Bitcoin

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com

https://www.facebook.com/tutorialspointindia https://twitter.com/tutorialspoint

About the Tutorial

The tutorial begins by introducing what bitcoins are, then proceeds with the installation of the bitcoin client software and wallets to make bitcoins transactions possible. It also discusses bitcoin mining, exchanges, and trading. Finally, it moves on to applications and future of bitcoins. After reading this tutorial, you will have learned all the basics of bitcoins; enough to use bitcoins and make money by trading and investing in bitcoins.

Audience

This tutorial has been prepared for professionals aspiring to learn all the essentials of Bitcoins and develop a habit of buying products and services using bitcoins and lastly making money by trading in this brand new cryptocurrency.

Prerequisites

Before you start proceeding with this tutorial, we assume that you have basic computer skills, knowledge of downloading and installing software like Java and other applications. Prior exposure to the Linux operating system flavors would be an added advantage.

Copyright & Disclaimer

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at contact@tutorialspoint.com.

Table of Contents

1. Bitcoin — Introduction

Bitcoin emerged out of the 2008 global economic crisis when big banks were caught misusing borrowers' money, manipulating the system, and charging exorbitant fees. To address such issues, Bitcoin creators wanted to put the owners of bitcoins in-charge of the transactions, eliminate the middleman, cut high interest rates and transaction fees, and make transactions transparent. They created a distributed network system, where people could control their funds in a transparent way.

Bitcoin has grown rapidly and spread far in a relatively short period of time. Across the world, companies from a large jewelry chain in the US, to a private hospital in Poland, accept bitcoin currency. Multi-billion dollar corporations such as Dell, PayPal, Microsoft, Expedia, etc., are dealing in bitcoins. Websites promote bitcoins, magazines are publishing bitcoin news, and forums are discussing cryptocurrencies and trading in bitcoins. Bitcoin has its own Application Programming Interface (API), price index, trading exchanges and exchange rate.

However, there are issues with bitcoins such as hackers breaking into accounts, high volatility of bitcoins, and long transaction delays. Elsewhere, particularly people in third world countries find Bitcoins as a reliable channel for transacting money bypassing pesky intermediaries.

How to use Bitcoins?

We can make bitcoin transactions as we do with our familiar fiat currencies. While we use Bitcoin, the purchaser is actually referenced to our digital signature, which is a security code encrypted with sixteen different symbols. The purchaser decrypts the code with his device to get the cryptocurrency. Therefore we can say that cryptocurrency is an exchange of digital information that permits us to buy or sell goods and services.

The transaction is secured and made trustworthy by running it on a peer-to-peer network that is akin to a file-sharing system.

How does Bitcoin handle double spending problem?

For digital cash system, a payment network necessarily should have valid accounts, balances and transaction records. The biggest bottleneck common to every payment network is the double spending problem which is the case when same money is used multiple times to do transactions.

To prevent double spending, all transactions have to be recorded and validated every time in a central server where all the balance records are kept. However, in a decentralized network, every node on the network has to do the job of a server; it has to maintain list of transactions and balance records. Thus, it is compulsory for all nodes/entities in the network to keep a consensus about all these records. This was achieved by using the blockchain technology in bitcoins.

So we can say that bitcoins like other cryptocurrencies are mere token entries stored in the decentralized databases that keep consensus of all balance and account records. It is to be noted that cryptography is used extensively to secure the consensus records. Bitcoins and other cryptocurrencies are secured by math and logic more than anything else.

Bitcoins and cyptocurrencies have gained recognition and adoption based on their perceived value by their creators and users.

Bitcoin works on the same concept, **the more people participate; the more value is created**.

History of Bitcoins

The first Bitcoin protocol and proof of concept was published in a Whitepaper in 2009 by a shadowy individual or group under the pseudonym Satoshi Nakamoto. Eventually Nakamoto, who remained mysterious, left the project in late 2010. Other developers took over and the Bitcoin community has since grown exponentially.

While Satoshi Nakamoto's real identity remains shrouded in mystery, it is on record that he communicated extensively in Bitcoin's early days. Let us speculate on questions like when he started working on Bitcoin, to what extent he was inspired by similar ideas and what was the motivation for bitcoin.

Creation of the first bitcoin domain

It is believed that Satoshi started coding Bitcoin around May 2007. He is said to have registered the domain bitcoin.org in August 2008. Around that time, he started sending emails to a few individuals he thought might be interested in the idea of bitcoins.

In October 2008, he publicly published a white paper that dwelt on the Bitcoin protocol, and released the Bitcoin code as well. Then he stayed in contact for about two years, during which he interacted actively in forums, communicated with several developers and later he also submitted patches to the initial code. He maintained the source code along with other developers, tackling issues as they happened. By December 2010, as others had slowly taken over, he quietly left the scene.

Entities

The entities involved in the implementation and maintenance of Bitcoins are:

- The Blockchain platform
- Cryptographic algorithms
- Bitcoin miners which are computers or specialized machines that mint the currency and make possible transactions
- People who participate in the transactions and thus help to move the payment system

The philosophy of Bitcoin, and in general, of all cryptocurrencies is that they are distributed systems where there is no central entity that manages the activities such as transactions, among others. It is a peer-to-peer (p2p) system that operates at the level of participants.

Bitcoin Transactions

We shall now see how a new block of bitcoin transaction is created.

A bitcoin miner creates a block by using the following steps:

- Gathering pending transactions, preferentially those with transaction fees first, and then the free ones

- Verifying the transactions for their validity

- Solving a hashing problem

According to the statistics, in October, 2015, blockchain.info site stated that, the average number of transactions per block was 411, and as of May 2018, the current number of pending unconfirmed transactions is around 2495.

Reward and cost per bitcoin transaction

Assuming that one bitcoin is worth $400, the reward of 25 bitcoins per block is worth around $10,000, ignoring negligible amount of transaction fees. Taking average number of transactions per second as 2, and the number of transactions per block as 1200, the reward per transaction works out to $8.33. It is found that the cost of electricity consumed in mining is close to the reward which makes mining bitcoins not so profitable. The basic problem of mining as of now, is the 1 MB limit on block size which makes it possible to have at most only 10 transactions per second.

Confirmation of a bitcoin transaction

A transaction is considered to have received **n** confirmations if it has been published in a block in the block chain, and **n-1** more blocks have also been added. A transaction is normally considered "confirmed" once it has six confirmations. Newly created Bitcoins are considered confirmed after they have received about a hundred confirmations.

How does Bitcoin have value?

It is the common consensus, belief and the perception that gives value to the bitcoin. All the participants in this system have consensus on the following:

- immutability and integrity of the blockchain
- security and validity of the payments
- rules of the system

Bitcoin was the first practical implementation of blockchain technology and is currently the most significant triple entry bookkeeping system globally. In a bitcoin ecosystem, access to entire source code is available to everyone always and any one can review or modify the code. The authenticity of each transaction is secured by digital signatures of the sending parties thus ensuring that all users have complete control over sending bitcoins.

Thus, leaving a little room for fraud, no chargebacks and no identifying information that could be hacked resulting in identity theft.

Here is a list of some of the entities who accept Bitcoins:

- Wordpress

- Namecheap
- Microsoft
- Dell Computers
- Archive.org
- Bitpay
- Bitspend.net

2. Bitcoin — Environmental Setup

Satoshi Nakamoto released the first bitcoin software as open source code in January 2009. He later renamed it to "**Bitcoin Core**" to differentiate it from Bitcoin network.

