The Blockchain

Decentralized Consensus

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

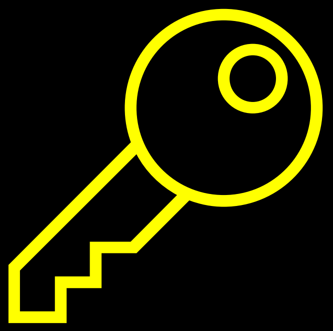
Hong Kong, May 25, 2017

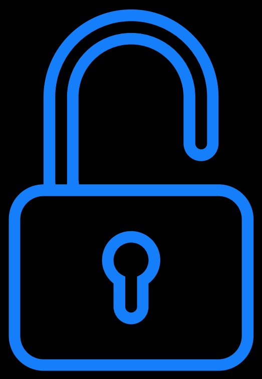
Core Functionalities of a Blockchain

- Authentication: Keys and addresses
- Transactions: receiving and sending
- Mining: Ordering transactions

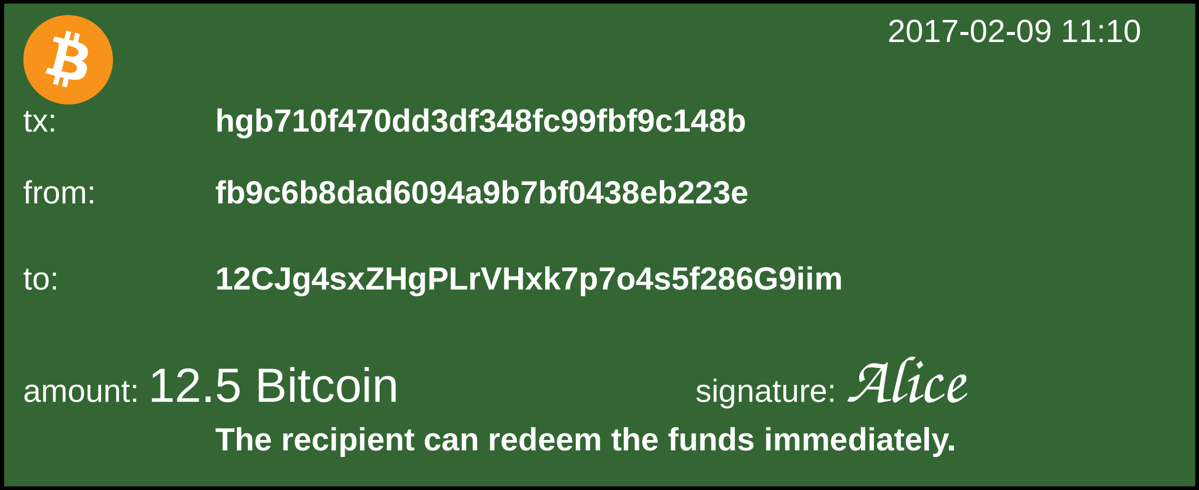
Asymmetric Encryption

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





Bitcoin Transaction



2017-02-09 11:10

tx: **hgb710f470dd3df348fc99fbf9c148b**

from: **fb9c6b8dad6094a9b7bf0438eb223e**

to: **12CJg4sxZHgPLrVHxk7p7o4s5f286G9iim**

amount: 12.5 Bitcoin signature: *Alice*

The recipient 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

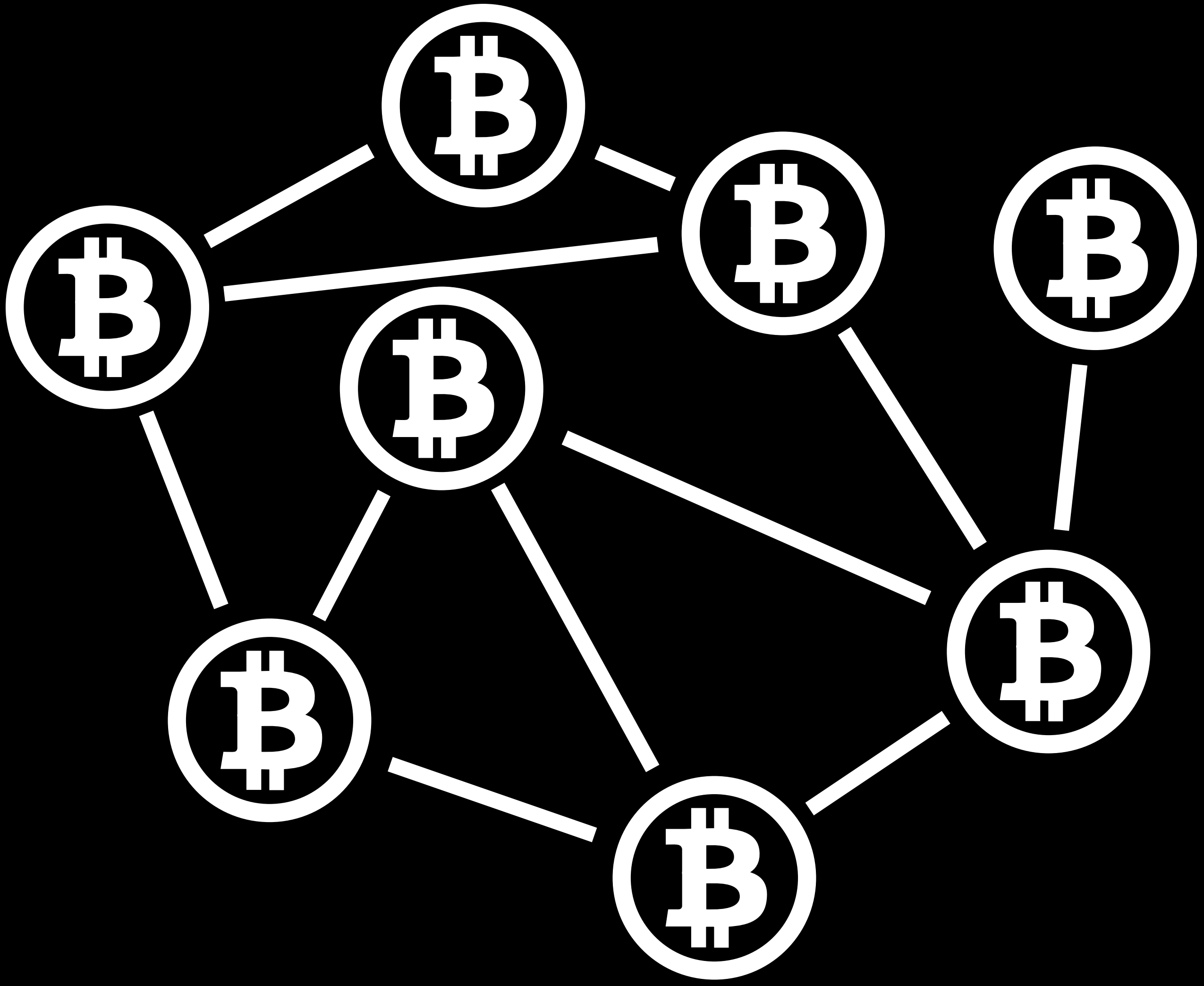
Name	Email	Password	Amount
John	john@gmail.com	yq4HRadgd1	14.50
Eve	eve@mail.ru	Kr391108Dy	68.90
Rob	rob@mail.com	32ERb9BJfc	16.80
Mary	mary@yahoo.com	Ffv60Tl7Gx	10.00
Tricia	tricia@gmx.com	B8gjKSQ8WJ	0.00
Jenny	jenny@gmail.com	9cz9a6lF6E	3.14
Lisa	lisa@168.com	9rbj4awx5c	76.00
Mike	mike@mail.com	JEDamykJR2	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

