ROHINI COLLEGE OF ENGINEERING AND TECHNOLOGY

Kanyakumari Main Road, near Anjugramam, Palkulam, Anjugramam, Tamil Nadu 629401

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ADD ON COURSE

VIRTUAL CURRENCY & BLOCK CHAIN TECHNOLOGY

COURSE MATERIAL

VIRTUAL CURRENCY & BLOCK CHAIN TECHNOLOGY

A type of digital currency present in electronic form is generally referred to as Virtual currency. These electronic currencies are stored and transacted through digital wallets using Internet. For this purpose, certain computer or mobile software are available in the market. Virtual currencies are a subset of the digital currency group. Cryptocurrencies are one type of it.

According to Bitcoins news, the term virtual currency came into existence around 2012, when the European Central Bank (ECB) defined it as "a way to classify digital money types in an unregulated environment which are issued and controlled by its developers and used as a payment method among members of a specific virtual community".

Virtual currencies are issued, managed and controlled by private issuers, developers, or the funding organization. These are often regarded as tokens and may be regulated during a legal tender for trust issues. The money is not issued by central bank or other banking regulatory authority unlike regular money. These are prone to fluctuations in their monetary value due to the lack of a centralized regulatory authority. The value is derived based on certain mechanisms such as mining in Cryptocurrencies, or the backing by the underlying asset.

Virtual currency can restrict its usage apart from public users. This can be done by circulating it among a particular online community or group members by carrying out their transactions through dedicated online networks virtually. Mostly, Virtual currencies are used in peer-to-peer payments and are found to be increasingly popular in goods and service purchases.

Digital currency covers a wide group representing monetary assets in digital form in comparison with virtual currency. Virtual currency or virtual money is a type of unregulated, digital money which is issued and controlled by its developers that are accepted and used among the members of a specific virtual community. Cryptocurrencies are those which use secured cryptographic techniques for authentic transactions, and for managing and controlling the creation of new currency units.

Digital currency is the overall superset that includes virtual currency and cryptocurrencies. A Digital currency may be regulated or unregulated and can be denominated to a sovereign currency, whereas Virtual currencies are often unregulated. Digital currencies are issued by a country's central bank as flat currency notes, but virtual currencies are subsets of digital currencies.

Bitcoin and Ethereum are Cryptocurrencies which are subsets of the virtual currency group.

Such cryptocurrencies do exist where transactions are carried out in an open common public network by means of dedicated block chain.

This means that anyone can join and carry out transactions in cryptocurrencies. The relationship between digital, virtual and crypto currencies can be depicted in figure

Virtual currencies can be implemented in various forms depending upon platforms such as social networks, social games, loyalty points and peer to peer networks. Generally, there are two categories of Virtual Currency platforms. They are

- Centralized virtual currency platforms and
- Decentralized virtual currency platforms.

A Virtual Currency system that resembles to the central bank in terms of central repository is known as the centralized virtual currency platform. The transferring of virtual currency takes place between individuals from one location to other location are monitored and maintained by that particular repository administrator. In contrast, a Virtual Currency system that does not possess a centralized repository with no single administrator is referred to as the decentralized virtual currency platform. It can be obtained through a manufacturing or a computing process.

he centralized and de-centralized platforms are used by various businesses which may include some of the methods explained in the following section. Figure shows the different methods used in virtual currency.

1 Obtaining and Generating Virtual Currency

In the digital medium, there are several different ways and methods to obtain or generate the virtual currencies. Some of the common methods followed are defined below:

- Pay for virtual currency method
- Offer based method Loyalty based method
- Self-effort-based method

This method is used to pay real money or its equivalent monetary in place of virtual currency.

i. Pay for virtual currency method

It may include pre-paid cards, credit cards or any e-payment systems such as PayPal. This method

is prominent in adult gaming and users. Only users above 18+ are permitted to use this method. The amount of money purchased has its own complement price and exchange rate based on the type of virtual currency platform. The purchased virtual currency in this method is stored in buyer's account which is created within the platforms by the operators.

- Offer based method Loyalty based method

These are one of the safest forms of earning virtual currencies. When users are unable to spend real money for virtual currencies, they choose this offer- based method. This permits users of minor and major ages to gain virtual currency though some forms. It may include survey answering, watching advertisement videos, registering for a trial subscription of products or services or winning maximum level in a game. In order to gain virtual currencies on gaming or other platforms, the users must complete publicizing it.

iii. Loyalty based method

This method is based on the loyalty of the customer towards any commercial companies or games. They are rewarded with vouchers, gifts and discounts for their loyalty. These rewards can also take the form of credit points during every purchase of goods or services. These points are redeemable and can be used in exchange of virtual currency for future purchases. Users can make use of these loyalty points in terms of virtual currency.

iv. Self-effort-based method

Decentralized virtual currency platforms say Bitcoin makes use of self-effort-based methods to generate peer-to-peer network's virtual currency. Bitcoins are usually generated in peer networks and so they are fixed, immutable and have only finite generation of virtual coins. This makes them different from centralized virtual currency platforms. Computer systems possess special software that produces virtual currencies by solving complex mathematical puzzles which are generated as a slower process and are distributed to the network and system users in a random manner. These virtual coins are fully controlled and managed by users and can be stored locally in user devices such as digital wallets.

2 Spending and Exchanging Virtual Currency

Spending and exchanging virtual currency can be divided into two main categories namely,

- Exchanging virtual currency for virtual items within the virtual environment and

- Exchanging virtual currency for real items.

Both these categories face many challenges and issues. It is prominent in the second category.

i. Exchanging Virtual Currency for Virtual items

Many online games and social networks are increasingly becoming popular for exchange of virtual currency for virtual items. Games provide an interactive environment for gamers by providing options of changing the look of the characters. For this the user has to purchase virtual items using virtual currencies earned through completing levels. At times, they may also require purchasing successive game levels using virtual currencies. For example, Bitcoins are used as the virtual currencies for buying virtual items.

ii. Exchanging Virtual Currency for Real items

Exchanging virtual currency for real items may include money, goods and services which are explained below,

- Virtual currency to real money
- Virtual currency to real goods
- Virtual currency to services

- **Virtual currency to real money** – Here the VC can be exchanged for real cash. For this purpose, the user needs a connection between the businesses and the real money systems for exchanging virtual currency for real cash. The exchanging rate is set up to control the financial exchanging. Bitcoin is an example of the virtual currency that can be exchanged for real cash. Many online markets with the help of exchange rate are used for exchanging Bitcoins and real money.
- **Virtual currency to real goods** – In this form, user uses virtual currency for buying real goods such as clothes, sunglasses and many more products. These products are bought using virtual currencies earned through game platforms. For example, VEN currency can be exchanged for real goods and commodities like clothes, accessories and Precious metals.
- **Virtual currency to services** – In this form, the exchange for virtual currency is with the services. For example, Gamers or users earn points through games and other applications to buy services such as free messages and calling.

5 Types of Virtual Currency

There are three major types of virtual currencies namely,

- Convertible currency
- Closed currency
- Peer-to-Peer currency

Figure 3 shows the three types of Virtual Currency.

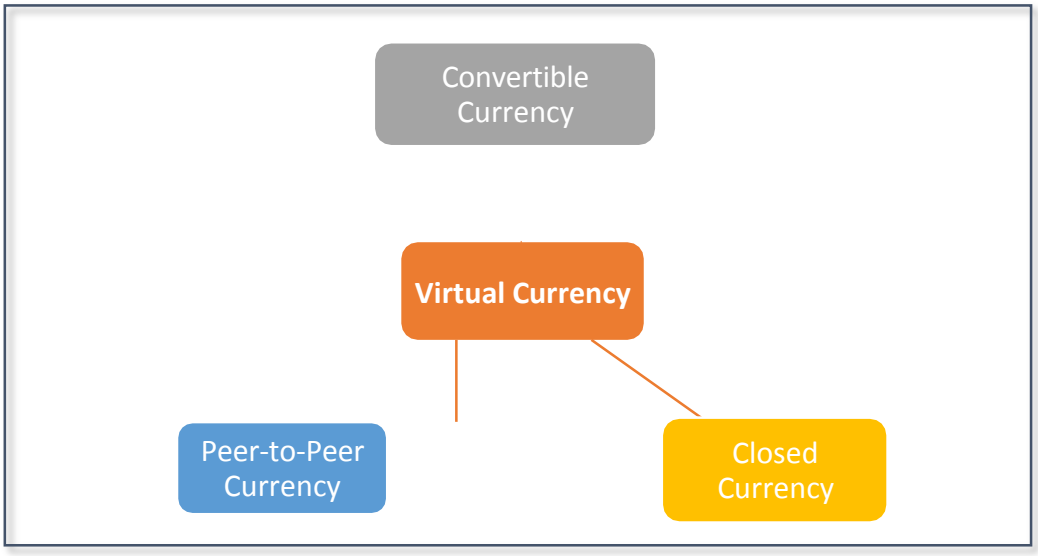


Figure Three Types of Virtual Currency

5.1 Convertible Virtual Currency

Convertible virtual currency is an unregulated digital currency that can be used as a substitute for real and legally recognized currency. It usually has a measurable value in real money, but what makes it convertible lies in its ability to be exchangeable. Not all virtual currencies can be exchanged for legal transactions. Convertible virtual currency is also called as Open Virtual Currency.

