



# CERTIFIED BITCOIN PROFESSIONAL

[Document subtitle]

## Abstract

[Draw your reader in with an engaging abstract. It is typically a short summary of the document.  
When you're ready to add your content, just click here and start typing.]

*Naveen Sharma and James Kerr*

# **CERTIFIED BITCOIN PROFESSIONAL**



# INTRODUCTION

The CryptoCurrency Certification Consortium (C4) establishes cryptocurrency standards that help ensure a balance of openness & privacy, security & usability, and trust & decentralization.

As the Cryptocurrency, Bitcoin and Blockchain space is exploding with new start-ups, these companies and those already established in the space are constantly seeking talent with a strong understanding of relatively new Bitcoin technology stack. Prior to C4 there was no way for these hiring managers and placement firms to validate Bitcoin knowledge in their candidates like they can with other knowledge such as networking, security, and accounting. C4 provides certifications so that professionals can assert their knowledge in cryptocurrencies the same way they are able to assert other skills.

## BOARD OF DIRECTORS

*Andreas M. Antonopoulos*

*Andreas is the author of Mastering Bitcoin, CTO of Third Key Solutions and a prolific Bitcoin speaker. Andreas has briefed governmental bodies about Bitcoin and served as a champion to Bitcoin since he was introduced to the technology.*

*Vitalik Buterin*

*Vitalik is the inventor of the Ethereum Project, a next-generation cryptocurrency designed with advanced programmability and customization in mind. Vitalik is an editor for Bitcoin Magazine and a contributor to Bitcoin Core. He has been invited to speak internationally on topics including Bitcoin, Ethereum, and information theory.*

*Joshua McDougall*

*Joshua's dedication to the legal support industry has afforded him the opportunity to spread cryptocurrency understanding to top law firms in Canada. He is also a co-founder of Coindroids, a role playing game played entirely within cryptocurrency blockchains.*

*Pamela Morgan*

*Pamela is an attorney, entrepreneur, and educator. She is CEO and founder of Third Key Solutions and founder and attorney at Empowered Law PLLC. She advises numerous organizations in the Bitcoin, blockchain, and education spaces and regularly speaks at events around the world on topics including law, education, and entrepreneurship.*

*Michael Perklin*

*Michael is Head of Security and Investigative Services at Ledger Labs Inc., a blockchain consulting firm operating out of Toronto, Canada. Michael is also board member of The Bitcoin Foundation and a founding member and director of the Bitcoin Alliance of Canada (BAC) where he had the opportunity to brief the Canadian Senate about the investigative impacts of Bitcoin technology. Michael has been invited to speak internationally on topics including digital forensics, information security, and Bitcoin security.*

## **ABOUT THE CERTIFIED BITCOIN PROFESSIONAL EXAM**

**WHY YOU SHOULD TAKE THIS EXAM?**

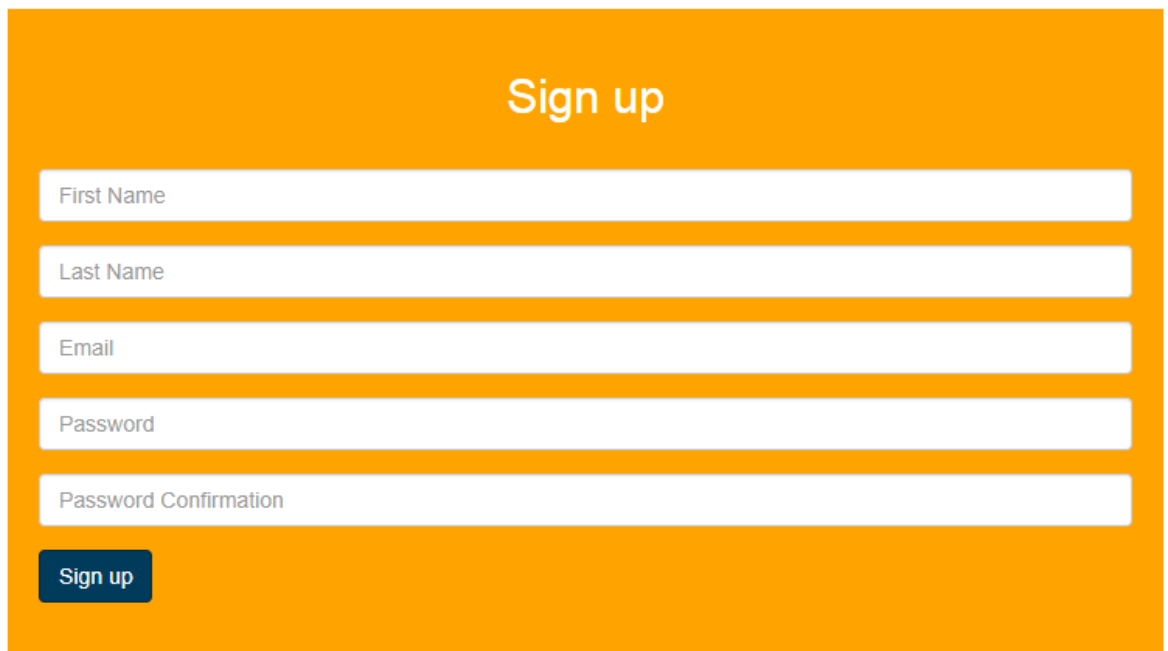
Why Should You Earn A Bitcoin Certification?

## REGISTERING FOR THE EXAM

Registering for the exam is a simple process, make sure you have sufficient bitcoin balance in your bitcoin wallet to pay for the certification fee. At the point of writing this book the fee for the certification was *0.01017 BTC*

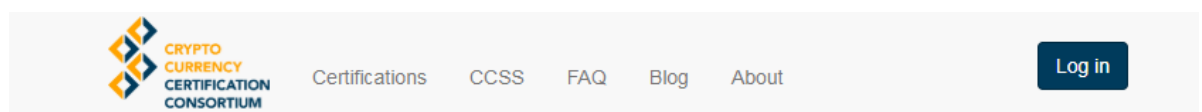
Now follow below steps to register for the exam

1. Go to <https://cryptoconsortium.org/users/new> in your favourite internet browser

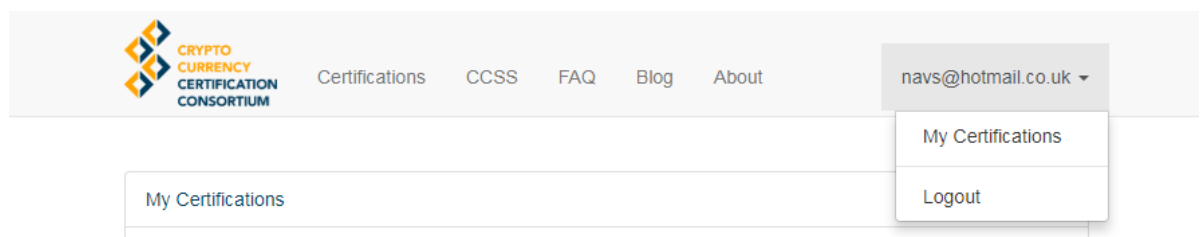


The image shows a 'Sign up' form on an orange background. The form includes five input fields: 'First Name', 'Last Name', 'Email', 'Password', and 'Password Confirmation'. Below these fields is a dark blue 'Sign up' button.

2. Follow sign up instructions, when successfully registered log back into the web site.



3. When successfully logged in click on **My Certifications** link





4. Now click on **Enroll** link to see instructions for paying exam fee

My Certifications
My Information
Logout

Certifications

Enroll

5. You will be presented with a bitcoin address and fee amount that you will have to pay, make sure you will pay the fee in full including any transaction fee required by your exchange.
6. When exam fee is received in full, you will be ready to take the exam

Examination Fee				Paid In Full
Price (CAD)	Amount paid (CAD)	Amount Due (BTC)	Address	
\$99.99	\$99.99	0.0	1KxMpJyuhrbjKmt972ZNj5e7ZK2NY9Q9YG	<div>View QR Code</div>



# HISTORY OF MONEY AND LEDGER-BASED ECONOMICS

## Ledger:

Ledger by definition is a book for keeping record of all the transactions. Since ancient times, ledgers have been at the heart of economic transactions to record contracts, payments, buy-sell deals or movement of assets or property. The journey which began with recording on clay tablets or papyrus, made a big leap with the invention of paper. Over the last couple of decades, computers provided the process of record keeping and ledger maintenance great convenience and speed. Today, with innovation, the information stored on computers is moving towards much higher forms which is cryptographically secured, fast and decentralized.

A simple example of a ledger is the one maintained by your local bank to keep record of all your transactions. It keeps record of all monies coming in (credit) and going out (debit), current balance is sum of all such transactions. These transactions are maintained and stored electronically in their central systems.

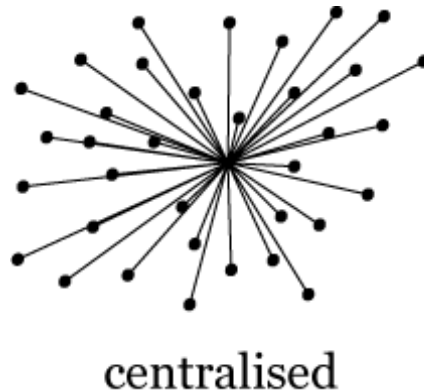
DATE	PARTICULARS	DR.	CR.	DR. OR CR.	BALANCE	DATE	PARTICULARS	DR.	CR.	DR. OR CR.	BALANCE
19-5-51						19-5-51					
Feb 23	Income		41.52		41.52	June 30	Income		20.97		20.97
March 17	Dr		74.65		116.37	July 4		10.00			
19		5.00				12 Dr			101.92		
		13.25						5.00			
23 July		56				18		50.00			
23		10.00				27 July		72			
24		17.75				Aug 29		2.95			
		10.85				Nov 29 Dr			250.00		
April 1		6.00				Dec 3 Dr			100.00		
		10.00						250.00			
12		17.00				8		10.00			
18 Dr			150.00			12		17.00			
19		128.80						45.00			
25		10.00				14 Dr			476.98		
28 July		1.00						21.70			
30 Dr		1.06				Oct 1		16.77			
			32.00			21		50.00			
June 7		10.00				21		20.00			
13		20.00				27		23.67			
24 Dr			104.69			Jan 5/6		28.00			
Balance		120.52			20.97	10 Dr			946.69		965.99

Ledger maintained on a book

## Centralized Ledgers

A centralized ledger also known as general ledger contains all the accounts for recording transactions relating to a company's assets, liabilities, owners' equity, revenue, and expenses. Anything in the world which has a financial value needs

a ledger. In modern days computerized ledger came into existence i.e. Enterprise resource planning (ERP), the general ledger works as a central repository for accounting data transferred from all sub ledgers cash management, fixed assets, purchasing and projects. The general ledger is the backbone of any accounting system which holds financial and non-financial data for an organization. The collection of all accounts is known as the general ledger. In a manual or non-computerized system this may be a large book. Each account in the general ledger consists of one or more pages.



