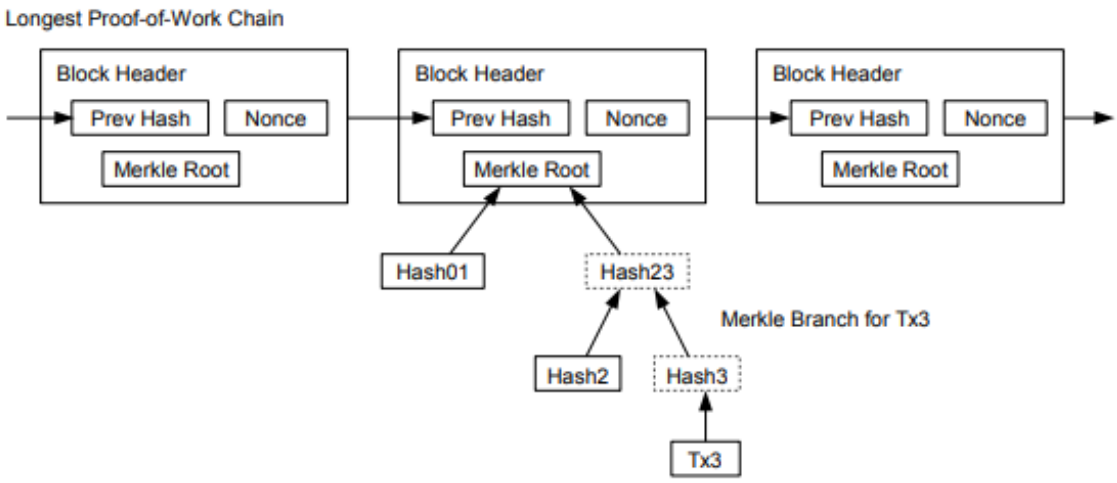


Four obvious truths about transactions:

1. Bitcoin amount that we send is always sent to an address.
2. Bitcoin amount we receive is locked to the receiving address – which is connected with our wallet.
3. Every time we spend Bitcoin, the amount we spend will always come from funds earlier received and currently present in our wallet.
4. Addresses receive Bitcoin, but they do not send Bitcoin – Bitcoin is sent from a wallet.

Payment Verification

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced, he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



Advantages:

- Accessibility and liquidity
- User anonymity and transparency
- Independence from a central authority
- High return potential

Disadvantages:

- Volatility
- No government regulations
- Irreversible
- Limited use

Conclusion

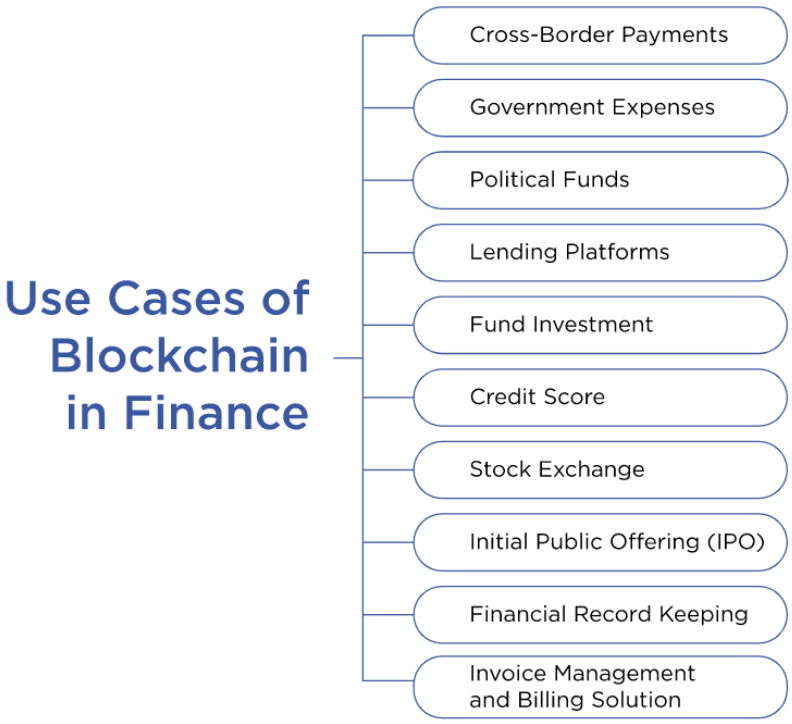
Bitcoin is the foremost broadly popular cryptocurrency with a big user base and a wealthy network, all hinging on the incentives in place to retain the important Bitcoin blockchain. Bitcoin is a latest Internet currency that anybody can get started pulling out. Currently 90% of blocks are mined by known pools or syndicates of miners, and if a little pool joins together, they could cause changes and affirm control over the network.

Future scope

The market of cryptocurrencies is fast and wild. Nearly every day new crypto currencies emerge, old die, early adopters get wealthy and investors lose money. Every cryptocurrency comes with a promise, mostly a big story to turn the world around. The most widely used crypto currency is bit coin and their working smoothly for business, a large scope for marketing so using high secured transactions without interruptions of third party.

