The Blockchain

Decentralized Consensus

Leonhard A. Weese
President, Bitcoin Association of Hong Kong
leo@bitcoinhk.org

HKSTP, August 17, 2016

The Bitcoin Blockchain

Simple innovation or major disruption?

- A short explanation of the Bitcoin Blockchain
- Blockchain, the ‘underlying technology’
- The current state of the Blockchain ecosystem

Core Functionalities of a Blockchain

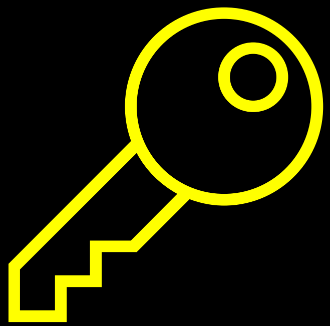
- Authentication: Keys and Addresses

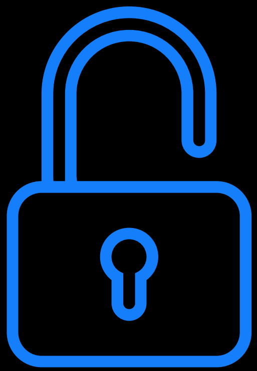
- Transactions: Receiving and Sending

- Mining: Ordering Transactions

Asymmetric Encryption

An algorithm creates a key and a lock that are mathematically linked (usually called public and private key).





Bitcoin Keys

A Bitcoin **private key** is a random number of the size 2^256

```
 96 249  65 252 210   5  46 154             60  f9  41  f2  d2   5  2e  9a
195 178  74 103  81 155 119  81             c3  b2  4a  67  51  9b  77  51
 68 120   6 134  89   4  22  43    🔑  ⟷    44  78   6  86  59   4  16  2b
 63  49 109 161 111 219  70 184             3f  31  6d  a1  6f  db  46  b8
```

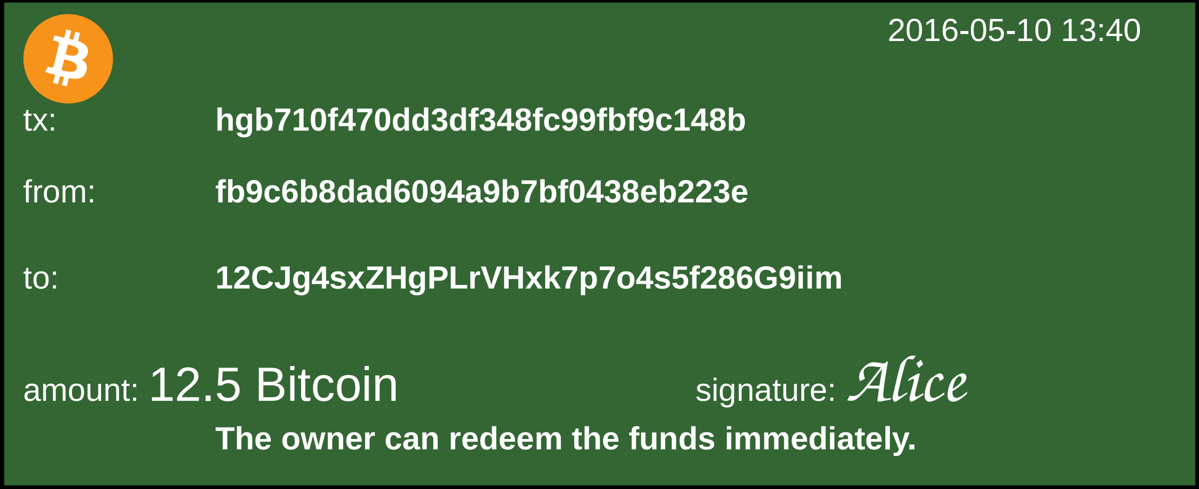
A Bitcoin **public key** is of the size 2^512, derived from the private key

```
153 186  18  34 219 170  96 172             B7  5c  95  73  c2  3d  aa  3c
 29  39  69  47  31 140 183  67             7f  75  67  6c  45  c7  d5  33
128 244 111 165 241  67 253  94             29  0f  83  4b  26  7b  c0  2e
  1 100 108  14  67  83 190 150    🔓  ⟷    cc  98  b1  d2  ed  a9  0a  f2
  4 220 165  87  97 107 198 179             94  ca  67  73  47  80  b8  60
148   1  49  36 155 168  96  32             54  c8  2f  ee  2a  bd  0b  06
104  72  83 144 234   0  32 249             7d  ef  80  87  51  25  dc  c3
177 184 142 210 110  89  67 122             db  3d  18  a1  b5  22  1e  a6
```

→ **19yebqamwdYPYrpchu4RXeefkeT4SnEQsR**

HKSTP, August 17, 2016

Bitcoin Transaction



2016-05-10 13:40

tx: **hgb710f470dd3df348fc99fbf9c148b**

from: **fb9c6b8dad6094a9b7bf0438eb223e**

to: **12CJg4sxZHgPLrVHxk7p7o4s5f286G9iim**

amount: 12.5 Bitcoin signature: *Alice*

The owner can redeem the funds immediately.

- Each transaction references a previous transaction
- Each transaction is signed by the sender
- The sender can specify more complicated rules
  (→ smart contracts)

The Blockchain

An open and public ledger of all transactions that ever occurred.
Anybody can connect to it and read, to write you must own Bitcoins.

