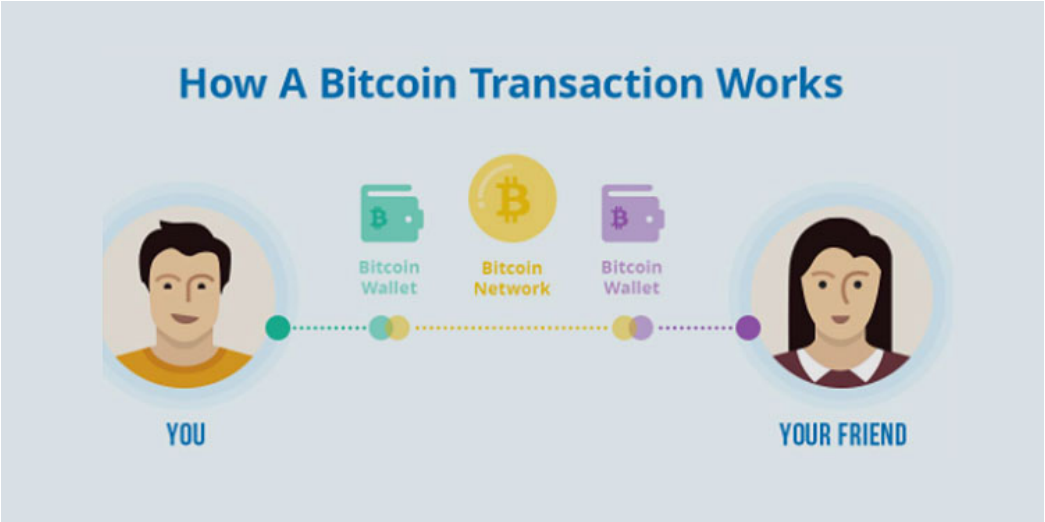
Working Principles



- For Bitcoin users, sending a transaction is as simple as entering an amount and an address in their wallet and pressing send.
- They don't have to worry about the technicalities of how it works.
- Many users are curious how it works in practice though.
- Bitcoin makes use of public-key cryptography to ensure the integrity of transactions created on the network.
- In order to transfer bitcoin, each participant has pairs of public keys and private keys that control pieces of bitcoin they own.
- A public key is a series of letters and numbers that a user must share in order to receive funds.
- In contrast, a private key must be kept secret as it authorizes the spending of any funds received by the associated public key.
- Using the private key associated with their bitcoin, a user can sign transactions and thereby transfer the value to a new owner.
- The transaction is then broadcast to the network to be included in the blockchain.

- **Overview of a Bitcoin Transaction**
- To better illustrate how value is transferred in the Bitcoin network, we will walk through an example transaction, where Alice sends .05 bitcoin to Bob.
- At a high level, a transaction has three main parts:
- Inputs. The bitcoin address that contains the bitcoin Alice wants to send. To be more accurate, it is the address from which Alice had previously received bitcoin to and is now wanting to spend.
- Outputs. Bob's public key or bitcoin address.
- Amounts. The amount of bitcoin Alice wants to send.
- In order for Alice to send the .05 bitcoin to Bob, she signs a message with the transaction details using her private key.

- The message contains the input, output, and amount as described above.
- The transaction is then broadcast to the rest of the Bitcoin network where nodes verify that Alice's private key is able to access the inputs (by checking that Alice's private key matches the public key she is claiming to own).
- Once a transaction is broadcasted to a node, this node then passes it along the network until it reaches a mining node.
- Miners will then order this transaction into what is called a block template.
- This is a blueprint for the block which the miner is attempting to add to the blockchain.
- If a miner finds the next block in the chain, then this block template is mined and becomes an immutable block on the blockchain.
- Finally, this block is broadcasted to the network's nodes who will include it in their copy of the chain.

Bitcoin Invalid Transactions

- The main reason a transaction would fail is that the transaction used too low of a fee during a time of high network congestion.
- In general, a Bitcoin transaction will only be rejected if the fee offered is lower than the current network fee.
- However, this doesn't mean that a Bitcoin transaction can't take a long time.
- Bitcoin nodes follow a “first-seen” policy, which means that node software considers the first transaction they receive as valid, and any subsequent transaction they see attempting to spend the same coins will be considered invalid and will not propagate.
- The transaction is verified by a mining node and included in a block of transaction that is recorded on the blockchain.
- Once recorded on the blockchain and confirmed by sufficient subsequent blocks, the transaction is a permanent part of the bitcoin open distributed ledger and is accepted as valid by all participants.