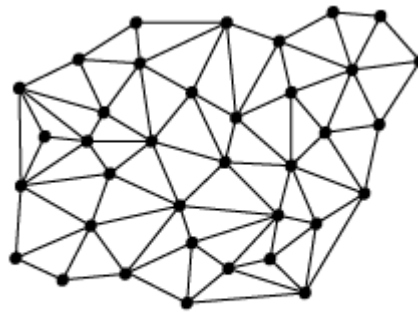
In centralised ledger systems e.g. your high street bank that keeps record of your financial transactions has total control over which transactions are posted on the ledger because it's a centralized asset ledger which lists all transactions that is controlled by a single entity, such as a bank statement, by this they can fine you and directly take money away from you without your consent. This is a danger of centralized ledgers because if the entity-in-charge has malicious intent, it can do some serious damage to its clients.

Also in case of a malicious attack on the central database, the attacker can manipulate transactions.

Another disadvantage of a centralized ledger is the controlling entity can shut down without notice and transactions will no longer be processed. Giving this kind of authority to someone will result in error, whether it be accidental or not. We have recently seen this when Lehman Brothers went under administration during 2008 financial crisis

## Distributed Ledger

A distributed ledger is essentially append only asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network (Here network is nothing but all the people who are connected each other with their computers) can have their own identical copy of the ledger.



distributed

Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically by Blockchain protocol.

## Blockchain

A Blockchain technology is a shared public timestamped transaction ledger that everyone can inspect but not subject to any form of central control. And while it offers potential for a variety of applications, its most famous is providing the platform for virtual currencies like bitcoin

Blockchain ledger is a record of a chronological series of transactions that a network of nodes distribute to each other. The first instance of a Blockchain was Bitcoin. A bitcoin unit in a Blockchain represents an unspent transaction output that is written to a globally distributed, replicated, undeletable, timestamped database. It simply means that anyone in the world gets the same answer when querying the system. The value in this technology is that anything can be etched into this type of ledger to create a distributed consensus protocol. This could be money, title, copyright, notarization, real-time triple entry accounting, data storage, stocks, votes, digital or tokenized physical assets; it's essentially creating a distributed proof of ownership that is logically centralized and organizationally decentralized. Before the Blockchain, there was no sort of computational system that enabled this

## **Advantages**

1. Users are in control of all their information and transactions.
2. Data is complete, consistent, timely, accurate, and widely available.
3. Due to the decentralized networks, Blockchain does not have a central point of failure and is better able to withstand malicious attacks.
4. Users can trust that transactions will be executed exactly as the protocol commands removing the need for a trusted third party.
5. Changes to public Blockchain are publicly viewable by all parties creating transparency, and all transactions are immutable, meaning they cannot be altered or deleted.
6. With all transactions being added to a single public ledger, it reduces the clutter and complications of multiple ledgers.
7. 24/7 availability.

## **Functions of Currency**

Bitcoin, powered by Blockchain has proven a very useful technology due to the fact that it allows transactions to take place without the need of any central authority. This alone is significant. The technology behind Bitcoin is also applicable in other areas where true ownership of assets is required, Namecoin is one such project to replace the centralized Domain Name system with Blockchain powered distributed Domain Name system.

Countless books and papers have described money, money is a very complex thing which serves many functions. Keith Hart has written about the "Two Sides of the Coin," heads on one side, tails on the other. Bitcoin, a digital specie essentially, emerges as a new and rather unique form of money. It's built-in cryptographic limits on supply make it essentially a virtual commodity form of money, fixed and "hard", like Gold, yet digital and transferable electronically across global telecommunications networks. Bitcoin has attractive features that are required by a currency such as US dollar etc. These attributes are

1. Unit of account
2. Store of value.
3. Medium of exchange

Let's now explore each one of them

### ***Unit of account***

A crucial function of any currency that allows it to be used to value goods, pay for services, record debts and make calculations. In other words its measurement for value. A unit of account has three important characteristics relevant to money

**Divisible**

*A unit of account can be divided so that its component parts add up to original value e.g. if you divide dollar into four quarters, sum of four quarters will be one dollar. Same applies to gold, if we cut gold bar into two halves, the sum of two gold bar halves will equal to original gold bar.*

**Fungible**

*One unit is valued as the same any other unit with no change in value. A US dollar note is the same in value to any other US dollar note. Similarly 1 ounce of gold is same in value to other ounce of gold.*

**Countable**

*A unit of account is also countable and subject to mathematical operations i.e. you can easily add, subtract, divide and multiply units. This accounts people to calculate profits, loss, debts and wealth.*

**Store of value**

It simply means people can store it and use it at later stage. An example being taking some of your money and investing in stock market / government bonds etc. for it to grow in value. Anything that can retain its future purchasing power.

**Medium of exchange**

## Distributed Consensus

Consensus protocol has been studied for decades in computer science literature, its main purpose is to remove any central authority to confirm legitimacy of a transaction on distributed network such as Bitcoin. Traditional motivation behind consensus protocol is to establish reliability trust in distributed systems. Mining is a distributed consensus system that is used to confirm waiting transactions by including them in the block chain.

Transactions are stored in the block in chronological order and verified cryptographically to ensure their authenticity. Different nodes (participants) in the bitcoin network validate the transactions so that they can be added to the block and then eventually block is added to the Blockchain (distributed ledger).

A malicious node/attacker would require more than 51% of the network hash power to control the Bitcoin network. Which would be very expensive and could cost billions of dollars.

Only one healthy node in the bitcoin network is enough to rebuild the network in case of an attack.

### ***Conesus protocol enforces***

- Reliability in distributed systems
- Removes need for a central / third party to confirm true ownership
- Commit all or none
- Bitcoin is first application to solve distributed consensus
- The protocol terminates and all correct nodes decide on the same value
- This value must have been proposed by some correct node
-



## - History of Bitcoin

*2007 - Satoshi Nakamoto started to work on Bitcoin concept.*

*15 Aug 2008 - Neal Kin, Vladimir Oksman, and Charles Bry file an application for an encryption patent application. All three individuals deny a connection to Satoshi Nakamoto, the alleged originator of the Bitcoin concept.*

*18 Aug 2008 - Bitcoin.org is registered at anonymousspeech.com, a site that allows users to anonymously register domain names and currently accepts Bitcoins.*

*31 Oct 2008 - Nakamoto publishes a design paper through a metzdowd.com cryptography mailing list that describes the Bitcoin currency and solves the problem of double spending so as to prevent the currency from being copied.*

*9 Nov 2008 - The Bitcoin project is registered on SourceForge.net, a community collaboration website focused on the development and distribution of open source software.*

*3 Jan 2009 - Block 0, the genesis block, is established at 18:15:05 GMT.*

*9 Jan 2009 - Version 0.1 of Bitcoin is released. Compiled with Microsoft Visual Studio for Windows, it includes a Bitcoin generation system that would create a total of 21 million Bitcoins through the year 2040*

*12 Jan 2009 - The very first Bitcoin transaction recorded in block 170 between Satoshi and Hal Finney, a developer and cryptographic activists.*

*5 October 2009 - An exchange rate is established. New Liberty Standard publishes a Bitcoin exchange rate that establishes the value of a Bitcoin at  $US\$1 = 1,309.03 \text{ BTC}$ , using an equation that includes the cost of electricity to run a computer that generated Bitcoins*

*12 October 2009 - The #bitcoin-dev channel is registered on freenode IRC, a discussion network for free and open source development communities.*

## Price Derviation

Bitcoin price is not controlled by any entity, it is directly derived from Supply and Demand. As we already there only ever be 21 million Bitcoins in circulation as at 2041. People use crypto exchanges such as coinbase.com to buy/sell bitcoins and other digital/crypto currencies.

When demand for bitcoins increases, the price increases, and when demand falls, the price falls. There is only a limited number of bitcoins in circulation and new bitcoins are created at a predictable and decreasing rate, which means that demand must follow this level of inflation to keep the price stable. Because Bitcoin is still a relatively small market compared to what it could be, it doesn't take significant amounts of money to move the market price up or down, and thus the price of a bitcoin is still very volatile.

# BASIC CRYPTOGRAPHY

## Bitcoin address

Bitcoin address is a Base58Check representation of a Hash160 of a public key with a version byte 0x00 which maps to a prefix "1". Typically represented as text (ex. 1CBtcGivXmHQ8ZqdPgeMfcpQNJrqTrSAcG) or as a QR code.

A more recent variant of an address is a P2SH address: a hash of a spending script with a version byte 0x05 which maps to a prefix "3" (ex. 3NukJ6fYZJ5Kk8bPjycAnruZkE5Q7UW7i8).

Another variant of an address is not a hash, but a raw private key representation (e.g. 5KQntKuhYWSRXNqp2yhdXzjekYAR7US3MT1715Mbv5CyUKV6hVe). It is rarely used, only for importing/exporting private keys or printing them on paper wallets.