Secret

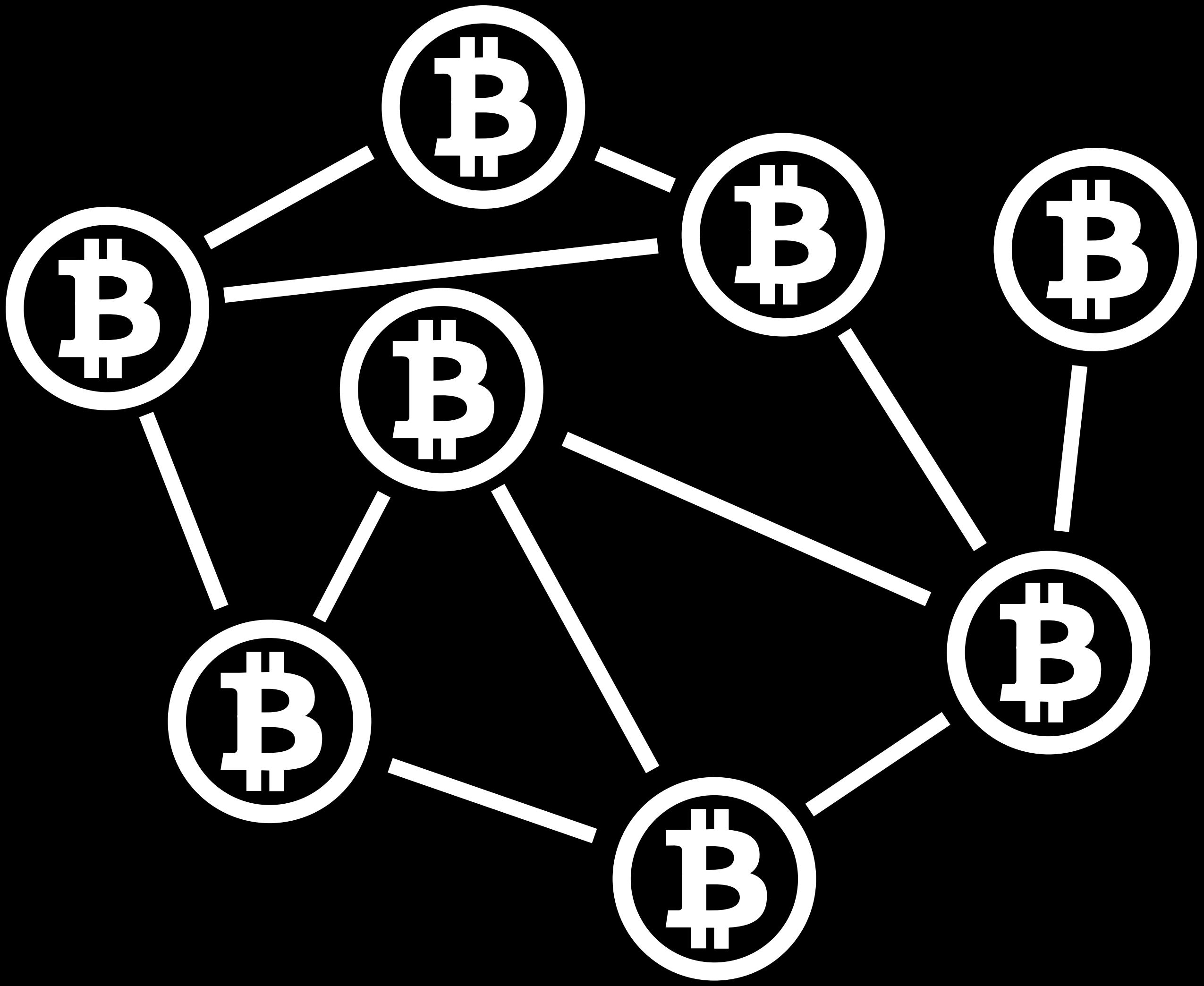
Name	Email	Password	Amount
John	john@gmail.com	yq4HRadgd1	14.50
Eve	eve@mail.ru	Kr391108Dy	68.90
Rob	rob@mail.com	32ERb9BJfc	16.80
Mary	mary@yahoo.com	Ffv60Tl7Gx	10.00
Tricia	tricia@gmx.com	B8gjKSQ8WJ	0.00
Jenny	jenny@gmail.com	9cz9a6lF6E	3.14
Lisa	lisa@168.com	9rbj4awx5c	76.00
Mike	mike@mail.com	JEDamykJR2	72.12
Linda	linda@mail.ru	UeHk5K0Cti	82.11
Bill	bill@yahoo.com	FoY1QqK19M	66.60
Barbara	barbara@mail.com	A15bgLRcYf	99.99
David	david@aol.com	K07nPtY6WQ	43.10
Rich	rich@hotmail.com	3JL1d8w8z0	0.11
Charles	charles@mail.com	0L28FkU0s6	76.89
Susan	susan@168.com	8cZ078KhYe	78.11
Chris	chris@gmx.com	FRiHp9Dyw1	99.34
Sarah	sarah@gmail.com	U1cTk3M759	82.00
Thomas	thomas@gmx.com	t58ZGcyfm1	23.50