5.2 Closed Virtual Currency

Closed virtual currency is an unregulated digital currency that is used only within certain virtual communities. It has no connection to the real economy and cannot be converted to legal

5.3 Peer-To-Peer Virtual Currency

tender. Closed virtual currency is also called non-convertible virtual currency, closed loop currency, closed-flow virtual currency and in-world money.

The exchange or sharing of information, data, or assets between parties without the involvement of a central authority is called as Peer-to-Peer (P2P). P2P virtual currency takes a decentralized approach to interactions between individuals and groups. This approach has been used in computers and networking (peer-to-peer file sharing), as well as with virtual currency trading.

Exchange and Bitcoin ATM's (available in few countries only) are the modes of exchange for convertible currency. Closed currency exists only in virtual communities and has no link to real economy. Virtual communities are mostly online gaming platforms. Some of the most renowned platforms such as World of Warcraft, EVE online, second life is virtual communities. Peer-to-Peer currency involves direct transfer with the involvement of a third party. Therefore, it is an independent entity.

Currently, other virtual currencies such as Peercoin are also flowing in the market. Most of them are cryptocurrencies. Bitcoin has been the most successful virtual currency so far. It is the most popular currency for market capitalization holding 90% of the total market. Litecoin, Dogecoin, Primecoin and Peercoin are some of the other virtual currencies in the virtual community.

6 Challenges and Issues in Virtual Currency

Virtual currencies often face many issues and challenges with respect to security in financial concerns. Some of the major issues and their effects are as follows:

- Security threats
- Collapse concerns in virtual currency systems
- Impact on real monetary systems
- Gold farming risks
- Fluctuation in virtual currency value
- Money laundering
- Unknown identity risks
- Black market for virtual currency

Figure 4 shows the various challenges and issues in virtual currency.

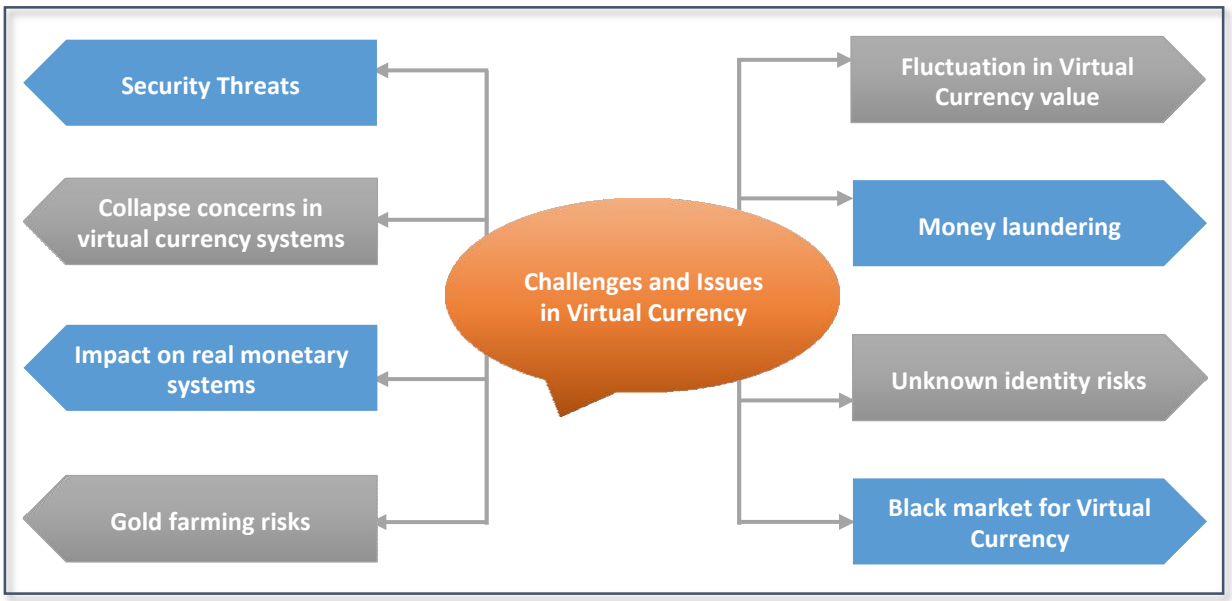


Figure Various Challenges and Issues in Virtual Currency

6.1 Security threats

Knowing the process of creating and generating virtual currencies, hackers and other illegal users can easily break into user systems. Hackers modify genuine user accounts to steal virtual currencies. They also create fake virtual currencies to fraud the legitimate users. For example, selling in-game virtual items and virtual currency are against World of Warcraft (WoW) game policies. Hence, to earn virtual gold by exchanging virtual currencies for what they need, users log into this WoW gold selling websites. Most of these websites are prone to security issues and vulnerable to threats where users complain about exchanging virtual currencies for real money.

6.2 Collapse concerns in Virtual Currency Systems

Some economic problems arise due to unlimited usage of virtual currency in communities and organizations. These issues are not dependent on the demand and supply of goods and products. For the purpose of gaining larger real revenues for virtual

items, unlimited issue of Linden Dollars were carried out which led to the downfall of virtual currency system and other economic issues.

6.3 Impact on real monetary systems

The demands and supply of the real monetary systems get affected due to several virtual currency system platforms. This can be minimized by allowing users for purchasing real goods and services. Virtual money can be used for purchasing instead of real money. Some virtual currency platforms allow users in exchanging virtual currencies for real money increasing the demand. This fluctuation affects the real monetary systems.

6.4 Gold farming risks

Gold farming is prominent in China and other developing countries. Here the gamers play games like WoW for earning gold as virtual currency which can then be exchanged with real monetary system. Gaining of virtual currency becomes a competition for targeted users where frequent users use some practices to trick them knowing their time limitation involved in playing. The flow of huge cash are not controlled and regulated in gold farming. During exchange of virtual currency with real money there arise many fraudulent and financial risks.

6.5 Fluctuation in virtual currency value

The value of virtual currency is devalued with the decrease in the popularity of the virtual community. For instance, users owning 1000 units of virtual currency can usually buy 100 different items. If there is a downfall in the virtual currency, then the purchase of 100 items also downfalls to 10 items. This normally takes place in a closed virtual community consisting of few goods and services.

6.6 Money laundering

During exchange of virtual currency with real money there arises an issue of money laundering since virtual currencies can be laundered during exchanges. For example, money laundering case that happened in Korea during 2008 where criminal s were arrested for selling virtual currency by converting $38 million. The money was generated through gold farming methods as an exchange of currency.

6.7 Unknown identity risks

Most of the financial online transactions become unmonitored due to unauthorized accounts created in social media and gaming. Many unknown identities are created during illegal transactions as users create and use more than one account with real as well as unreal details. This paves way to identify the creation and transaction of virtual currencies source. In addition, the tracking of money laundering or suspicious transactions becomes difficult. Due to the unknown identities the criminals has an easy way to pay for their illegal activities with virtual currencies.

6.8 Black market for virtual currency

The black markets are usually created with the activity of buying and selling virtual currencies mostly in social games. The increase in the popularity of virtual currency paves to the growing of black markets during trading process. This can be monitored for occurrence of fraud cases in online games. For example, a gamer quitting the game must sell or offer the virtual currency earned during playing levels in the game forum. The existence of malicious users is high due to incomplete transactions or variance after paying. As a result, they are returned with virtual currency and money invested.

2 Blockchain Technology

A blockchain is a decentralized, distributed database that is used to maintain a continuously growing list of records, known as the blocks. Each block contains a timestamp and is linked to the previous block by means of a hash pointer. Blockchains are inherently resistant to data modification by design and purpose. Functionally, a blockchain serves as an open, distributed ledger capable of recording transactions that takes place between two parties efficiently and effectively.