## Altcoin

A clone of the protocol with some modifications. Usually all altcoins have rules incompatible with Bitcoin and have their own genesis blocks. Most notable altcoins are Litecoin (uses faster block confirmation time and script as a proof-of-work) and Namecoin (has a special key-value storage). In theory, an altcoin can be started from an existing Bitcoin blockchain if someone wants to support a different set of rules (although, there was no such example to date). See also Fork.

## ASIC

Stands for "application-specific integrated circuit". In other words, a chip designed to perform a narrow set of tasks (compared to CPU or GPU that perform a wide range of functions). ASIC typically refers to specialized mining chips or the whole machines built on these chips. Some ASIC manufacturers: Avalon, ASICMiner, Butterfly Labs (BFL) and Cointerra.

## ASIC Miner

A Chinese manufacturer that makes custom mining hardware, sells shares for bitcoins, pays dividends from on-site mining and also ships actual hardware to customers.

## Base58

A compact human-readable encoding for binary data invented by Satoshi Nakamoto to make more user-friendly addresses. It consists of alphanumeric characters, but does not allow "0", "O", "I", "l" characters that look the same in

some fonts and could be used to create visually identical looking addresses. Lowercase "o" and "1" are allowed.

## Base58Check

A variant of Base58 encoding that appends first 4 bytes of Hash256 of the encoded data to that data before converting to Base58. It is used in addresses to detect typing errors.

## BIP

Bitcoin Improvement Proposals. RFC-like documents modeled after PEPs (Python Enhancement Proposals) discussing different aspects of the protocol and software. Most interesting BIPs describe hard fork changes in the core protocol that require supermajority of Bitcoin users (or, in some cases, only miners) to agree on the change and accept it in an organized manner.

## Bit

Name of a Bitcoin denomination equal to 100 satoshis (1 millionth of 1 BTC). In 2014 several companies including Bitpay and Coinbase, and various wallet apps adopted bit to display bitcoin amounts.

## Bitcoin

Refers to a protocol, network or a unit of currency.

As a protocol, Bitcoin is a set of rules that every client must follow to accept transactions and have its own transactions accepted by other clients. Also includes a message protocol that allows nodes to connect to each other and exchange transactions and blocks.

As a network, Bitcoin is all the computers that follow the same rules and exchange transactions and blocks between each other.

As a unit, one Bitcoin (BTC, XBT) is defined as 100 million satoshis, the smallest units available in the current transaction format. Bitcoin is not capitalized when speaking about the amount: "I received 0.4 bitcoins."

## Bitcoin Core

New name of BitcoinQT since release of version 0.9 on March 19, 2014. Not to confuse with CoreBitcoin, an Objective-C implementation published in August 2013. See also Bitcore, a JavaScript implementation for Node.js by Bitpay.

## Bitcoinj

A Java implementation of a full Bitcoin node by Mike Hearn. Also includes SPV implementation among other features.

## Bitcoinjs

A JavaScript Bitcoin library. Allows signing transactions and performing several elliptic curve operations. Used on [brainwallet.org](http://brainwallet.org). See also Bitcore, another JS library.

## BitcoinQT

Bitcoin implementation based on original code by *Satoshi Nakamoto*. Includes a graphical interface for Windows, OS X and Linux (using QT) and a command-line executable *bitcoind* that is typically used on servers.

It is considered a *reference implementation* as it's the most used *full node* implementation, especially among *miners*. Other implementations must be bug-for-bug compatible with it to avoid being *forked*. BitcoinQT uses OpenSSL for its ECDSA operations which has its own quirks that became a part of the standard (e.g. non-canonically encoded public keys are accepted by OpenSSL without an error, so other implementations must do the same).

## Bitcoind

Original implementation of Bitcoin with a command line interface. Currently a part of *BitcoinQT* project. "D" stands for "daemon" per UNIX tradition to name processes running in background. See also *BitcoinQT*.

## Bitcoin-ruby

A Bitcoin utilities library in Ruby by Julian Langschaedel. Used in production on *Coinbase.com*.

## Bitcore

A Bitcoin toolkit by Bitpay written in JavaScript. More complete than *Bitcoinjs*.

## Block

A data structure that consists of a *block header* and a *merkle tree* of transactions. Each block (except for *genesis block*) references one previous block thus forming a tree called the *blockchain*. Block can be thought of as a group of transactions with a timestamp and a *proof-of-work* attached.

## Block Header

A data structure containing a previous block hash, a hash of a merkle tree of transactions, a timestamp, a *difficulty* and a *nonce*.

## Block Height

A sequence number of a block in the blockchain. Height 0 refers to the *genesis block*. Several blocks may share the same height (see *Orphan*), but only one of them belongs to the *main chain*. Block height is used in *Lock time*.

## Blockchain

A public ledger of all confirmed transactions in a form of a tree of all valid *blocks* (including *orphans*). Most of the time, "blockchain" means the *main chain*, a single most *difficult* chain of blocks. Blockchain is updated by *mining* blocks with new transactions. *Unconfirmed transactions* are not part of the blockchain. If some clients disagree on which chain is main or which blocks are valid, a *fork* happens.

## Blockchain.info

A web service running a Bitcoin *node* and displaying statistics and raw data of all the transactions and blocks. It also provides a *web wallet* functionality with *lightweight clients* for Android, iOS and OS X.

## Brain wallet

Brain wallet is a concept of storing *private keys* as a memorable phrase without any digital or paper trace. Either a single key is used for a single address, or a *deterministic wallet* derived from a single key. If done properly, a brain wallet greatly reduces the risk of theft because it is completely deniable: no one could say which or how much bitcoins you own as there are no actual wallet files to be found anywhere. However, it is the most error-prone method as one can simply forget the secret phrase, or make it too simple for anyone to brute force and steal all the funds. Additional risks are added by a complex wallet software. E.g. BitcoinQT always sends *change* amount to a new address. If a private key is imported temporarily to spend 1% of the funds and then the wallet is deleted, the remaining 99% will be lost forever as they are moved as a change to a completely new address. This already happened to a number of people.

## Brainwallet.org

Utility based on bitcoinjs to craft transactions by hand, convert *private keys* to addresses and work with a *brain wallet*.

## BTC

The most popular informal currency code for 1 Bitcoin (defined as 100 000 000 *Satoshis*). See also *XBT* and *Bit*.

## Casascius Coins

Physical collectible coins [###a href="https://www.casascius.com/">](https://www.casascius.com/)produced by Mike Caldwell. Each coin contains a *private key* under a tamper-evident hologram. The name "Casascius" is formed from a phrase "call a spade a spade", as a response to a name of Bitcoin itself.

## Change

Informal name for a portion of a *transaction output* that is returned to a sender as a "change" after spending that output. Since *transaction outputs* cannot be partially spent, one can spend 1 BTC out of 3 BTC output only by creating two new outputs: a "payment" output with 1 BTC sent to a payee address, and a "change" output with remaining 2 BTC (minus *transaction fees*) sent to the

payer's addresses. *BitcoinQT* always uses new address from a *key pool* for a better privacy. *Blockchain.info* sends to a default address in the wallet.

Paper wallet or a *brain wallet* is to make a change transaction to a different address and then accidentally delete it. E.g. when importing a private key in a temporary *BitcoinQT* wallet, making a transaction and then deleting the temporary wallet.

## Checkpoint

A hash of a block before which the *BitcoinQT* client downloads blocks without verifying digital signatures for performance reasons. A checkpoint usually refers to a very deep block (at least several days old) when it's clear to everyone that that block is accepted by the overwhelming majority of users and *reorganization* will not happen past that point.

It also helps protecting most of the history from a *51% attack*. Since checkpoints affect how the *main chain* is determined, they are part of the protocol and must be recognized by alternative clients (although, the risk of reorganization past the checkpoint would be incredibly low).

## Client

See *Node*.

## Coin

An informal term that means either 1 bitcoin, or an unspent *transaction output* that can be *spent*.

## Coinbase

An input script of a transaction that generates new bitcoins. Or a name of that transaction itself ("coinbase transaction"). Coinbase transaction does not spend any existing transactions, but contains exactly one input which may contain any data in its script. *Genesis block* transaction contains a reference to The Times article from January 3rd 2009 to prove that more blocks were not created before that date. Some *mining pools* put their names in the coinbase transactions (so everyone can estimate how much *hashrate* each pool produces).

Coinbase is also used to vote on a protocol change (e.g. *P2SH*). Miners vote by putting some agreed-upon marker in the coinbase to see how many support the change. If a majority of miners support it and expect non-mining users to accept it, then they simply start enforcing new rule. Minority then should either continue with a forked blockchain (thus producing an *altcoin*) or accept new rule.

## Coinbase.com

US-based Bitcoin/USD exchange and web wallet service.

## Colored Coin

A concept of adding a special meaning to certain transaction outputs. This could be used to create a tradable commodity on top of Bitcoin protocol. For instance, a company may create 1 million shares and declare a single transaction output containing 10 BTC (1 bln *satoshis*) as a source of these shares. Then, some or all of these bitcoins can be moved to other addresses, sold or exchanged for anything. During a voting process or a dividend distribution, share owners can prove ownership by simply signing a particular message by the private keys associated with addresses holding bitcoins derived from the initial source.

## Cold Storage

A collective term for various security measures to reduce the risk of remote access to the private keys. It could be a normal computer disconnected from the internet, or a dedicated hardware wallet, or a USB stick with a wallet file, or a *paper wallet*.

## CompactSize

Original name of a variable-length integer format used in transaction and block serialization. Also known as "Satoshi's encoding". It uses 1, 3, 5 or 9 bytes to represent any 64-bit unsigned integer. Values lower than 253 are represented with 1 byte. Bytes 253, 254 and 255 indicate 16-, 32- or 64-bit integer that follows. Smaller numbers can be presented differently. In *bitcoin-ruby* it is called "var\_int", in *Bitcoinj* it is VarInt. *BitcoinQT* also has even more compact representation called VarInt which is not compatible with CompactSize and used in block storage.