Public

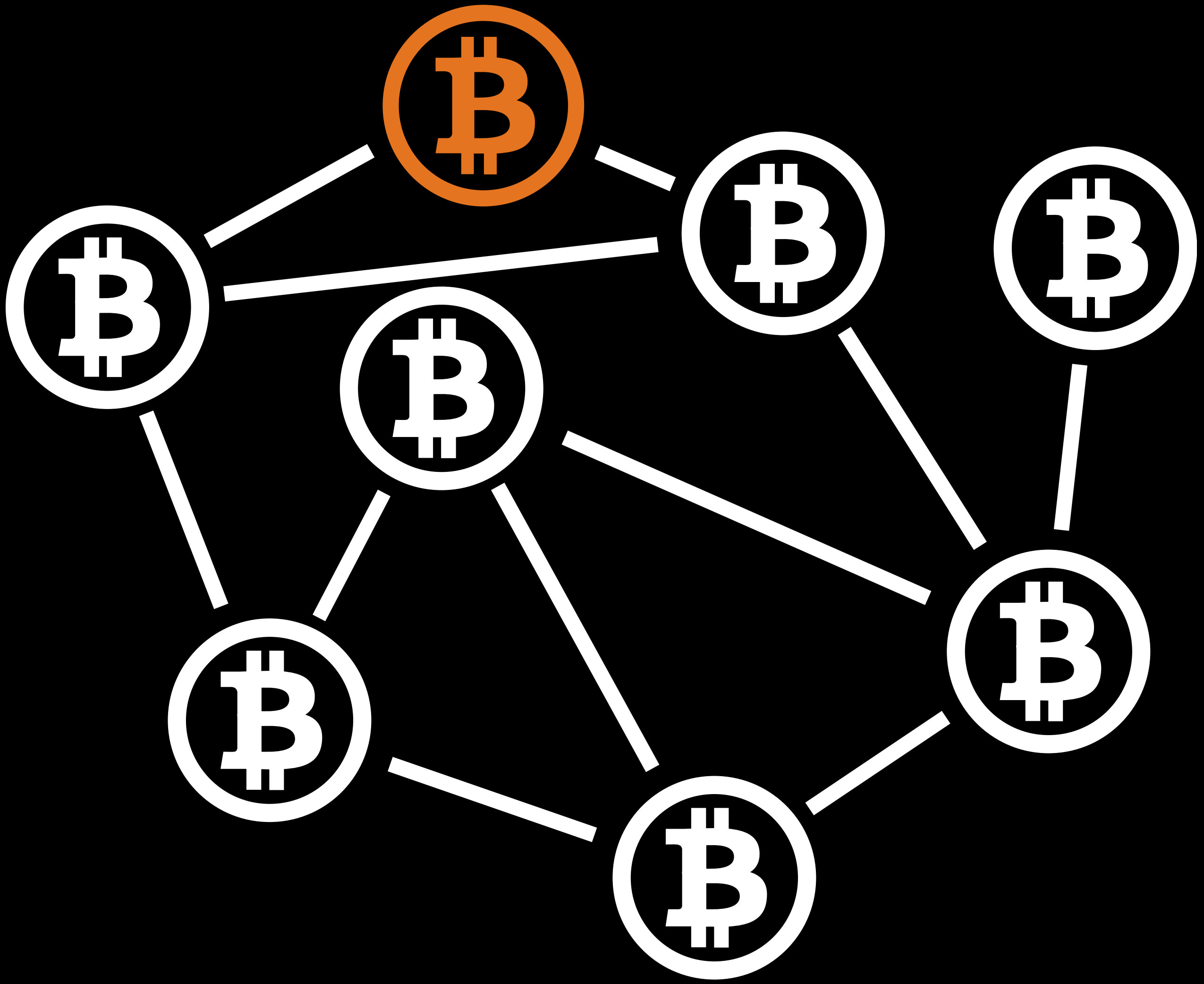
Bitcoin Address	Amount
1N1SHh6xaHJdip5RurTa4LFTGmYXUUXD1	1.000001
132bVSVq1FFUpE3kKbzWEefC4SBfWNhExP	12.000000
1LBC2T2TDbQaYhJMaARYQ8yRiKzDYAxkBL	0.001020
16fxvZvKuqWVc4S6Dv5xF9AzxB74gWoPEn	56.000000
16qd5N4o1wVtEpZnemyZGQ5uUqoVkFZhrj	76.999999
1KjNjQicZ9WqicwJsFFg3FbY4kxEE9Xkk7	3.141592
1JUy3ykdCEifUEGYFVybFyMtMhPtSS2rCw	67.154123
1MBgjx3PJMWYFc3FNR2ZvZ6pmkbguqRBkc	7.689000
1Ew4PUxcSvcZ2kaDTbF37B8wYEbDdv7WSo	12.342211
1FWKtbZA9Qf6gqoXzMCyLZHnjhngz7dYcR	86.124500
1BPdV2VU7gtQoThXTLb81maF2PusQ3cjih	34.233233
1GSS44GudHHE72jk5kQAjWziS2bnyBfua	123.235311
18bAdKMvJRq6wYENThHa5oP4mcQjgpbtRt	63.000000
196R1YruHX5GZh4bPRJXAiKQ7h55TdR8Ku	0.000001
15vpZ7RUuzgEknfdsoRY1uHgvVBCZFyGnR	11.113456
16J9F5wzDg8ZgcRq1abPKwaRV8YdDzni2a	89.666111
1Eo88wpghmqvUDNfvbckf7C9wAdn2FW8P7	11.438811
1EpYRLWsVXpVcTF8aEeNdLN74F5tjRGh1	666.893234

Nodes

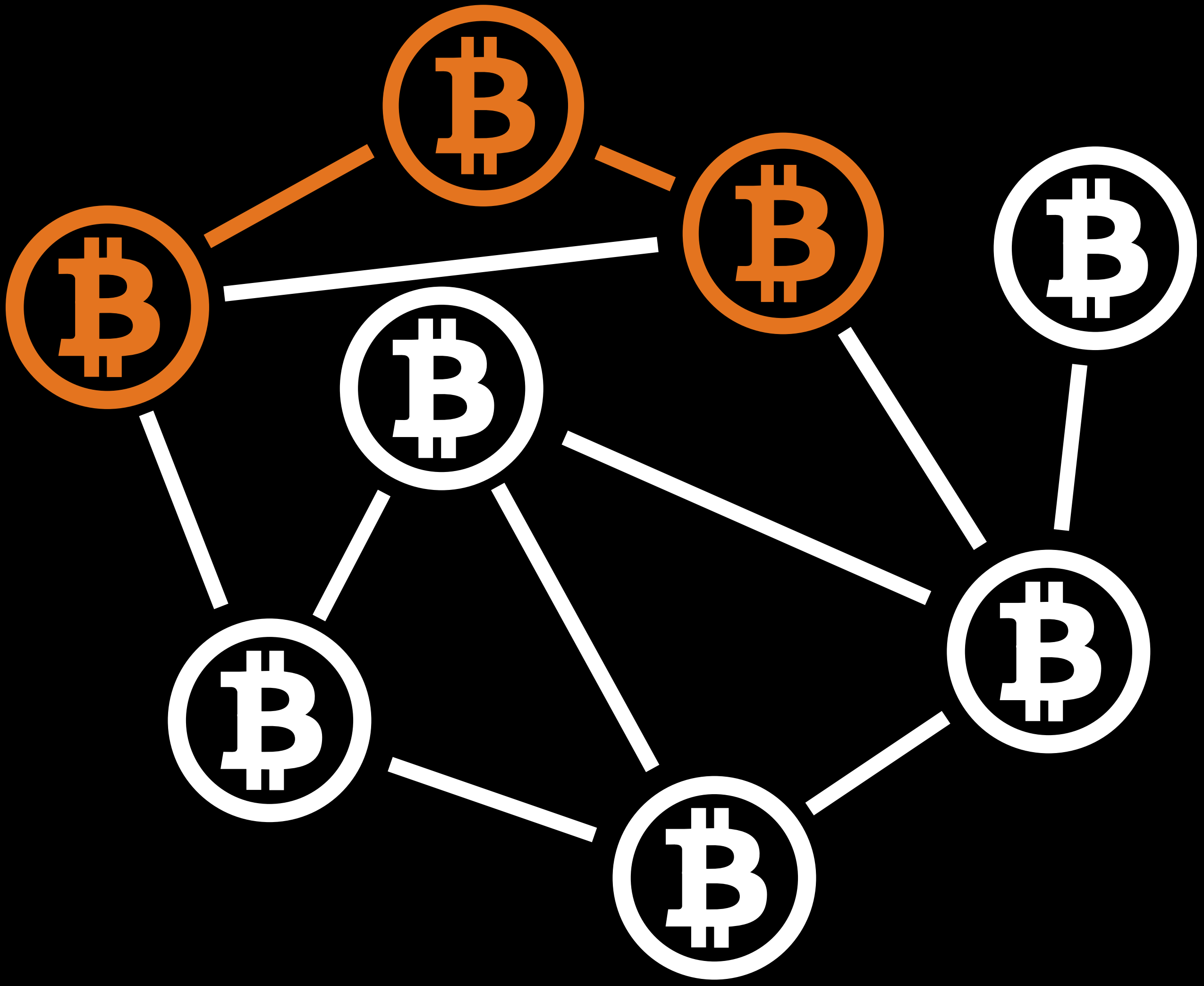
- Nodes make up the Bitcoin network
- Anybody can connect to other nodes and download the blockchain
- Nodes listen to transactions and check if they are valid
- Valid transactions are forwarded and stored, invalid ones rejected



