Introduction to Bitcoin and Blockchain Technology

For first-time users

Konstantinos Karasavvas

What is it?

- Bitcoin is:
  - **a decentralized digital (crypto-)currency**
  - **a decentralized payment network**
  - **a technology**
    - a peer-to-peer network/protocol
    - an immutable public transaction ledger (aka blockchain)
    - a proof-of-work algorithm
    - a decentralized trustless platform using elliptic-curve cryptography (PKI)
    - a novel consensus mechanism

Decentralized Digital Cryptocurrency

- bank creates/controls currency
- transfer of value via an institution
- higher-fees / centralized control

Centralized

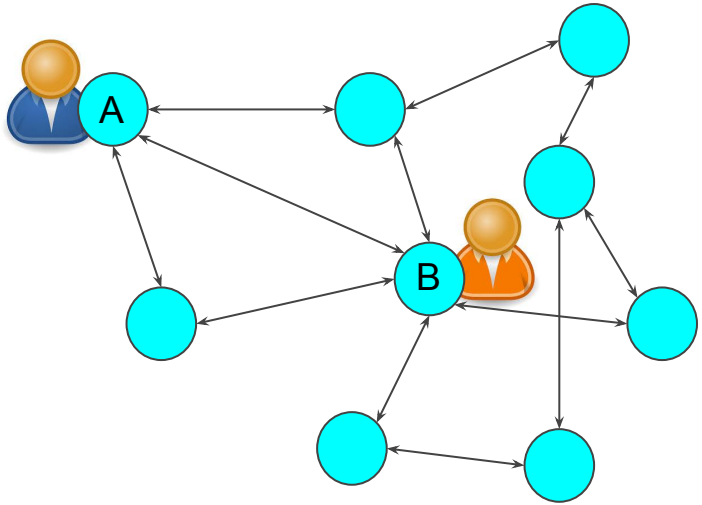
Decentralized Digital Cryptocurrency

- bank creates/controls currency
- transfer of value via an institution
- higher-fees / centralized control

Centralized

- currency is created algorithmically and distributed
- direct transfer of value from A -> B
- no intermediaries / no corruption

Decentralized



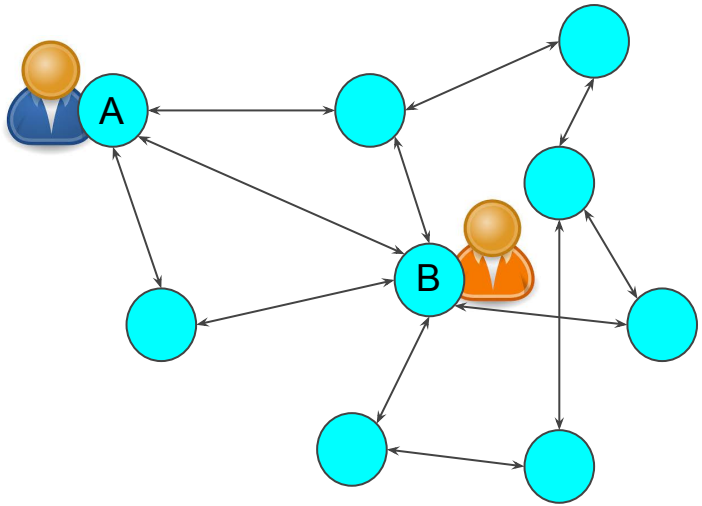
Decentralized **Digital** Cryptocurrency

- digital
  - 9.00 -15.00 Mon-Fri
  - inter-institution fees

Centralized

- digital
  - only pre-requisite is an internet connection
  - Global
  - 24/7

Decentralized



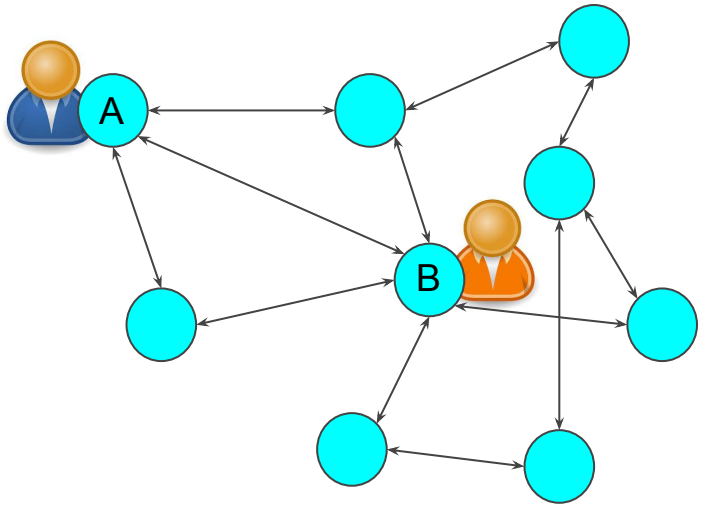
Decentralized Digital **Cryptocurrency**

- anti-counterfeiting
  - centralized control
  - enforced by bank -> state -> police

