Yasin Charles Nicolas

Movember 28, 2016

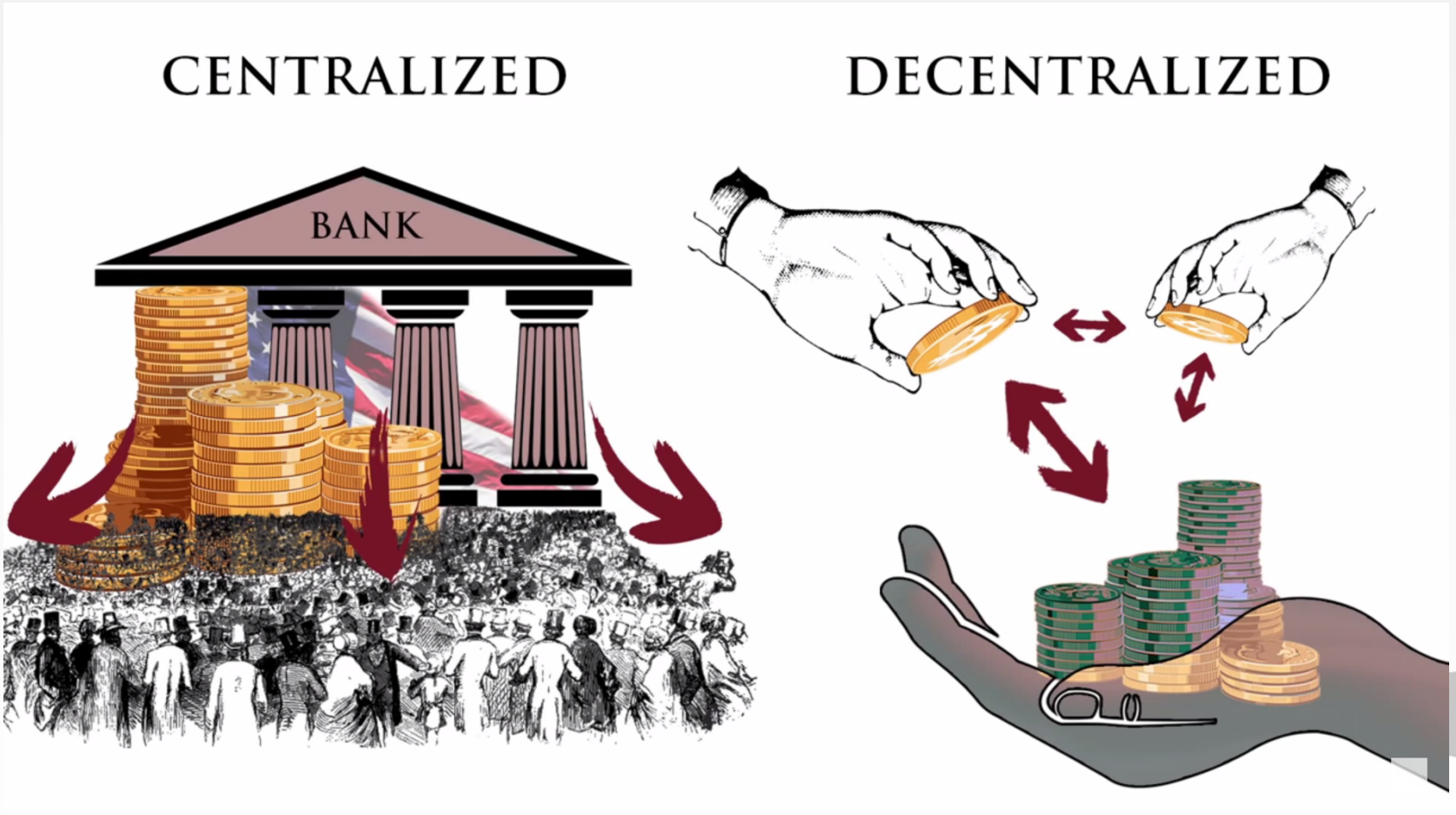
What is Bitcoin?

Bitcoin

Bit : binary digit
Coin : medium of exchange, currency

- Cryptocurrency (digital currency relying on cryptography)
- Invented by Satoshi Nakamoto
- Introduced on 31st October 2008
- Released Open Source 2009
- Peer-to-peer

Decentralized digital currency



Simple user

- Simply creates a wallet and perform transactions
- Rely on advanced users to handle your transactions and manage the network