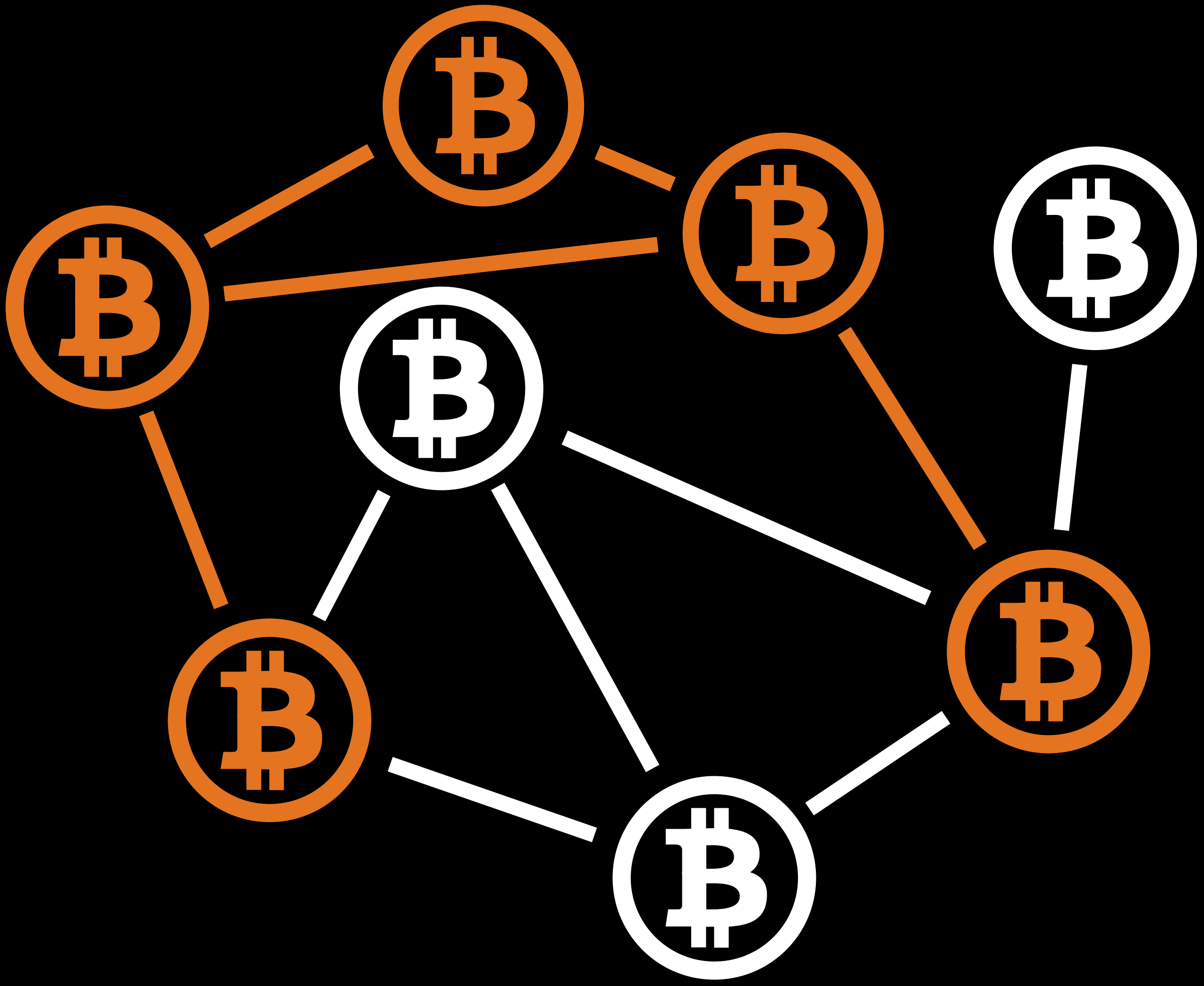
HKSTP, August 17, 2016



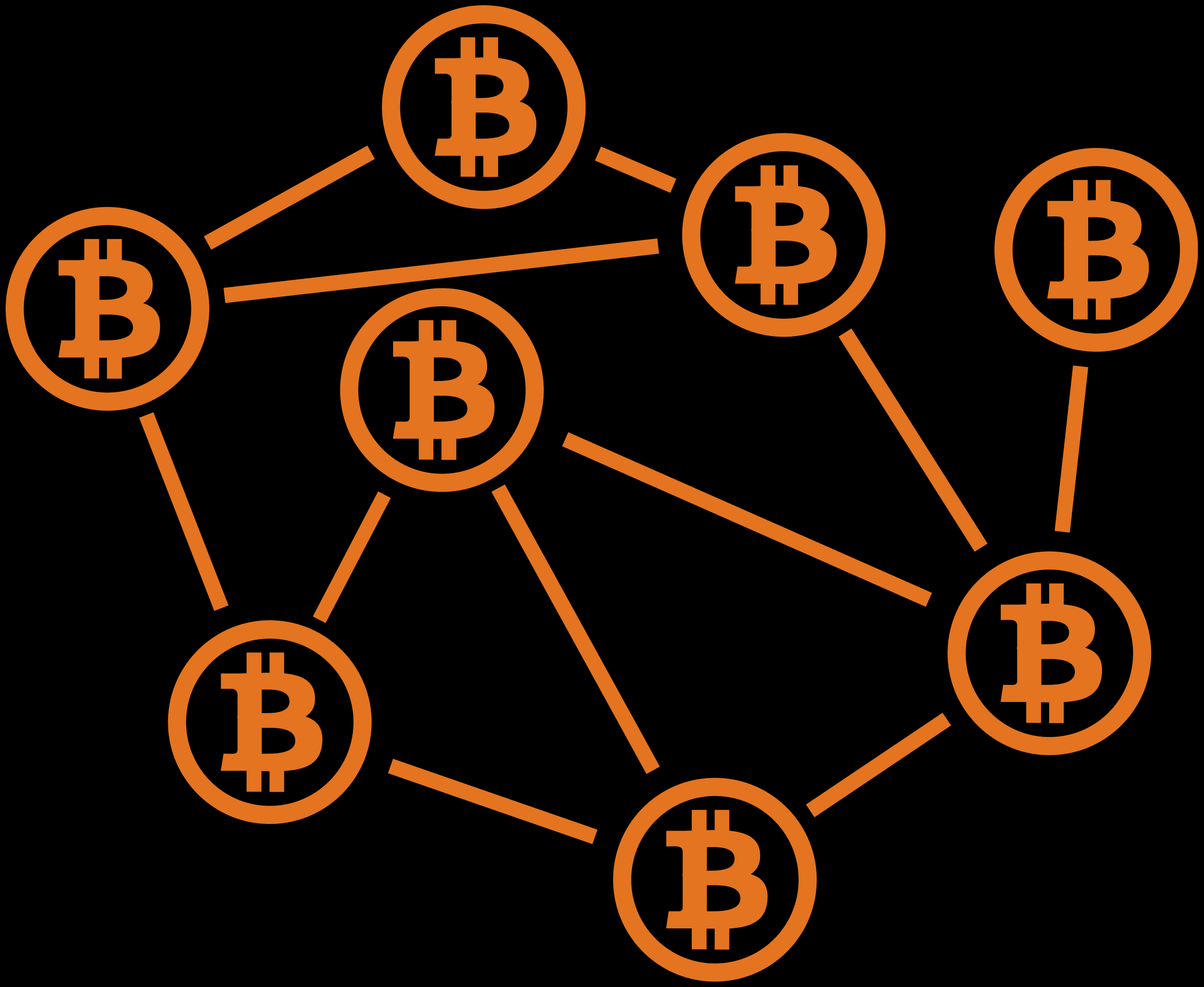
HKSTP, August 17, 2016



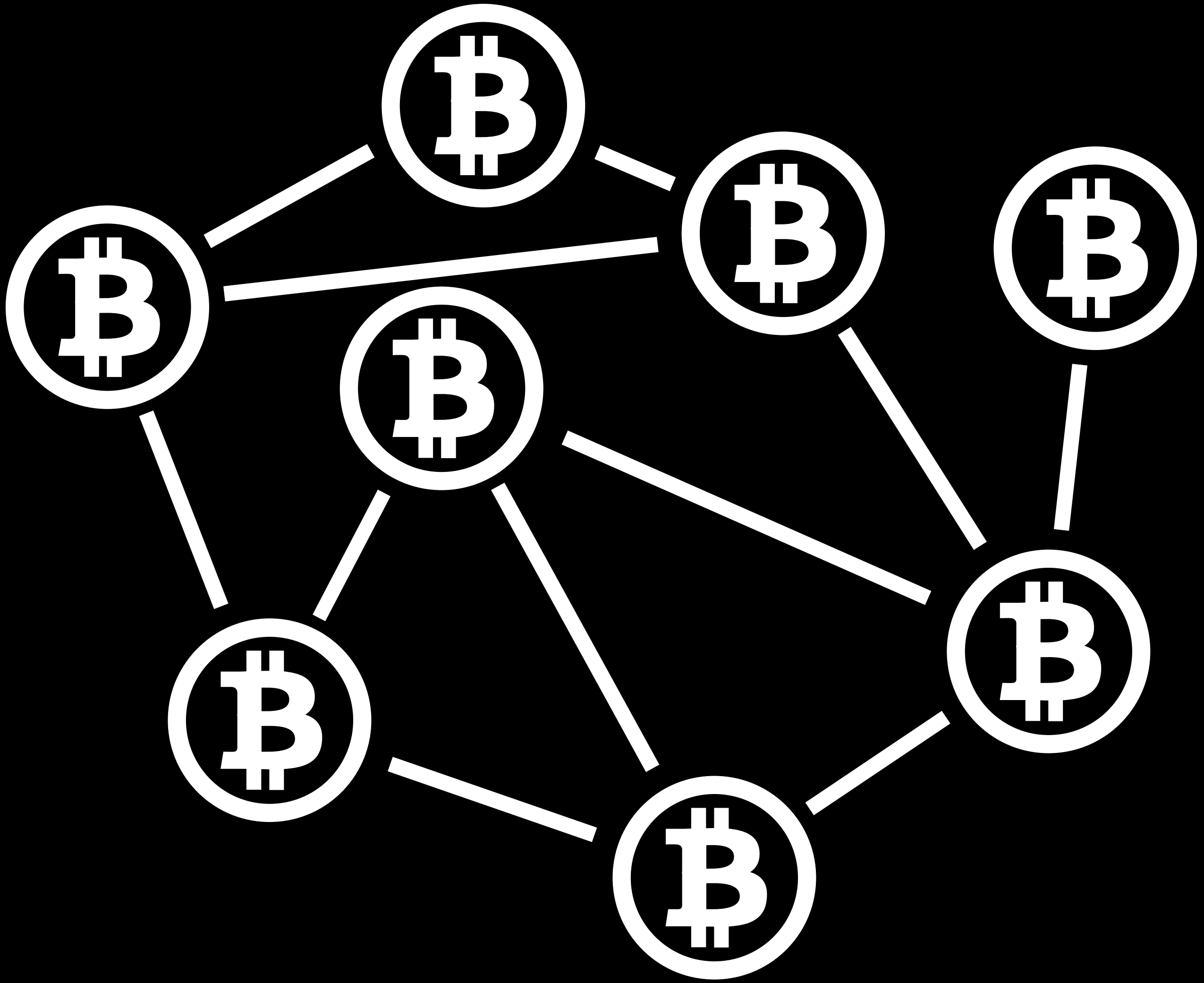
HKSTP, August 17, 2016



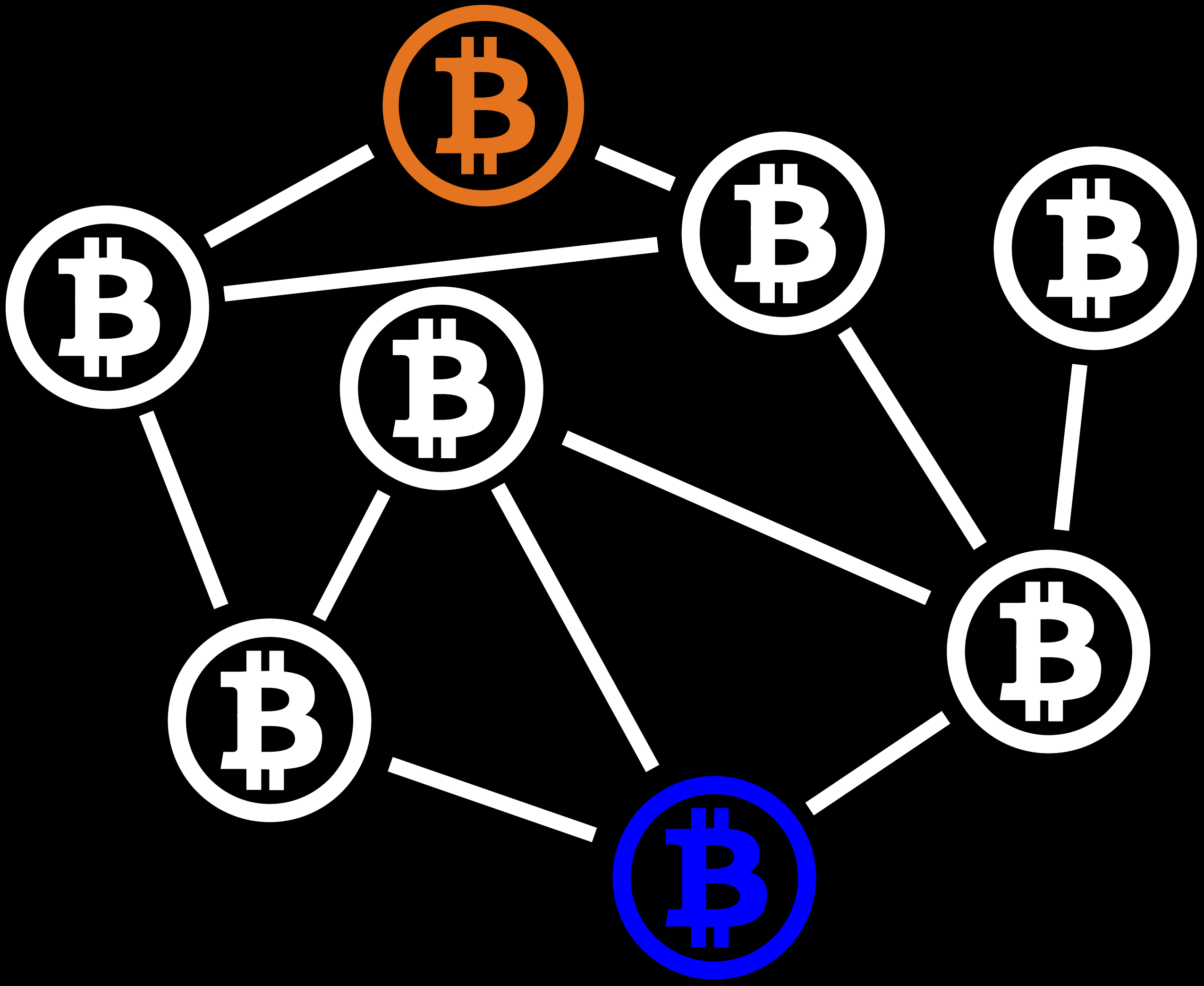
HKSTP, August 17, 2016



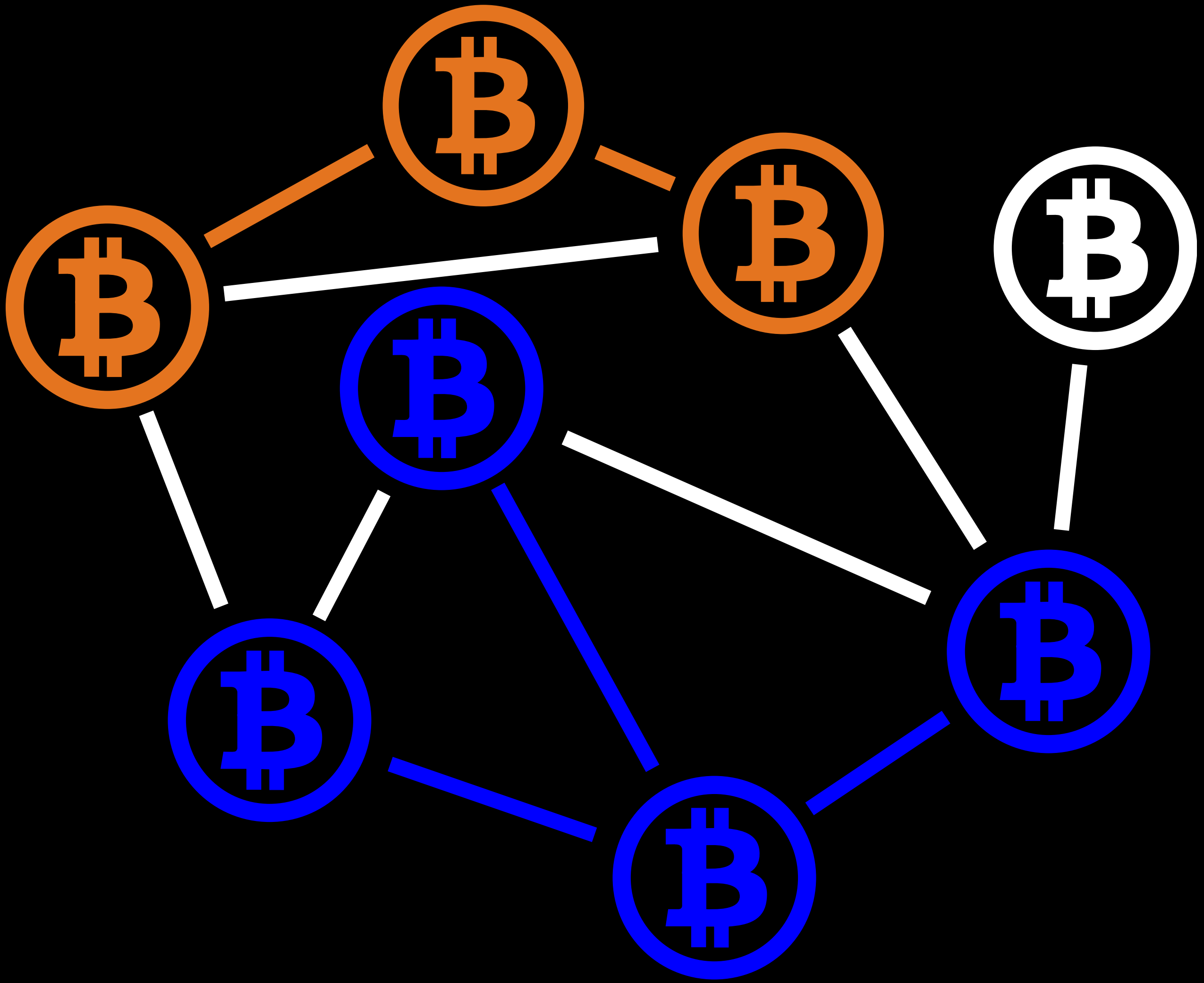
HKSTP, August 17, 2016



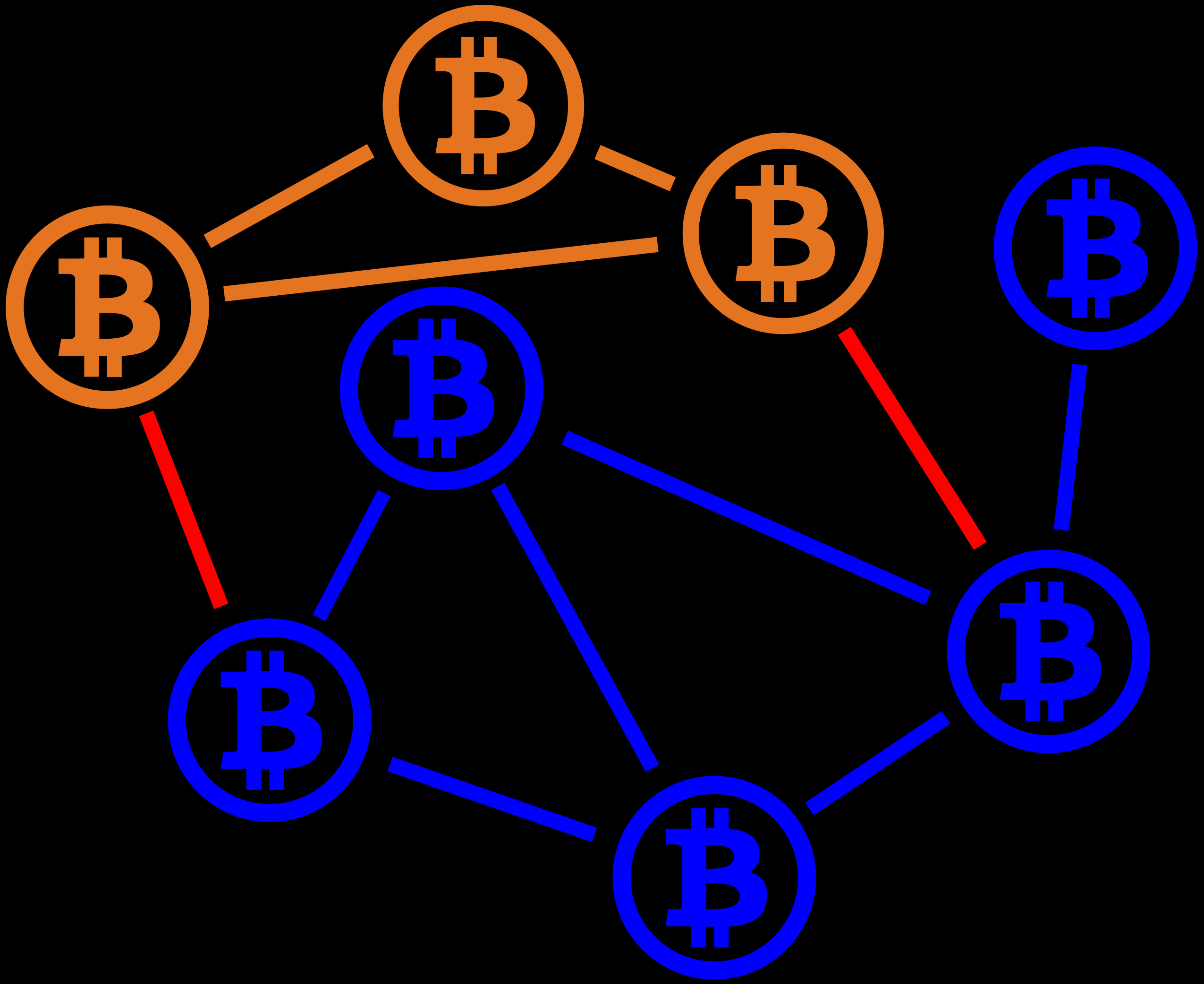
HKSTP, August 17, 2016



HKSTP, August 17, 2016



HKSTP, August 17, 2016



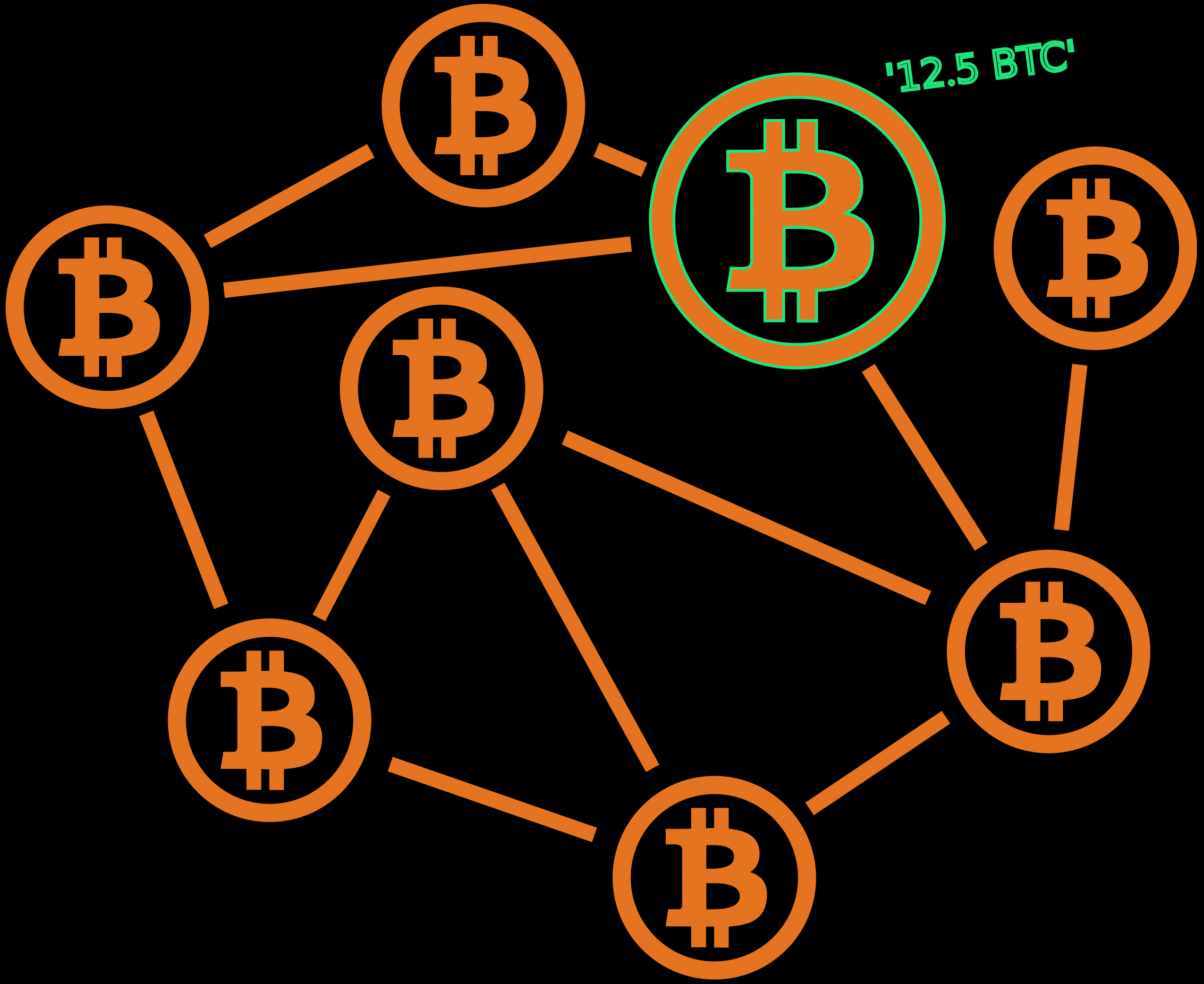
Mining

Which node gets to build the next block?

- Pick any node?
- Pick the richest node?
- Pick the node that is working the most!

Work is Force times Distance

- Take the hash of the previous block and all transactions
- Guess a random number