## Confirmed Transaction

Transaction that has been included in the blockchain. Probability of transaction being rejected is measured in a number of confirmations. See *Confirmation Number*.

## Confirmation Number

Confirmation number is a measure of probability that transaction could be rejected from the *main chain*. "Zero confirmations" means that transaction is *unconfirmed* (not in any block yet). One confirmation means that the transaction is included in the latest block in the main chain. Two confirmations means the transaction is included in the block right before the latest one. And so on. Probability of transaction being reversed ("*double spent*") is diminishing exponentially with more blocks added "on top" of it.

## Difficulty

Difficulty is a measure of how difficult it is to find a new block compared to the easiest it can ever be. By definition, it is a maximum *target* divided by the current target. Difficulty is used in two Bitcoin rules: 1) every block must be meet difficulty target to ensure 10 minute interval between blocks and 2) transactions are considered confirmed only when belonging to a *main chain* which is the one with the biggest cumulative difficulty of all blocks. As of

July 27, 2014 the difficulty is 18 736 441 558 and grows by 3-5% every two weeks. See also *Target*.

## Denial of Service

Is a form of attack on the network. Bitcoin *nodes* punish certain behavior of other nodes by banning their IP addresses for 24 hours to avoid DoS. Also, some theoretical attacks like *51% attack* may be used for network-wide DoS.

## Depth

Depth refers to a place in the blockchain. A transaction with 6 *confirmations* can also be called "6 blocks deep".

## Deterministic Wallet

A collective term for different ways to generate a sequence of *private keys* and/or *public keys*. Deterministic wallet does not need a *Key Pool*. The simplest form of a deterministic wallet is based on hashing a secret string concatenated with a key number. For each number the resulting hash is used as a private key (public key is derived from it). More complex scheme uses *elliptic curve arithmetic* to derive sequences of public and private keys separately which allows generating new *addresses* for every payment request without storing private keys on a web server.

## DoS

See *Denial of Service*.

## Double Spend

There are two major ways to perform a double spend: reverting an unconfirmed transaction by making another one which has a higher chance of being included in a block (only works with merchants accepting zero-confirmation transactions) or by mining a parallel blockchain with a second transaction to overtake the chain where the first transaction was included.

Bitcoin *proof-of-work* scheme makes a probabilistic guarantee of difficulty to double spend transactions included in the *blockchain*. The deeper transaction is recorded in the blockchain, the more expensive it is to "reverse" it.

## Dust

A transaction output that is smaller than a typically fee required to spend it. This is not a strict part of the protocol, as any amount more than zero is valid. BitcoinQT refuses to mine or relay "dust" transactions to avoid uselessly increasing the size of unspent transaction outputs (UTXO) index. See also discussion about UTXO.



## ECDSA

Stands for *Elliptic Curve Digital Signature Algorithm*. Used to verify transaction ownership when making a transfer of bitcoins.

## Elliptic Curve Arithmetic

A set of mathematical operations defined on a group of points on a 2D elliptic curve. Bitcoin protocol uses predefined curve A simplest possible explanation of the operations: you can add and subtract points and multiply them by an integer. Dividing by an integer is computationally infeasible (otherwise cryptographic signatures won't work). The private key is a 256-bit integer and the public key is a product of a predefined point G ("generator") by that integer:  $A = G * a$ . Associativity law allows implementing interesting cryptographic schemes like Diffie-Hellman key exchange (ECDH): two parties with private keys  $i$  and  $i/i$  may exchange their public keys  $A$  and  $i/i$  to compute a shared secret point  $C$ :  $C = A * b = B * a$  because  $(G * a) * b == (G * b) * a$ . Then this point  $C$  can be used as an AES encryption key to protect their communication channel.

## Extra nonce

A number placed in coinbase script and incremented by a miner each time the nonce 32-bit integer overflows. This is not the required way to continue mining when nonce overflows, one can also change the merkle tree of transactions or change a public key used for collecting a block reward.

## Fork

Refers either to a fork of a source code (see Altcoin) or, more often, to a split of the blockchain when two different parts of the network see different main chains. In a sense, fork occurs every time two blocks of the same height are created at the same time. Both blocks always have the different hashes (and therefore different difficulty), so when a node sees both of them, it will always choose the most difficult one. However, before both blocks arrive to a majority of nodes, two parts of the network will see different blocks as tips of the main chain.

Term fork or hard fork also refers to a change of the protocol that may lead to a split of the network (by design or because of a bug). On March 11 2013 a smaller half of the network running version 0.7 of bitcoind could not include a large (>900 Kb) block at height 225430 created by a miner running newer version 0.8. The block could not be included because of the bug in v0.7 which was fixed in v0.8. Since the majority of computing power did not have a problem, it continued to build a chain on top of a problematic block. When the issue was noticed, majority of 0.8 miners agreed to abandon 24 blocks incompatible with 0.7 miners and mine on top of 0.7 chain. Except for one double spend experiment against OKPay, all transactions during the fork were properly included in both sides of the blockchain.

## Full Node

A node which implements all of Bitcoin protocol and does not require trusting any external service to validate transactions. It is able to download and validate the entire blockchain. All full nodes implement the same peer-to-peer messaging protocol to exchange transactions and blocks, but that is not a requirement. A full node may receive and validate data using any protocol and from any source. However, the highest security is achieved by being able to communicate as fast as possible with as many nodes as possible.

## Genesis Block

A very first block in the blockchain with hard-coded contents and a all-zero reference to a previous block. Genesis block was released on 3rd of January 2009 with a newspaper quote in its coinbase: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" as a proof that there are no secretly pre-mined blocks to overtake the blockchain in the future. The message ironically refers to a reason for Bitcoin existence: a constant inflation of money supply by governments and banks.

## Halving

Refers to reducing reward every 210 000 blocks (approximately every 4 years). Since the genesis block to a block 209999 in December 2012 the reward was 50 BTC. Till 2016 it will be 25 BTC, then 12.5 BTC and so on till 1 satoshi around 2140 after which point no more bitcoins will ever be created. Due to reward halving, the total supply of bitcoins is limited: only about 2100 trillion satoshis will ever be created.

## Hard Fork

Some people use term hard fork to stress that changing Bitcoin protocol requires overwhelming majority to agree with it, or some noticeable part of the economy will continue with original blockchain following the old rules. See Fork and Soft Fork for further discussion.

## Hash Function

Bitcoin protocol mostly uses two cryptographic hash functions: SHA-256 and RIPEMD-160. First one is almost exclusively used in the two round hashing (Hash256), while the latter one is only used in computing an address (see also Hash160). Scripts may use not only Hash256 and Hash160, but also SHA-1, SHA-256 and RIPEMD-160.

## Hash, Hash256

When not speaking about arbitrary hash functions, Hash refers to two rounds of SHA-256. That is, you should compute a SHA-256 hash of your data and then another SHA-256 hash of that hash. It is used in block header hashing, transaction hashing, making a merkle tree of transactions, or computing a checksum of an address. Known as `BTCHash256()` in CoreBitcoin, `Hash()` in BitcoinQT. It is also available in scripts as `OP_HASH256`.

## Hash160

SHA-256 hashed with RIPEMD-160. It is used to produce an address because it makes a smaller hash (20 bytes vs 32 bytes) than SHA-256, but still uses SHA-256 internally for security. `BTCHash160()` in CoreBitcoin, `Hash160()` in BitcoinQT. It is also available in scripts as `OP_HASH160`.

## To hash

To compute a hash function of some data. If hash function is not mentioned explicitly, it is the one defined by the context. For instance, "to hash a transaction" means to compute Hash256 of binary representation of a transaction.

## Hashrate

A measure of mining hardware performance expressed in hashes per second (GH/s). As of July 27, 2014 the hash rate of all Bitcoin mining nodes combined is around 135 799 000 GH/s. For comparison, AMD Radeon graphics cards produce from 0.2 to 0.8 GH/s depending on model.

## Hash Type (hashtype)

A single byte appended to a transaction signature in the transaction input which describes how the transaction should be hashed in order to verify that signature. There are three types affecting outputs: ALL (default), SINGLE, NONE and one optional modifier ANYONECANPAY affecting the inputs (can be combined with either of the first three). ALL requires all outputs to be hashed (thus, all outputs are signed). SINGLE clears all output scripts but the one with the same index as the input in question. NONE clears all outputs thus allowing changing them at will. ANYONECANPAY removes all inputs except the current one (allows anyone to contribute independently). The actual behavior is more subtle than this overview, you should check the actual source code for more comments.

## Height

See Block Height.

## Input

See Transaction Input.

## Key

Could mean an ECDSA public or private key, or AES symmetric encryption key. AES is not used in the protocol itself (only to encrypt the ECDSA keys and other sensitive data), so usually the word key means an ECDSA key. When talking about keys, people usually mean private keys as public key can always be derived from a private one. See also Private Key and Public Key.

## Key Pool

Some wallet applications that create new private keys randomly keep a pool of unused pre-generated keys (BitcoinQT keeps 100 keys by default). When a new key is needed for change address or a new payment request, the application provides the oldest key from the pool and replaces it with a fresh one. The purpose of the pool is to ensure that recently used keys are always already backed up on external storage. Without a key pool you could create a new key, receive a payment on its address and then have your hard disk died before backing up this key. A key pool guarantees that this key was already backed up several days before being used. Deterministic wallets do not use a key pool because they need to back up a single secret key.

## Lightweight client

Comparing to a full node, lightweight node does not store the whole blockchain and thus cannot fully verify any transaction. There are two kinds of lightweight nodes: those fully trusting an external service to determine wallet balance and validity of transactions (e.g. blockchain.info) and the apps implementing Simplified Payment Verification (SPV). SPV clients do not need to trust any particular service, but are more vulnerable to a 51% attack than full nodes. See Simplified Payment Verification for more info.

