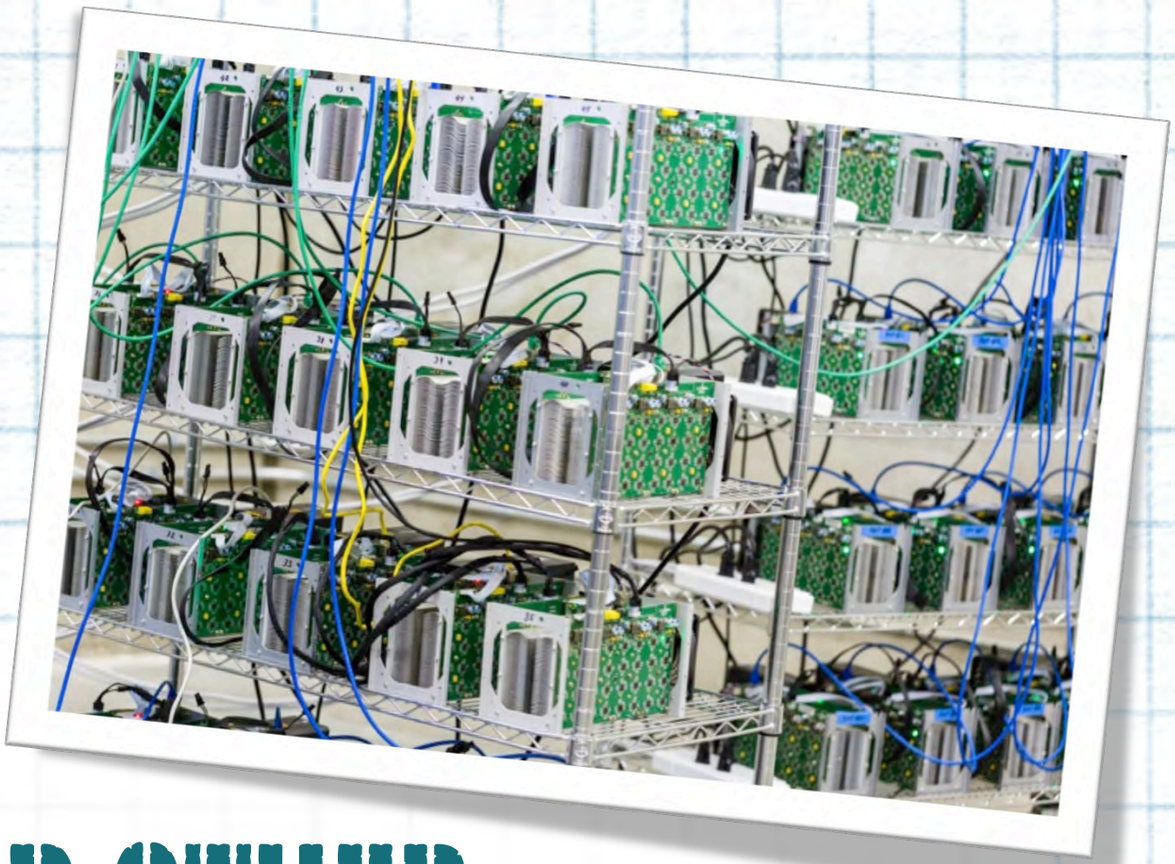
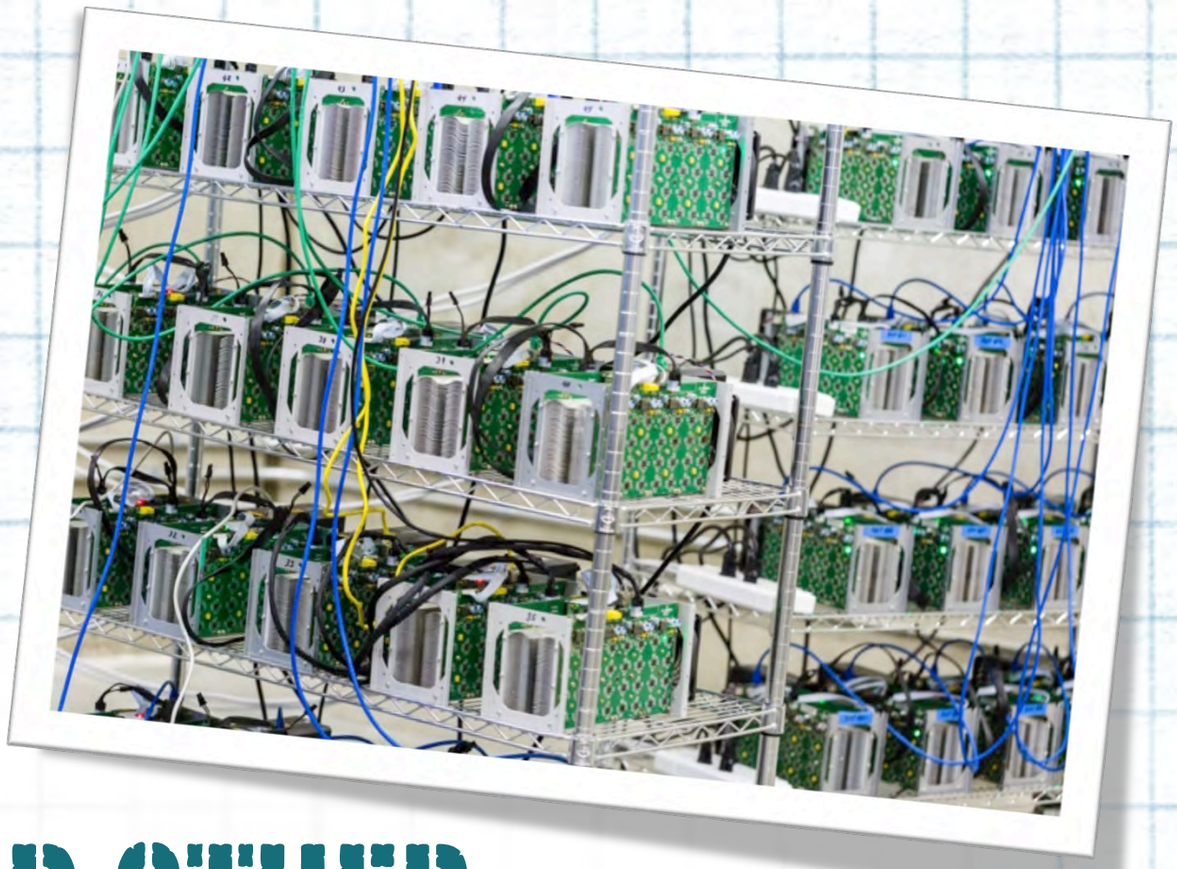