A blockchain is a chain of blocks which contains specific information (database) that is grouped together in a secure and genuine 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. The blockchain technique allows digital information to be distributed, rather than copied. This distributed ledger provides transparency, trust, and data security. The figure 5 displays the different forms of blockchains such as centralized, de-centralized and distributed.

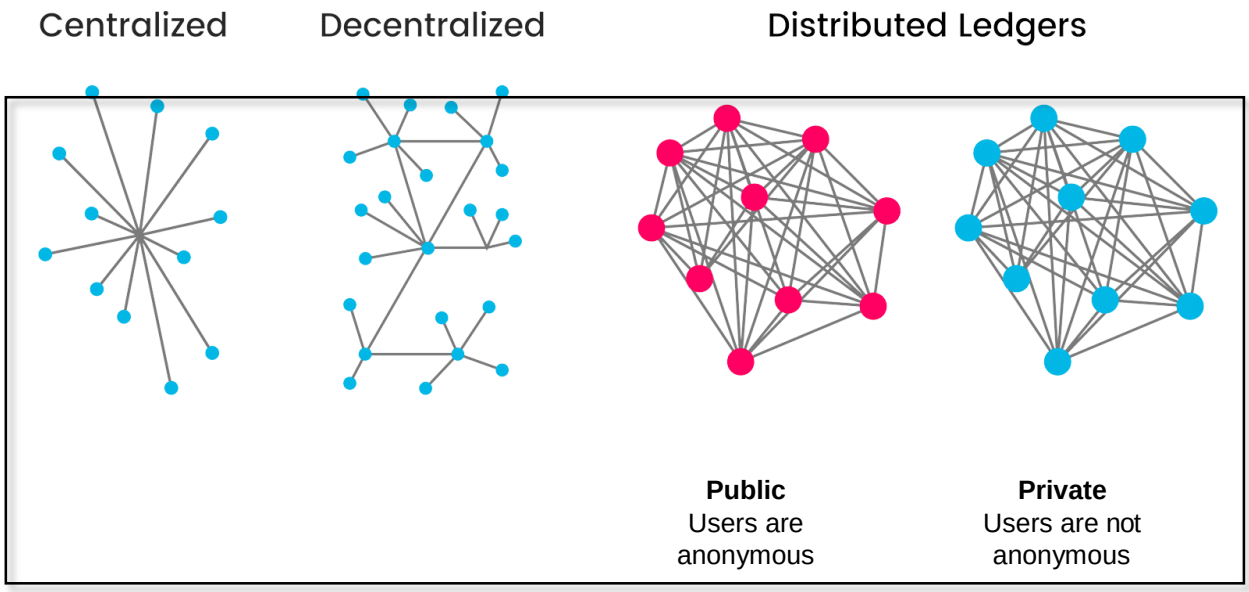


Figure Different forms of Blockchain Technology

1 History of Blockchain

The first concept of digital currency was developed and conceptualized relying on central server architecture, the function was to avoid double-spending. This concept still was failing to have unity of double-spending avoidance, anonymity and centralization. There were a few more concepts introduced during 1990's. In 1991, a research on cryptographically secured chain of blocks was conducted by Haber and Stornetta. There was a publication by Anderson in 1996, and in 1997 by Doyle. During 1990's, Szabo was developing a mechanism for a decentralized digital currency which was named as bit gold.

More than 10 years later, the Bitcoin cryptocurrency was introduced. The initial Bitcoin technology was based on decentralized system which had evolved using Chaum's concept. Today, the concept of Blockchain is widely spread, while there are opposite opinions about the technology. In Satoshi Nakamato's (2008) whitepaper, the nouns "block" and "chain" were used separately and later the technology was named as block chain. During 2016 the concept was merged into one word – "Blockchain".

There have been five major Blockchain-based inventions during the last ten years.

- The first major Blockchain-based innovation was Bitcoin, which is a digital currency. Bitcoin is used by millions of people for online and secure payments, also including the banking sector.
- The second invention was the Blockchain itself. Despite of being the hidden technology it allowed Bitcoin to be separated from the currency and used for all types of cooperation.

- The third innovation was named as a “smart contract” also called as Ethereum. The Ethereum platform provided few developments of small programs directly into Blockchain.
- The fourth major innovation, the most innovative part of the Blockchain thinking, is “proof of stake.” The actual generation of Blockchains is secured by “proof of work” where decisions are made by a group with the largest amount of computing power. These groups are known as “miners” and they control huge data centres to ensure security, by having cryptocurrency payments. Proof of stake systems remove these data centres, and replace them with complex financial tools, with similar or higher- level security.
- The fifth major innovation is Blockchain scaling. At present, in the Blockchain, each member in the network processes every transaction that is really slow. With the use of the scaled Blockchain, there is a possibility to speed up the process without security threats.

2 Blockchain Architecture

Blockchain architecture is popularly used in the financial industry. During these days, this technology is not only employed for cryptocurrencies, but also for keeping records, digital notary, and smart contracts.

1 Technical architecture and a high-level view of Blockchain

In general, a blockchain system consists of a number of **nodes**, each of which has a local copy of a **ledger**. In most systems, the nodes belong to different organizations. The nodes communicate with each other in order to gain agreement on the contents of the ledger and do not require a central authority to coordinate and validate transactions.

The process of gaining this agreement is called consensus, and there are a number of different algorithms that have been developed for this purpose. Users send transaction requests to the blockchain in order to perform the operations the chain is designed to provide. Once the transaction is completed, the record of the transaction is added to one or more of the ledgers and can never be altered or removed. This property of the blockchain is called **immutability**. The figure 6 shows the technical architecture of Blockchain.

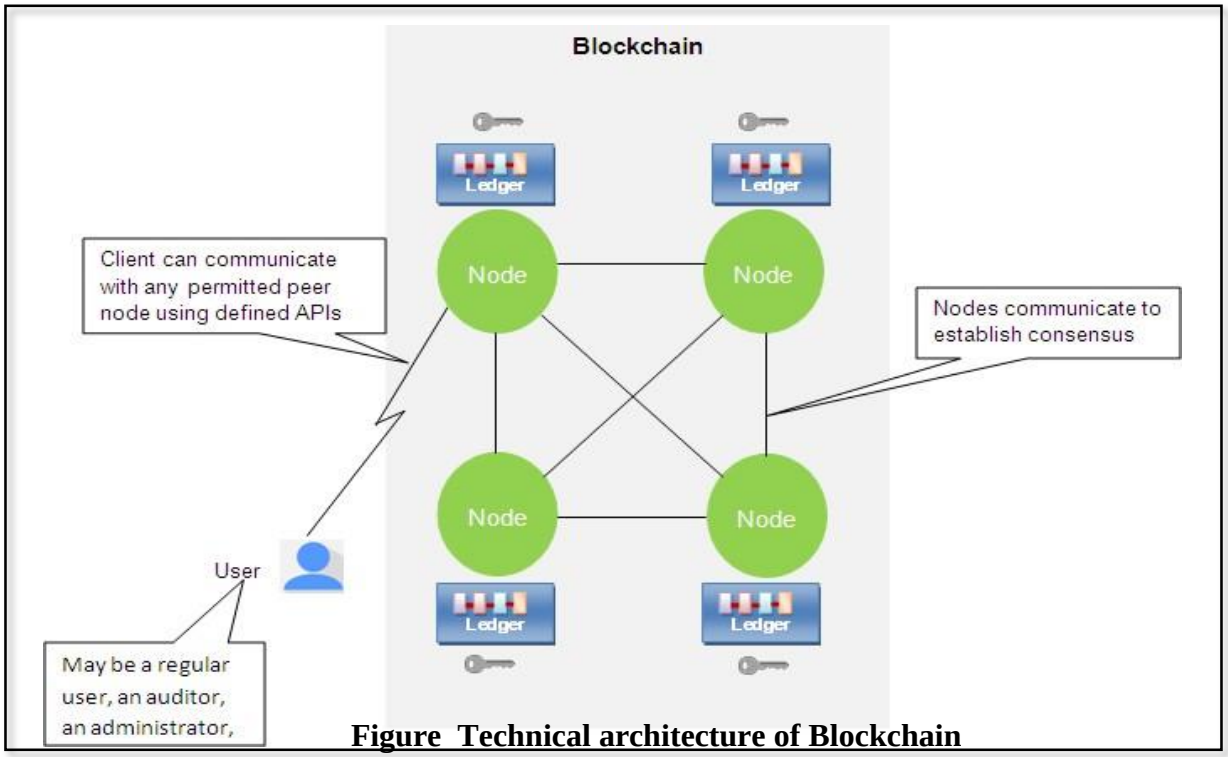


Figure Technical architecture of Blockchain

2 Core Components of Blockchain Architecture and Its Working

Following are the core components of block chain architecture:

- Node
- Transaction
- Block
- Chain
- Miners
- Consensus

These are displayed in figure.