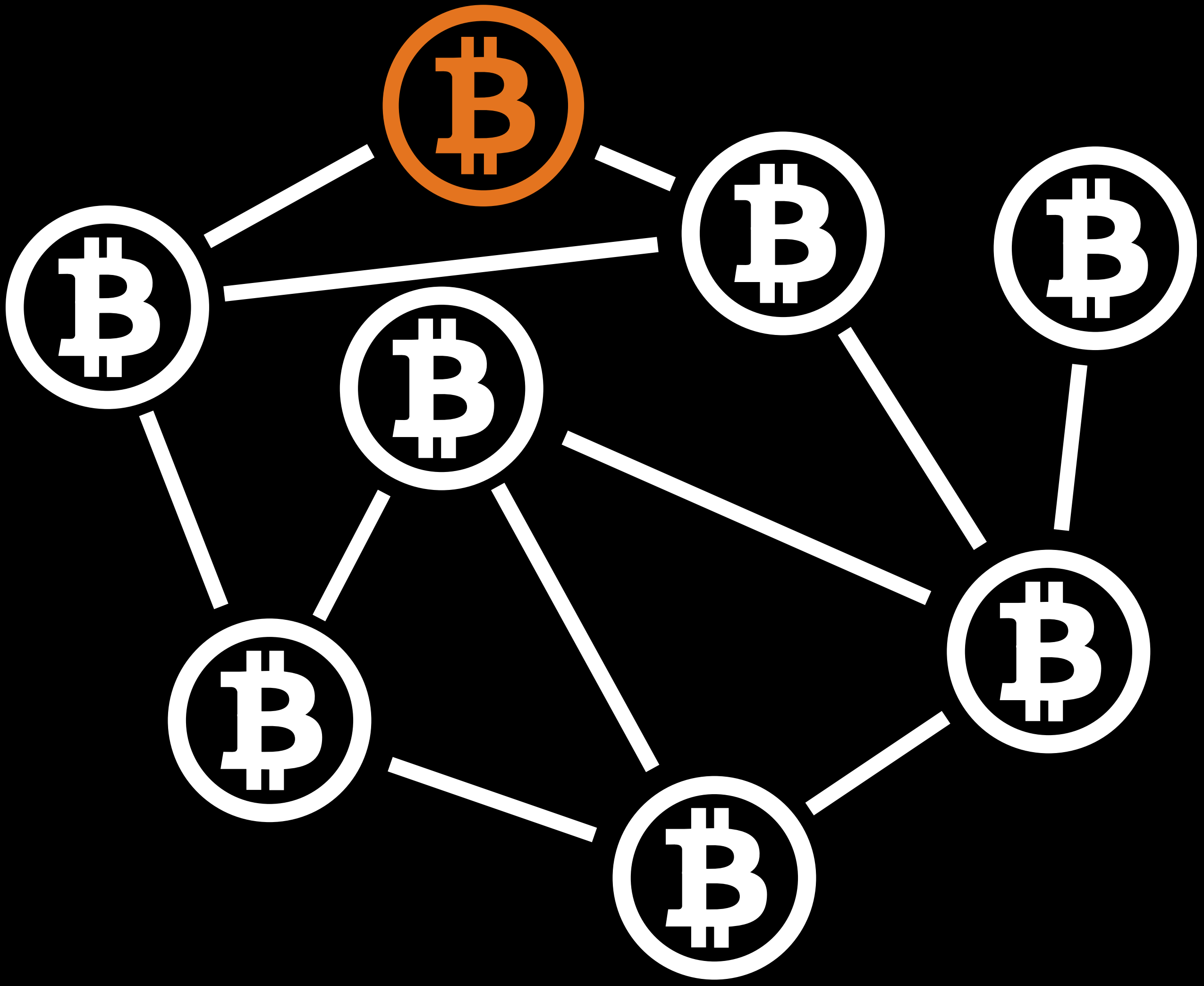
Bitcoin Address	Amount
1N1SHh6xaHJdip5RurTa4LFTGmYXUUXD1	1.000001
132bVSVq1FFUpE3kKbzWEefC4SBfWNhExP	12.000000
1LBC2T2TDbQaYhJMaARYQ8yRiKzDYAxkBL	0.001020
16fxvZvKuqWVc4S6Dv5xF9AzxB74gWoPEn	56.000000
16qd5N4o1wVtEpZnemyZGQ5uUqoVkFZhrj	76.999999
1KjNjQicZ9WqicwJsFFg3FbY4kxEE9Xkk7	3.141592
1JUy3ykdCEifUEGYFVybFyMtMhPtSS2rCw	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

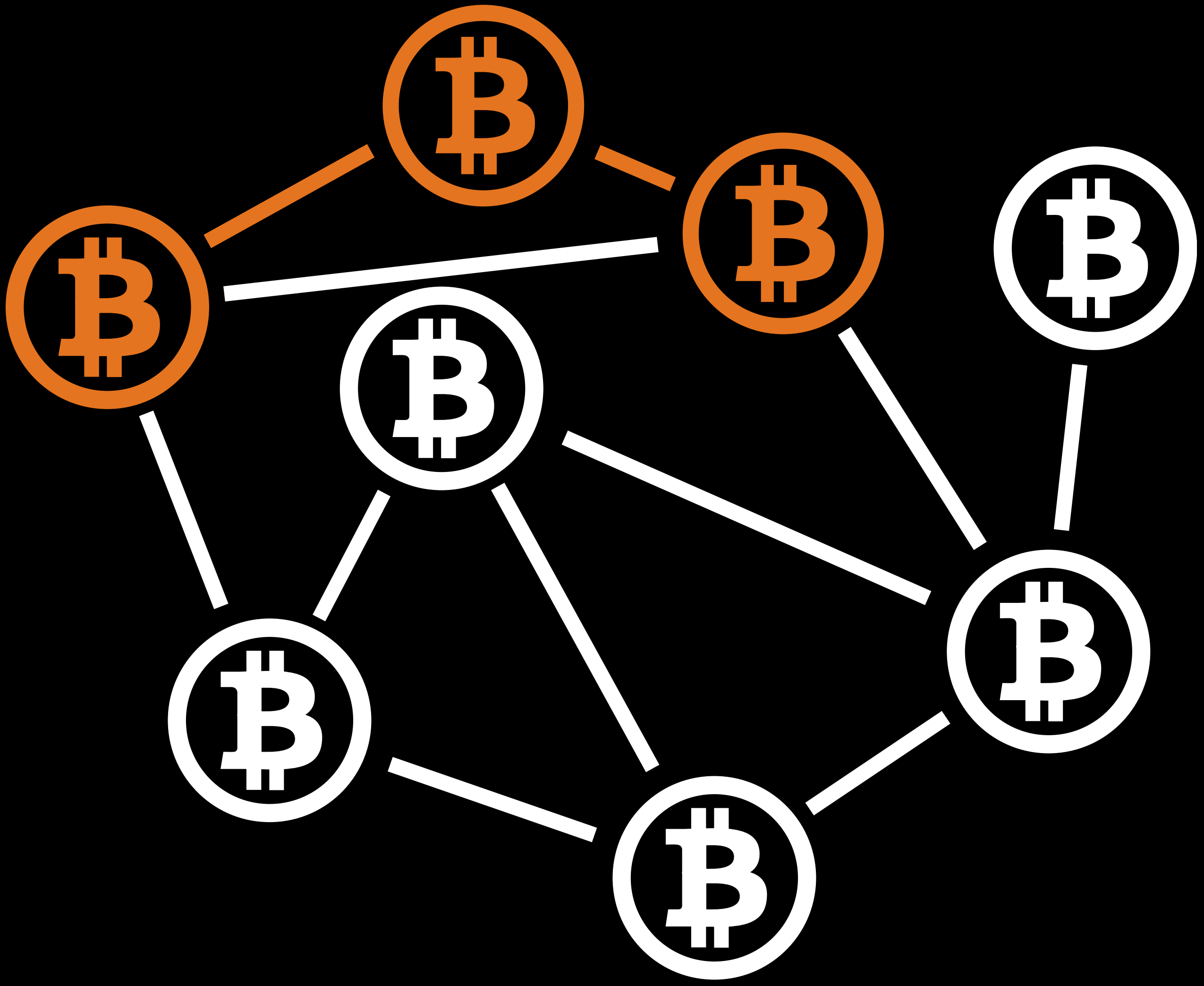
- Nodes make up the Bitcoin network
- Anybody can connect to other nodes and download the blockchain
- Nodes listen to transactions and check if they are valid
- Valid transactions are forwarded and stored, invalid ones rejected