- anti-counterfeiting
  - algorithms
  - enforced by cryptography

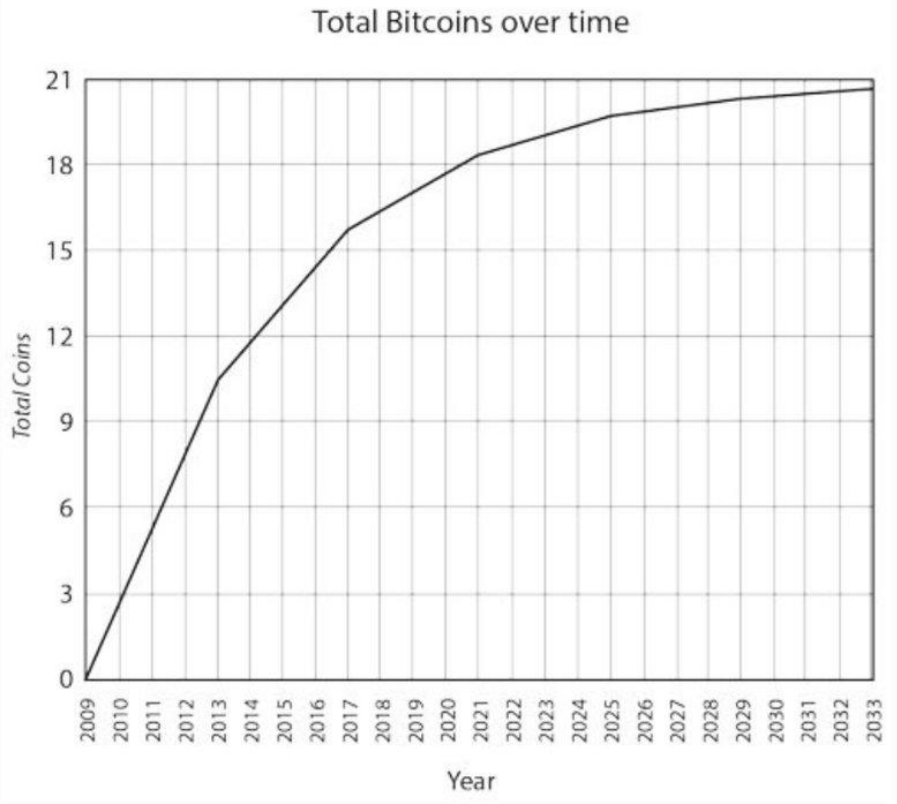
Centralized

Decentralized



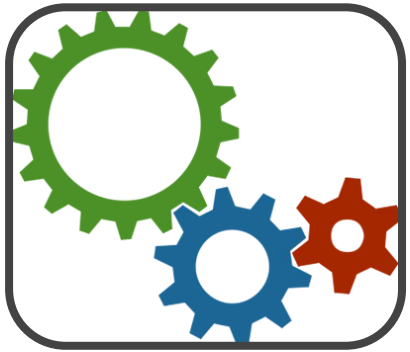
Currency characteristics (controlled supply)

- Bitcoin
  - issued every ~10 minutes
  - 99% up to ~2040
  - deflationary
- Fiat currency (euro, dollars, etc.)
  - inflationary



Currency characteristics (transparent rules)

- Transparent rules
  - which transactions are valid?
  - how is ownership determined?
  - how are new coins distributed?
- Open source software
  - anyone can verify

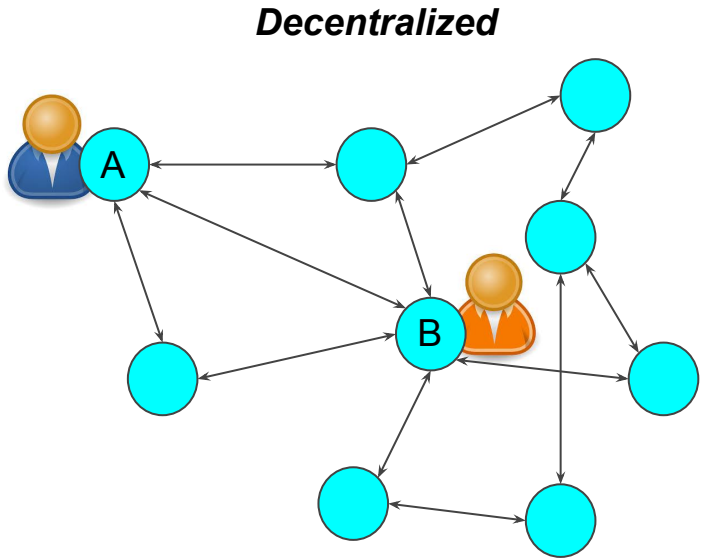


Currency characteristics (consensus-based)

- valid rule set
  - majority governs current
  - e.g. which transactions occurred

How it works

- Bird’s eye view
  - peer-to-peer network (of)
  - bitcoin nodes (open source software)
  - run and secure the network
  - transaction history (aka blockchain)
- Why run a bitcoin node?
  - volunteerism
  - bitcoin rewards
- Mining
  - secures the network
  - the process of minting new coins



Next: Some use cases

Applications

- **Remittances**
- **Payments**
- **Micropayments**
- **Bank services for the unbanked**
- **Store of Value**
- Digital Tokens
- Decentralized Applications
- Proof of Existence
- Smart Contracts
- Decentralized Autonomous Organizations
- Internet of Things / Machine to Machine
- Voting / Identity
- Private Blockchains
- Other?

Remittances

- €600 billion market
  - Western Union (15%)
  - MoneyGram
- High fees
  - depends on location
  - up to 25%
  - more for same day delivery
- Up to same day delivery
- Anywhere there is an agent
- Working hours
  - plus extended hours

Remittances

- €600 billion market
  - Western Union (15%)
  - MoneyGram
- High fees
  - depends on location
  - up to 25%
  - more for same day delivery
- Up to same day delivery
- Anywhere there is an agent
- Working hours
  - plus extended hours

- Bitcoin slowly gains momentum
- ~4¢ irrespective of amount
  - 1BTC = €378
- Up to an hour
  - in practice it is much faster
- Anywhere there is a connected machine
  - Internet (no need for permanent access)
- Anytime
  - 24/7
- No intermediaries, but…
  - bitspark.io
  - rebit.ph
  - bitpesa.co

Making/Receiving Payments

- Online
- Credit cards
  - 3%-6% + small flat rate
- Debit cards
  - 2%-3% + small flat rate
- Paypal
  - 2.9% + $0.30
- Bitcoin
  - none
  - but the sender typically pays ~4¢

Making/Receiving Payments

- Online
- Credit cards
  - 3%-6% + small flat rate
- Debit cards
  - 2%-3% + small flat rate
- Paypal
  - 2.9% + $0.30
- Bitcoin
  - none
  - but the sender typically pays ~4¢

- Merchants can offer discounts for bitcoin!
- Payment Processing?
  - Coinbase, BitPay

Making/Receiving Payments

- Online
- Credit cards
  - 3%-6% + small flat rate
- Debit cards
  - 2%-3% + small flat rate
- Paypal
  - 2.9% + $0.30
- Bitcoin
  - none
  - but the sender typically pays ~4¢

- Merchants can offer discounts for bitcoin!
- Payment Processing?
  - Coinbase, BitPay

- Some major companies
  - Overstock
  - Microsoft
  - Dell
  - Expedia
  - Time Inc.
  - DISH Network
  - Newegg
  - Zynga
  - UK's Theatre Tickets Direct
  - AirBaltic
  - CheepAir
  - …
- Do they keep their bitcoins?
- Can Bitcoin handle demand if widely adopted?