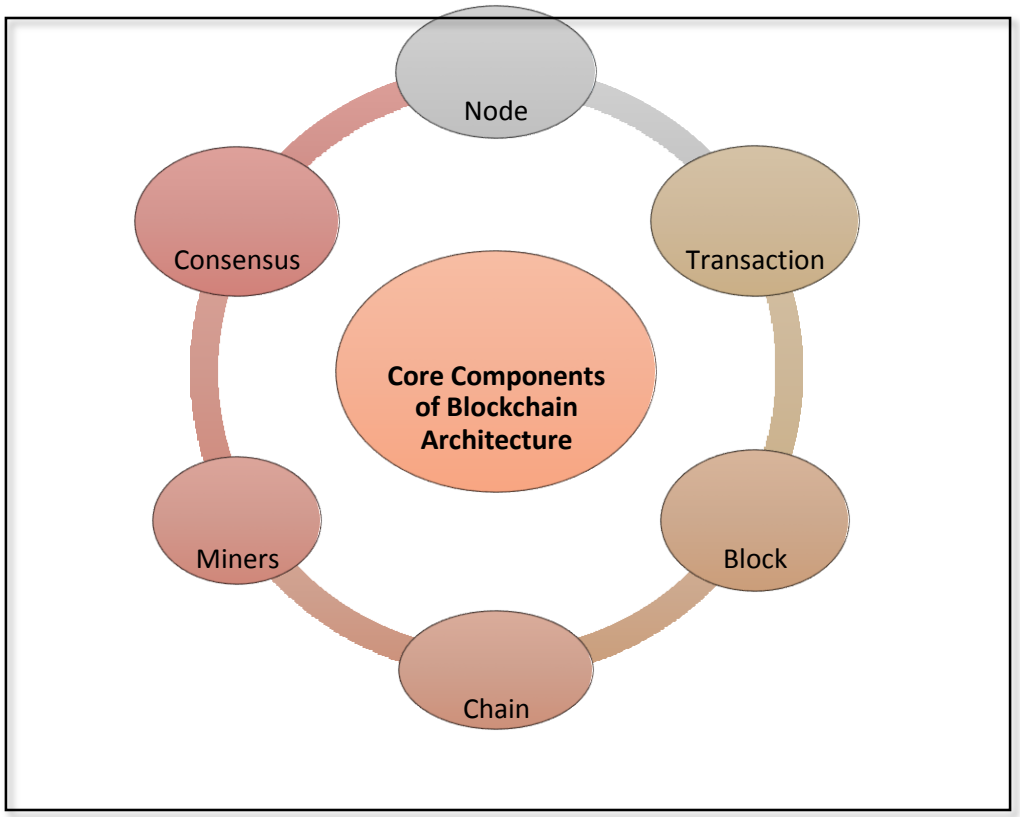


Figure Core Components of Blockchain Architecture

- **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 the 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 figure 8 displays the transaction process of blockchain.

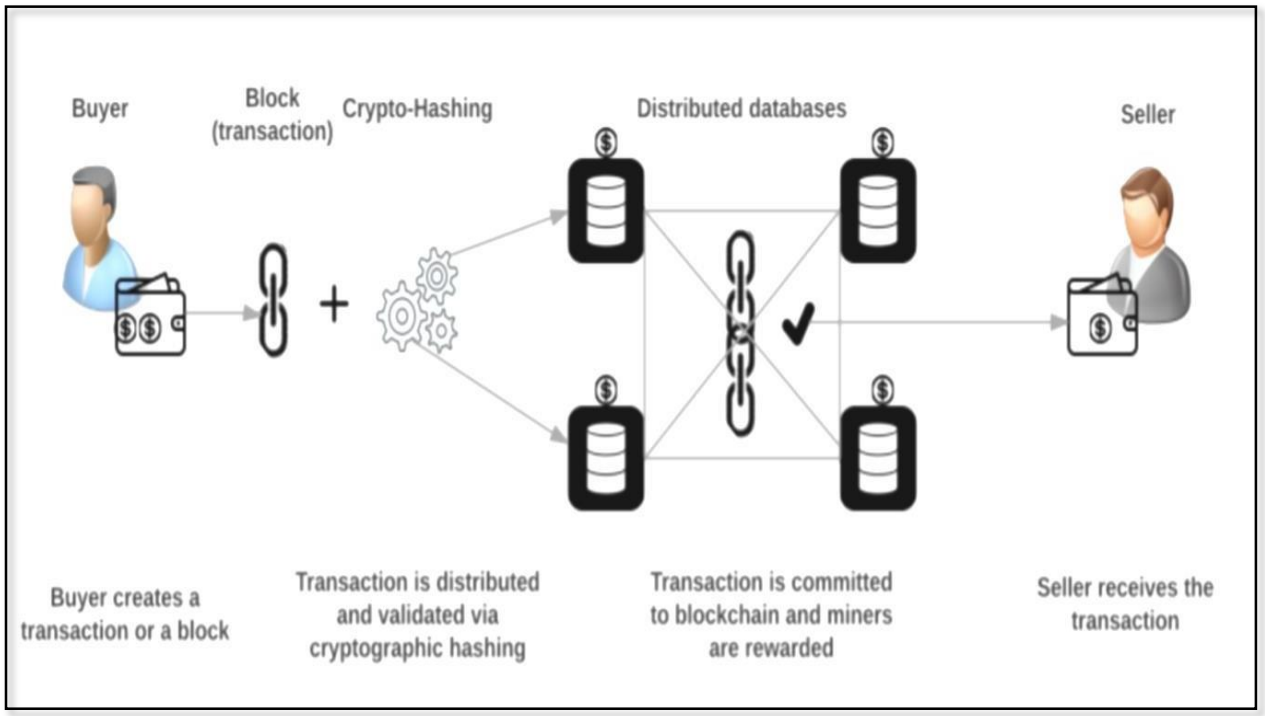
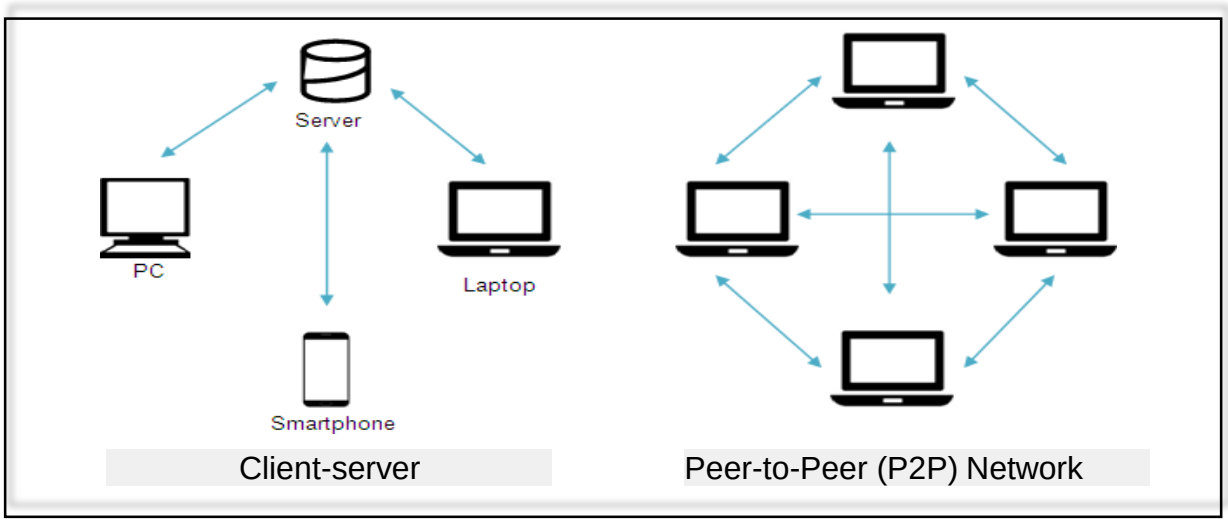


Figure Blockchain Transaction Process

3 Database Vs. Blockchain Architecture

The traditional architecture of the World Wide Web uses the client-server paradigm. In this case, the server keeps all the required information in one place so that it is easy to update. Server being a centralized database, it is 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. The figure 9 shows the connection between the nodes in client-server network and peer-to-peer network.



In summary, block chain is a decentralized, distributed ledger (public or private) of different kinds of transactions with a P2P network. This network consists of many computers, but the data cannot be altered without the consensus of the whole network, in other words 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.