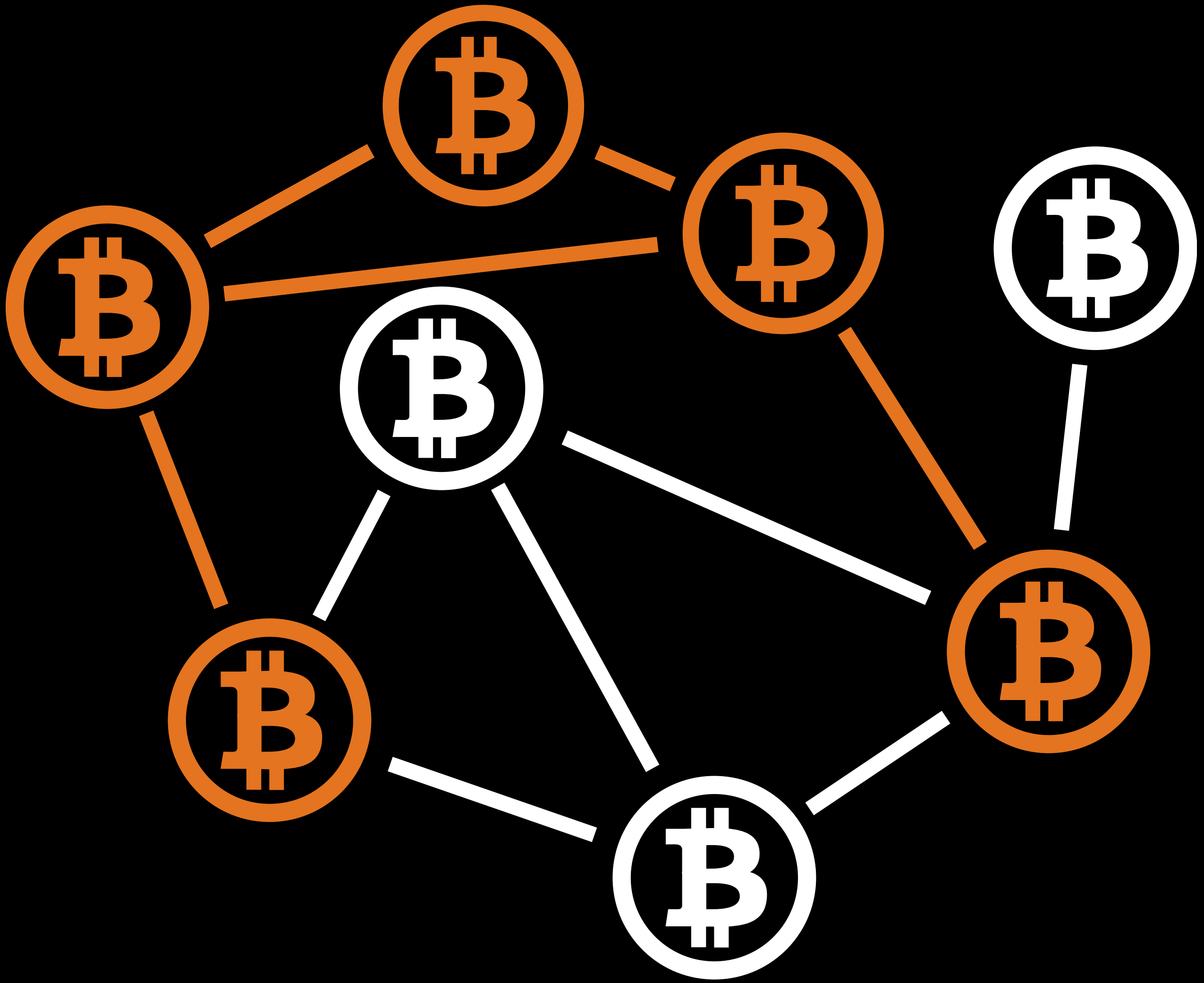
Hong Kong, May 25, 2017



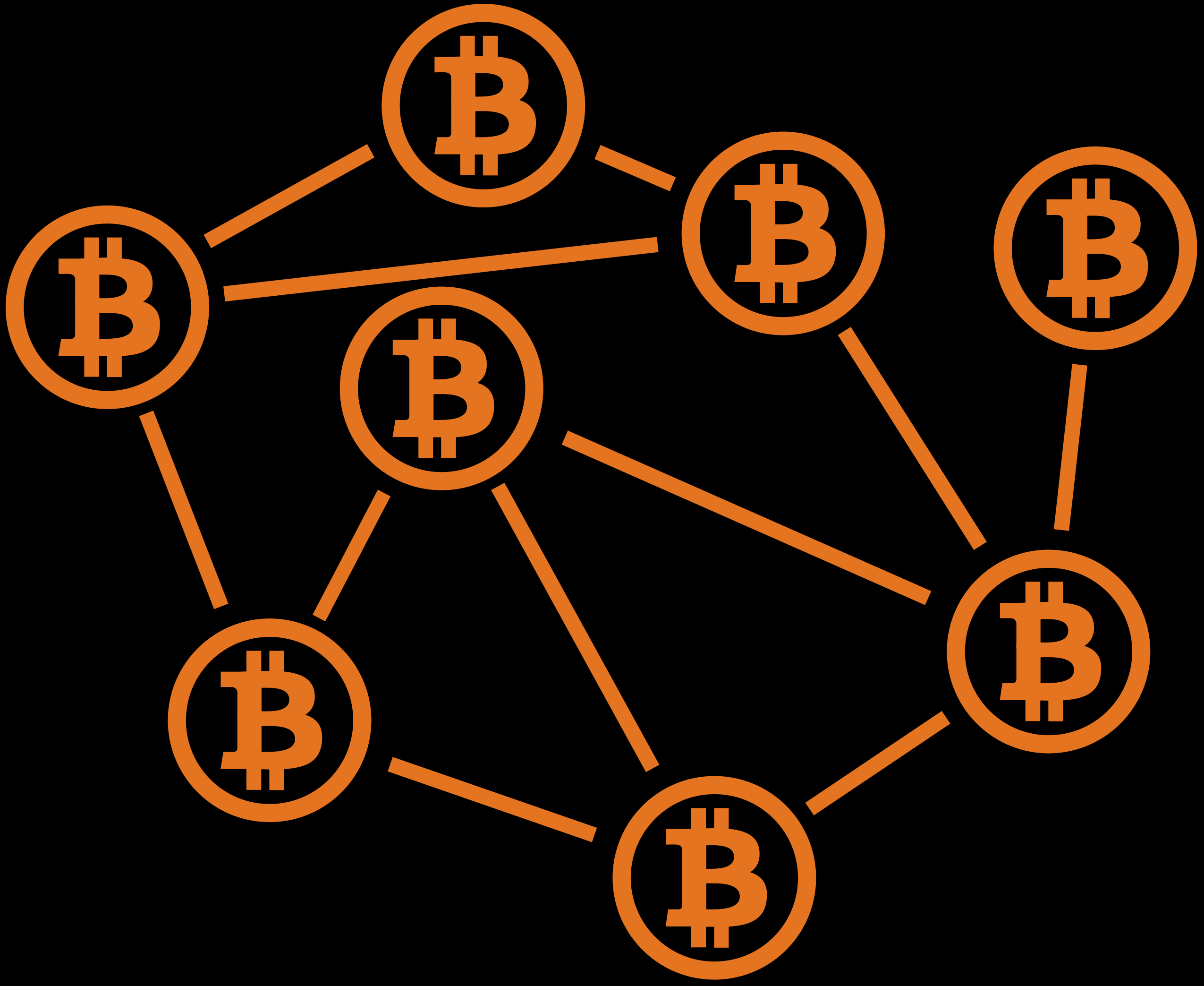
Hong Kong, May 25, 2017



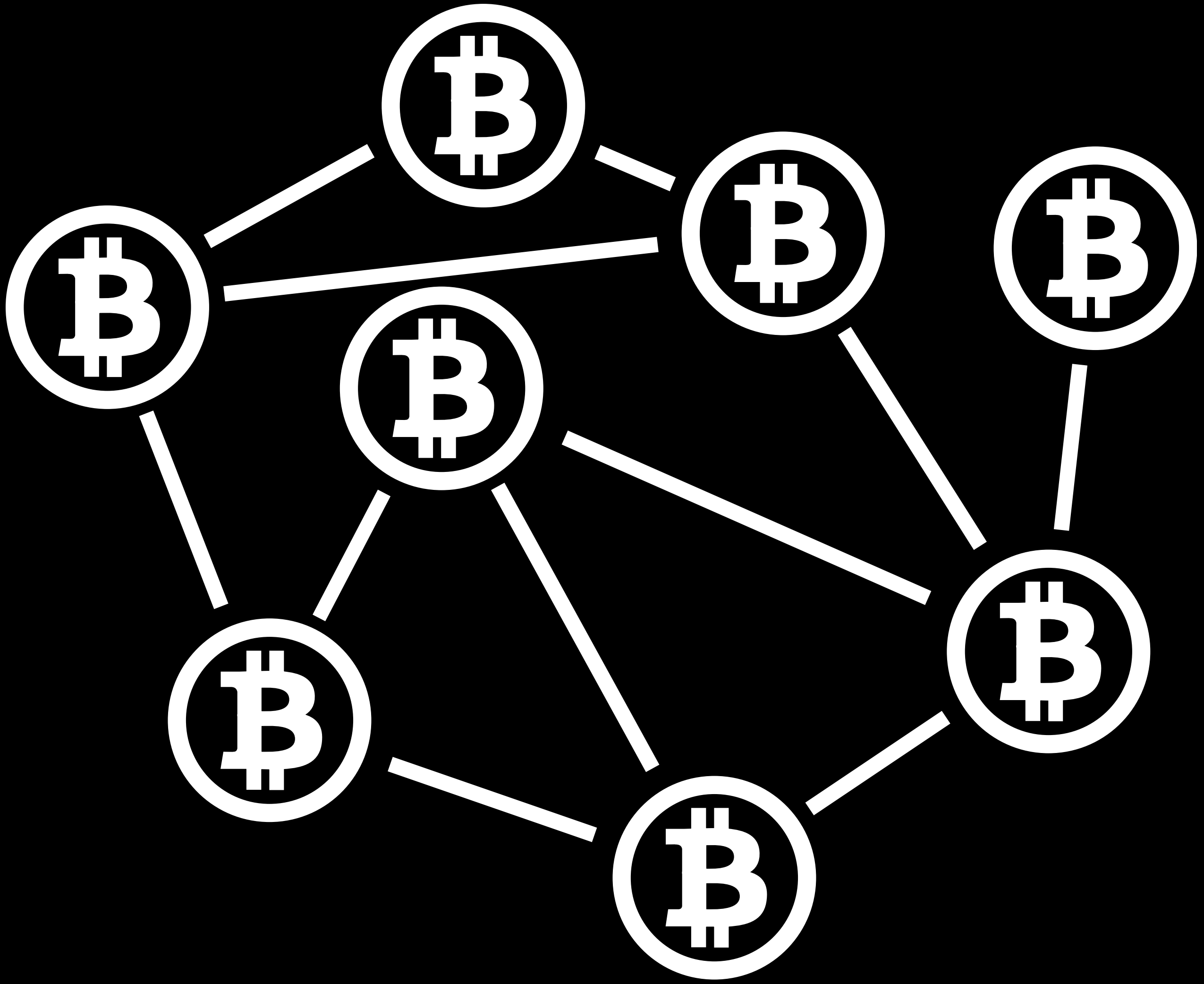
Hong Kong, May 25, 2017



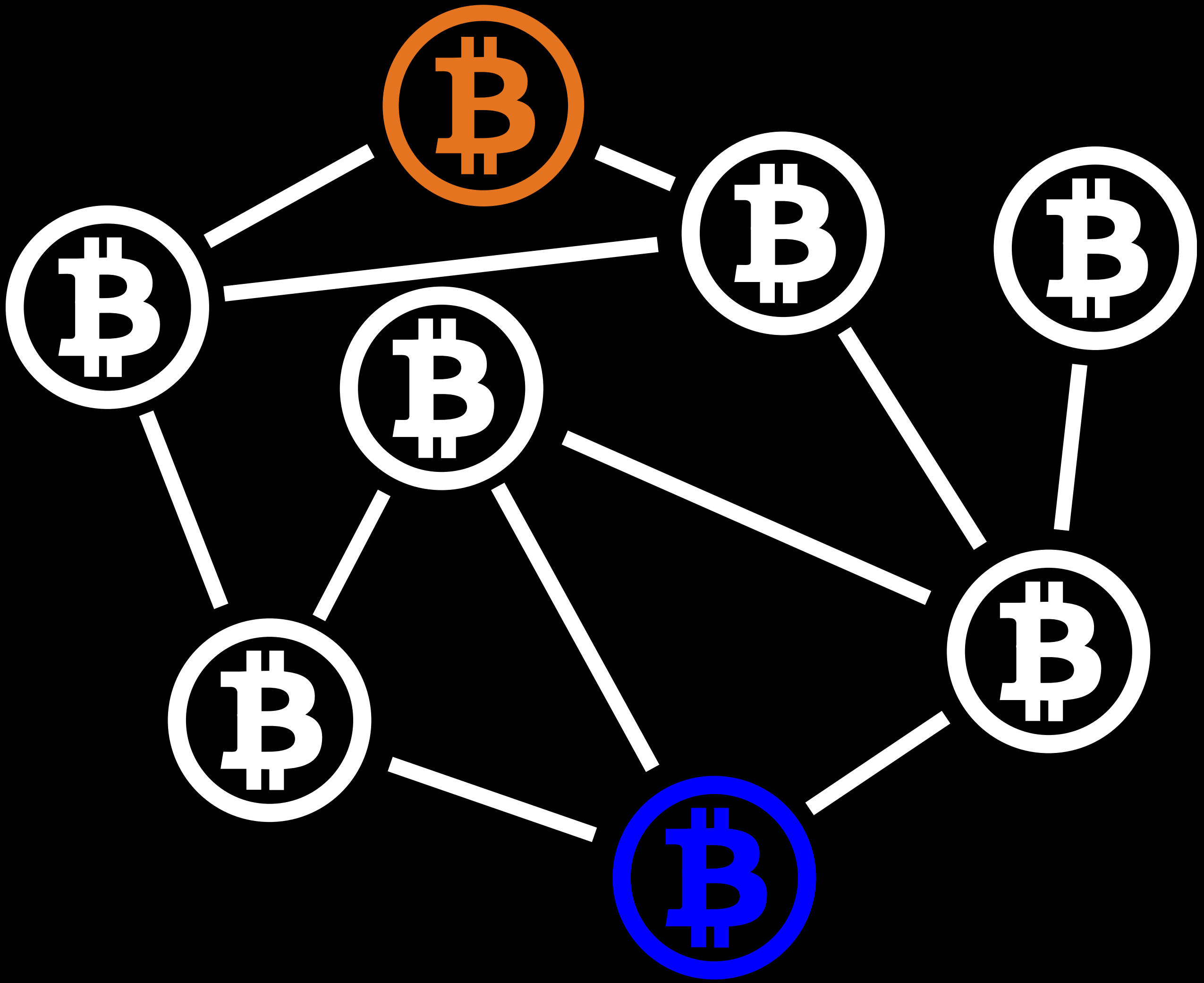
Hong Kong, May 25, 2017



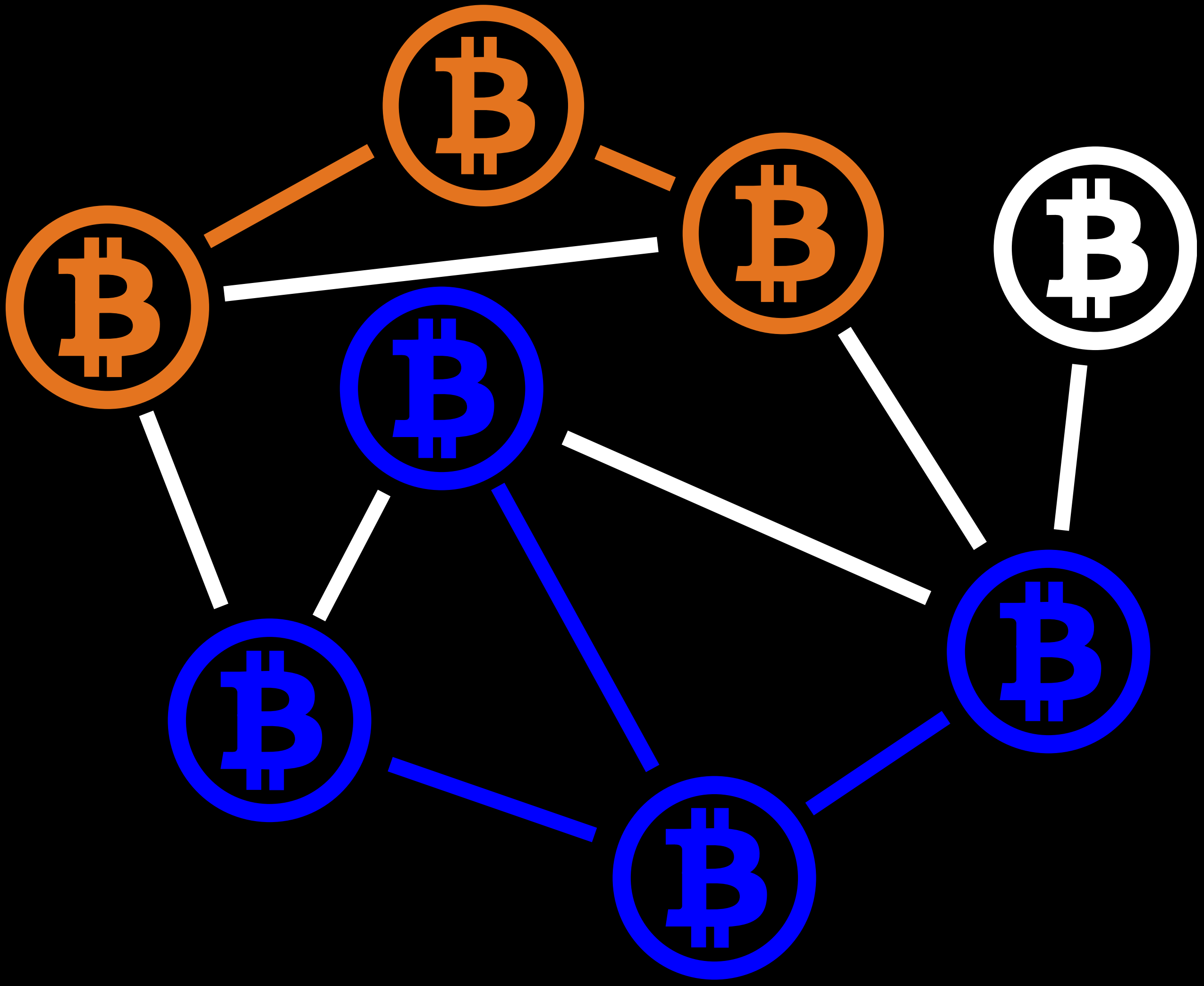
Hong Kong, May 25, 2017



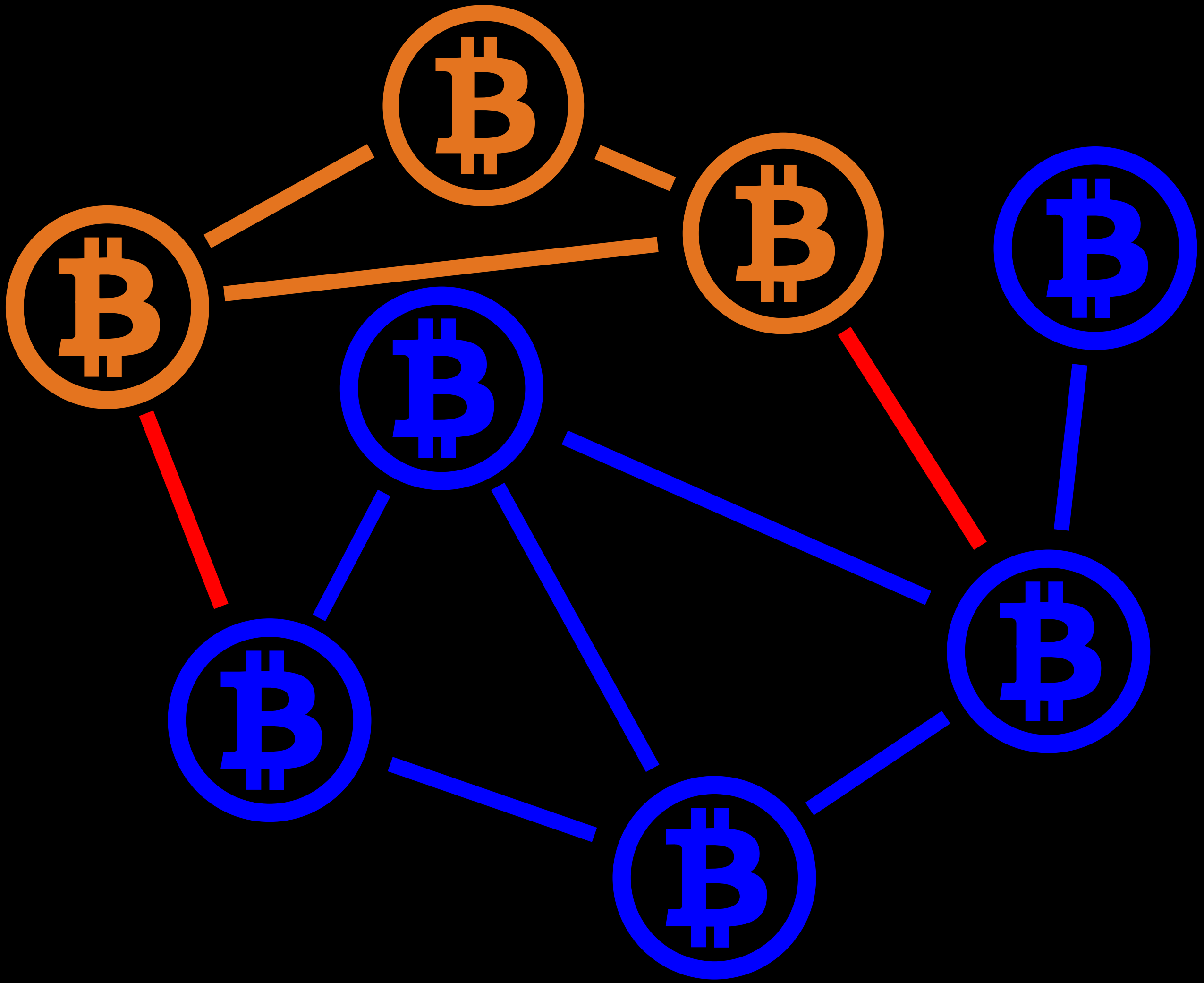
Hong Kong, May 25, 2017



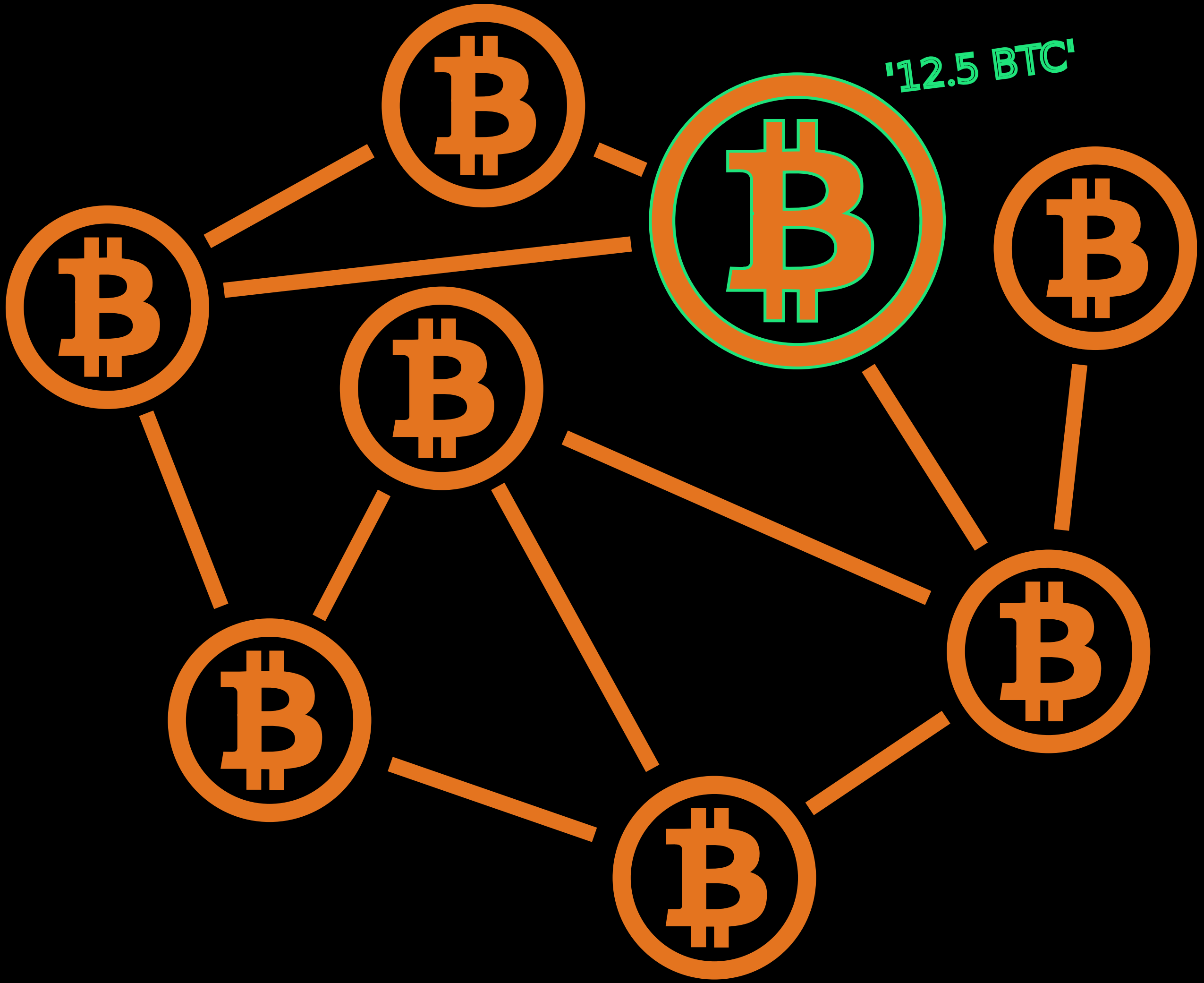
Hong Kong, May 25, 2017



Hong Kong, May 25, 2017



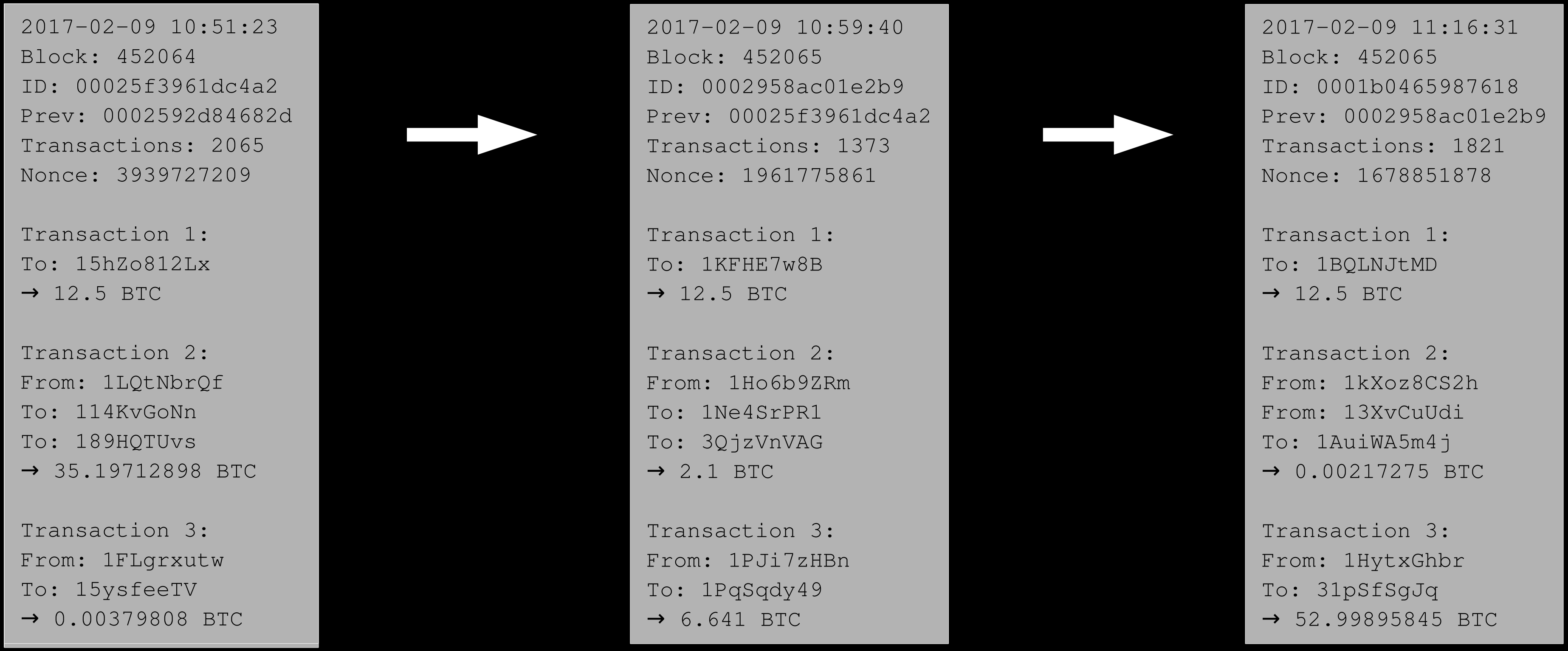
Hong Kong, May 25, 2017



Hong Kong, May 25, 2017

Blocks

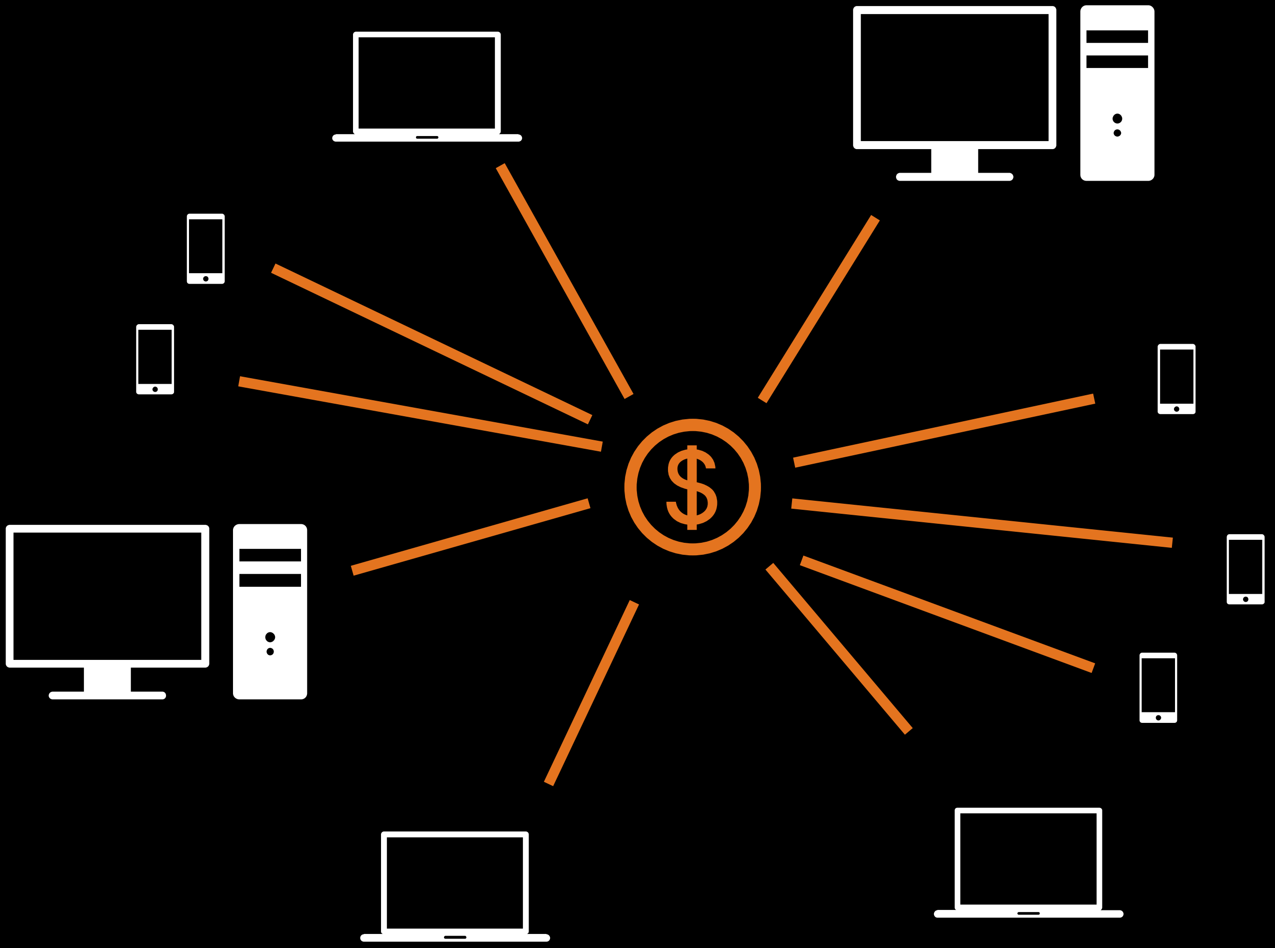
- New blocks are added to the chain