Use case of Private Blockchain: Financial services

The utilization of blockchain technology in the financial service sector has long been lauded for its impeccable capability to introduce, transparency, time efficiency, and productivity to the ecosystem Simply put, blockchain helps reduce the chances of data breaches as well as operational risks.



Advantages:

- Improving Transparency
- Simplifying Operations
- Quicker Settlement
- Smart Contracts Enabling Automation
- Improving Customer Experience

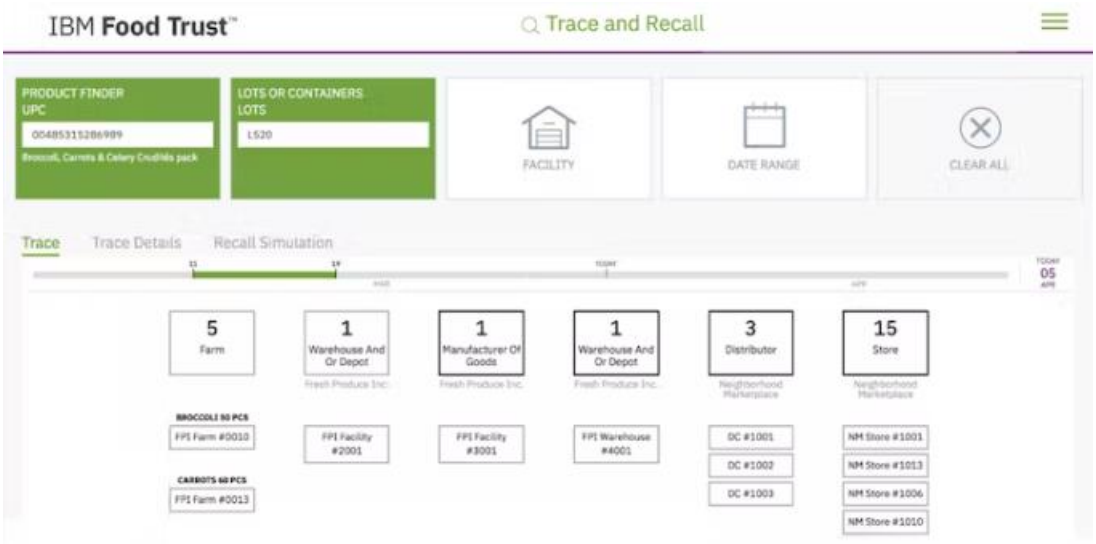
Disadvantages:

- Relatively New
- Differing Methodology
- Lack of Interoperability
- Affordability
- Poor Adoption

Conclusion

Blockchain technology and its use in the financial services sector are still relatively nascent. In the future, we expect two significant developments – interoperability and improvements in transaction processing. These improvements will make the technology more useful for financial institutions.

Use case of Consortium Blockchain: Pharmaceuticals & food tracking



In terms of food traceability, IBM Food Trust is the leading example. IBM has created an ecosystem of producers, manufacturers, retailers, suppliers, and others working together in food supply chain process with the aim of increasing safety, transparency. There are currently 50 brands across the IBM Food Trust network.

Walmart is one of the leading participants. A player in the food ecosystem can apply to become a trusted provider in the Food Trust system through APIs for data upload and integration with your ERP system.

IBM FOOD Trust creates a digital ledger that tracks food from the farm to processing facilities, to distributors and grocery shelves. One of the rationales for this is to trace bacteria outbreaks quickly before they spread. The current tracing is paper-based and takes weeks. With blockchain, scanning product is easy and can trace back to the source with the precision of seconds instead of weeks, according to Vice President of Food at Walmart. At the farm, the information is captured on a handheld system as well at the packing house. With a permissioned blockchain, different players come together as validators hence increasing transparency and efficiency. No one party can change the information without notifying the others. Traceability is also highly enhanced.

Advantages:

- Ensure traceability and hence food safety in terms of detecting bacteria such as E.coli
- Ensuring higher quality ingredients
- To enable compliance with different food standards
- Reducing food waste

- Providing transparency to consumers by showing products are authentic. (This is becoming key competitive point as customers now want more transparency in sourcing).

Disadvantages:

- The group of people in authority might face coordination issues among themselves.
- It becomes evident that not all the members of this group would have access to the same amount of computing power to equally manage the network.
- Added to this, internal conflicts can pose a greater risk to the integrity of the network.

Conclusion

It seems most of the blockchain use case for industries is optimizing for shared databases to improve visibility, tracking, auditing in certain aspects of business operations. In banking finance, it is to improve interoperability between banks and payment companies, in shipping, it is for improving visibility and tracking, the same case for food and most of the other supply chain-based operations. With big players such as IBM, Microsoft, Walmart experimenting with aspects of shared databases in one way or another, it is only a matter of time before industry-wide applications become mainstream.