Figure 10 displays the sequence of records connected using pointers.

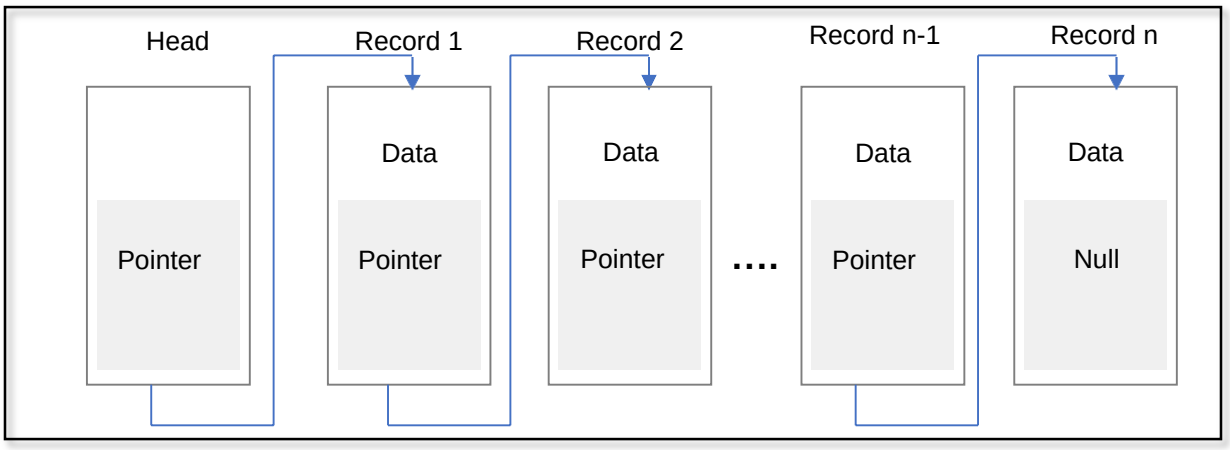


Figure Sequence of records connected using pointers

Logically, the first block does not contain the pointer since it is the first in the chain. At the same time, there is potentially a final block within the blockchain database that has a pointer with no value. The figure 11 depicts the blockchain sequence connecting list of records using linked lists.

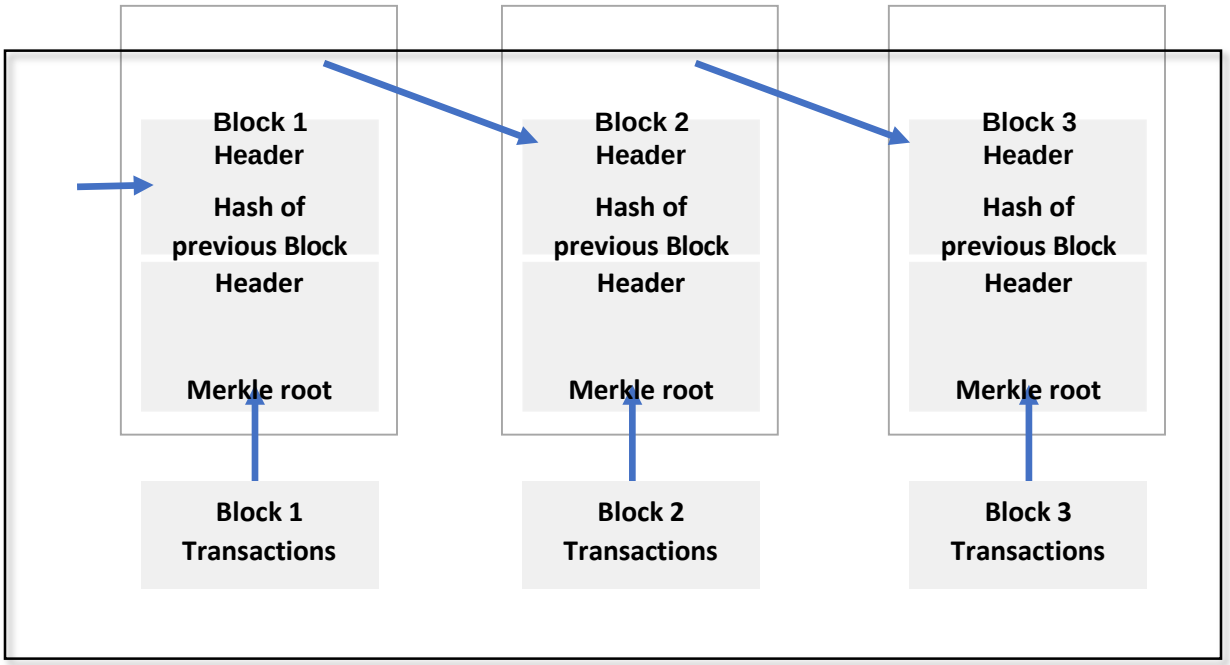


Figure Blockchain sequence connecting list of records using linked lists

4 Updations in the Structure of Blockchain

Blockchain is a technology which consists of sequence of blocks, which holds a complete list of transaction records like conventional public ledger. The first block of a blockchain is called genesis block which has no parent block. A block consists of the block header and the block body with the following fields:

- Block version
- Merkle tree root hash
- Timestamp
- nBits
- Nonce
- Parent block hash

o **Block version –** indicates which set of block validation rules to follow

o **Merkle tree root hash –** the hash value of all the transactions in the block.

- **Timestamp –** current time as seconds in universal time since January 1, 1970.
- **nBits –** target threshold of a valid block hash.
- **Nonce –** a 4-byte field, which usually starts with 0 and increases for every hash calculation.
- **Parent block hash –** a 256-bit hash value that points to the previous block.

Blocks are chained together with each block containing the hash of the previous block's header, thus forming the block chain. If a previously published block were changed, it would have a different hash. This in turn would cause all subsequent blocks to also have different hashes since they include the hash of the previous block. This makes it possible to easily detect and reject altered blocks.

Each block contains a complex mathematical equation or hash functions, to prone the integrity and non-repudiation of its data. Each member of the network has a copy of the Blockchain database, and the computers are synchronized frequently to make sure that all of them have the original and correct version of the shared database.

The copy of Blockchain consists of all transactions happened in the currency. Thus, any node of the network can discover a balance of each address at any timeframe. In case, when the block is mined, and a few others are created just in several seconds apart, the nodes build onto the block they received first. The first mined block will be included as a part of the main chain, because the chain will be the longest at that moment. However, from the initial block, there might be several chains or forks. Blockchain works by validating transactions through a distributed network in order to create a permanent, verified and unalterable ledger of information.

5 Advantages of Blockchain 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 and secure from cybercrimes 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 an ever-growing archive, while a centralized database is more of a snapshot of information at a specific point.

- **Data Validity and 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 a compound processing power. This means that the system sacrifices performance speed, instead it guarantees high data security and validity.

3 Key Characteristics of Blockchain

1 Decentralization

In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.

2 Persistency

Transactions can be validated quickly, and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.

3 Anonymity

Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. However, blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint.

4 Auditability

Bitcoin blockchain stores data about user balances based on the Unspent Transaction Output (UTXO) model. Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switch from unspent to spent. So, transactions could easily be verified and tracked.

5 Digital

All the information on blockchain is digitized, eliminating the need of manual documentation.

6 Distributed

Transactions are grouped into blocks for processing and standard network protocol used ensures that every node receives every transaction in near real-time and applies the same rules. Blockchain is designed to be distribute and synchronized across the networks, which makes it ideal for multi-organizational business networks such as supply chain or financial associations. It also encourages organizations to come out from their firewalls and share data.

7 Immutability

Data is immutable in the blockchain. Once the participants agree upon a transaction and record, it is nearly impossible to delete or rollback the transactions since they are included in the blockchain. If someone subsequently tries to record another transaction, it is impossible to hide the original transaction. This gives the idea of provenance of assets, which means that for any asset one can tell where it is, where it has been and what had happened throughout its life.

8 Consensus

The algorithms/mechanisms used to ensure that all nodes agree on the integrity of transaction data in the system, replacing the need for a trusted third party. Before one can execute a transaction, there must be an agreement between all the participants that the transaction is valid.

This process is known as “consensus” and it helps to keep inaccurate or fraudulent transactions out of the blockchain. A block that includes invalid transactions could be revealed immediately.

9 Traceable

Every transaction added to a public or private blockchain is digitally signed and time stamped, which means that organization can trace back to a specific time for each transaction and also identify the corresponding party on the blockchain. So, every block is immutably and verifiably linked to the previous block.