## Lock Time (locktime)

A 32-bit field in a transaction that means either a block height at which the transaction becomes valid, or a UNIX timestamp. Zero means transaction is valid in any block. A number less than 500000000 is interpreted as a block number (the limit will be hit after year 11000), otherwise a timestamp.

## Mainnet

Main Bitcoin network and its blockchain. The term is mostly used in comparison to testnet.

## Main Chain

A part of the blockchain which a node considers the most difficult (see difficulty). All nodes store all valid blocks, including orphans and recompute the total difficulty when receiving another block. If the newly arrived block or blocks do not extend existing main chain, but create another one from some previous block, it is called reorganization.

## Merkle Tree

Merkle tree is an abstract data structure that organizes a list of data items in a tree of their hashes (like in Git, Mercurial or ZFS). In Bitcoin the merkle tree is used only to organize transactions within a block (the block header contains only one hash of a tree) so that full nodes may prune fully spent transactions to save disk space. SPVclients store only block headers and validate transactions if they are provided with a list of all intermediate hashes.

## Mempool

A technical term for a collection of unconfirmed transactions stored by a node until they either expire or get included in the main chain. When reorganization happens, transactions from orphaned blocks either become invalid (if already included in the main chain) or moved to a pool of unconfirmed transactions. By default, bitcoind nodes throw away unconfirmed transactions after 24 hours.

## Mining

A process of finding valid hashes of a block header by iterating millions of variants of block headers (using nonce and extra nonce) in order to find a hash lower than the target (see also difficulty). The process needs to determine a single global history of all transactions (grouped in blocks). Mining consumes time and electricity and nowadays the difficulty is so big, that energy-wise it's not even profitable to mine using video graphics cards. Mining is paid for by transaction fees and by block rewards (newly generated coins, hence the term "mining").

## Mining Pool

A service that allows separate owners of mining hardware to split the reward proportionally to submitted work. Since probability of finding a valid block hash is proportional to miner's hashrate, small individual miners may work for months before finding a big per-block reward. Mining pools allow more steady stream of smaller income. Pool owner determines the block contents and distributes ranges of nonce values between its workers. Normally, mining pools are centralized. P2Pool is a fully decentralized pool.

## Miner

A person, a software or a hardware that performs *mining*.

## Mixing

A process of exchanging coins with other persons in order to increase privacy of one's history. Sometimes it is associated with money laundering, but strictly speaking it is orthogonal to laundering. In traditional banking, a bank protects customer's privacy by hiding transactions from all 3rd parties. In Bitcoin any merchant may do a statistical analysis of one's entire payment history and determine, for instance, how many bitcoins one owns. While it's still possible to implement KYC (Know Your Customer) rules on a level of every merchant, mixing allows to separate information about one's history between the merchants.

Most important use cases for mixing are: 1) receiving a salary as a single big monthly payment and then spending it in small transactions ("cafe sees thousands of dollars when you pay just \$4"); 2) making a single payment and revealing connection of many small private spendings ("car dealer sees how much you are addicted to coffee"). In both cases your employer, a cafe and a car dealer may comply with KYC/AML laws and report your identity and transferred amounts, but neither of them need to know about each other. Mixing bitcoins

after receiving a salary and mixing them before making a big payment solves this privacy problem.

### M-of-N Multi-signature Transaction

A transaction that can be spent using M signatures when N public keys are required (M is less or equal to N). Multi-signature transactions that only contain one OP\_CHECKMULTISIG opcode and N is 3, 2 or 1 are considered standard.

### Node

Node, or client, is a computer on the network that speaks Bitcoin message protocol (exchanging transactions and blocks). There are full nodes that are capable of validating the entire blockchain and lightweight nodes, with reduced functionality. Wallet applications that speak to a server are not considered nodes.

### Nonce

Stands for "number used once". A 32-bit number in a block header which is iterated during a search for proof-of-work. Each time the nonce is changed, the hash of the block header is recalculated. If nonce overflows before valid proof-of-work is found, an extra nonce is incremented and placed in the coinbase script. Alternatively, one may change a merkle tree of transactions or a timestamp.

### Non-standard Transaction

Any valid transaction that is not standard. Non-standard transactions are not relayed or mined by default BitcoinQT nodes (but are relayed and mined on testnet). However, if anyone puts such transaction in a block, it will be accepted by all nodes. In practice it means that unusual transactions will take more time to get included in the **blockchain**. **If some kind of non-standard** transaction becomes useful and popular, it may get named standard and adopted by users (like it ). See also Standard Transaction.

### Opcode

8-bit code of a script operation. Codes from 0x01 to 0x4B (decimal 75) are interpreted as a length of data to be pushed on the stack of the interpreter (data bytes follow the opcode). Other codes are either do something interesting, or disabled and cause transaction verification to fail, or do nothing (reserved for future use). See also Script.

### Orphan, Orphaned Block

A valid block that is no longer a part of a main chain. Usually happens when two or more blocks of the same height are produced at the same time. When one of them becomes a part of the main chain, others are considered "orphaned". Orphans also may happen when the blockchain is forked due to an attack (see 51% attack) or a bug. Then a chain of several blocks may become abandoned. Usually a transaction is included in all blocks of the same height, so its confirmation is not delayed and there is no double spend. See **also Fork**.

## Output

See Transaction Output.

## P2SH

See Pay-to-Script Hash.

## Pay-to-Script Hash

A type of the script and address that allows sending bitcoins to arbitrary complex scripts using a compact hash of that script. This allows payer to pay much smaller transaction fees and not wait very long for a non-standard transaction to get included in the blockchain. Then the actual script matching the hash must be provided by the payee when redeeming the funds. P2SH addresses are encoded in Base58Check just like regular public keys and start with number "3".

## Paper Wallet

A form of cold storage where a private key for Bitcoin address is printed on a piece of paper (with or without encryption) and then all traces of the key are removed from the computer where it was generated. To redeem bitcoins, a key must be imported in the wallet application so it can sign a transaction. See also Casascius Coins.

## Proof-of-Work (PoW)

A number that is provably hard to compute. That is, it takes measurable amount of time and/or computational power (energy) to produce. In Bitcoin it is a hash of a block header. A block is considered valid only if its hash is lower than the current target (roughly, starts with a certain amount of zero bits). Each block refers to a previous block thus accumulating previous proof-of-work and forming a Blockchain.

Proof-of-work is not the only requirement, but an important one to make sure that it is economically infeasible to produce an alternative history of transactions with the same accumulated work. Each client can independently consider the most difficult chain of valid blocks as the "true" history of transactions, without need to trust any source that provides the blocks.

Note that owning a very large amount of computational power does not override other rules enforced by every client. Ill-formed blocks or blocks containing invalid transactions are rejected no matter how difficult they were to produce.

## Private Key (Privkey)

A 256-bit number used in ECDSA algorithm to create transaction signatures in order to prove ownership of certain amount of bitcoins. Can also be used in arbitrary elliptic curve arithmetic operations. Private keys are stored within wallet applications and are usually encrypted with a pass phrase. Private keys may be completely random .

## Reference Implementation

BitcoinQT (or bitcoind) is the most used full node implementation, so it is considered a reference for other implementations. If an alternative implementation is not compatible with BitcoinQT it may be forked, that is it will not see the same main chain as the rest of the network running BitcoinQT.

## Relaying Transactions

Connected Bitcoin nodes relay new transactions between each other on best effort basis in order to send them to the mining nodes. Some transactions may not be relayed by all nodes. E.g. non-standard transactions, or transactions without a minimum fee. Bitcoin message protocol is not the only way to send the transaction. One may also send it directly to a miner, or mine it yourself, or send it directly to the payee and make them to relay or mine it.

## Reorg, Reorganization

An event in the node when one or more blocks in the main chain become orphaned. Usually, newly received blocks are extending existing main chain. Sometimes (4-6 times a week) a couple of blocks of the same height are produced almost simultaneously and for a short period of time some nodes may see one block as a tip of the main chain which will be eventually replaced by a more difficult block(s). Each transaction in the orphaned blocks either becomes invalid (if already included in the main chain block) or becomes unconfirmed and moved to the mempool. In case of a major bug or a 51% attack, reorganization may involve reorganizing more than one block.

## Reward

Amount of newly generated bitcoins that a miner may claim in a new block. The first transaction in the block allows miner to claim currently allowed reward as well as all transaction fees from all transactions in the block. Reward is halved every 210 000 blocks, approximately every 4 years. As of July 27, 2014 the reward is 25 BTC (the first halving occurred in December 2012). For security reasons, rewards cannot be spent before 100 blocks built on top of the current block.

## Satoshi

The first name of the Bitcoin's creator Satoshi Nakamoto and also the name of the smallest unit used in transactions. 1 bitcoin (BTC) is equal to 100 million satoshis.

## Satoshi Nakamoto

A pseudonym of an author of initial Bitcoin implementation. There are multitude of speculations on who and how many people worked on Bitcoin, of which nationality or age, but no one has any evidence to say anything definitive on that matter.

## Script



A compact turing-incomplete programming language used in transaction inputs and outputs. Scripts are interpreted by a Forth-like stack machine: each operation manipulates data on the stack. Most scripts follow the standard pattern and verify the digital signature provided in the transaction input against a public key provided in the previous transaction's output. Both signatures and public keys are provided using scripts. Scripts may contain complex conditions, but can never change amounts being transferred. Amount is stored in a separate field in a transaction output.

## scriptSig

Original name in bitcoind for a transaction input script. Typically, input scripts contain signatures to prove ownership of bitcoins sent by a previous transaction.

## scriptPubKey

Original name in bitcoind for a transaction output script. Typically, output scripts contain public keys (or their hashes; see Address) that allow only owner of a corresponding private key to redeem the bitcoins in the output.

## Sequence

A 32-bit unsigned integer in a transaction input used to replace older version of a transaction by a newer one. Only used when locktime is not zero. Transaction is not considered valid until the sequence number is 0xFFFFFFFF. By default, the sequence is 0xFFFFFFFF.