Bitcoin Core is a bitcoin implementation. It is a full Bitcoin client and is backbone of the network which provides high levels of security, stability, and privacy. It also assists network in relaying transactions. It requires at least 50 GB of hard disk space and is not recommended for new Bitcoin users who can opt for lightweight mobile or desktop wallets.

What is a Bitcoin full node?

A **full node** is a software program that fully validates transactions and blocks. Most full nodes also assist the network by accepting and validating transactions and blocks from other full nodes, and then relaying them further to other full nodes.

Bitcoin Core full nodes need to have certain requirements. If a node is run on weak hardware, it may work — but with a host of issues. It will be an easy-to-use node, if the following requirements are met:

- Desktop or laptop hardware running latest versions of Windows, Mac OS X, or Linux
- About 150 Gb of free disk space, accessible at a minimum speed of 100 MB/s
- 2 GB of RAM memory
- A broadband internet connection with upload speed of at least 50 kilobytes per second
- Preferably, an unmetered connection, a connection with high upload limits. It is common for full nodes on high-speed connections to use 200 GB upload or more a month. Download usage is around 20 GB a month, plus an additional 150 GB the first time you start your node
- 6 hours a day of full node running

Bitcoin Core can be downloaded from the site https://bitcoin.org.

Apart from downloading bitcoin client, we have to set up several accounts. Going further in this tutorial, we will learn how to open accounts in bitcoin sites and to create accounts in bitcoin wallets, bitcoin exchanges, bitcoin mining sites, faucet sites, and sites that offer bitcoin tools and value added services.

Java Installation

To run a mining software like **BitMinter client**, we need to have latest compatible version of Java installed. BitMinter client can be downloaded from https://bitminter.com.

To install Java, you can follow these steps:

- Go to www.java.com/download.

- Click on the button "**Free Java Download**".
- Click on "**Agree and Start Free Download**" button.
- Select the version that is compatible with your operating system.
- Follow the onscreen instructions to continue installing the software.
- Once the installation is completed, click on **Finish** button.
- Continue on to the next step to set up a **miner**.

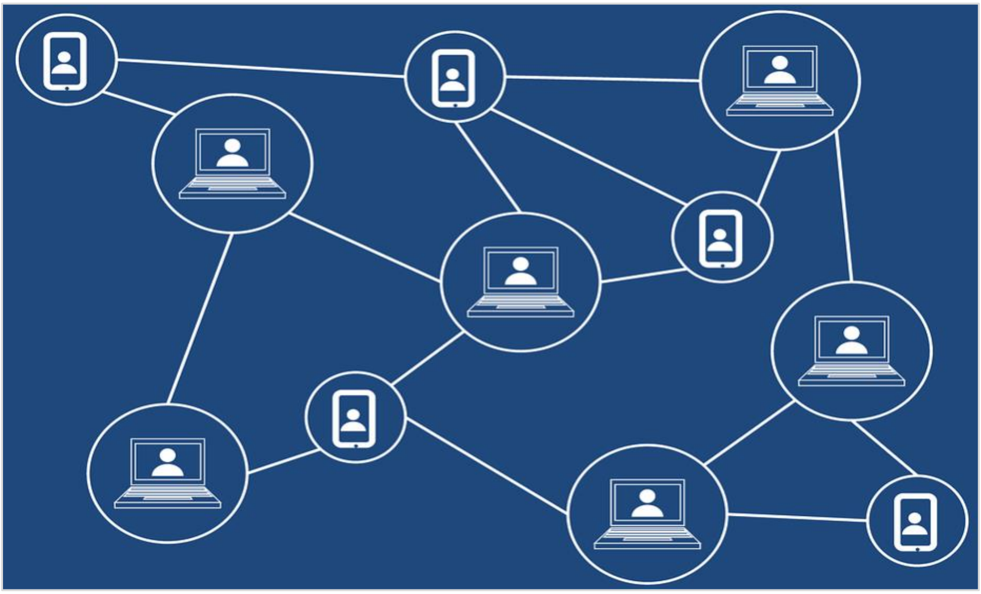
3. Bitcoin — Blockchain Technology

It is believed that **Blockchain** is a new age technology that is solution waiting for a host of problems. There is no doubt that it is a new wonder in the field of computing.

What is a blockchain?

A **blockchain** is basically a perpetually growing list of records, called **blocks**. These blocks are linked and secured by using cryptography. Each block generally contains a cryptographic hash of the previous block along with timestamp and transaction data. By its design, a blockchain does not allow modification of the data.

It is an open, distributed ledger that records transactions between different parties efficiently and in a verifiable and permanent way. A blockchain, as shown in figure below is typically managed by a p2p or peer-to-peer network collectively following a protocol for communication between nodes and for validating new blocks. Once recorded, the data in any given block cannot be altered without consensus of the network majority.



In case of bitcoins, the blockchain is a public ledger that records bitcoin transactions. It is implemented as a **chain of blocks**. Each block contains a hash of the previous block up to the genesis block which is the first block of the bitcoin blockchain. This is however achieved without any trusted central authority: the working of the blockchain is performed by a network of communicating nodes running bitcoin software. Transactions of the type payer A sends B bitcoins to payee C are broadcast to this network using existing software applications.

Nodes in the network validate new transactions, add them to their copy of the ledger, and then convey these ledger additions to other nodes. Each network node stores its own copy of the blockchain. Roughly every 10 minutes, a new group of validated transactions, a block, is created, and added to the blockchain, and then quickly published to all network nodes. This makes it possible for bitcoin software to determine when a particular bitcoin amount has been spent, and this prevents double-spending in a decentralized environment. It is noted that the blockchain is the only place where bitcoins can be said to exist in the unspent form.

Blockchain technology has led to the development of new, digital currencies like Bitcoin and Litecoin that are not issued or managed by government or any central bank of a country. This frees individuals from any kind of control and intermediaries like banking systems that are scam and subject to collapses. It has also led to distributed computing technologies like Ethereum, which has introduced smart contracts.

Blockchain is a replicated, shared ledger technology that allows any participant in the network to see ledger and make changes. It is open source, bringing down costs, improving efficiencies, increasing accessibility, addressing exciting and topical business challenges across a broad spectrum. Linux Foundation's Hyperledger is a project developing an open source, open standards shared ledger technology.

Nowadays, consumers demand transparency regarding products and their making. Governments require more information about corporate supply chains, with penalties for non-compliance. In such scenario, blockchain technology promises to deliver such expectations. It enables secure digital transfer of value or property across supply chains.

Advantages of Blockchain Technology

The following are the advantages of Blockchain Technology:

- Transactions are now verifiable, disallowing any party from making changes
- Greater efficiencies are being achieved through greater transparency
- Consumers have been empowered to make informed purchases
- Now governments are able to procure reliable information.

Many experts believe that blockchain technology can be used in online voting, crowdfunding and other emerging technologies and novel ideas. Major financial institutions such as JP Morgan Chase are confident that cryptocurrencies can lower transaction costs and make payment processing more efficient.

Bitcoin is one of the most popular and successful implementations of blockchain technology. It is an open source cryptocurrency that uses distributed peer-to-peer computing. There is no need of a central authority to manage bitcoin network. It was created by a person or group under the pseudonym of **Satoshi Nakamoto**. The transactions on this network are verified by proof-of-work algorithms on computers running a mining software.