8.2.3.10 Cryptography

Blockchain transactions are validated and trustworthy due to the complex computations and cryptographic proof among involved.

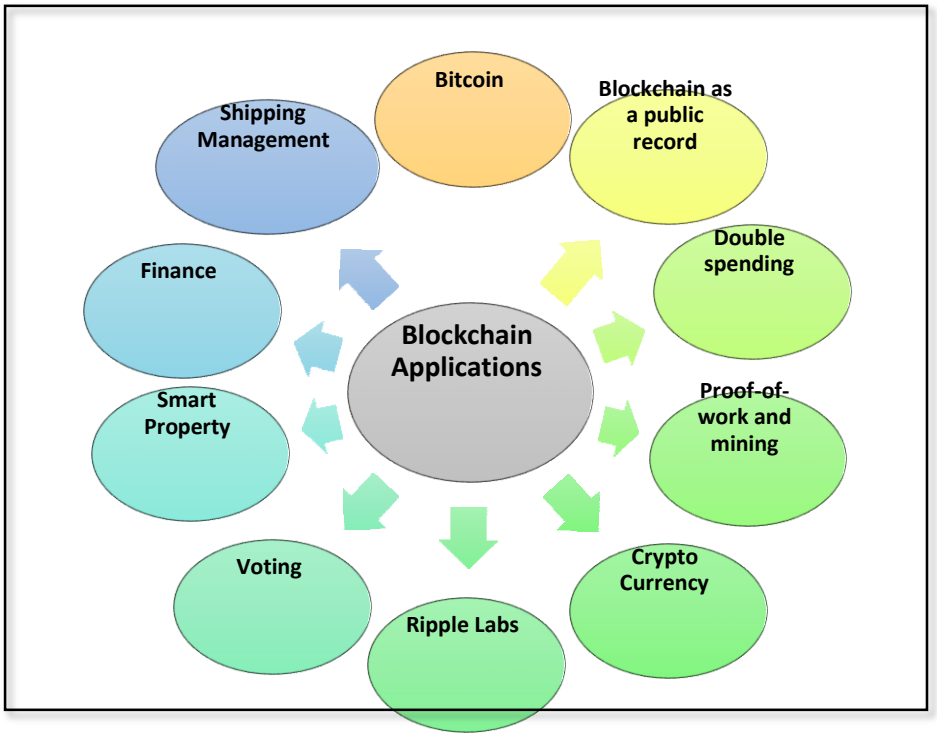
8.2.3.11 Provenance

It refers to the fact that it is possible to track the origin of every transaction inside the blockchain ledger.

12 Transparency

Blockchain system cannot be corrupted. This is very unlikely to happen, as it requires huge computing power to overwrite the blockchain network completely.

Information technology providing large number of advantages beyond digital currencies in a variety of fields. It is a suite of related protocols that has changed Finance and Technology operations through its groundbreaking application. Some of the applications of blockchain can be displayed in figure 1



Various Applications of Blockchain

1 Bitcoin

The first application of blockchain technology was Bitcoin, a digital currency based on a protocol that allows the users of the network to perform transactions with virtual money that exist only in their computers in a fast and secure manner.

2 Blockchain as a public record

Public blockchains such as Bitcoin takes no charge on an organization with respect to currency that differs from individual's thought of central bank power of controlling the money supply. This enables the public blockchain users as a collective bank.

3 Double Spending

Bitcoin block chain contains blocks where all transactions are connected together. These transactions are combined and verified periodically through mining processes into single blocks. The verification of the previous block is strengthened by verifying each subsequent block making double spending of Bitcoin transactions impossible.

4 Proof-of-work and mining

It is the method used to help users in avoiding double spending of transactions through an automated system which provokes large number of separate identities during transaction validation.

5 Crypto Currency

The first cryptocurrency came into existence during early 2009 with the mining of genesis block and the confirmation of the early transactions.

6 Ripple Labs

There exists three pre-mined cryptocurrencies namely Litecoin, Darkcoin and Primecoin. Litecoin is a user-friendly mining and transaction category which uses the Bitcoin protocol. Darkcoin provides a real anonymity during transactions, and Primecoin provides mining solutions based on prime numbers.

7 Voting

The blockchain users log into a system through any open source Internet connected devices

for modifying contents. This login becomes complete using a biometric authentication which confirms the user's identity. As a result, it provides two keys where a private key is used to access the vote rights and a public key is used for selecting preference and confirmation.

8 Smart Property

Smart property is defined as a physical asset combined with IoT and the Bitcoin infrastructure. It is owned and controlled by blockchains. It is based on IoT and is globally connected over growing networks.

9 Finance

Blocks contain the transcriptions of all transactions that take place in public or private equities, stocks, bonds or derivatives. It is also used to confirm the legitimacy by the local authority.

10 Shipping management

Every latest container received can be matched from its previous container based on a

5 Types of Blockchain

cryptographic hash. This tracking of containers takes place to avoid scams, modification of information or industrial espionage incidents.

Blockchains are generally of three types namely,

- Public Blockchain
- Private Blockchain
- Consortium or Federated Blockchain

5.1 Public Blockchain

If anyone can participate in reading, writing and auditing the blockchain without permission, it is known as a public block chain. It is open and transparent hence anyone can review the transaction at a given point of time. For example: Bitcoin, Ethereum, Litecoin and many others. Public blockchain are open and transparent and hence any individual can actively participate in reading, writing or auditing and there are no individual who takes in charge of these processes. It also enables one to review the processes at any given time. An example for transaction process in a

public blockchain can be depicted in figure 1

5.2 Private Blockchain

In private block chain, the write permissions are kept centralized to one organization. This is referred to as the private property of an organization or an individual. Read permissions may be public or restricted to an arbitrary extent. The consensus is achieved on the urge of the central in-charge who can give mining rights to anyone or restrict them totally. An example for transaction in a private blockchain can be depicted in figure 15.

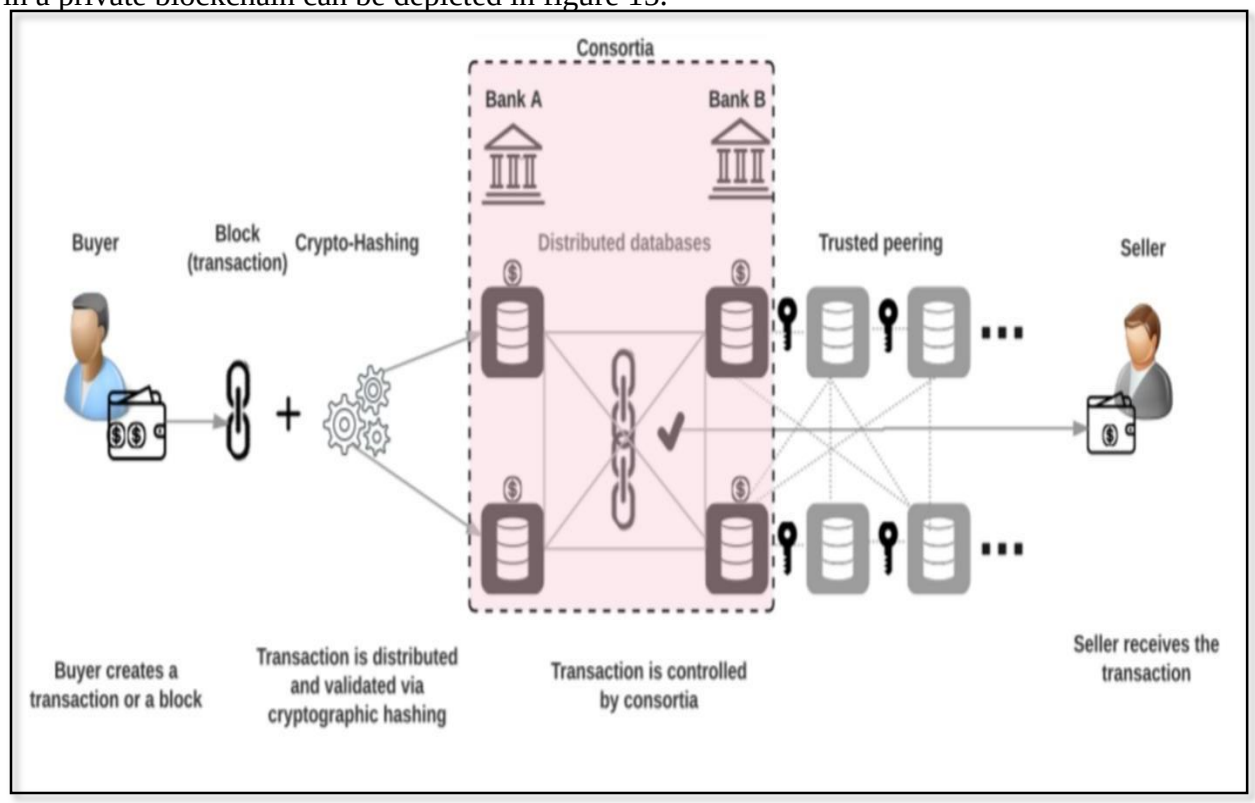


Figure Transaction process in Private Blockchain

5.3 Consortium or federated Blockchain

Consortium is sometimes considered as third type of blockchain platform, but typically it a special type of private blockchain. This type of blockchain removes the individual autonomy which is responsible for bringing changes in the blockchain as in private blockchain. Consortium or federated blockchains operate under the control of a group of institutions. Consortium blockchain does not allow everyone to participate in the process of verifying transactions.