Micropayments

- Pay content creators
  - media
  - blogs
  - forums
- Many failed
- Flattr
  - click to reward
  - 10% fee from receivers
- ChangeTip
  - Twitter, Reddit, YouTube, Google+, Tumblr, StockTwits
  - was 1%, for now none
- ProTip (Chrome extension)
  - open source
  - free
- Zapchain

Micropayments

- Pay content creators
  - media
  - blogs
  - forums
- Many failed
- Flattr
  - click to reward
  - 10% fee from receivers
- ChangeTip
  - Twitter, Reddit, YouTube, Google+, Tumblr, StockTwits
  - was 1%, for now none
- ProTip (Chrome extension)
  - open source
  - free
- Zapchain

- Pay as you go (by the second!)
  - content distribution
    - watchmybit.com
    - streamium.io
    - Netflix-like service?
  - wifi
    - BitMesh (company)
    - Wifiportal21 (open source)
  - other
    - web hosting
    - …

(payment channels: trustless, 2-2 multi-sig, nLockTime)

Be your own bank

- Bank services for the unbanked/underbanked
  - payments
  - remittances
  - micro-payments / donations
  - … using Mobiles

Be your own bank

- Bank services for the unbanked/underbanked
  - payments
  - remittances
  - micro-payments / donations
  - … using Mobiles

- Bank services for the banked
  - capital controls
  - censorship

Be your own bank

- Bank services for the unbanked/underbanked
  - payments
  - remittances
  - micro-payments / donations
  - … using Mobiles
- Bank services for the banked
  - capital controls
  - censorship
- Store of value (vs hyper-inflation)
  - gold
  - reserve currencies
  - bitcoin
    - deflationary
    - Latin/South America, China, Russia.

Applications

- **Remittances**
- **Payments**
- **Micropayments**
- **Bank services for the unbanked**
- **Store of Value**
- Digital Tokens
- Decentralized Applications
- Proof of Existence
- Smart Contracts
- Decentralized Autonomous Organizations
- Internet of Things / Machine to Machine
- Voting / Identity
- Private Blockchains
- Other?

Next: Basic concepts / usage

Basic concepts (Bitcoin address / private key)

Bitcoin Address

SHARE

1Atuv5zFi5P5dzgfHNGWWR8EWjRSzDbCEL

Private Key

SECRET

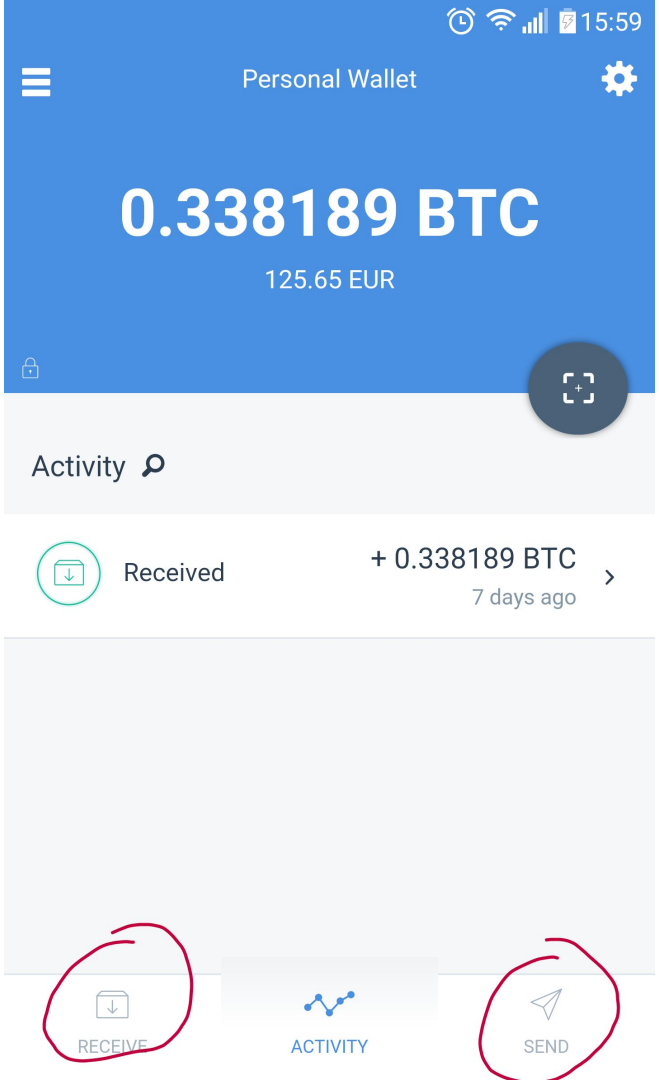
L13HRyX7Lj3TLve4jAx53ink49sR6eLrJP2q5kvijPQDzGBzVARG

Basic concepts (Bitcoin wallets)

- Wallet
  - manages bitcoin addresses (accounts)
  - can send (receive) bitcoins
- Types
  - desktop
  - mobile
  - online/web wallet
  - hardware wallet
- Wallet examples
  - Copay, Mycelium, ...
  - https://bitcoin.org/en/choose-your-wallet