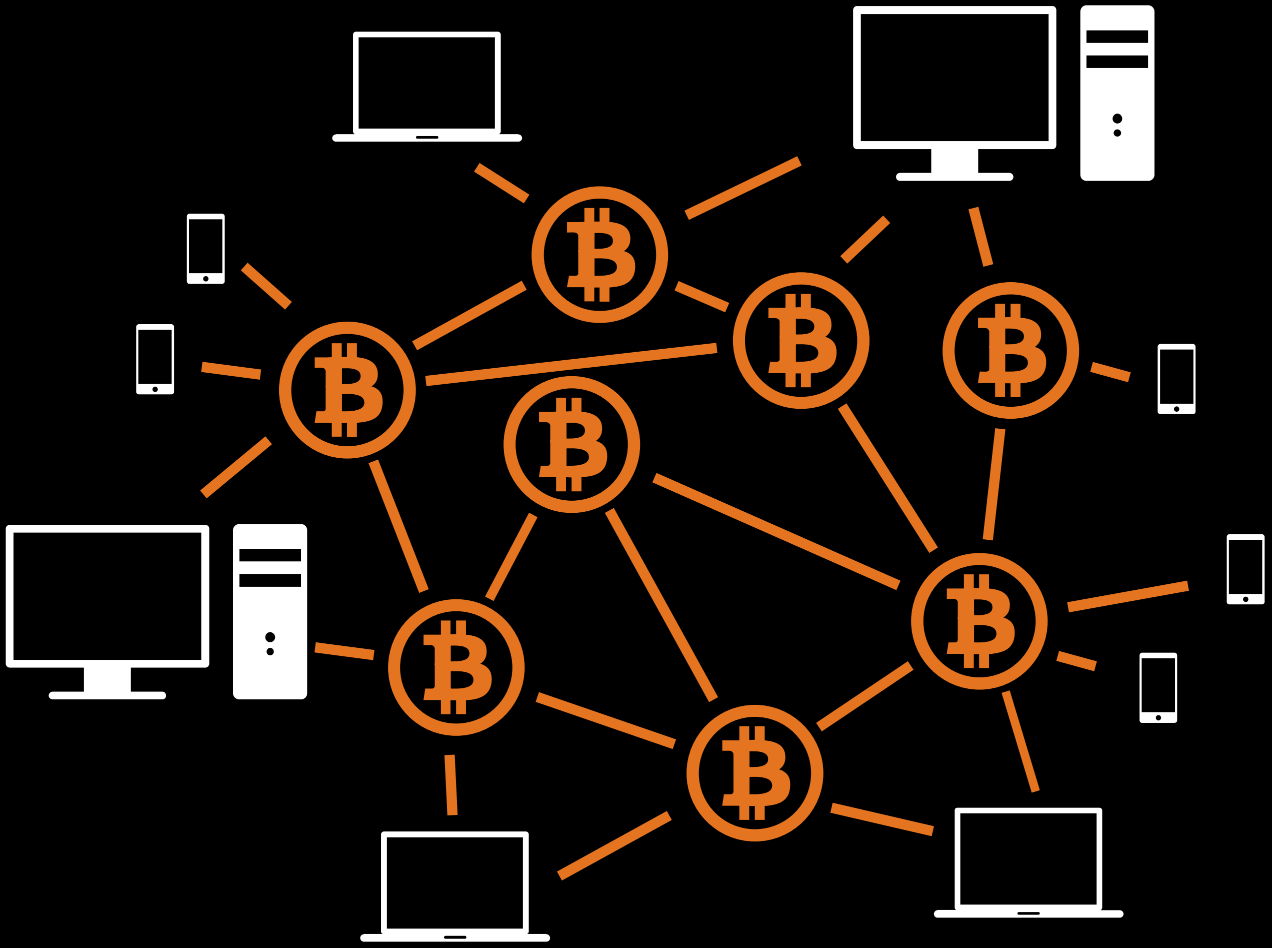
```
2017-02-09 10:51:23
Block: 452064
ID: 00025f3961dc4a2
Prev: 0002592d84682d
Transactions: 2065
Nonce: 3939727209

Transaction 1:
To: 15hZo812Lx
→ 12.5 BTC

Transaction 2:
From: 1LQtNbrQf
To: 114KvGoNn
To: 189HQTUvs
→ 35.19712898 BTC

Transaction 3:
From: 1FLgrxutw
To: 15ysfeeTV
→ 0.00379808 BTC
```

```
2017-02-09 10:59:40
Block: 452065
ID: 0002958ac01e2b9
Prev: 00025f3961dc4a2
Transactions: 1373
Nonce: 1961775861

Transaction 1:
To: 1KFHE7w8B
→ 12.5 BTC

Transaction 2:
From: 1Ho6b9ZRm
To: 1Ne4SrPR1
To: 3QjzVnVAG
→ 2.1 BTC

Transaction 3:
From: 1PJi7zHBn
To: 1PqSqdy49
→ 6.641 BTC
```

```
2017-02-09 11:16:31