## Signature

A sequence of bytes that proves that a piece of data is acknowledged by a person holding a certain public key. Bitcoin uses ECDSA for signing transactions. Amounts of bitcoins are sent through a chain of transactions: from one to another. Every transaction must provide a signature matching a public key defined in the previous transaction. This way only a proper owner a secret private key associated with a given public key can spend bitcoins further.

## Simplified Payment Verification (SPV)

A scheme to validate transactions without storing the whole blockchain (only block headers) and without trusting any external service. Every transaction must be present with all its parent and sibling hashes in a merkle tree up to the root. SPV client trusts the most difficult chain of block headers and can validate if the transaction indeed belongs to a certain block header. Since SPV does not validate all transactions, a 51% attack may not only cause a double spend (like with full nodes), but also make a completely invalid payment with bitcoins created from nowhere. However, this kind of attack is very costly and probably more expensive than a product in question. Bitcoinj library implements SPV functionality.

## Secret key

Either the Private Key or an encryption key used in encrypted wallets. Bitcoin protocol does not use encryption anywhere, so secret key typically means a private key used for signing transactions.

## Soft Fork

Sometimes the soft fork refers to an important change of software behavior that is not a hard fork (e.g. changing mining feepolicy). See also Hard Fork and Fork.

## Spam

Incorrect peer-to-peer messages (like sending invalid transactions) may be considered a denial of service attack (see DoS). Valid transactions sending very tiny amounts and/or having low mining fees are called Dust by some people. The protocol itself does not define which transactions are not worth relaying or mining, it's a decision of every individual node. Any valid transaction in the blockchain must be accepted by the node if it wishes to accept the remaining blocks, so transaction censorship only means increased confirmation delays. Individual payees may also blacklist certain addresses (refuse to accept payments from some addresses), but that's too easy to work around using mixing.

## Spent Output

A transaction output can be spent only once: when another valid transaction makes a reference to this output from its own input. When another transaction attempts to spend the same output, it will be rejected by the nodes already seeing the first transaction. Blockchain as a proof-of-work scheme allows every node to agree on which transaction was indeed the first one. The whole transaction is considered spent when all its outputs are spent.

## Split

A split of a blockchain. See Fork.

## SPV

See Simplified Payment Verification.

## Standard Transaction

Some transactions are considered standard, meaning they are relayed and mined by most nodes. More complex transactions could be buggy or cause DoS attacks on the network, so they are considered non-standard and not relayed or mined by most nodes. Both standard and non-standard transactions are valid and once included in the blockchain, will be recognized by all nodes. Standard transactions are: 1) sending to a public key, 2) sending to an address, 3) sending to a P2SH address, 4) sending to M-of-N multi-signature transaction where N is 3 or less.

## Target

A 256-bit number that puts an upper limit for a block header hash to be valid. The lower the target is, the higher the difficulty to find a valid hash. The maximum (easiest) target is 0x00000000FFFF000. The difficulty and the target are adjusted every 2016 blocks (approx. 2 weeks) to keep interval between the blocks close to 10 minutes.

## Testnet

A set of parameters used for testing a Bitcoin network. Testnet is like mainnet, but has a different genesis block (it was reset several times, the latest testnet is testnet3). Testnet uses slightly different address format to avoid confusion with main Bitcoin addresses and all nodes are relaying and mining non-standard transactions.

## Testnet3

The latest version of testnet with another genesis block.

## Timestamp

UNIX timestamp is a standard representation of time as a number of seconds since January 1st 1970 GMT. Usually stored in a 32-bit signed integer.

## Transaction

A chunk of binary data that describes how bitcoins are moved from one owner to another. Transactions are stored in the blockchain. Every transaction (except for coinbase transactions) has a reference to one or more previous transactions (inputs) and one or more rules on how to spend these bitcoins further (outputs). See Transaction Input and Transaction Output for more info.

## Transaction Fee

Also known as "miners' fee", an amount that an author of transaction pays to a miner who will include the transaction in a block. The fee is expressed as difference between the sum of all input amounts and a sum of all output amounts. Unlike traditional payment systems, miners do not explicitly require fees and most miners allow free transactions. All miners are competing between each other for the fees and all transactions are competing for a place in a block. There are soft rules encoded in most clients that define minimum fees per kilobyte to relay or mine a transaction (mostly to prevent DoS and spam). Typically, the fee affects the priority of a transaction. As of July 27, 2014 average fee per block is below 0.1 BTC. See also Reward.

## Transaction Input

A part of a transaction that contains a reference to a previous transaction's output and a script that can prove ownership of that output. The script usually contains a signature and thus called scriptSig. Inputs spend

previous outputs completely. So if one needs to pay only a portion of some previous output, the transaction should include extra change output that sends the remaining portion back to its owner (on the same or different address). Coinbase transactions contain only one input with a zeroed reference to a previous transaction and an arbitrary data in place of script.

## Transaction Output

An output contains an amount to be sent and a script that allows further spending. The script typically contains a public key(or an address, a hash of a public key) and a signature verification opcode. Only an owner of a corresponding private key is able to create another transaction that sends that amount further to someone else. In every transaction, the sum of output amounts must be equal or less than a sum of all input amounts. See also *Change*.

## Tx

See Transaction.

## Txin

See Transaction Input.

## Txout

See Transaction Output.

## Unconfirmed Transaction

Transaction that is not included in any block. Also known as "0-confirmation" transaction. Unconfirmed transactions are relayed by the nodes and stay in their mempools. Unconfirmed transaction stays in the pool until the node decides to throw it away, finds it in the blockchain, or includes it in the blockchain itself (if it's a miner). See also *Confirmation Number*.

## UTXO Set

A collection of Unspent Transaction Outputs. Typically used in discussions on optimizing an ever-growing index of transaction outputs that are not yet spent. The index is important to efficiently validate newly created transactions. Even if the rate of the new transactions remains constant, the time required to locate and verify unspent outputs grows.

Possible technical solutions include more efficient indexing algorithms and a more performant hardware. BitcoinQT, for example, keeps only an index of outputs matching user's keys and scans the entire blockchain when validating other transactions. A developer of one web wallet service mentioned that they maintain the entire index of UTXO and its size was around 100 Gb when the blockchain itself was only 8 Gb.

Some people seek social methods to solve the problem. For instance, by refusing to relay or mine transactions that are considered dust (containing outputs smaller than a transaction fee required to mine/relay them).

## VarInt

This term may cause confusion as it means different formats in different Bitcoin implementations. See CompactSize for details.

## Wallet

An application or a service that helps keeping private keys for signing transactions. Wallet does not keep bitcoins themselves (they are recorded in blockchain). "Storing bitcoins" usually means storing the keys.

## Web Wallet

A web service providing wallet functionality: ability to store, send and receive bitcoins. User has to trust counter-party to keep their bitcoins securely and ready to redeem at any time. It is very easy to build your own web wallet, so most of them were prone to hacks or outright fraud. The most secure and respected web wallet is Blockchain.info. Online exchanges also provide wallet functionality, so they can also be considered web wallets. It is not recommended to store large amounts of bitcoins in a web wallet.

## XBT

Informal currency code for 1 Bitcoin (defined as 100 000 000 Satoshis). Some people proposed using it for 0.01 Bitcoin to avoid confusion with BTC. There were rumours that Bloomberg tests XBT as a ticker for 1 Bitcoin, but currently there is only ticker XBTFUND for Second Market's Bitcoin Investment Trust. See also BTC.

## 0-Confirmation (Zero-Confirmation)

**See** *Unconfirmed Transaction* **and** *Confirmation Number*.

## 51% Attack

Also known as >50% attack or a double spend attack. An attacker can make a payment, wait till the merchant accepts some number of confirmations and provides the service, then starts mining a parallel chain of blocks starting with a block before the transaction. This parallel Blockchain then includes another transaction that spends the same outputs on some other address. When the parallel chain becomes more difficult, it is considered a main chain by all nodes and the original transaction becomes invalid. Having more than a half of total hashrate guarantees possibility to overtake chain of any length, hence the name of an attack (strictly speaking, it is "more than 50%", not 51%). Also, even 40% of hashrate allows making a double spend, but the chances are less than 100% and are diminishing exponentially with the number of confirmations that the merchant requires.

This attack is considered theoretical as owning more than 50% of hashrate might be much more expensive than any gain from a double spend. Another variant of an attack is to disrupt the network by mining empty blocks, censoring all transactions. An attack can be mitigated by blacklisting blocks that most of "honest" miners consider abnormal. Under normal conditions, miners and mining

pools do not censor blocks and transactions as it may diminish trust in Bitcoin and thus their own investments. 51% attack is also mitigated by using checkpoints that prevent reorganization past the certain block.

## Hash Functions

Hash functions play a very important role in Bitcoin ecosystem. A hash function is a mathematical algorithm that for a given input returns a fixed output. It's a one way function meaning no matter how many times to run a has function, it will always return same output for a given input. A slightest change in the input will result into a completely different output or has value. Also it is impossible to generate input from hash value.

Every hash value should map to only one input. If two different inputs generate same hash value this is called a hash collision. Good hash algorithms are hash collision proof.

Another important property of hash function is that it should take input of any variable length but always generate/produce a hash value of fixed length.

Bitcoin network uses SHA256 cryptographic hash function, which stands for Secure Hash Algorithm 256-bit.

Bitcoin transactions are relayed to each of the peers in the network. Miners collect these transactions, perform a number of checks to make sure they're valid and then add them to their memory pool. It's at this point that they begin the process of creating a block.