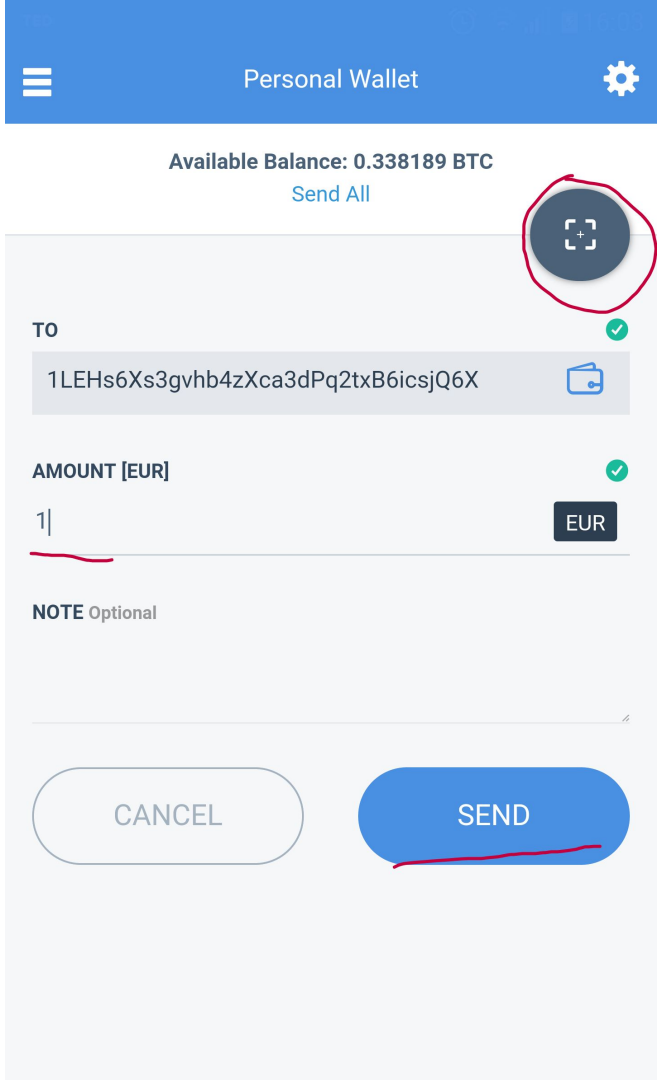
Usage: send bitcoins (1)

- Balance
- Activity
- Receive
- Send



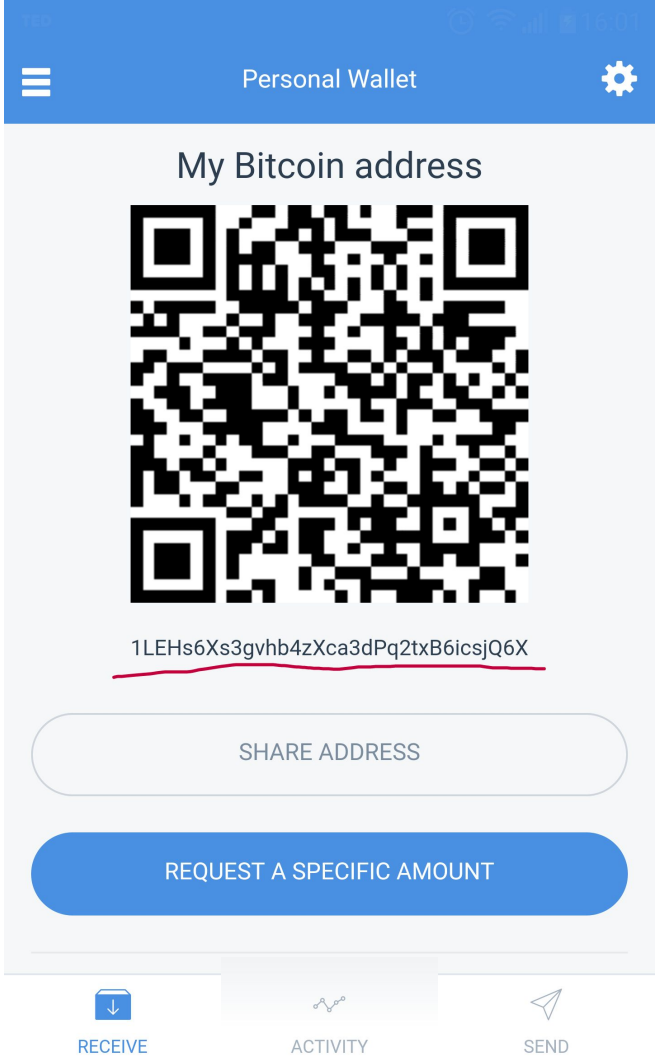
Usage: send bitcoins (2)

- To: (address / QR code)
- Amount: (in bitcoins or preferred currency)



Usage: receive bitcoins (1)

- Provide address string, or
- QR code



How to get Bitcoins

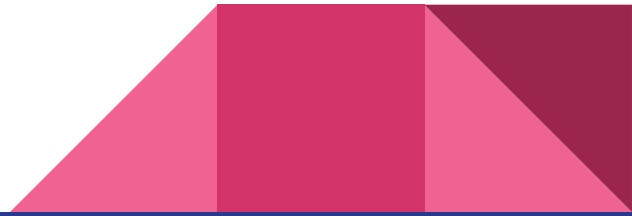
- Mine Bitcoins
  - nowadays very competitive / difficult
- Buy Bitcoins from an online exchange
  - bitcoins and/of fiat on exchange are controlled by the exchange
- Buy Bitcoins from an ATM
- Buy Bitcoins directly from another user
- Sell services or goods for bitcoins

Next: Tx Propagation and Mining

Proof of Work

From wikipedia:

> A **proof-of-work** (**POW**) **system** (or **protocol**, or **function**) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer.