Comparison on three blockchain types

Table 1 shows a simple comparison between the public, private and consortium or federated blockchain types.

Table 1 Comparison of three types of Blockchain

S.no	Property	Public Blockchain	Private Blockchain	Consortium/Federated Blockchain
	Read Permission	Public users	Public or restricted users	Public or restricted users

	Run access	Anyone can run full node	Restricted users can run a full node	Selected members of consortium can run a full node
	Transactions	Anyone can make transactions	Anyone cannot make transactions	Selected members of the consortium can make transactions
	Review/Audit	Anyone can review/audit the blockchain	Only private users can review/audit the blockchain	Selected members of the consortium can review/audit the blockchain
5.	Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
6.	Efficient use of resources	Low efficient	Highly efficient	Highly efficient
7.	Centralization	De-centralized	Centralized	Partially centralized
	Consensus permission	Does not require permission	Requires permission	Requires permission

6 Security issues in Block Chain

Blockchain model is also subject to certain threats. Some of the significant security threats can be listed as follows,

- Double-spending security threats
- Mining pools security threats
- Wallet security threats
- Blockchain Technology network threats

Figure 16 shows various security issues in blockchain.

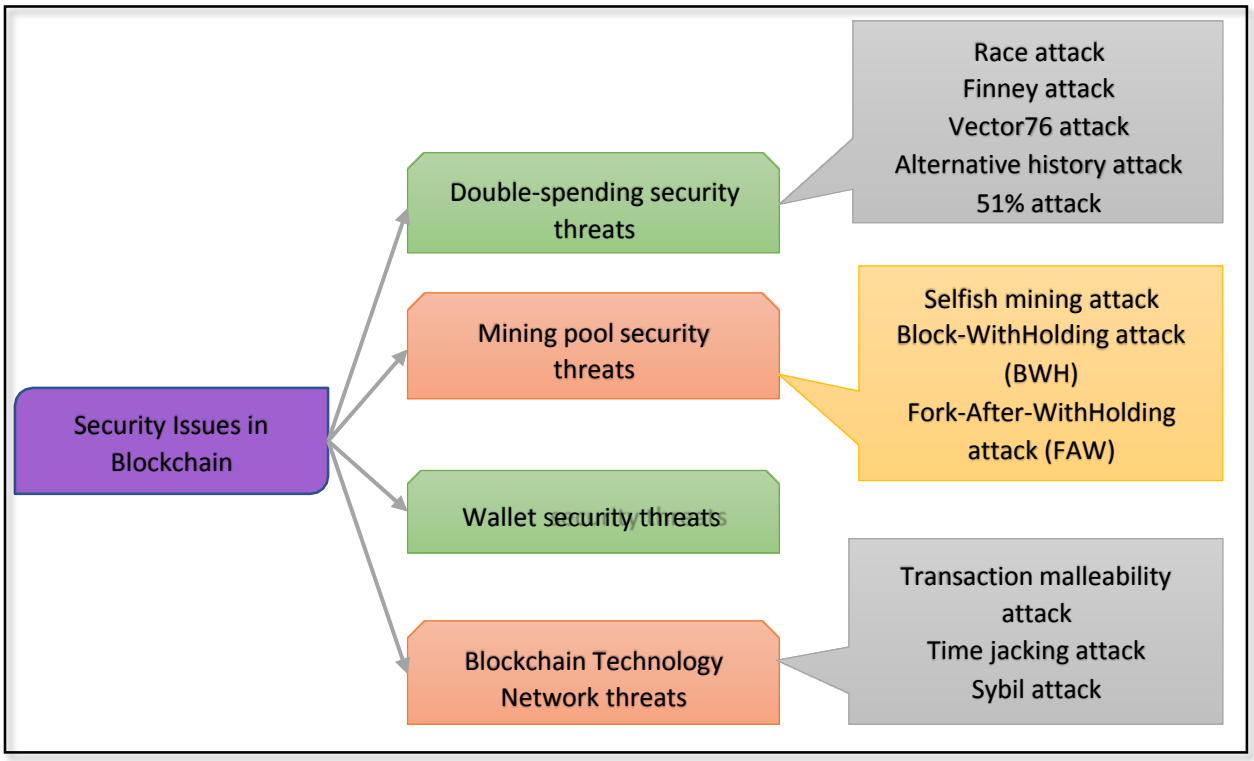


Figure Various Security Issues in Blockchain

6.1 Double- Spending Security Threats

A double-spending attack is an attack where a consumer uses the same cryptocurrency multiple times for transactions. The figure 17 shows an example scenario of a double spending attack model against fast payment in Bitcoin.

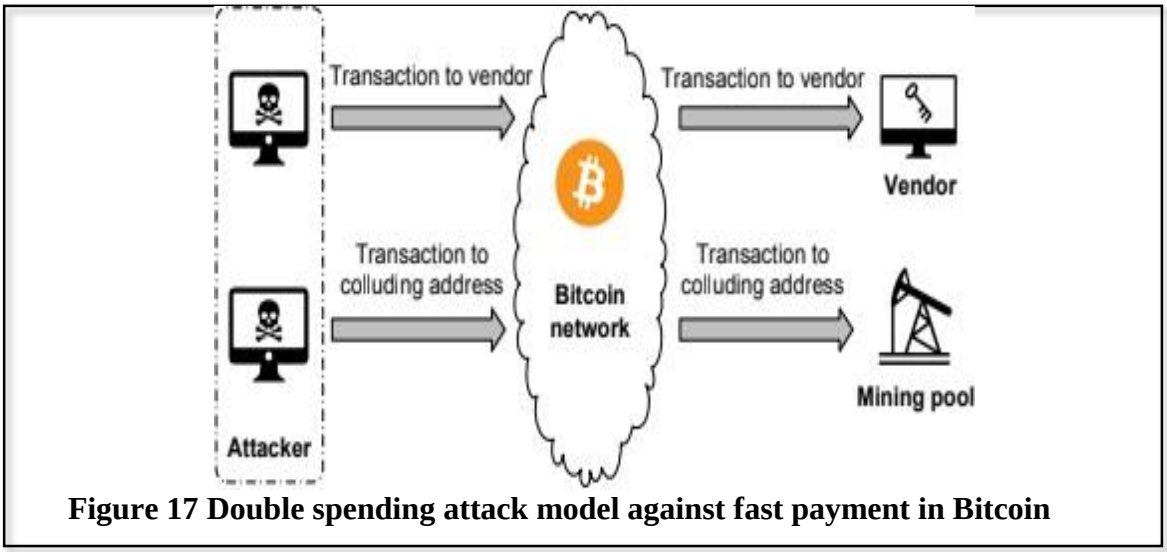


Figure 17 Double spending attack model against fast payment in Bitcoin

The various double spending attacks are

- Race attack
- Finney attack
- Vector76attack
- Alternative history attack, and
- 51% attack

- **Race attack –** Race attack happens when an attacker sends two conflicting transactions in rapid succession into the Bitcoin network. This type of attack is relatively easy to implement in PoW-based blockchain.
- **Finney attack –** An attacker pre-mined one transaction into a block and spends the same coins before releasing the block to public network to invalidate that transaction. This is called a 58 Finney attack. The Finney attack is a fraudulent double-spent that requires the participation of a miner once a block has been mined. An adversary can only perform a double-spending in the presence of one confirmation vendors.
- **Vector76 attack –** Vector76 is also called a one-confirmation attack, in which the attacker uses the privately mined block to perform a double-spending attack on the exchanges. It is a combination of the race attack and the Finney attack such that a transaction that even has one confirmation can still be reversed. A vector76 attack is possible when a wallet service such as crypto currency exchange runs a node that accepts direct (incoming) connections. Assuming that this node is using astatic IP address, it will not be difficult for the attacker to find the IP address.
- **Alternative history attack –** The alternative history attack is still possible in case of multiple confirmations. It requires high hash-rate and risk of significant expenses in wasted electricity to the attacking miner.
- **Fifty-one percent attack –** Blockchain relies on the distributed consensus mechanisms to maintain mutual trust in the network. However, the consensus mechanisms themselves have 51% vulnerability which can be exploited by the attackers to control the entire blockchain network. The blockchain is designed with the assumption that honest nodes control the network, when a user or group of users are able to take control of more than50% of the hash power in Proof-of-Work, then the51% attack may be launched. The 51% attack is considered the most threatening attack on

  the blockchain network. It gives power to the attacker to destroy the stability of the whole

network including actions such as double spending attack. This attack is also known as >50% attack or majority hash rate attack.