4. Bitcoin — Cryptocurrencies

Cryptocurrency is digital currency that uses cryptography to secure its transactions. It is difficult to make counterfeit crypto currency because of this security feature. A remarkable feature of any cryptocurrency, is the fact that it is not issued by any central bank or government authority, making it immune to any government manipulation.

There are over 17 million bitcoins in circulation as of May 2018, with a total market capitalization of over $140 billion. Bitcoin's success has given rise to a number of similar cryptocurrencies called altcoins: Namecoin, Litecoin, PPCoin, etc.

Pros and Cons of Cryptocurrencies

Cryptocurrencies make it possible to transfer funds between parties and these transfers are effected through the use of public and private keys as a means of security. These fund transfers are carried out with nominal or zero processing fees, allowing users to avoid the exorbitant fees charged by most banks and other financial intermediaries for the transfers.

Apart from the fact that prices of cryptocurrencies are based on supply and demand, it has been found that the exchange rates of cryptocurrency fluctuate widely due to a host of reasons.

The anonymous feature of cryptocurrency transactions renders them vulnerable to illegal transactions, such as money laundering, drug and weapons dealing, terror funding and tax evasion by criminals. However, anonymity of transactions has its own host of plus points. Cryptocurrencies are also considered by some economists to be a passing phenomenon or a speculative bubble that can burst any moment because of their virtual or digital nature. Bitcoin has indeed seen some exponential surges and sudden collapses in value.

Cryptocurrencies are also not totally secure from hacking. In Bitcoin's short life-span, the currency has been subject to over 40 hackings, including few that topped $1 million in value. Still, many see cryptocurrencies with hope as a medium of exchange that preserves value, facilitates easy exchange, is more liquid and portable than bullion, and is outside the purview of central banks and governments.

Through many of their unique properties, cryptocurrencies allow exciting applications that could not be provided by any traditional payment systems.

There is no physical cryptocurrency, but balances are secured with public and private keys. These balances are maintained on public ledgers, along with all transactions, that are verified by a huge amount of computing power.

In early 2014, the Inland Revenue Service of the US declared that all crypto-currencies, including Bitcoin, would be taxed as property rather than currency. It was stated that all gains or losses from such currencies held as capital will be treated as capital gains or losses, while those held as inventory will attract ordinary gains or losses.

5. Bitcoin — Features

We have seen that bitcoins are becoming more and more popular and their usage is increasing at accelerated pace geographically. We will understand this process if we study different useful features of bitcoin that make them what they are.

Features of bitcoins

One of the most direct benefits of Bitcoins is that they are out of purview of governments, banks and other intermediaries who cannot interrupt user transactions or freeze Bitcoin accounts. The users experience greater freedom vis-à-vis dealing in national currencies. There cannot be inflation in case of bitcoins by printing more money as in the case of fiat currencies. By design, the number of bitcoins that can be minted is limited.

Since there is no way to identify, track or intercept bitcoin transactions, one of the major advantages of bitcoin usage is that taxes are not added onto any purchases.

Bitcoin transactions are relatively faster as compared to bank transfers in traditional currencies. Bitcoin transactions are done with nominal or sometimes zero transaction charges. These transactions are anonymous with no names involved. Every transaction is a public record which anyone can see. Your private key is the only link between you and your bitcoins. As long as the private key is secure, your money is safe. It is very easy to send and receive bitcoins because of ease of operation of bitcoin accounts.

Small amounts of bitcoin that are used as alternative units are: **millibitcoin (1 mBTC = 0.001 BTC), and satoshi (1 sat =0.000001 BTC) which is a millionth of a biticoin in value**.

You can use different wallets and tools for transacting in bitcoins.

Drawbacks of bitcoins

Let us examine the cons or drawbacks of bitcoins. These limitations of bitcoins make them less attractive and makes us seek better options. We have to somehow overcome or eliminate these limitations of bitcoins to make them user friendly.

- Bitcoins are a new emerging currency whose work is still in progress.
- Their value is highly volatile and unstable seeing wild fluctuations.
- It is internet-based, without which it cannot function.
- It is totally virtual currency and money can be lost due to computer breakdown or the absence or failure of a backup.
- Losing your private key can result in losing your bitcoins.
- There is no way that the transactions can be reversed or cancelled once completed.
- There can be misuse of anonymity of bitcoin transactions for criminal activities.
- The benefits of bitcoins are skewed highly in favor of early adopters.

- Bitcoin can be replaced with a better similar product and there is uncertainty regarding its continuation over a long period of time.
- Governments can ban bitcoins and make transactions in bitcoins difficult.
- The slowness of transaction verification is also an issue.
- The current version of bitcoins is not fit to handle very high volume of transactions.

6. Bitcoin — How do they work?

The process of creating or minting bitcoins is difficult to hack and this gives security to bitcoins. Another layer of security is the provision that every transaction has to be verified before being validated. This verification is effected through "mining". Mining is a process where some high-level computing like SHA256 decoding is done to verify transfers of bitcoins.

Bitcoins are stored in a “digital wallet”, which exists either on a user’s computer or on the cloud. The wallet is a type of virtual bank account that facilitates users to send or receive bitcoins, pay for goods and services or save their money.

How do bitcoin transactions work?

Every bitcoin account consists of a public key which works like a bitcoin address and a private key. Anyone can send you bitcoins if he/she knows your public key. To spend bitcoins, you have to use your private key for authentication. Every bitcoin transaction appears on the bitcoin network. The miners confirm the transactions after verification to validate them.

Addresses

An example of a bitcoin address is as follows:

```
73nRKoXJAUqKYYbzw6Nrqh9gW2p26zerpZ
```

There are 2^{160} or about 10^{48} possible addresses.

The corresponding private key is as given below:

```
5HuEupY3DNF87UypjFtXDTm4BVuAwZtAgYf94sMALPyakgafVnU
```

Private keys are of 256-bit length. There are about 10^{77} possible private keys.