Hashcash

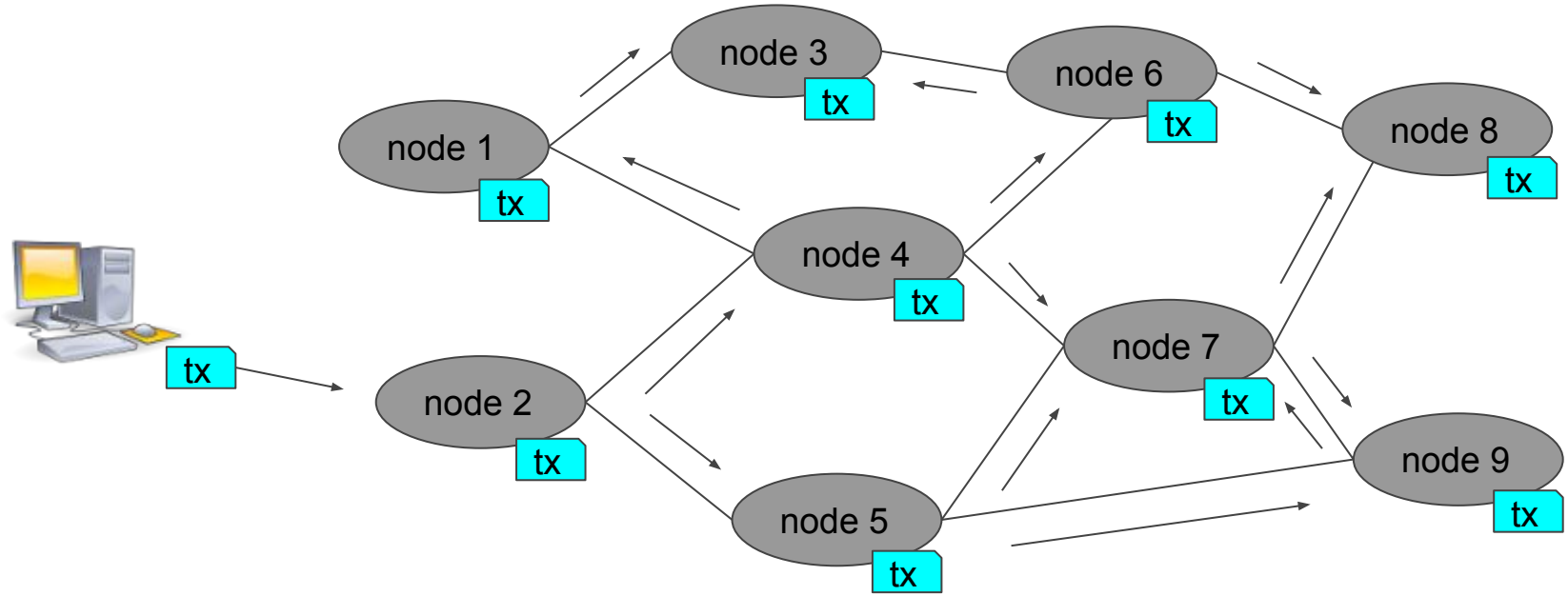
- Proof-of-work system
- hashing
  - arbitrary size to fixed size
  - one-way function

SHA256(“Bitcoin meetup!”) =>
d7d8992096b2261cd5fb01306149e1ab14a1cefa07e67
41feade682ecb307e89c

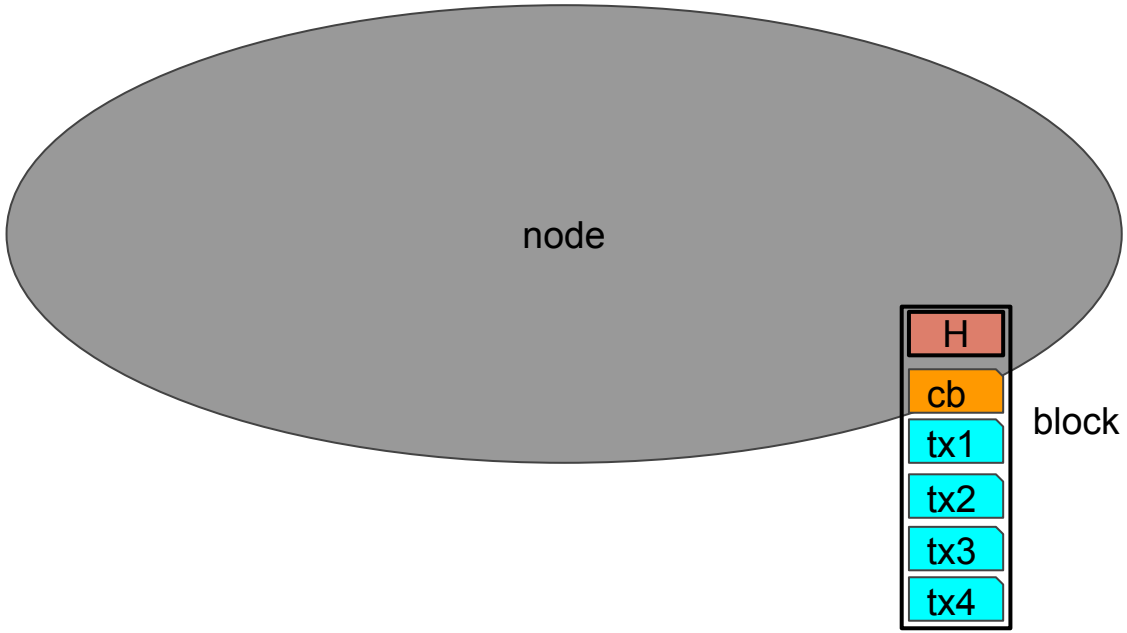
SHA256(“Bitcoin meetup.”) =>
a0236682605c9b25eddf5a82fc9cbe326ae7bffe69807
47ba39f5d4cd7cc2d17

- Example: dealing with email spam
  - hashcash stamp is required in the email
  - email and random number are hased
  - first 20 bits need to be zero
  - validation requires finding only one hash
  - proposed by Adam Back in 1997
- Example: dealing with Bitcoin transaction spam