Parameters that invalidate the transactions

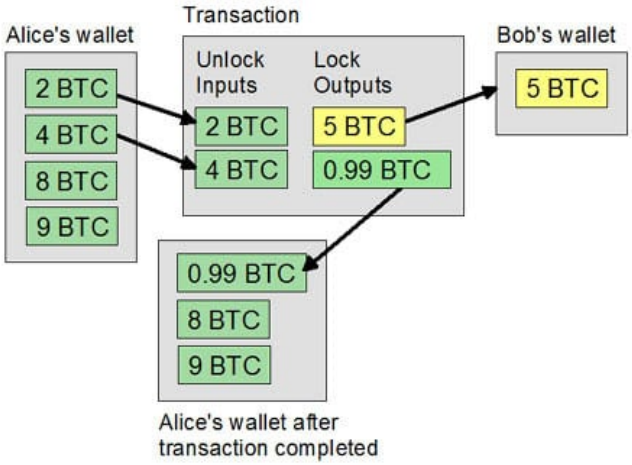
- Invalid transactioncode is often returned from the issuer when they do not accept the transaction.
- This can possibly be when a transaction for the same amount and merchant is attempted multiple times quickly for the same card.
- The card holder should contact their issuing bank.
- If your transaction fee is too low (or not assigned), some miners will reject it.
- Too many rejections on a congested network result in a failed transaction.
- Issues with the receiver's wallet: Sometimes, you can see multiple nodes confirming your transactions, but your transaction still shows up as unconfirmed.

Scripting language in Bitcoin

- Bitcoin's scripting language is called a stack-based language because it uses a data structure called a stack.
- A stack is a very simple data structure that can be visualized as a stack of cards.
- A stack allows two operations: push and pop.
- Push adds an item on top of the stack.
- Pop removes the top item from the stack.
- Operations on a stack can only act on the topmost item on the stack. A stack data structure is also called a Last-In-First-Out, or "LIFO" queue.
- The scripting language executes the script by processing each item from left to right.
- Numbers (data constants) are pushed onto the stack.
- Operators push or pop one or more parameters from the stack, act on them, and

might push a result onto the stack.

- For example, OP_ADD will pop two items from the stack, add them, and push the resulting sum onto the stack.
- Conditional operators evaluate a condition, producing a boolean result of TRUE or FALSE.
- For example, OP_EQUAL pops two items from the stack and pushes TRUE (TRUE is represented by the number 1) if they are equal or FALSE (represented by zero) if they are not equal.
- Bitcoin transaction scripts usually contain a conditional operator, so that they can produce the TRUE result that signifies a valid transaction.
- Bitcoin Script is the language Bitcoin uses to do everything it can do, from sending funds from a wallet to allowing the creation of multi-user accounts.
- Language is not full turing because its functionality is limited and cannot loops.
- So it is not capable of solving any type of problem such as turing machines.
- However, this limitation is intentional as this prevents infinite or endless looping and error execution.
- Where malicious parts of the program can be free to create complicated operations to consume the rate of hash and slow down the Bitcoin system through infinite loops.
- A programming language is necessary because it allows us to write programs and that computers execute our wishes.
- Therefore, Bitcoin Script is essentially a set of programmed instructions that are recorded with every transaction made.
- These instructions describe how users can access and make use of the bitcoins available on the network.
- A stack-based scripting language embedded in Bitcoin transactions.
- When bitcoins are sent to a recipient, Script commands in an unlocking script (scriptSig) validate the available bitcoins (UTXOs), while Script commands in a locking script (scriptPubKey) set the conditions for spending them.