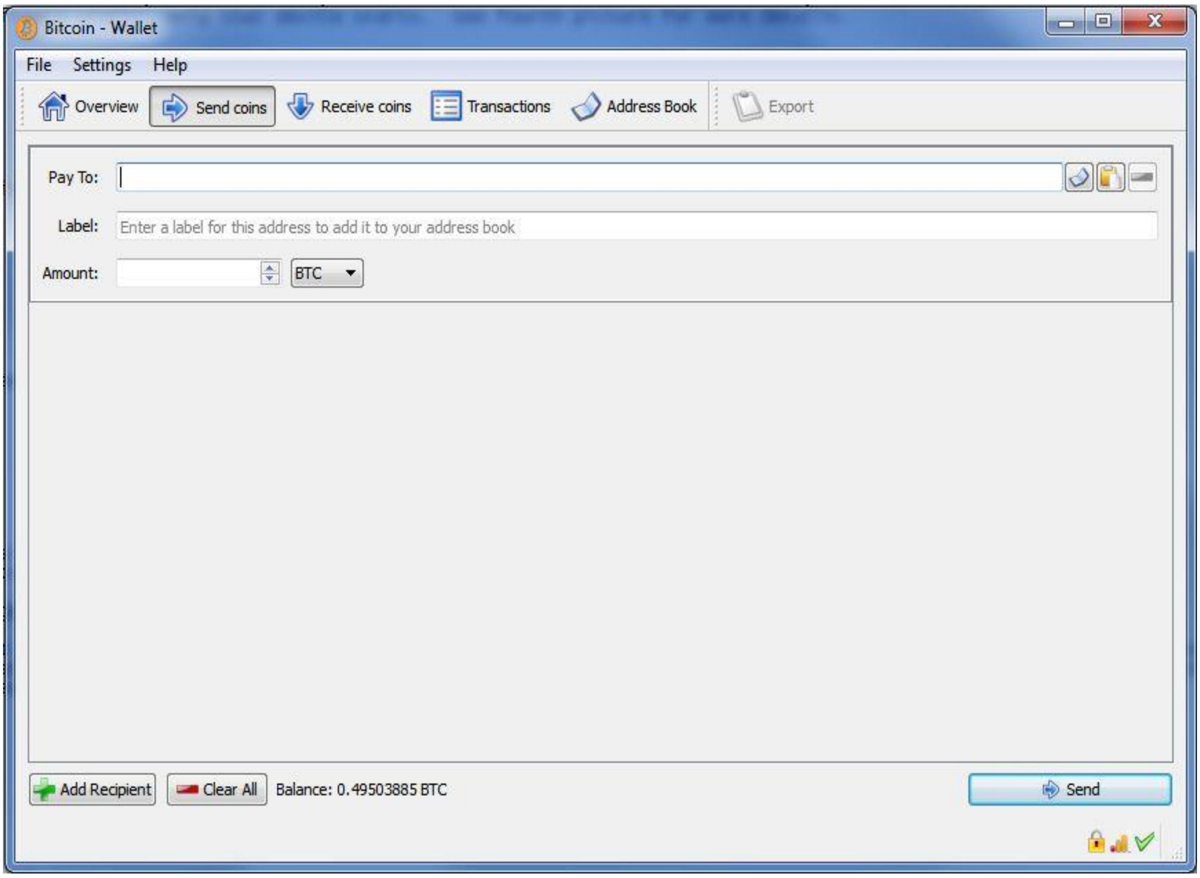
How to send bitcoins?

In the previous section we have seen how a bitcoin transaction works. Now, we shall discuss how to send bitcoins.

To buy some merchandise or pay for some services, you will have to send bitcoins to the address of vendor. To receive bitcoins, you will have to share your address with the vendor.

Following is the process of sending bitcoins to someone:

- Copy the vendor's address and open your bitcoin wallet.
- Click on the "Send coins" tab and enter the address in the 'Pay to' field to which you want to send bitcoins.
- If you have to send bitcoins to the same person or a group several times, you can create a label so as to find them in the address book.
- Enter amount in the next field and click send to complete the operation.



Pay To:

Label: Enter a label for this address to add it to your address book

Amount: BTC

Balance: 0.49503885 BTC

Confirmations

In the mining process, all transactions are collected in a container called block. A new block is created in about every 10 minutes. In case of small payments or transactions with trusted peers, confirmations may not be necessary. However, for large transactions to be considered safe, the norm is 6 confirmations.

Anonymity of Bitcoin transactions

The level of anonymity can be customized depending on the requirement. Every transaction from one address to another address is public. The analysis of the transactions through their addresses or public keys whose records are public is called traffic analysis. The larger the transfer the easier the traffic analysis.

To increase anonymity, mixing services are used. It is also advisable to create a new public key or new address for every transaction to ramp up security and anonymity. From the point of view of a user, Bitcoin is nothing but a mobile app or software that makes available a personal Bitcoin wallet which allows a user to send and receive bitcoins. However, at the backend, the Bitcoin network shares a humongous public ledger called the "block chain". This ledger carries the record of every transaction ever processed that makes it possible for a user's system to verify the validity of each transaction.

The need of consensus for compatibility

In order to maintain compatibility with each other, all users of Bitcoins have to use the software following the same rules. Bitcoin can only work correctly as long as there is a complete consensus among all the users. Thus, it is imperative that all users and developers maintain and protect this consensus.

Securing a blockchain

Bitcoins are not stored on your computer unless you host a node on the network. You carry a clone of the ledger which is secure as each block is hashed before being appended to the chain. This means, changing even one bit of any data on the previous blocks changes the hash of the ledger which marks it as counterfeit.

Hash function is an irreversible function that is used extensively in cryptography; the output of this function is shorter than the input. Validation of bitcoin transactions is just a process of quickly checking the keys like finding if the sender has the private key that can unlock any record in the ledger/blockchain.

7. Bitcoin — Wallet

As we have already discussed, Bitcoin is a virtual currency made up of **0s** and **1s**. They are collected and stored in a software portfolio called a **wallet**. A wallet identifies amount of cryptocurrency with unique addresses that are used to send and receive money.

A cryptocurrency wallet is a digital wallet that is used to store and transact in different cryptocurrencies. The crypto wallet doesn't exactly "store" the currency as real-world wallets do. Instead, it stores **public** and **private keys** which help in sending and receiving money. Bitcoin owners save bitcoins in either an online wallet or a paper wallet which are similar to a physical wallet. Wallet holds keys to each bitcoin, securing them and preventing any fraud.

What are public and private keys?

The public key is the address to which others can send you the money, while the private key is that which you will use to send money to anyone. It is important that ONLY you should know your private key; otherwise anyone who knows your private key can steal your money.

You should not lose or reveal your private key come what may. Otherwise, losing your private key is similar to losing your money. You should use at least two different techniques to save and store your private keys.

As of now, let us discuss two methods of storage that can be used to store crypto money; hot storage, and cold storage.

As a recap, **a wallet is used to:**

- Send and receive money as cryptocurrency
- Collect and store coins created by the miner
- Synchronize blockchain with all nodes of the network

Opening a wallet is fairly simple; one can download free and paid bitcoin wallets from internet. Some deal only in bitcoins while others handle multiple cryptocurrencies.

A Bitcoin wallet is simply an app, software, website, or device that manages Bitcoin private keys for you.

Types of Bitcoin Wallets

There are several types of wallets available in the market. They can be of several types as follows

- Hardware
- Paper
- Mobile
- Desktop
- Web

Paper Wallets

A paper wallet is a piece of paper on which the public address and private address are printed, usually in the form of QR code. Public address is used to receive bitcoins, and the private address is used to send or transfer the bitcoins stored at that address. The paper wallet should be used securely and not revealed or lost. The paper wallet can be generated by using services like **Bitcoinpaperwallet** or **Bitaddress**, and then can be printed out.

Mobile, Desktop and Web Wallets

These are software apps available on mobile phones, desktops, laptops or websites that allow bitcoin transactions.

For those people who use Bitcoins frequently, paying for goods and services, a mobile bitcoin wallet is a necessary tool. A mobile app runs on your smartphone, has your private keys and allows making payments directly from your phone.

A full Bitcoin client would require access to the complete Blockchain ledger, which needs several gigabytes of storage. Therefore, mobile wallets use simplified payment verification (SPV) technology which works with very small subsets of the Blockchain. In spite of being a convenient on-the-go solution for Bitcoin transactions, mobile wallets are very susceptible to hacker attacks and also if the mobile is lost, others can access the wallet.

Hardware Wallets

A hardware wallet is a physical electronic device to **secure** bitcoins. The hardware wallet must be connected to your computer or smartphone, before bitcoins may be spent.