Transaction Network Propagation



Miner Nodes - Blocks

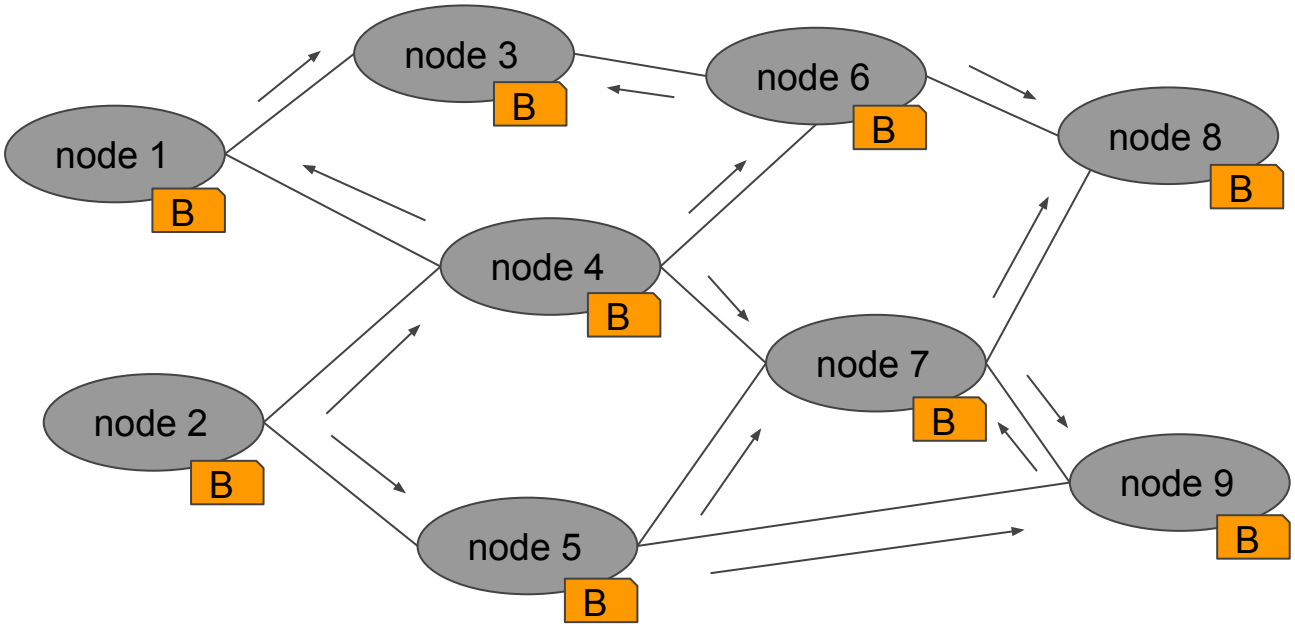


Bitcoin Mining

- block is decided
- mining process begins
  - block header is hashed
  - until hash is below target
  - nonce is increased
  - repeat
- nonce space limited (~4.2B)
  - timestamp
  - coinbase transaction

Block Header
Version
hashPrevBlock
hashMerkleRoot
timestamp
target / difficulty
nonce

Block Network Propagation



Block Propagation and Validation

- Blocks need to propagate to all known peers
  - of each node
- Each node will validate the new block
  - and add it to their blockchain
  - forever (!) - immutable ledger
- Miner with first valid new block gets the reward
  - After 100 confirmations!

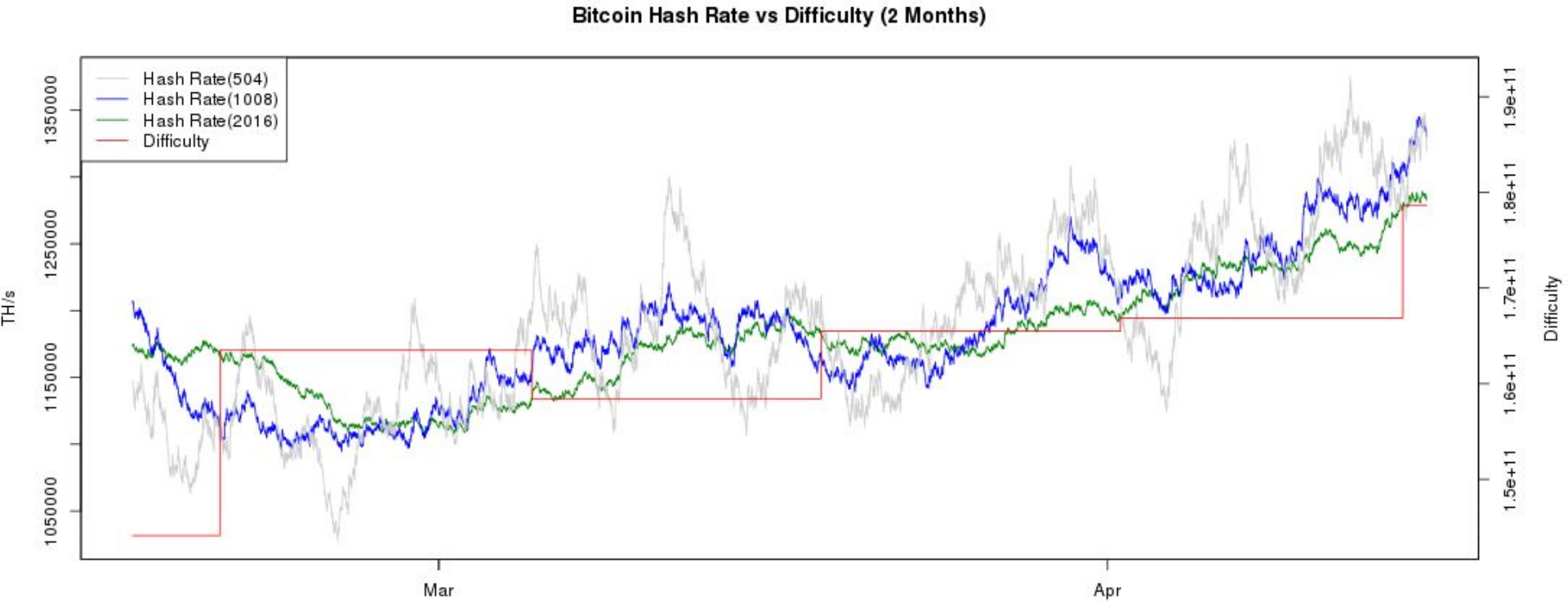
- How do we ensure that miners will not spam the network?
- How do we ensure consistent coin generation?