- Hash it
- Does it have enough leading zeroes?


'12.5 BTC'

Mining

- The random number is the solution
- Published with the block to other nodes
- The miner is allowed to send themselves ~~25~~ 12.5 Bitcoins 'from nowhere'
  - > Bitcoins are slowly distributed to miners
- Miners mine at the margin and need to pay electricity, creating a liquid market for Bitcoins

There are Problems

- Bitcoin can only handle ~7 transactions per second
- Fungibility cannot be guaranteed
- Unexpected behavior of bitcoin software
- Information security in a horrible state
- Mining consumes vast amounts of energy
- Attractive for criminals
- Strong fluctuations in value

Beyond Bitcoin

- A blockchain can do a lot beyond currency
- A blockchain can do nothing without currency

- Blockchains have insane network effects.
  → a single blockchain will likely dominate
  → unattractive if only few participants

Beyond Bitcoin

- Separate blockchains (Ethereum)
- Colored coins (Counterparty)
- Sidechains (Liquid)
- Database with version control on Bitcoin (Nasdaq Private Market)
- Permissioned Blockchains

Permissioned Blockchains

- How to permission a blockchain?
  - Limit 'mining' and nodes to select organizations
  - Require users to register their public keys
  - Hold the majority of funds

- How to deal with privacy issues?
- When is a blockchain just a database?

On the Blockchain

- Currency (Bitcoin, Dollars, Airmiles)
- Identity (URLs, User Names)
- Assets (Stock, Art)
- Rights (Music, Land)