The three most popular and best Bitcoin hardware wallets are as follows:

- Ledger Nano S
- TREZOR
- KeepKey

Hardware wallets are the preferred choice if large amounts of bitcoins need to be stored and are secure, reliable, and convenient. Bitcoin hardware wallets isolate private keys from internet-connected devices that are vulnerable to hackers. Your private keys are held in a secure offline environment on the hardware wallet.

Hot Wallets

Hot wallets are Bitcoin wallets that run on internet connected devices like a computer, mobile phone, or tablet. Private keys are secret codes that hot wallets generate on an internet connected device. As such we cannot say these private keys are completely secure.

Hot wallets are like your physical wallets which you use to store some cash, but not your life savings. Hot wallets are useful if you make frequent and small payments, but are not suitable to store a large amount of bitcoins.

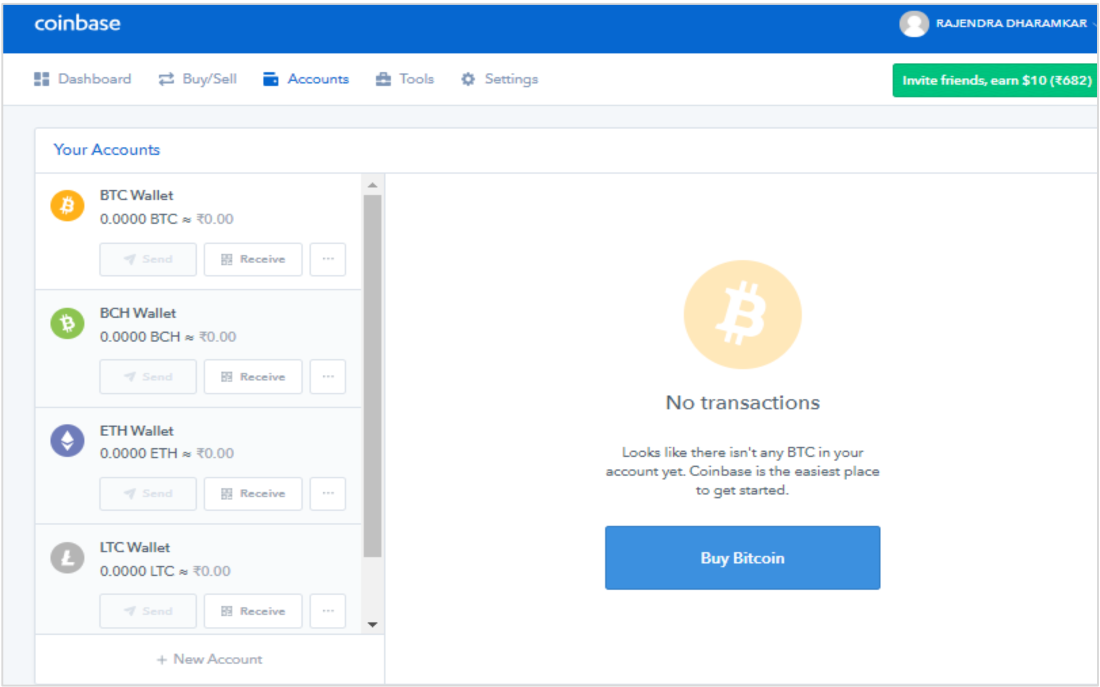
Software wallets allow us to send and receive bitcoins and are mostly free. There are some paid software wallets which provide some extra value-added services.

Opening a Bitcoin Wallet Account

We can go to sites like **coinbase.org** and sign up with our name, email id and phone number. Opening a wallet account is like opening a bank account where we can send, receive and store money in bitcoins.

In Coinbase, we can create multiple wallets which is a great way to organize the record of your expenses and savings. By default, there are following wallets in Coinbase, namely, **Bitcoin BTH wallet, Bitcoin Cash BCH wallet, Ethereum ETH Wallet and Litecoin LTC Wallet.** You have a wallet in US dollars as well so that you can buy and sell the cryptocurrencies using US dollars.

Each account on Coinbase is a bunch of addresses. New addresses are generated for each transaction on Coinbase automatically and stay mapped with your account forever and it is secure to reuse them.



RAJENDRA DHARAMKAR

Your Accounts

BTC Wallet
0.0000 BTC ≈ ₹0.00

BCH Wallet
0.0000 BCH ≈ ₹0.00

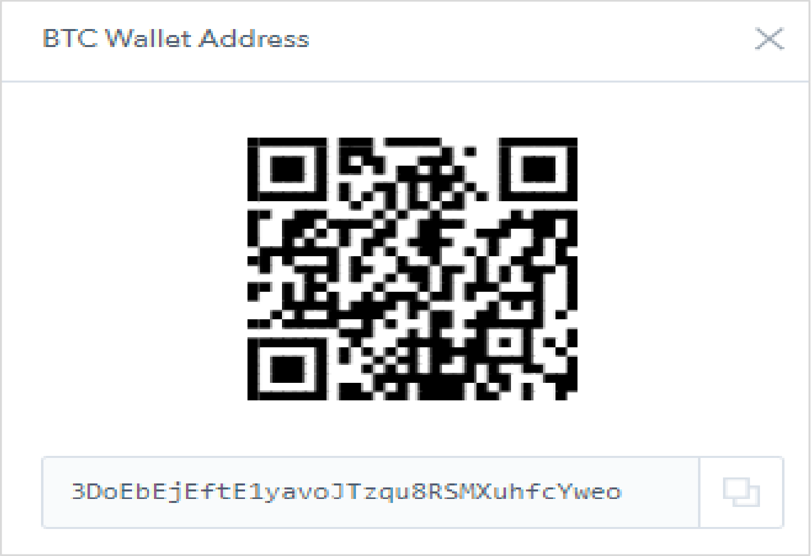
ETH Wallet
0.0000 ETH ≈ ₹0.00

LTC Wallet
0.0000 LTC ≈ ₹0.00

No transactions

Looks like there isn't any BTC in your account yet. Coinbase is the easiest place to get started.

Each wallet account is associated with an address and QR code as displayed. For example, selecting bitcoin wallet and then clicking on the BTC wallet address shows below address along with its QR code.



BTC Wallet Address

3DoEbEjEftE1yavoJTzqu8RSMXuhfcYweo

We can download bitcoin software client which might take a few hours to download all blocks to our computer that now acts as a node in the network. We have to ensure that there is enough bandwidth and storage for full block chain size which is over 145 GB. It is also possible to use a wallet without downloading the bitcoin client.

8. Bitcoin — Mining

With Bitcoins, the process of creating the currency is called mining. Bitcoin miners use specialized software and hardware to verify bitcoin transactions and to solve complex math problems and are compensated by a certain number of bitcoins in exchange. This is how bitcoin currency is issued and anyone can mine bitcoins. We can use mining to create or earn our own bitcoins. Presently, a successful miner is rewarded with 25 bitcoins for every new block that is created roughly for every 10 minutes. This mutually agreed value will halve after every 210,000 blocks are added to the chain.

Bitcoin mining involves verifying and adding transaction records to Bitcoin's public ledger of past transactions or blockchain. The blockchain is used to confirm transactions as having taken place to the rest of the network.

Bitcoin nodes use the blockchain to legitimate or validate genuine Bitcoin transactions and prevent double spending of bitcoins, that is, stop re-spend of coins that have already been spent elsewhere.