Mining predictability (15/04/2016)

- current network hashrate: 1,279,029 Th/s (1.27 Eh/s)
  - new block / ~10 minutes
- current difficulty: 178,678,307,672
  - many leading zeros
- but hashrate is fluctuating
  - 2016 blocks (~14 days)

```
Difficulty    = hashrate / (2^256 / max_target / intended_time_per_block)
              = hashrate / (2^256 / (2^208*65535) / 600)
              = hashrate / (2^48 / 65535 / 600)
              = hashrate / 7158388.055
```

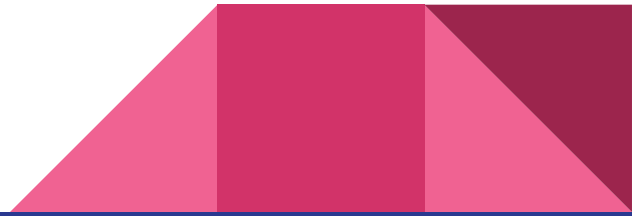
Bitcoin Hash Rate vs Difficulty



Next: Bitcoin Forking & Consensus

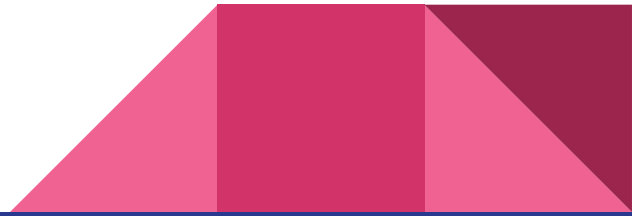
Introduction

- What is forking?
- Different types of forks
- Challenges and dangers



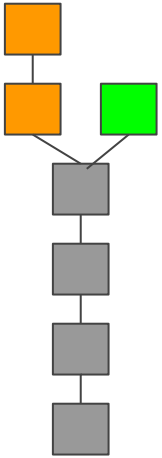
Fork (software)

- software engineering
  - project fork
  - source code is copied
  - developed independently
  - not just a development branch, but **divergence of direction**
- project and community splits in two
- examples
  - Linux Mint from Ubuntu (from Debian)
  - MariaDB from MySQL
  - PostgreSQL from Ingres
  - OpenSSH from OSSH
  - Inkscape from Sodipodi (from Gill)
  - Plex from XBMC

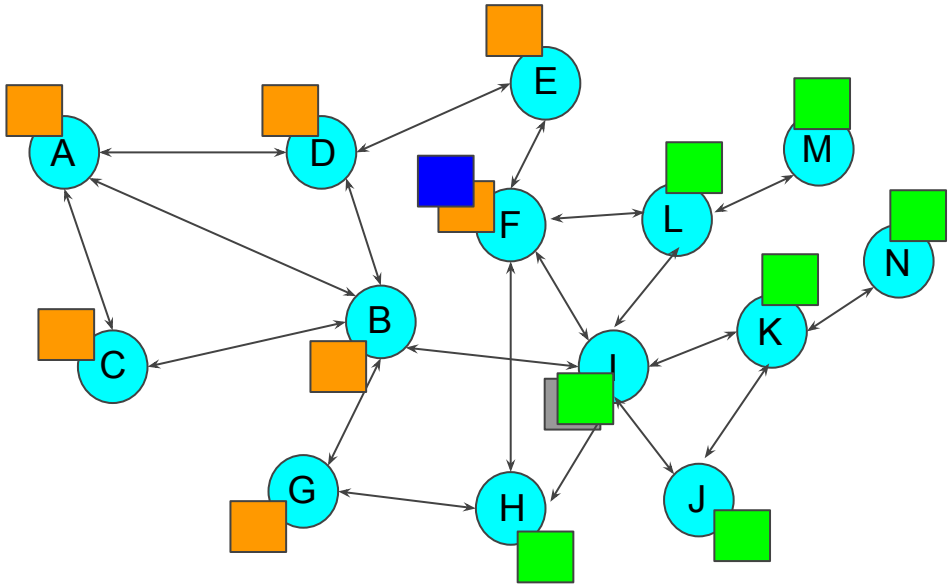


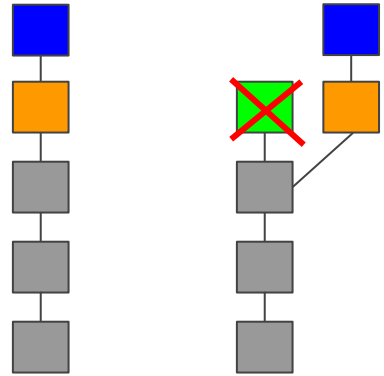
Fork (blockchain)

- blockchain
  - when the chain of blocks diverges/splits in two
  - forks are expected
  - part of decentralized consensus
- regular forks
- soft-forks
- hard-forks



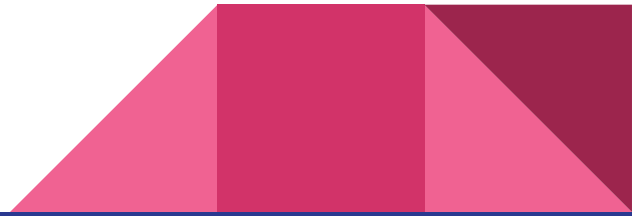
Regular forks (frequent)





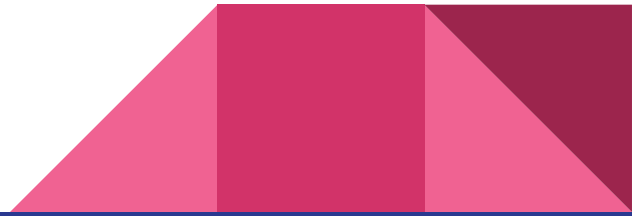
Soft- and Hard-forks

- nodes run the bitcoin open source software
  - different compatible versions (e.g. v0.11.2, v0.12.0)
  - different competing versions (e.g. Satoshi v.0.12.0, Classic v0.12.0)
  - even different implementations (e.g. btcd in GoLang)
- different rules will cause forks
  - intentional forks (software upgrades, alternative implementations)
  - unintentional forks (incompatibilities, bugs)
- soft-forks
  - blocks that would be valid are now invalid
- hard-forks
  - blocks that would be invalid are now valid



