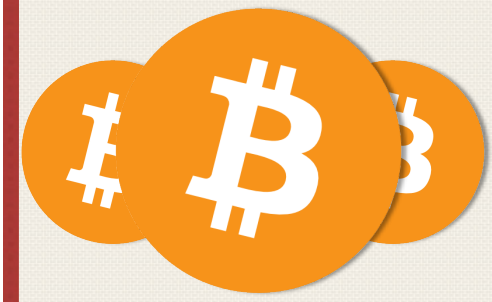
2009 2014

Bitcoin:

A Technical Guide for Non-Technical Users

WHAT IS



BITCOIN?

Dictionary

bit·coin[1] | `bit koyn | noun

1 a **cryptocurrency** enabling: secure *point to point* transfers of funds via digitally *signed entries* in a *public ledger*

2 a **global payment network** *lots* of people work for *new bitcoins* (they are called miners) by *verifying transactions*

Bitcoin -- Beyond the basics

Bitcoin, with a capital B, is a payment processing network utilizing a public ledger and secure **"digital signatures"** to allow owners of currency units, called bitcoins, to transfer ownership to one another.

Computers participating in the Bitcoin peer to peer network, run by users all over the world, verify these digital signatures as well as audit the chain of custody to prevent double spending. These computers also perform laborious computations involving a **"block"** of many individual transactions that relies on similar calculations from the previous block of transactions to secure the open public ledger and prevent transactions from being tampered with in the future. The reward for this computational service is newly created bitcoins and this process is called **"bitcoin mining."**

The process of bitcoin mining creates a series of "blocks" of transactions that are linked together in an unchangeable order. This series of blocks is called the **block chain** and constitutes the public transaction ledger. All bitcoins ever mined and all transactions ever made are recorded in the unbreakable block chain, the public ledger of Bitcoin.

To protect privacy, Bitcoin users do not use their identities to sign transaction in the block chain (public ledger). Rather, users use wallet software that maintains large numbers of **"key pairs"** in place of identities. One half of a key pair is kept secret and used by the **wallet software** to sign transactions (that is, spend bitcoins) while the other key is public and serves as a destination, or address, for bitcoins (like a drop box).

❑

฿ MORE INFO

1. Wallets: bitcoin.org
2. Education: Bitcoin Education Project (btcedproject.org)
3. Course: On Udemy search "bitcoin" at udemy.com
4. Infrastructure: Bitcoin Foundation bitcoinfoundation.org

฿ WALLETS

1. Store public address & private keys pairs
2. Uses private key to sign transactions
3. See bitcoin.org to see many wallet software solutions

฿ MINING

1. Effectively comprises the Bitcoin payment network
2. Verifies transactions
3. Secures the block chain
4. Requires specialized

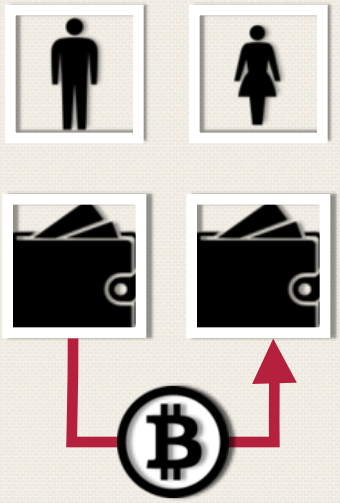
No Central Bank - ฿ is Global Cash - No Central Bank - ฿ is Global Cash - No Central Bank

2009 2014

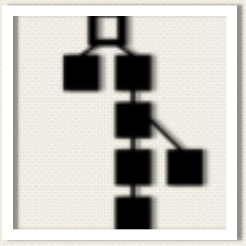
Bitcoin:

A Technical Guide for Non-Technical Users

A Bitcoin Transaction (or how Bella sends money to Murray)

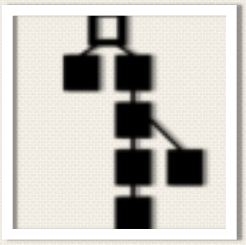


Murray creates a new address in his wallet so that Bella can send bitcoins to that address. Bella the purchaser, initiates the transaction by telling the network that she is going to pay Murray 1.3 BTC. This tells the network to deduct 1.3 BTC from a particular address in Bella's wallet and add 1.3BTC to that new address in Murray's wallet.



Murray and Bella's transaction is bundled along with other recent tranactions (by other unrelated people) into a block. The entire block is validated by miners. Validation is highly compute intensive and miners are rewarded for their work via transaction fees and bitcoins if they actually solve the validation for that block. Once the transaction is fully validated the transaction is complete.

The Block Chain Is:



Part of bitcoin's "magic" is that all transactions and all validation is done fully decentralized. Peer to peer connections are made between seller and purchasers. Miners are distributed worldwide and there is no central control of any aspect of the network.

Bitcoin Mining Is

The act of validating transactions. Miners are rewarded for validating blocks of transactions. Each block contains a "coinbase" transaction which upon solution pays a reward to the miner. In addition there are small transaction fees paid to the miner for each transaction. The current reward for a block is 25BTC. The reward is halved over time.

Validation of blocks also requires the solution to all previous blocks. This prevents someone from modifying the block chain as it would invalidate the cryptography used to solve the blocks.

This enables people who do not know or trust each other to perform valid commerce.

No Central Bank - ฿ is Global Cash - No Central Bank - ฿ is Global Cash - No Central Bank