Block: 452065
ID: 0001b0465987618
Prev: 0002958ac01e2b9
Transactions: 1821
Nonce: 1678851878

Transaction 1:
To: 1BQLNJtMD
→ 12.5 BTC

Transaction 2:
From: 1kXoz8CS2h
From: 13XvCuUdi
To: 1AuiWA5m4j
→ 0.00217275 BTC

Transaction 3:
From: 1HytxGhbr
To: 31pSfSgJq
→ 52.99895845 BTC
```



Hong Kong, May 25, 2017



Hong Kong, May 25, 2017

There are Problems

- Bitcoin can only handle ~5 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 is timestamping service, similar to a public notary
- Creates irrefutable proof that data existed at a point in time
- It doesn’t prove the correctness of the data
- Because of endless replication, Blockchains are slow, expensive and limited in capacity

The Blockchain Industry

- Companies building on top of the Bitcoin or Ethereum Blockchain
- Separate Blockchains (Factom, MaidSafe)
- Settlement systems with native currencies (Ripple)
- Settlement systems and consortia (Hyperledger, Corda)
- Blockchain-inspired Databases (Monax, BigchainDB)

Evolution of Blockchains

- Today: Payments
- Tomorrow: Documents
- Soon: Smart Contracts
- Maybe: Supply Chain Integrity

Payments

Bitcoin payments are attractive:

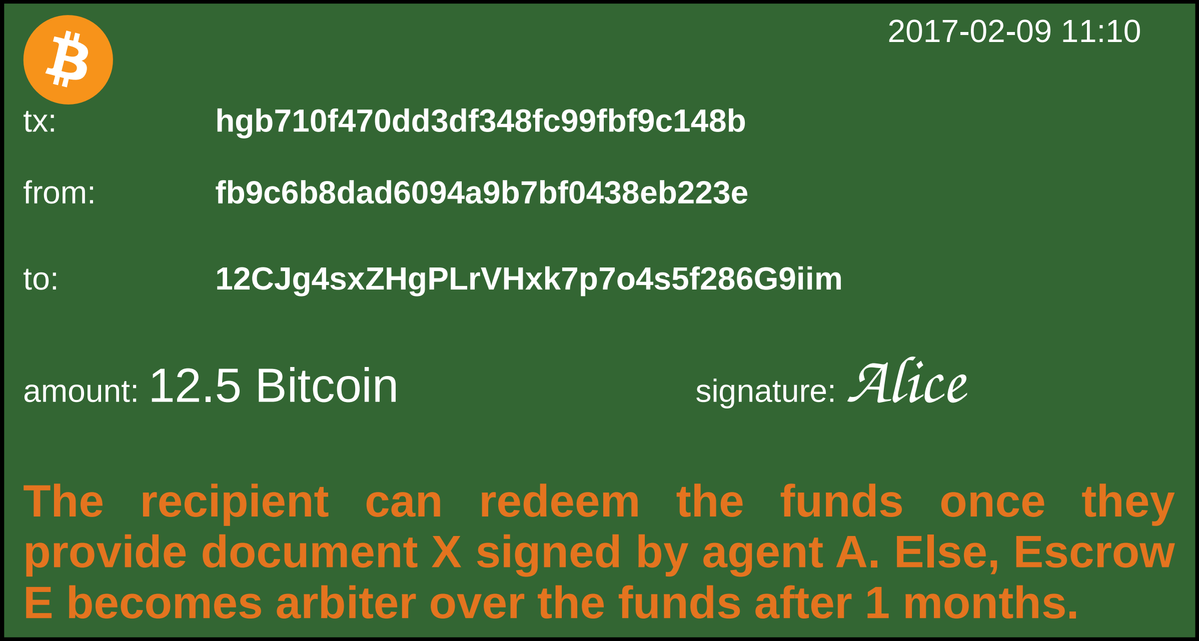
- For the underbanked
- Where there are currency restrictions
- Cheaper for small payments
- Cheap, fast, electronic escrow

Documents

Timestamping hashes on a Blockchain:

- Proof of existence
- Documents cannot be altered
- Publicly verifiable without compromising privacy
- Possible without a Blockchain, why is it not popular?

Smart Contracts



2017-02-09 11:10

tx: hgb710f470dd3df348fc99fbf9c148b

from: fb9c6b8dad6094a9b7bf0438eb223e

to: 12CJg4sxZHgPLrVHxk7p7o4s5f286G9iim

amount: 12.5 Bitcoin

signature: *Alice*

The recipient can redeem the funds once they provide document X signed by agent A. Else, Escrow E becomes arbiter over the funds after 1 months.

- Allow for a trustless, efficient automation of payments, especially where court systems are not trusted

Supply Chain Integrity

- Every document and payment is recorded
- Publicly verifiable trail of all inputs into a product
- Undesired privacy implications
- The Blockchain is only one small and late step in a long evolution of data digitization and publication

Without a Blockchain

- Everything can technically be done without a Blockchain
- Private systems are more efficient than Blockchains
- Blockchains eliminate trust and intermediaries
- Blockchains are available to everyone
- Blockchains enable ‘illegal’ things, and make it easier for individuals to make ‘illegal’ transaction, which is hard for corporates to engage in

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

Hong Kong, May 25, 2017