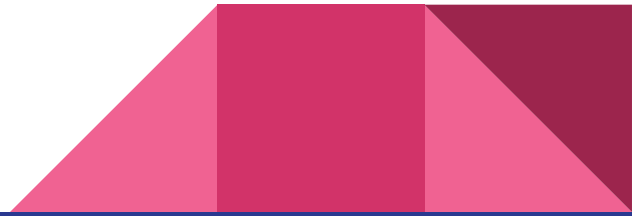
Soft-forks

- blocks that would be valid are now invalid
  - both old and new nodes produce blocks
  - new node blocks are fine
  - old node blocks are valid *only* to old nodes
  - forward compatible
- Bitcoin software upgrades
- optional upgrade
  - node can ignore the new blocks
  - at least 51% is needed for upgrade to succeed
- but
  - need to upgrade to use new features



Soft-forks (risks)

- *fake confirmation* vulnerability
  - old node blocks are valid *only* to old nodes
  - old node blocks will split the network
  - possibility to double spend even after one or more confirmations
  - until fork is resolved
- security risks for the old nodes
  - developers could make new node blocks to appear valid
  - old nodes will not understand the semantics but they will accepted it
  - used for P2SH transactions (BIP 16)
- *temporary* hard-fork (old nodes > 51%)

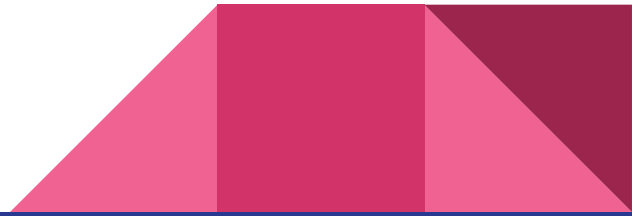


Hard-forks

- blocks that would be invalid are now valid
  - both old and new nodes produce blocks
  - old node blocks are valid *only* to old nodes
  - new node blocks are valid *only* to new nodes
- Bitcoin network is in conflict
  - two incompatible chains are supported
  - only resolution is for one of the sides to change software

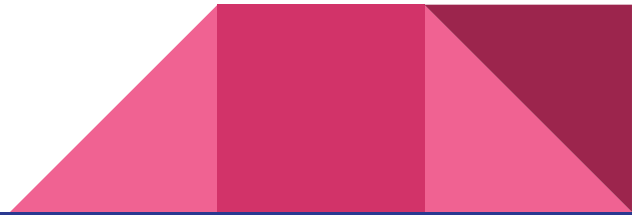
Hard-forks (risks)

- two chains simultaneously
  - fake confirmations vulnerability
  - **community splits**
- example
  - unintentional fork, March 2013
  - version 0.8 adopted by 60%
  - bug (Berkeley DB -> LevelDB)
  - detected quickly
  - people discussed resolution
  - major miner downgraded to 0.7
  - details: BIP 50



What will happen in a hard-fork?

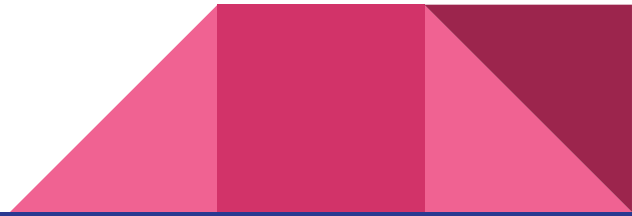
- blockchain is split in two parallel blockchains
- all bitcoins exist in both blockchains (!)
- miners, merchants, users have to choose
  - directly
  - indirectly
- all transactions after the split are in danger
  - If the split resolves some tx will be rollbacked (possible double-spends)
  - If not, trust in Bitcoin will diminish with price following after, …
- effectively the value of the network is split



Next: Alt-coins and Meta-coins

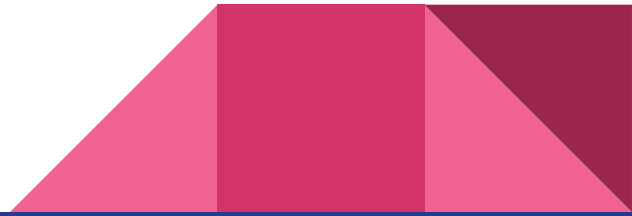
Alt-coins

- Coinmarketcap.com
  - ~680 currencies
- Forked Bitcoin’s codebase
  - Litecoin (scrypt, 2.5 mins, …)
  - Dash (X11, anonymity, master node architecture, …)
  - Monero (Cryptonight, anonymity, …)
- Cryptocurrency 2.0 projects
  - Ethereum
  - NXT
  - Bitshares
  - MaidSafe



Meta-coins

- Layer on top of Bitcoin’s infrastructure
  - Zerocoin (superceded by Zerocash)
  - Colored Coins (Open Assets)
  - CounterParty



Applications

- Remittances
- Payments
- Micropayments
- Bank services for the unbanked
- Store of Value
- **Digital Tokens**
- **Decentralized Applications**
- **Proof of Existence**
- **Smart Contracts**
- **Decentralized Autonomous Organizations**
- **Internet of Things / Machine to Machine**
- **Voting / Identity**
- **Private Blockchains**
- Other?

Greek Community

- Bitcoin and Blockchain Tech Meetup (Thessaloniki)
  - http://www.meetup.com/BlockchainGreece-1/
- Bitcoin and Blockchain Tech Meetup (Athens)
  - http://www.meetup.com/BlockchainGreece-0/
- Bitcointalk forum (Greek section)
  - https://bitcointalk.org/index.php?board=120.0
- Blog
  - http://www.bitcoin-gr.org/
- Facebook
  - https://www.facebook.com/groups/bitcoin.gr/?fref=ts
- Reddit
  - reddit.com/r/bitcoin_greece

Questions?

Linkedin: https://www.linkedin.com/in/kkarasavvas
Twitter: @kkarasavvas
Email: kkarasavvas@gmail.com
Bitrated: https://www.bitrated.com/kostas