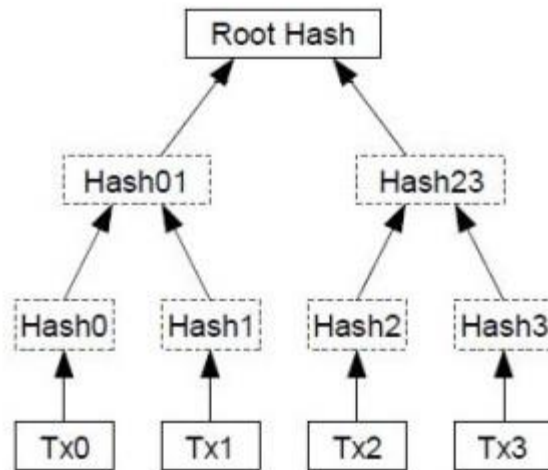
The first step in the process is to hash each transaction in the memory pool using SHA256. The raw transaction data may look something like this:

```
01000000017a06ea98cd40ba2e3288262b28638cec5337c1456aaf5eedc8e9e5a
20f062bdf000000008a473044022030e2d23be71a907a3ad7de846b3bbe8886c4
a839e1aa2cf0d314b1d327f12d2a022039718fc3886a171e4ec2b138e6547b03dd
326ef7f12295d06e351e7c02010068014104e0ba531dc5d2ad13e2178196ade1a
23989088cfbeddc7886528412087f4bffa2ebc19ce739f25a63056b6026a269987fcf
5383131440501b583bab70a7254b09effffffff01b02e052a010000001976a9142d
bde30815faee5bf221d6688ebad7e12f7b2b1a88ac00000000
```

After hashing above transaction using SHA256 hashing algorithm it will look like

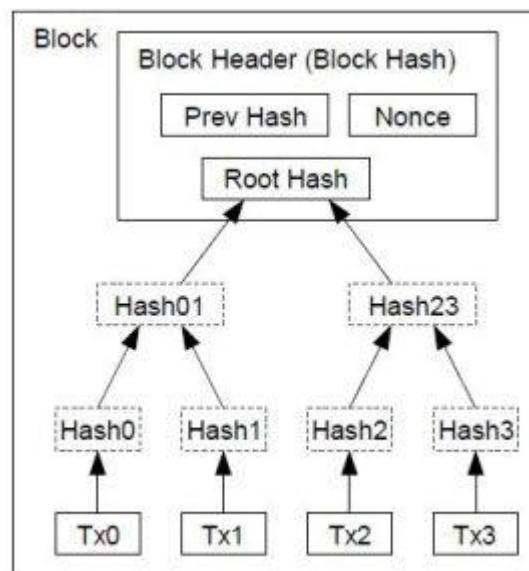
```
2d94683fa2f8aaae4a6f377d93b875f680adf96b9c3e9577554b742f412fa9ad
```

Transaction hashes are then organised into a tree structure called Merkle tree or simply hash tree. The hashes of transactions are organised into pairs to two, then they are joined together and hashed again. See image below



Hash at the top of the tree is called Merkle Root.

Block header contains Hash of the Merkle root along with Hash of the previous block and a random number called nonce. Block header looks like below



Block Header

Hash of Block header is used to identify block in the Blockchain data structure. So lots of hashes and hashes of hashes put together to identify block and then transactions inside the Blockchain.

## Proof of work

A proof of work is a piece of data that is difficult to produce but easy to verify. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hashcash proof of work system.



00000000000000000002e9759d58adea2a299a65e9d3728d98c8b6eb8177a323a

## Cryptography

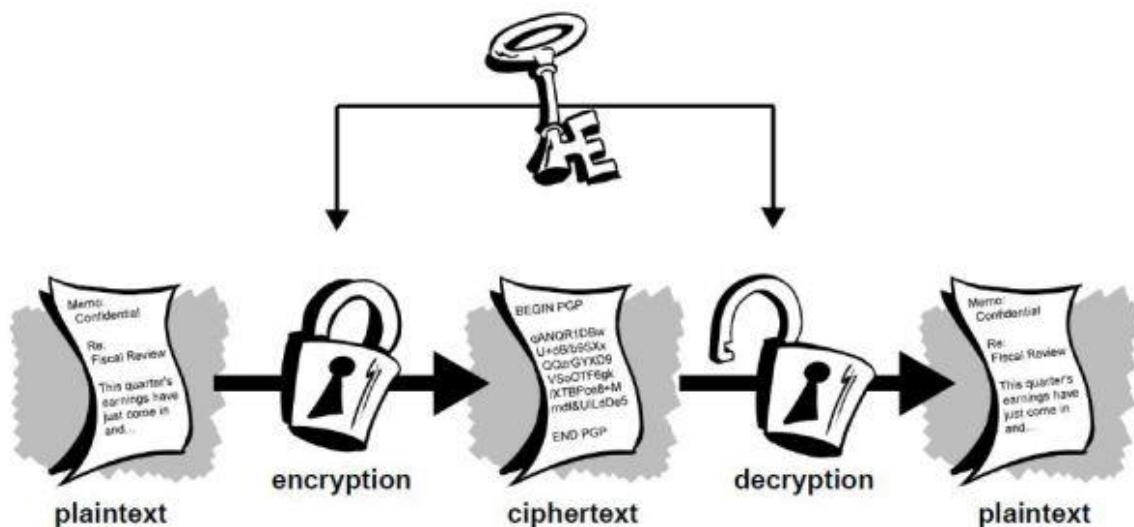
*"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files." —Bruce Schneier*

Cryptography is the science of using mathematics to encrypt and decrypt data so that we can either store it or transmit it to someone so that only the intended recipient can read it. In practice we take plaintext (the unencrypted data) and encrypt it using a cipher, a mathematical algorithm used to securely encrypt and decrypt data, to produce cipher text (unreadable encrypted data).

## Symmetric key Encryption

In conventional cryptography the same key is used to both encrypt and decrypt the data. This practice is called symmetric-key encryption.

Grand mother



Pic - Symmetric-key

The most widely used symmetric-key cipher is the Advanced Encryption Standard (AES). AES was established in 2001 by the US Government's National Institute

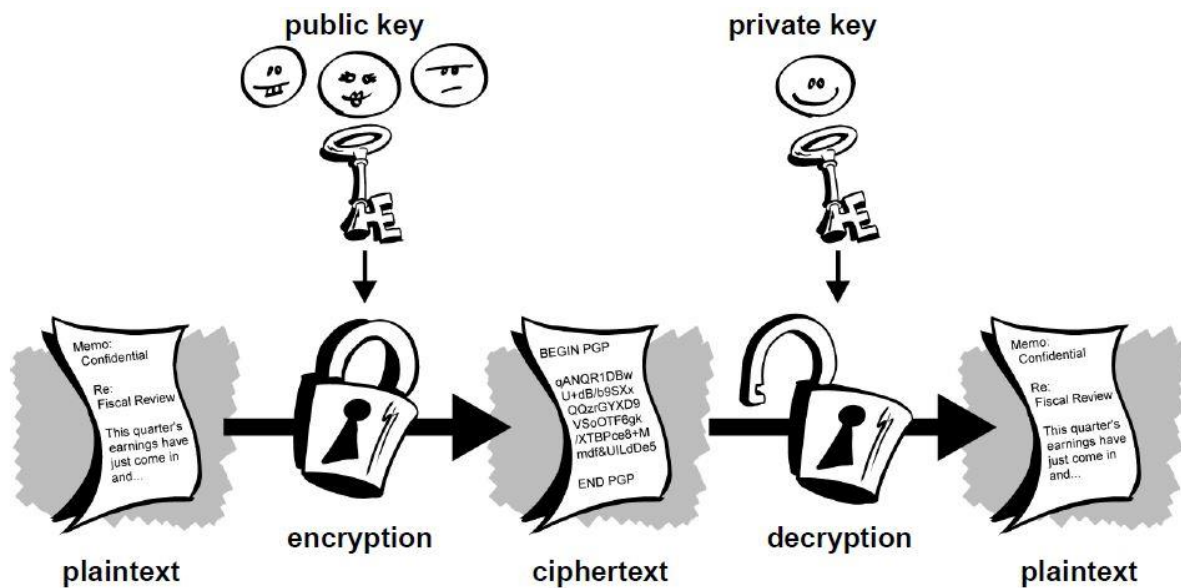
of Standards and Technology after it held an open competition to create a replacement for the cracked Data Encryption Standard (DES). Fifteen designs were submitted by cryptographers from around the world. The list was narrowed down to five finalists: Rijndael, Serpent, Twofish, RC6, and MARS. Ultimately, Rijndael, developed by two Belgian cryptographers, was selected as the cipher for AES.

The AES algorithm is part of the public domain. That means it's not only free for anyone to use, but also that it has undergone an enormous amount of cryptanalysis. As of today there are no known feasible attacks. The NSA has even approved AES for use in the encryption of Top Secret classified information. You can take that as a bit of a vote of confidence. You can find various implementations of AES to use for encrypting your files simply by googling around.

While symmetric-key encryption works well for encrypting data on your computer or on a server, it isn't that great for communication. Since it uses the same key for both encryption and decryption, two parties that wish to communicate with each other need some way to agree on a key. Obviously, the whole reason you are encrypting your communications to begin with is that you don't believe your communication channel is secure. You just can't send an encryption key in an email or text or phone call since it will be intercepted. Short of meeting in person, it can be difficult for two parties to securely share an encryption key. Imagine the plight of Edward Snowden trying to send top secret files to Glenn Greenwald without having previously shared an encryption key.

## Asymmetric Encryption / Public-Key Cryptography

Public-key cryptography represents an advance over symmetric-key cryptography as far as communications are concerned. Instead of using a single key for both encryption and decryption, separate keys are used for both. A user generates a pair of keys that are mathematically linked to each other. One key (the public key) is used for encryption and the other (the private key) is used for decryption. The algorithm is designed in such a way that it is infeasible for an attacker to derive the private key from a given public key.



Pic - Public-key

Using this scheme, a person can share his public key, usually by posting it on a keyserver or a website, and anyone can download it and use it to encrypt files to send to him. Once encrypted, they can only be decrypted with the corresponding private key.