Bitcoin mining is willfully designed to be resource-intensive and difficult so that the number of blocks mined each day by miners remains moderate and steady. Individual blocks are also required to contain a proof of work to be considered valid. This proof of work is verified by other Bitcoin nodes every time they receive a block. Bitcoin employs the hashcash proof-of-work function for its working.

The primary goal of mining is to facilitate Bitcoin nodes to reach a secure, tamper-proof consensus. Mining is also the mechanism used to introduce Bitcoins into the bitcoin eco system: Miners earn (if any) transaction fees as well as a "reward or bounty" of newly created bitcoins.

This both serves the purpose of distributing new coins as well as motivating people to secure the system.

Proof of work

A proof of work is a piece of data which was resource-intensive and time-consuming to produce so as to satisfy certain requirements.

Producing a proof of work is usually a random process with low probability, and a lot of trial and error is required before a valid proof of work is generated. Bitcoin uses the Hashcash type of proof of work.

Additionally, the miner is awarded the transaction fees paid by users. The fee is a sort of incentive for the miners to include the transaction in their block. In the future, the fees will make up a significant percentage of mining income.

There are two main types of mining: **Solo** and **Pool.**

Solo Mining

Solo mining is done alone or on your own. With the configuration of a normal desktop or laptop, it would take years to earn actual bitcoins as mining requires enormous computing power.

Pool Mining

The second method we can use is **pool mining**. It involves signing up for an account with any one of the different pooling sites. Using their software and hardware, these sites pool the mining efforts of a lot of people's computers. Every person in the pool gets small number of bitcoins as his share as a reward. For individuals, pooling is preferable over solo mining.

BitMinter

BitMinter is a bitcoin mining pool that aims to make it easy for anyone to make bitcoins. It is one of the oldest pools. Since its opening in 2011, over 450000 people have registered accounts with it. In the earlier period, CPUs and GPUs were used for bitcoin mining. Now we need to have specialized Application Specific Integrated Circuits (in short ASIC) machines for bitcoin mining. The speed of these machines is given by their hash rate which is presently of the order of tera hashes/second or T H/s.

ASICs took over mining in 2013. Mining just one bitcoin with an ordinary PC would take quite lot of time. You will need a 1 TH/s or faster ASIC machine to start a small mining operation at your home.

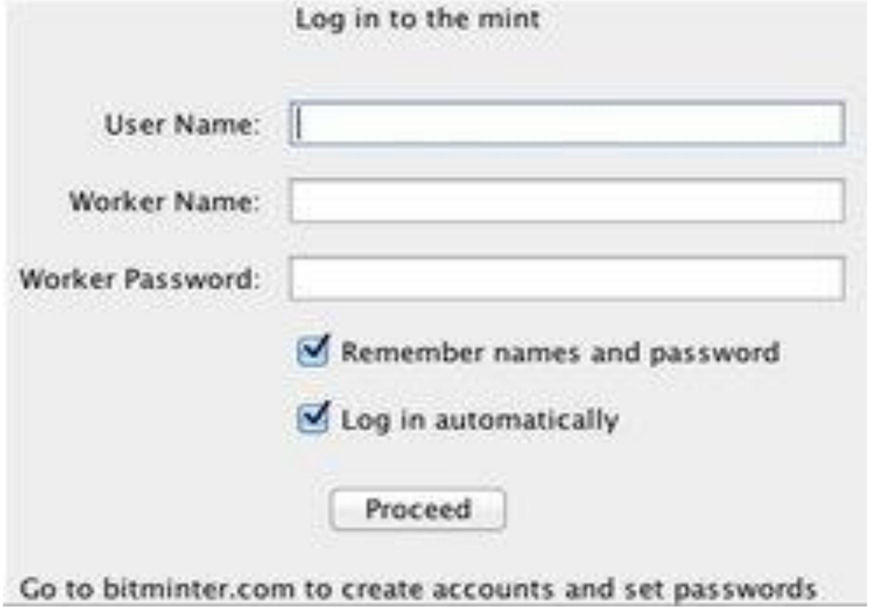
Using BitMinter for Mining

Below is the process to use BitMinter for mining:

Step 1: First, we signup with **BitMinter site** using our google or yahoo mail accounts and then confirm our mail id by clicking on the link in our mail received from BitMinter.

Step 2: We set up a **Worker account** with a worker name and worker password besides the username created when creating BitMinter account. We link the Bitminter Client to the worker account.

Step 3: Then we log in by **filling up account details** as shown below.



Log in to the mint

User Name:

Worker Name:

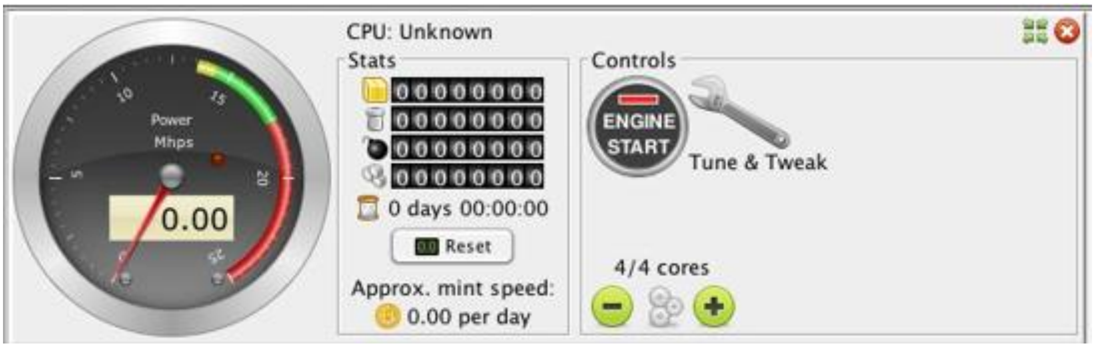
Worker Password:

☑ Remember names and password

☑ Log in automatically

Go to bitminter.com to create accounts and set passwords

Step 4: After this by opening the **BitMinter Client application**, we get following console as shown below:



CPU: Unknown

00000000

00000000

00000000

00000000

0 days 00:00:00

Approx. mint speed:
0.00 per day

4/4 cores

Step 5: We press the Engine Start button to start mining. We have to ensure that our machine clocks a hashrate speed of atleast **25 million hashes/second** or **25 M H/s**.

Step 6: We will also need to change a few settings regarding automation. We can leave our machine on all day and all night.

Step 7: We can go to **Settings > Options** to change these settings. Automated devices are a list of devices that you set so that they start automatically when the software starts.

Step 8: We will let our machine run at night increasing the prospect of making more number of bitcoins.

Mining secures the transactions by finding random strings that make the block to hash to a value with lot of leading zeros. The more the zeros, the more difficult it is to decrypt. Mining bitcoins does not mean finding new bitcoins; these are awarded by the network for completing validation of all outstanding transactions of a block and solving some complex math puzzle.

Ways to Earn Bitcoins

The best way to earn bitcoins is to find and execute work paying in bitcoins. We can purchase the bitcoins as well. Lastly, if we want to earn them the hard way, we should go for mining. To mine bitcoins, we can buy some cheap hardware on sites: ebay.

9. Bitcoin — Exchanges

Cryptocurrency exchange is where users can come together and trade in different cryptocurrencies and fiat currencies. Online currency exchanges are websites that are used for trading, that is, buying or selling bitcoins for dollars or any other currencies like Euros, Pounds, Yen, etc. We can transfer money through any online currency transfer services to trade in bitcoins on these exchanges.