Mobile Desktop Hardware Web


Bitcoin Core


Bitcoin Knots


breadwallet


Bither


GreenBits


BitGo


Green Address


Coinomi


Coin.Space


Copay


Airbitz


Mycelium

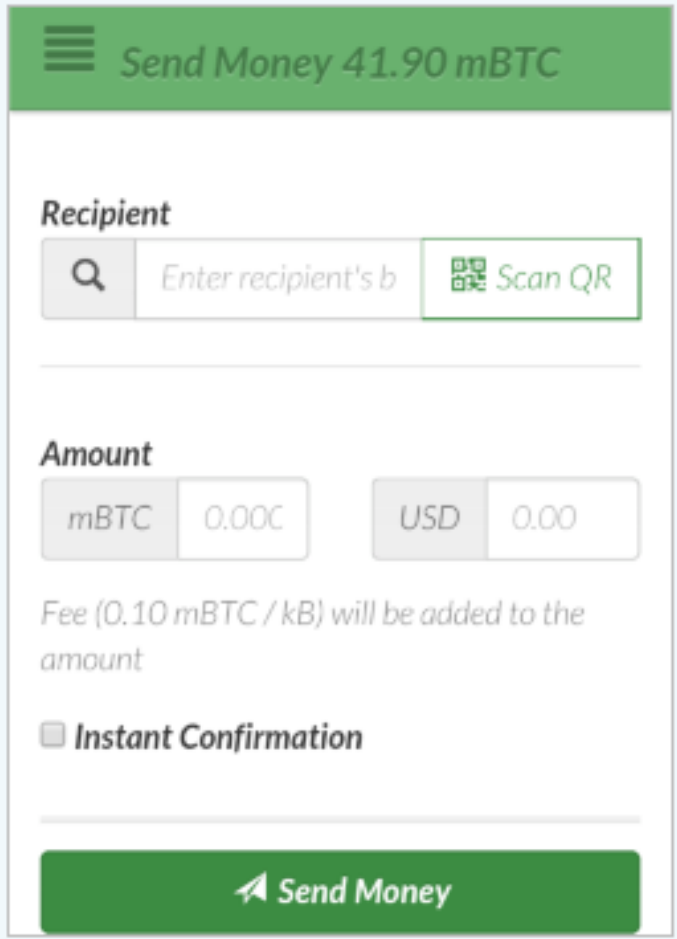
Simple user

GreenAddress

Install | Source code

- Shared control over your money
- Decentralized validation
- Basic transparency
- Two-factor authentication
- Basic privacy

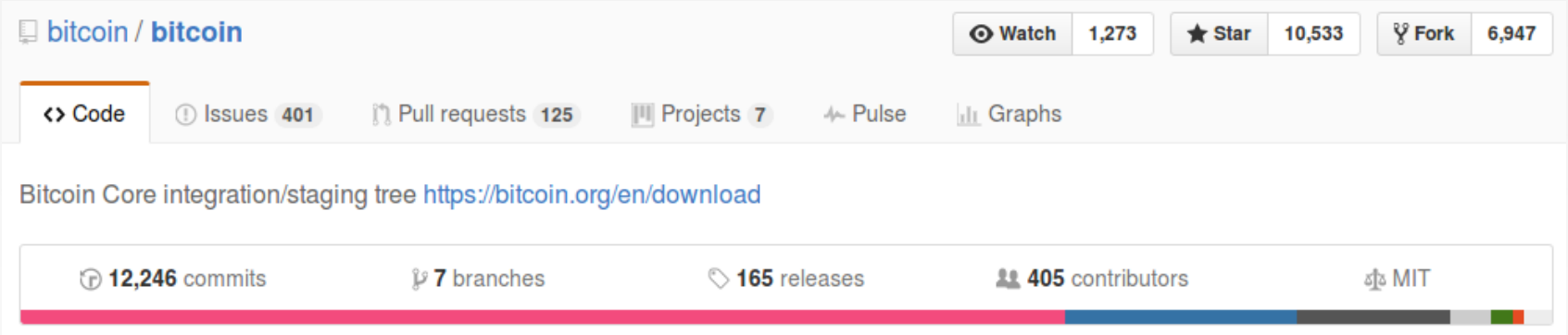
GreenAddress is a user-friendly multi-signature wallet with improved security and privacy. At no time are your keys server side, even encrypted. For security reasons, you should always use 2FA and the browser extension or Android App.



How to acquire bitcoins ?

- Accept them as payment for goods or services
- Exchange them from a more traditional form of currency
- Mine them (-> Advanced users)

Advanced user



- Be a node of the network
- Take part in verifying and propagating other users' transactions
- Mine blocks

Secured through cryptography

How it's done

- hash the network timestamp of the transaction
- put it into an ongoing chain of hash-based proof-of-work
- it forms a record that cannot be changed without redoing the proof of work

- "Base58" encoding relying on SHA-256

The blockchain

- sizeof(BlockChain) $>$ 80GB
- length(nodeList) $>$ 5300

The Truth

honest nodes controlling a majority of CPU power makes computationally impossible for attackers to change the history of transactions

Supporting the system

Receive Bitcoins

Successfully mining/discovering a block is rewarded by the whole network as a bounty
Currently 25BTC (<1800$)

Generate blocks

Difficulty is adjusted every 14 days to adjust for new miners on the network
Became so hard that it is now impractical
(i.e catch up with 1250kW of CPU farms working together)

The value of Bitcoins

Gaining value as time passes

Originally .31$ per BTC
Bitcoins become more valuable as they get harder to mine
They get harder to mine as more people join in
Currently sitting at 731$ per BTC

Volatility and incidents

High volatility : lack of liquidity?
Generally valuable but not immune to bubbles
Goes through cycles of appreciation and depreciation

Legality

Some countries outlawed Bitcoin

Russia
China

Bitcoins and criminal activities

Funding terrorism : Lack of oversight and regulation
Black markets : Deep Web, drugs (Silk Road)
Theft, money laundering etc.

Where can I use Bitcoins?

Bitcoin-friendly retailers and companies

Wikipedia, Whole Foods, Newegg etc
Now over 100K merchants
First car ever bought with Bitcoins from Tesla (Jan. 26 2014)

Personal transactions and trade

Buy and sell anything to anyone with or for Bitcoins
Risk : Bitcoin comes with no guarantee (no chargebacks or fraud protection)

Paypal

Pros over Bitcoin

More widely supported
Relies on regular currencies which are more stable (supposedly)

Cons compared to Bitcoin

High comission on all transactions
Very "corporate", could be seen as partial or corrupted

Others

The other cryptocurrencies

A lot of new cryptocurrencies keep popping up
A fair share of them don't last long
How reliable are they?
Can they replace Bitcoin?

Non-digital alternative currencies

Seeds, bartering

Discussion : how do you feel about it ?

Already using

I'm an explorer

Yeah, why not

I've got an open mind

N-E-V-E-R

I'm a conservative