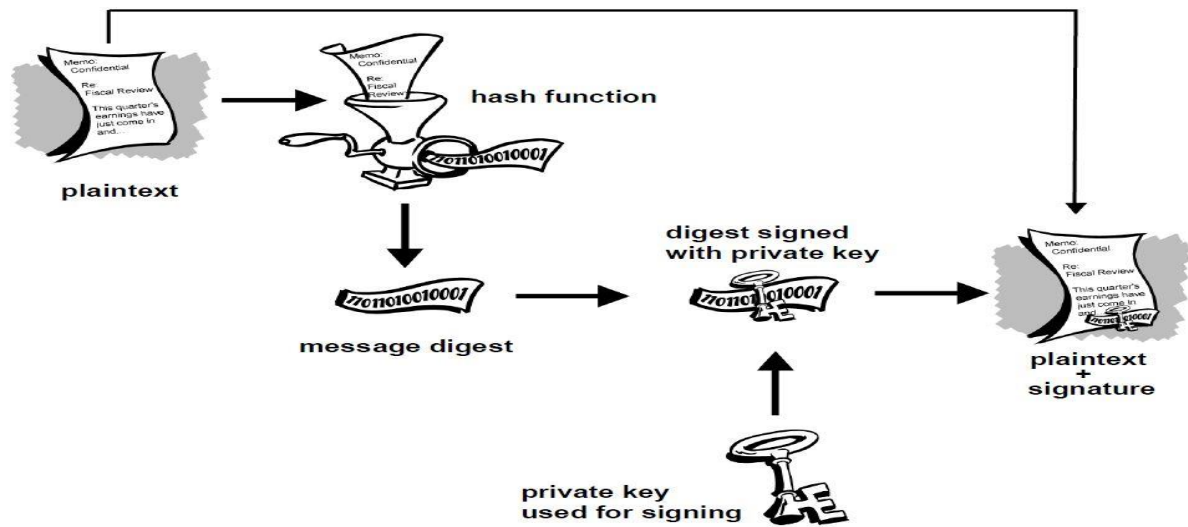
The most popular implementation of public-key encryption is Pretty Good Privacy (PGP) and its free open source counterpart the GNU Privacy Guard (GPG).

## Digital Signatures

Public-key cryptography has a second benefit beyond just the encryption and decryption of data. It can be used to create something called a digital signature which can be used to simultaneously provide authentication, data integrity, and non-repudiation, all of which are critical to Bitcoin's operation.

One of the features of a digital signature is that the signed data is actually an integral part of the signature. If the data (the message in this case) is altered in even the slightest way, the signature will show as invalid when checked. This feature allows for the secure transfer of data while ensuring that nobody can just take the signature and attach it to another file in an attempt to forge a signature. This feature is key in Blockchain technology to establish true ownership of digital assets be it Bitcoin or an image or a text file or a message.

A Bitcoin address is a public-private key pair using Elliptic Curve Digital Signature Algorithm (ECDSA). The public key is hashed several times until it looks like the familiar Bitcoin address.



Pic – Digital Signature

# **BITCOIN BASICS**

## **Bitcoin Community**

Below listed are part of the Bitcoin communities

### **Users**

Anyone who holds bitcoin wallet address is a user of Bitcoin ecosystem.

### **Educators**

Anyone who is teaching and educating others on Bitcoin and related technologies e.g. authors, bloggers, content writer etc.

### **Marketers**

Bitcoin Marketers help to discover and connect to new potential customers, clients. Bitcoin entrepreneurs and follow Bitcoin market trends to help grow your business. Listed below are some of the areas Bitcoin Marketers help business to grow and focus on

- Website design
- Front end development
- Search engine optimization
- Logo, booth, and promotional design
- Landing pages, conversion optimization
- Analytics analysis
- Currency trading / market making
- Mining
- News articles, press releases
- Consulting, networking, advice
- Resourcing

### **Faucets**

A bitcoin faucet is a reward system, in the form of a website or app that dispenses rewards in the form of a satoshi, which is a hundredth of a millionth BTC, for visitors to claim in exchange for completing a captcha or task as described by the website.

The first bitcoin faucet was called The Bitcoin Faucet and was developed by Gavin Andresen in 2010 It originally gave out 5 bitcoins per person.

### **Miners**

Bitcoin uses public-key cryptography, peer to peer networking and proof of work to process and verify transactions (payments).

Bitcoin mining is the process of validating and adding transaction records to the Bitcoin ledger i.e. Bitcoin Blockchain. It is essential part of the Bitcoin ecosystem and ensures that only valid and legitimate transaction records are added to the Blockchain. In returns miners who own these mining equipment and participate

in the bitcoin network are rewarded with new bitcoins every time a new block is added to the bitcoin public Blockchain.

Current reward is 12.5 BTC and it halves every 210,000 blocks.

## Bitcoin Addresses and Keys

Bitcoin address which you can closing relate to your high street bank account number or your email address. In case of bank account number this is the address or entry in the banking ledger where your funds are held and in case of email address this is the address where your emails are stored.

Bitcoin address has two parts public key and private key. Public key like your email address can be shared with others. Private key which can be related to your email password is the something that only you should have access to. Public and private keys are mathematically linked. You need private key to unlock your bitcoin account and send transactions, same way you would require your email address to send emails to others.

You should never share your private key or you risk losing your bitcoin funds.

In bitcoin world, private key is used to encrypt something and matching public key is used to decrypt it.

As mentioned above your Bitcoin public key is your address where funds are deposited and you can ask someone to send bitcoins to you by giving them your public key i.e. bitcoin address

Example bitcoin address: **323iShCfAGbGqAje9L6tY9dwFCdypzsKyU**

### **Feel free to deposit any coins to my above bitcoin address**

Bitcoin Transactions is initiated by the bitcoin owner address to transfer Bitcoin value to another Bitcoin address. Transactions are broadcasted to the Bitcoin network for validation and processing. Several transactions are grouped into a block and then finally blocks are added to the bitcoin public Blockchain. A transaction typically has following attributes

- Input - Bitcoin address used to send Bitcoin
- Amount - Number of Bitcoins being sent
- Output – Bitcoin address of the recipient

Please note that Bitcoins do not come with a receipt when a transaction is processed

Bitcoin transactions are public and can be viewed by using **Blockchain.info** or **blockexplorer.com** and other similar systems.

## Bitcoin Blockchain Ledger

Bitcoin Blockchain ledger is a decentralised database of Blockchain blocks and transactions. Once a block is written after enough confirmation (ref – to proof of work), it is not possible to reverse or overwrite these transactions. Follow below link to explore bitcoin Blockchain

<https://www.blockchain.com/explorer>

## Bitcoin the Unit

[Text goes here]

## Bitcoin the Network

Bitcoin Network is decentralised what that means is there is no central computer to control the network, there is no single point of failure in the Bitcoin network. All participating nodes/computers have equal stake in the network and if a node goes offline for fails, Bitcoin network still stays alive and continue to function as normal.

Another important attribute of Bitcoin network is that it is not controlled or owned by an individual or organisation.

In Bitcoin network there are mainly two types of participating nodes

- *Full nodes*
  - o Full nodes provides following functions and services
    - 
    - Wallet services
    - Mining
    - Adding blocks to the Blockchain

- *Lightweight nodes*

Also known as partial nodes do not store the complete ledger, instead they use simplified payment verification (SPV) mode which only requires them to download a part of the Bitcoin Blockchain. Partial nodes connect to the full nodes and use bloom filters to ensure that they only receive transactions relevant to their operations.

## BIPs

[Text goes here]

## Buying and selling bitcoin

[Text goes here]

## Blockchain Explorers

[Text goes here]

## UTXOs

[Text goes here]



## MINING

### Purpose and Function

[Text goes here]

### Algorithm

[Text goes here]

### Mining Pools

[Text goes here]

### Mining Hardware

[Text goes here]

### Security and Centralization

○

## WALLETS, CLIENTS AND KEY MANAGEMENT

### Wallet Types

[Text goes here]

### Bitcoin Clients

[Text goes here]

### Deterministic Wallets (AKA BIP32)

[Text goes here]

### Passphrase-Encrypted Wallets (AKA BIP38)

[Text goes here]

### Backup

[Text goes here]

### Importing and Exporting

## **BITCOIN COMMERCE**

### **Bitcoin as a Merchant**

[Text goes here]

### **Bitcoin Payment Processors**

[Text goes here]

### **Secure Payment Protocol (AKA BIP70)**

[Text goes here]

## ***Citation and Bibliography***

1. <https://cryptoconsortium.org/certifications>
2. <https://domsteil.com/2014/12/29/distributed-consensus-protocols/>
3. <http://hyperledger.com/>
4. <https://bitcoin.org/bitcoin.pdf>
5. <https://eris.projectdouglas.org/>
6. <https://www.ethereum.org/>
7. <http://www.blockstream.com/sidechains.pdf>
8. <http://counterparty.io/docs/protocol/>
9. <http://unenumerated.blogspot.co.uk/2014/12/the-dawn-of-trustworthy-computing.html>
10. <http://continuations.com/post/105272022635/bitcoin-clarifying-the-foundational-innovation-of>
11. <http://joel.mn/post/103546215249/the-blockchain-application-stack>
12. <http://www.dmytri.info/bitcoin-and-public-money/>
13. <https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained/>
14. [https://en.bitcoin.it/wiki/Proof\\_of\\_work](https://en.bitcoin.it/wiki/Proof_of_work)
15. <https://en.bitcoin.it/wiki/Hashcash>
16. <https://www.coindesk.com/bitcoin-explained-five-year-old/>
17. <http://historyofbitcoin.org/>
18. <http://twitter.com/oleganza>
19. <https://en.bitcoin.it/wiki/Secp256k1>
20. [https://en.wikipedia.org/wiki/Bitcoin\\_faucet](https://en.wikipedia.org/wiki/Bitcoin_faucet)
- 21.
- 22.
- 23.