Applications of Bitcoin script

- All Bitcoin transactions use Script to define how outputs can be spent.
- In other words, the script of a Bitcoin transaction determines to whom the bitcoin was sent.
- Bitcoin has a few different scripts, with Pay-to-Public-Key-Hash (P2PKH) being the most popular.
- P2PKH is a simple script which pays bitcoin to an address.
- The main properties of Bitcoin language and scripts are the following: every Bitcoin script can only produce two outcomes.
- It can either execute successfully or return an error.
- Bitcoins are being used to buy goods and services as more and more stores across the world are accepting bitcoin payments.
- Bitcoin transactions provide a customized level of anonymity and it is relatively difficult to trace their trail. So bitcoins are being used to transact anonymously.
- International payments can be made easily and cheaply as bitcoins are not related to any country or subject to any government regulation.
- There is the freedom of the fact that there is no need of permission from any authority for your transactions.
- Bitcoins provide a way to transact securely online as they use very strong cryptographic algorithms.
- Users and businesses like bitcoin payments because there are no credit card fees to pay.
- Bitcoins can be as an investment, expecting that their value will appreciate significantly in future.
- Bitcoins can be used to gamble on online sites like SatoshiDice, RoyalBitcoin, Bitzino, Peerbet, etc.
- Bitcoins are being used to shop online as increasing numbers of vendors are allowing bitcoin transactions.
- Users now can make payments in bitcoins on their smartphones through bitcoin wallet apps.
- Unlike credit card or bank payments, there is no need to provide personal information to complete the transactions. So the hassle of providing identity can be avoided.

Nodes and network of Bitcoin

- Bitcoin nodes are the underlying infrastructure of the Bitcoin network, securing and maintaining it.
- But despite their importance, Bitcoin nodes are often misunderstood or not understood at all.
- Bitcoin is a network; it is a collection of interconnected computers that share

information.

- Bitcoin is a protocol; it is a set of rules for how information can be shared on the network.
- Bitcoin is software; it is a computer program that knows the protocol rules and is run by computers on the network so that they can share information with each other.

What are nodes?

- In general, a node is a point on a network.
- For example, a car is a node on a network of highways, or a work colleague a node in a professional network.
- In the world of computers, nodes are devices connected to a computer network that transmit, process, and store information.
- Nodes consist of two things: hardware and software. Hardware is the physical stuff—microchips, processors, etc—required to run software. Software is a set of instructions that can be stored and run by hardware.
- For example, your **smartphone is a node on the internet**.
- The apps you run (browsers, messaging apps, maps, etc) are pieces of software that can connect to the internet and give it instructions for what type of information to send, receive, and store (such as websites, text messages, and directions).
- These instructions and pieces of information are processed and stored on tangible pieces of hardware that are inside your phone and other computers connected to the internet.
- Compared to the internet and cell phones, the Bitcoin network and Bitcoin nodes are extremely simple.
- While the internet and cellphones are designed to transmit and store all sorts of information, the Bitcoin network and Bitcoin nodes are designed to transmit and store one type of information—data representing BTC transactions.

What are Bitcoin nodes?

- Bitcoin nodes are computers that run Bitcoin software and are connected to the Bitcoin network. Bitcoin nodes validate, broadcast, process and store BTC transactions.
- BTC transactions are batched and stored into groups called blocks.
- This is where the term blockchain comes from—historical transactions stored in blocks that are linked together. Before a block is added to the blockchain, nodes must verify that the block's transactions are valid.
- This verification involves checking things like whether the same BTC was spent twice, or whether a sender actually has the BTC they are trying to send.
- The process of individual nodes collectively agreeing upon the validity of a block (and the transactions it contains) before adding it to the blockchain is known as consensus.

- Because Bitcoin is a peer-to-peer payment system, it does not have intermediaries or middlemen to enforce consensus rules on the Bitcoin network.
- Therefore, nodes must achieve consensus amongst themselves.
- They do this using the Bitcoin software.
- In addition to the Bitcoin protocol rules, the Bitcoin software contains a full copy of the Bitcoin blockchain.
- So, when a node downloads the Bitcoin software and connects to the Bitcoin network, it has the same transaction history and works off of the same set of rules for verifying transactions as every other Bitcoin node.
- This way, when a new transaction is broadcast to the network, each individual node does its own work to check a transaction's validity.
- Similarly, when a new block is broadcast to the network, each node decides whether or not to add it to their copy of the blockchain.
- This design allows for nodes to trustlessly verify BTC transactions and blocks.