Exchanges of Bitcoin

The following exchanges dominate Bitcoin market:

Bitfinex: Bitfinex is the world's #1 Bitcoin exchange if trading volume in US dollars is considered. Here about 25,000 BTC are traded every day.

Bitstamp: Bitstamp, founded in 2011, is one of the oldest exchanges of Bitcoins. It is presently the second largest exchange in the world based on USD volume, with around 10,000 BTC traded per day.

OKCoin: This bitcoin exchange is based in China but trades in US Dollars.

Coinbase: This was the first regulated Bitcoin exchange in the United States. About 8,000 BTC are traded daily on this exchange.

Kraken: Kraken is the #1 trading exchange in Euros handling nearly 6,000 BTC transactions per day.

10. Bitcoin — Trading

Bitcoin trading can be highly profitable for professional investors as well as beginners. The market is new, highly fragmented and has huge spreads. It is open to arbitrage and margin trading. Thus, it is possible for many people to make money trading bitcoins.

Arbitrage in bitcoins

Arbitrage is basically buying a security or asset like bitcoin in one market and simultaneously selling it in another market at a higher price, making a profit from the temporary difference in prices.

Margin trading in bitcoins

Margin trading is the process in which a trader borrows money from the broker to either buy or sell more stock or bitcoins than that trader would have been able to with his funds. It is like a short-term loan that increases the leverage and buying power of the trader.

Each bitcoin bubble drums up a hype that puts Bitcoin in the news. The media attention makes more people interested in bitcoins, and the price rises until the hype dies down.

Trading in bitcoins

Trading in bitcoins is simple as bitcoin is global currency and easy to send anywhere. Bitcoin has very little barrier to entry. In many cases, even verification is not required for trading in bitcoins. Because of steep increase in bitcoin prices, investors and speculators are attracted to trading to make profits.

There are no official bitcoin exchanges or official bitcoin price. This makes arbitrage trading possible. Unlike other stock trading, bitcoin trading works 24/7.

Bitcoin trading is exciting because of Bitcoin's wild price movements, its global nature, and 24/7 trading. It is important, however, to understand and remember the risks that come with trading in Bitcoins.

Types of trading

When we enter the trading system, there are two ways we work. One is trading on a day-to-day basis or doing long term investing, where there is buying and then waiting for their value to appreciate over time.

These two strategies can be followed simultaneously by day-to-day trading in some bitcoins while investing in some other bitcoins for long term gains. In both cases, we have to open an account on one of the several crypto-currency exchanges.

Coinbase and trading

One of the best options is to open an account on Coinbase, a safe and reliable crypto currency exchange. On Coinbase, we can buy Bitcoin (BTC), Ethereum (ETH) and Litecoin

(LTC) currencies either by making a transfer in Euros, or by direct purchase using a credit card. The fee for each transaction is a nominal 4%.

Coinbase is extremely simple and intuitive, and this makes it the perfect choice to start trading in important cryptocurrencies now on the market. **mt.gox** used to be a popular Japanese exchange in bitcoins till a scam led to its closure.

11. Bitcoin — Glossary

In this chapter, we shall learn bitcoin glossary which describes over 50 bitcoin terms.

ADDRESS

A bitcoin address allows us to send and receive bitcoins on the bitcoin network. It is also the public key or address that is used to transact in bitcoins.

ALTCOIN

Altcoin is a group of ‘alternate’ cryptocurrencies other than bitcoins. Examples of altcoins include Ethereum, Litecoin and PPcoin.

ASIC

An **Application Specific Integrated Circuit** (ASIC) is built specially to process the SHA-256 hashing equations that are used in mining bitcoins.

ASIC MINER

An ASIC miner is the latest mining hardware used in bitcoin mining. It is used to calculate the SHA-256 equation faster than a CPU or a GPU. ASIC miners are custom-built and connect to the network through a wireless or Ethernet connection.

BITCOIN PRICE INDEX (BPI)

The **Bitcoin Price Index**, designed by Coin Desk, shows the average bitcoin prices across the top global currency exchanges.

BITCOIN WHITEPAPER

The Bitcoin Whitepaper dubbed as the Bible of the Bitcoin ecosystem, was submitted by the currency’s mysterious founder, Satoshi Nakamoto, in 2008. It gives a detailed description of the bitcoin protocol, and is a good reference material for newbies and experienced people alike.

BLOCK CHAIN

This chain contains the records of all bitcoin ‘blocks’ that have been mined since the start of the currency. The chain is designed such that each block contains the hash of the preceding block, which makes the chain secure against counterfeit mining operations.

BLOCK REWARD

A reward is given to each miner who completes a transaction block. It can be in the form of coins or transaction fees; Bitcoin network currently rewards 25 coins for each completed block. Once the threshold of blocks has been mined (which currently stands at 210,000 blocks) the reward is halved; such an event as described above is called halving. The next halving is due to take place in 2020. Then the reward would become 12.5 coins for mining one block.

BTC

BTC is the abbreviation of bitcoin, similar to USD and GBP for US dollar and Great.

BITCOIN CLIENT

This is the software program that connects a device, whether a desktop computer, laptop or mobile phone to the bitcoin network.

CONFIRMATION

A confirmation of a transaction is its successful hashing into the block of a blockchain. It can take up to ten minutes, though larger transactions may require up to 6 confirmations.

COLOURED COINS

Coloured coins is a proposed new feature of bitcoins that allows users to define their own attributes of the currency. It is intended that users could mark a bitcoin as a physical asset, which could then be exchanged as a token for other property.

COINBASE

The name of a bitcoin wallet operator that offers payment processing for merchants, and acts as an intermediary in bitcoin exchanges.

COIN AGE

A coin's age is calculated by the product of the currency amount and the period of time it has been owned.

CRYPTOCURRENCY

A cryptocurrency is considered legal tender by consensus and is secured by using cryptography based on mathematical formulas.

CRYPTOGRAPHY

It is the field where math formulas and algorithms are used to create the codes that encrypt and decrypt information.

DOUBLE SPENDING

This is the criminal act of spending the same bitcoins more than once. The user completes a transaction using his bitcoins and then makes a second transaction with some other party using the same bitcoins. So confirmation is necessary to validate a transaction and prevent double spend. So zero-confirmation transactions are risky as they could involve double spending.

DUST TRANSACTION

This is a transaction that has a record in the block chain but has very little worth. Steps are being taken to minimise the number of dust transactions that take place by introducing a minimum transaction amount.

ECDSA

ECDSA is the name of a code and an abbreviation for Elliptic Curve Digital Signature Algorithm. It is used in the Bitcoin protocol to sign transactions.

ESCROW

An escrow is a kind of third party online wallet that stores funds securely during a transaction between two parties. It is used in cases where two parties cannot transact bitcoins till certain conditions are met, and want to ensure that their money is not 'stolen' digitally.

FAUCET

A faucet is the method of mining a certain number of coins when launching a new cryptocurrency, and then giving these away in order to promote interest in the new currency. There are several bitcoin faucet sites that give away very small amounts of bitcoins to promote them

FIAT CURRENCY

A Fiat currency is another name for token money used across the world that has been declared legal tender by governments and central banks and is not backed by a physical commodity.

FORK

A fork in a blockchain is said to occur when one group of miners starts hashing a different set of transaction blocks. It can also happen when a new version of the bitcoin client is introduced. A fork is deemed successful if it becomes the longer version of the chain.