- Contracts (Loans, Derivatives)
- Programs (Voting, Quality Control)

Identity

- URLs highly valuable
- Transfer of ownership expensive and difficult
- DNS records easy to manipulate and censor

- In Namecoin anybody can register a .bit domain, update its DNS records, transfer it

Art

- Value comes from originality (eg old masters)
- Value comes from scarcity (eg limited prints)
- Traded on second market through trust

- Bitcoin Blockchain can prove originality, scarcity and ownership through Colored Coins

Land Registry

- Often not even centralized database over who owns which land. Risk of corruption
- Proof of ownership becomes trivial
- Transfer requires little trust

- Database and transactions can be hashed into the Bitcoin Blockchain and published separately

Stock

- Expensive and complicated to hold stock yourself
- Transferring stock between markets is difficult
- Proving ownership and voting requires trust
- Payouts make anonymous ownership impossible

- Cryptostock

Land Registry

- Often not even centralized database over who owns which land. Risk of corruption
- Proof of ownership becomes trivial
- Transfer requires little trust

- Database and transactions can be hashed into the Bitcoin Blockchain and published separately

Leonhard A. Weese

President, Bitcoin Association of Hong Kong

leo@bitcoinhk.org

@LeoAW

https://www.bitcoinhk.org

PGP: A087 7877 C0CF E886 1B35 118D 832E 6328 4080 D73A

icons from iconfinder.com

HKSTP, August 17, 2016