6.2 Mining Pools Security Threats

Mining pools are created by a group of miners to work together, pool their resources, and contribute to the generation of a block, and then share the block reward according to the added processing power. The figure 18 presents a chart of the most mining pools across the world. It has Bitcoin network hash rate till March 10, 201

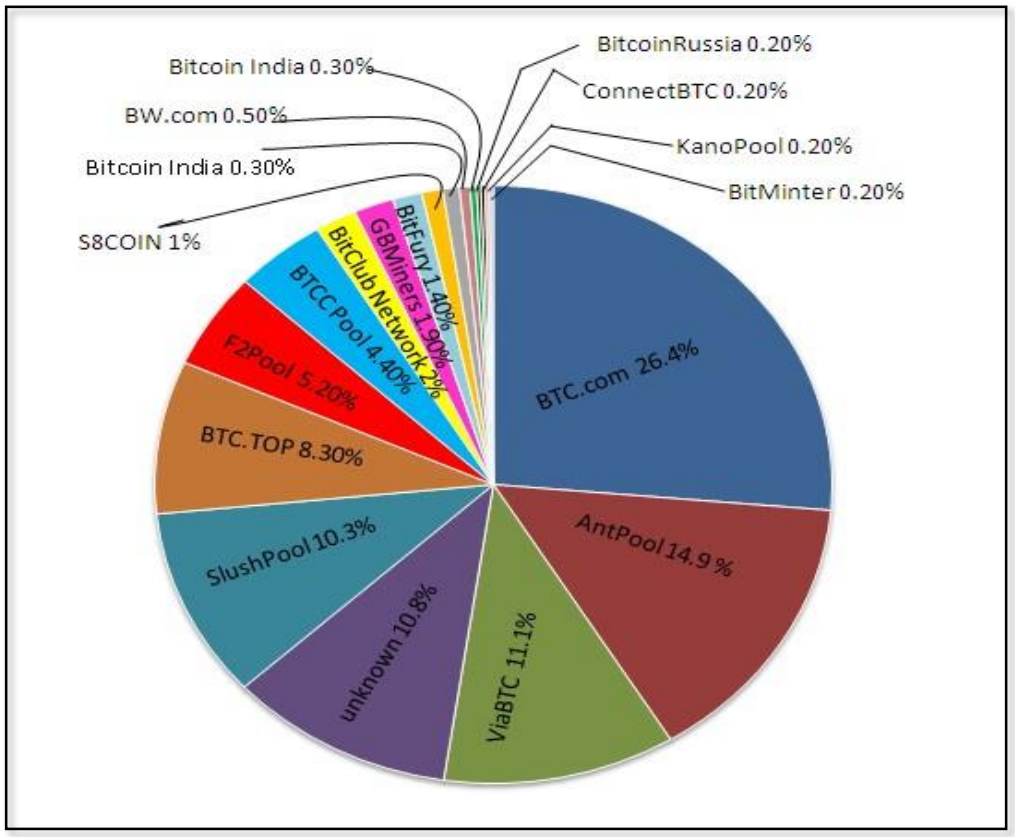


Figure Mining pools of Bitcoin network hash rate till 2018

The mining pools security threats are again of three types namely,

- Selfish mining attack
- Block-withholding attack (BWH)
- Fork-After-Withholding attack (FAW)

- **Selfish Mining Attack –** It was first introduced by Eyal and Sirer. In selfish mining attack, a

dishonest miner does not publish and distribute a valid solution to the rest of the network. In this attack, the dishonest miner rather than acting like a regular

miner and publishing blocks to the network immediately upon finding them, he/she selectively releases blocks, or publishing many blocks all at once and thus forcing the rest of the network to discard their blocks and lose revenue. The primary motive of selfish mining is to obtain an unfair reward which is bigger than their share of computer power spent and confuse other honest miners and lead them to waste their resources in a wrong direction.

- **Block-withholding attack (BWH) –** In block withholding attacks, blocks are discarded, and dishonest miner never publishes a mined block to sabotage the pool revenue and just keeps the mined block secret until the right time comes to release them. It is usually made by infiltrating another pool.
- **Fork-After-Withholding attack (FAW) –** It was introduced by Kwon, Kim, Son, Vasserman. FAW is another variant of BWH attack. In this attack, the attacker's reward is always equal to or greater than that for a BWH attacker and it is fourtimes more practical per pool than the BWH attack. The FAW attack combines components of selfish mining and BWH attack.

6.3 Wallet Security Threats

Blockchain-based currencies use private key-based authentication, though passwords remain the most common form of user authentication. Users need their public and private keys, to access coins or make transactions in the blockchain. A Bitcoin wallet is a collection of private keys that are used to manage those keys and to make transactions on the Bitcoin network. Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA) which is a variant of the Digital Signature Algorithm (DSA) to sign and validate transactions. A digital signature of a transaction is an encryption of the transaction hash calculated with a private key. The signature of the transaction can be verified with an associated public key. The digital signature proves that the transaction has not been altered, and the owner of the private key has issued that transaction. In the process of creating signature a pre-selected random value is used along with the private key, and the random value should be different for each transaction.

Vulnerable signature – In Bitcoin, the private key is the major authentication component and it used ECDSA to sign and validate transaction. The ECDSA has

insufficient randomness in signature generation, which could lead to private key compromise.

The wallets could be either online (hot - connected to the Internet) or offline (cold

disconnected from the Internet). Online and offline wallets could be summarized into four categories namely software, hardware, paper and online wallets.

- Software wallets are applications or software that users can download in their desktop, laptop, or mobile devices. This is used to store their private keys local and are considered online wallet. The different types of software wallets are Bitcoin core, Bitcoin XT, Armory.
- Hardware wallets are stand-alone hardware cold-storage that is used to store private keys offline. The Popular hardware wallets are Ledger Nano, TREZOR, PI wallet.
- A paper wallet is a fancy term for printing out the public and private keys on a piece of paper, and sometimes QR barcode is used to store the private key.
- In online wallets or web-based wallets, private keys are stored in the cloud rather than a local computer. Most of the currency exchange offers web-based wallet facilities.

7 Blockchain Network Security Threats

The blockchain uses peer-to-peer network concept, which includes all the nodes that maintain and run the blockchain protocols and provide services, under the blockchain network. In case of the Bitcoin, there are two types of nodes: those that accept incoming TCP connection, and generate blocks in the blockchain (miners) and other nodes (users) who only create transaction and submit it into the Bitcoin network.

The blockchain network security threats comes from various types of attacks namely,

- Transaction malleability attack
- Time jacking attack
- Sybil attack

7.1 Transaction malleability attack

-

The transaction malleability is considered as a flaw in the original Bitcoin protocol. In transaction malleability attacks, attacker tricks his target into believing that a transaction has failed. Then he asks for the transaction to be repeated. In this way, the

attacker who was already owned X Bitcoins could fraudulently obtain twice the amount. This could happen by changing the transaction hash of a Bitcoin transaction.

7.2 Time jacking attack

Time jacking attack is an attack on the Bitcoin network due to a theoretical vulnerability in Bitcoin timestamp handling. In this attack, attacker tries to announce inaccurate timestamps when connecting to a node. Once the network time counter of node is altered by the attacker, the deceived node may accept an alternate blockchain. This could significantly increase the chances of successful double-spending.

7.3 Sybil attack

The Sybil attack is an attack where the reputation of the system is challenged by forging identities in P2P networks, (i.e.) attacker assumes many identities. In a Sybil attack, the attacker subverts the reputation of a P2P network, by creating a large number of pseudo identities and then use them to gain a suspiciously large influence. A Sybil attack in Bitcoin network is an attack where a single adversary is controlling multiple nodes in the Bitcoin network.

****