GENESIS BLOCK

The original block in a chain.

GPU

This is a graphical processing unit, as found in standard PC graphics card. As GPUs are designed to process huge data at faster speeds in pixel-heavy computer games, they are also perfect for processing calculations required in cryptocurrency mining.

HASH

A hash is the mathematical processing done during bitcoin mining. It is a complex process that makes the currency secure and renders decryption very difficult and alteration of the output detectable.

HASH RATE

Hash rate counts the number of hash calculations done in a second. This generally indicates how fast and successful a mining operation is.

INPUT

Input shows where a bitcoin transaction has originated, and is generally a bitcoin address, unless it is a generation transaction meaning that the bitcoin has been newly-mined.

LITECOIN

It is a type of alternate crypto currency that uses the Scrypt hashing formula.

MEGAHASHES/SEC

It is the number of hashes per second measured in millions of hashes (a Megahash).

MARKET ORDER

A market order can be placed at an exchange when buying or selling bitcoins instantly, and at the prevailing market rate.

MBTC

A small amount: one thousandth of a bitcoin (0.001 BTC).

MICRO-TRANSACTION

Paying a very small amount as part of a transaction online, these are hard to execute under traditional payment systems. It is like paying for a bag of snack with a credit card.

MINING

Mining can be done by anyone who wants to mint some new bitcoins for his wallet. For this he should validate a block of outstanding transactions and solve cryptographic equations using some hashing algorithms.

NODE

Every connected computer in the bitcoin network that relays transactions to other computers is called a node.

ORPHAN BLOCK

Any block that was part of a discarded fork is known as an orphan block. This is not part of the valid blockchain.

OUTPUT

The output is the final address of a bitcoin transaction. It is quite possible that there can many outputs for a single transaction.

PAPER WALLET

This is a physical record of public bitcoin addresses and their private keys. It can be a piece of paper, and presents a safer way to store bitcoins that cannot be hacked or corrupted.

POOL

A group of miners working in tandem is called a pool. These miners pool their work together to mine a block, and then share the reward accordingly. Mining pools improve the chances of successfully mining a block.

PP COIN

PP coin is sometimes known as peer coin or P2P coin. This is an altcoin that uses a ‘proof of stake’ calculation apart from proof of work for validation of work done.

PRIVATE KEY

The security of private key is important in keeping bitcoins safe. The private key of an account is unique, and only the owner should know the private key. It is usually a string that signs a digital communication hashed with corresponding public key.

PROOF OF WORK

This calculation is used to give reward for mining work done in bitcoins. It does take a lot of time and effort to hash a block successfully, and this is considered as a proof of work which is rewarded appropriately.

PUBLIC KEY

A public key is a bitcoin address, which is public or known or accessible to everyone. When a public key is hashed with a private key it makes a digital communication secure.

QR CODE

A QR Code is a graphic that contains a data sequence. QR codes are scanned by mobile phones and other devices and are used in encoding bitcoin addresses and in facilitating bitcoin transactions.

RIPPLE

Ripple is a payment network on which users exchange any currency. Payments are done on an ‘IOU’ basis and are based on trust. The network consists of nodes and gateways operated by authorized people.

SATOSHI

Satoshi, the name of the creator of bitcoin, is also the smallest denomination of bitcoin: 1 sat = 0.00000001 BTC.

SCRYPT

A proof of work system meant for altcoin miners; it is relatively simple as compared to SHA-256; that is why altcoins using Scrypt are mined more than those using CPU and GPU set-ups.

SIGNATURE

When private and public keys are hashed together, they make a digital signature that authenticates the originating address of a bitcoin transaction.

SHA-256

It is the standard cryptographic equation that is used in the proof of work system of bitcoin mining.

SPV

The Simplified Payment Verification makes it possible for users to verify their transactions without downloading the massively-sized full block chain. Here users make by simply downloading the block headers only.

TRANSACTION BLOCK

The transaction block is the record of transactions which are collated and hashed, and then appended to the block chain.

TRANSACTION FEE

Some bitcoin transactions will be charged a small fee when sent across the network. This fee is paid to the miner who has successfully hashed the block that contains that transaction.

UBTC

Another very small denomination of bitcoin; a uBTC is a ‘microbitcoin’

1 uBTC = 0.000001 BTC

VOLATILITY

The fluctuations in price of bitcoin are defined as its volatility.

WIRE TRANSFER

A wire transfer is a method of transferring bitcoin currency to and from a bitcoin exchange. This transfer is done electronically, and can be secured to a bank account anywhere in the world.

ZERO-CONFIRMATION TRANSACTION

It is a transaction where a vendor sells a product or service in return for a bitcoin payment, yet the transaction cannot yet be confirmed by a miner or added to the chain. This is where ‘double spending’ can happen.

12. Bitcoin — Applications

The following is a list of applications of bitcoins

- 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.

13. Bitcoin — Future

Since Bitcoin is a new emerging technology which is underway, unforeseen developments can make its existence and continuation difficult. Concerning its security and future, there are numerous questions which no one can answer. How far can we trust Bitcoins? Are they a bubble that is going to burst? Are they a passing phenomenon and a fad that would fizzle out over a period of time? Or are they going to stay put and perhaps dominate other currencies in future?

As of now, bitcoins are mostly unregulated, however this may change. Governments are worried about losing taxes and control over the currency. They may bring legislations to regulate bitcoin which may hugely impact the advantages that bitcoins have over other currencies. The volatility of bitcoin prices is one huge issue. The wild fluctuations in its index is sign of such volatility. In recent years, bitcoin prices have risen exponentially and after some corrections have dipped but still they are on the high side. Many expect that the price will further increase.

Favoring Growth Factors

The things that favor the growth of bitcoin adoption are as follows:

- There are limited number of bitcoins.
- The awareness about bitcoins is growing and so their acceptance and adoption.
- The number of bitcoin transactions is increasing day by day.
- A large number of wealthy people do not want government's regulations on their wealth and would rather prefer storing in bitcoins.

Next halving is scheduled to occur in 2020. This will further decrease the rate of supply of bitcoins while bitcoin usage would have increased manifold by 2020. As of now, the number of bitcoin transactions is way behind the number of credit card transactions and the former has to significantly increase to realize the full potential of bitcoins.

Some of the issues which have to be tackled to help bitcoin's growth are as follows:

- Bitcoin transaction time or the time required to get confirmations is still on the high side as compared to credit or debit card transactions.
- The security of Bitcoins has become a major issue. As the usage of Bitcoin is increasing, hacking of bitcoin wallets and even exchanges has been more widespread.
- As of now Bitcoins are too technical for common people and are not so user friendly. It is difficult for people to understand why bitcoin prices are so volatile, why transaction time is so high and how they should safeguard their bitcoins.

Governments of several countries including India are discouraging legal use of Bitcoins as they understand that Bitcoin is a parallel financial system beyond their control. However, countries like Japan, Australia and several European countries have made

Bitcoin legal as they realized that they cannot stop the usage of bitcoins. Some countries have banned bitcoin exchanges. People are using global exchanges to hide their transactions. Meanwhile India and China have been discouraging Bitcoin transactions. China has tried to ban all Bitcoin Exchanges in their country while India has not banned any exchange. Zebpay and Unocoin are Bitcoin Exchanges that are under operation in India. They require submission of KYC documents before executing any Buy or Sell transaction.