Warning!
None of the information
in this talk should be construed
as legal or financial advice!
quickmeme.com



# Bitcoin and other Cryptocurrencies:

## Illegal Money or a New Global Payment Option?

Carola F. Berger, ATA56

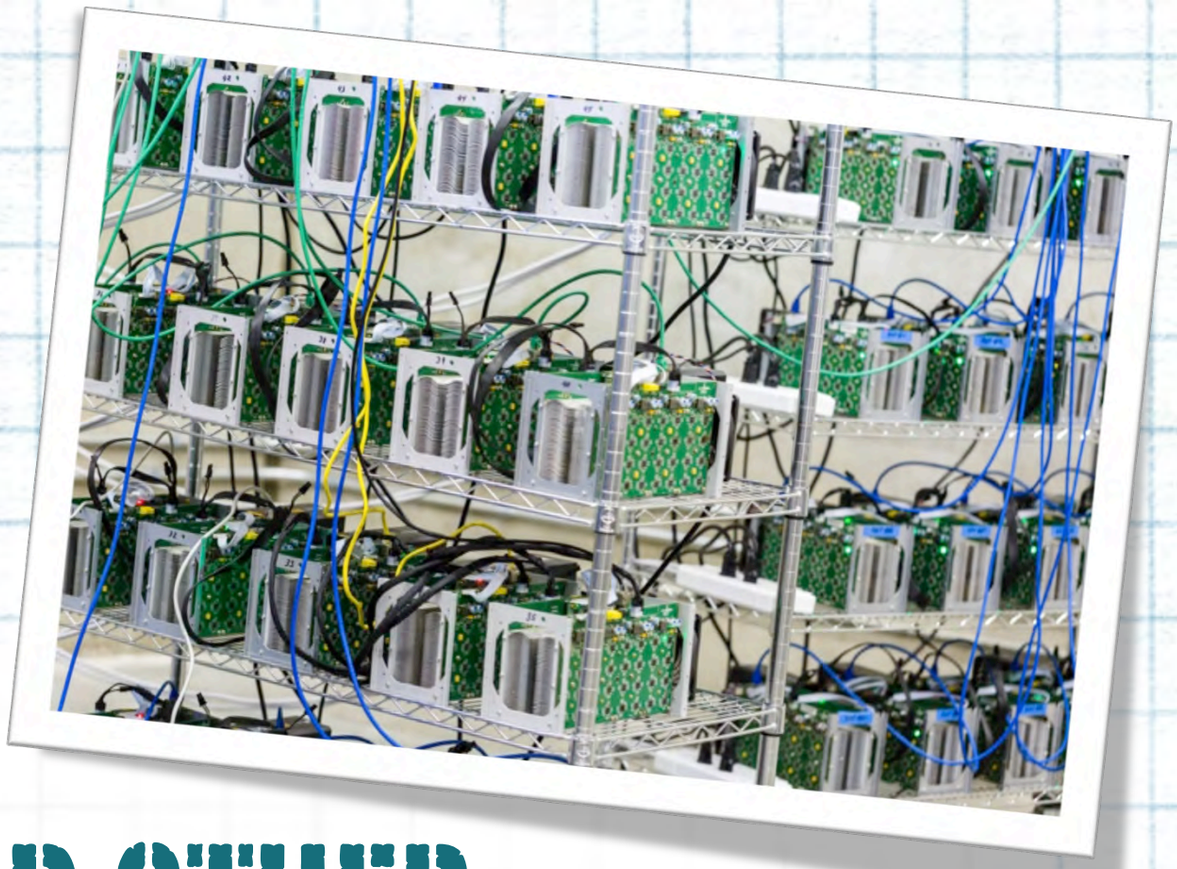


# Bitcoin and other Cryptocurrencies:

## Illegal Money or a New Global Payment Option?

**Both**

Carola F. Berger, ATA56



# Bitcoin and other Cryptocurrencies:

## Illegal Money or a New Global Payment Option?

**Both**

**Neither**

Carola F. Berger, ATA56

# Math

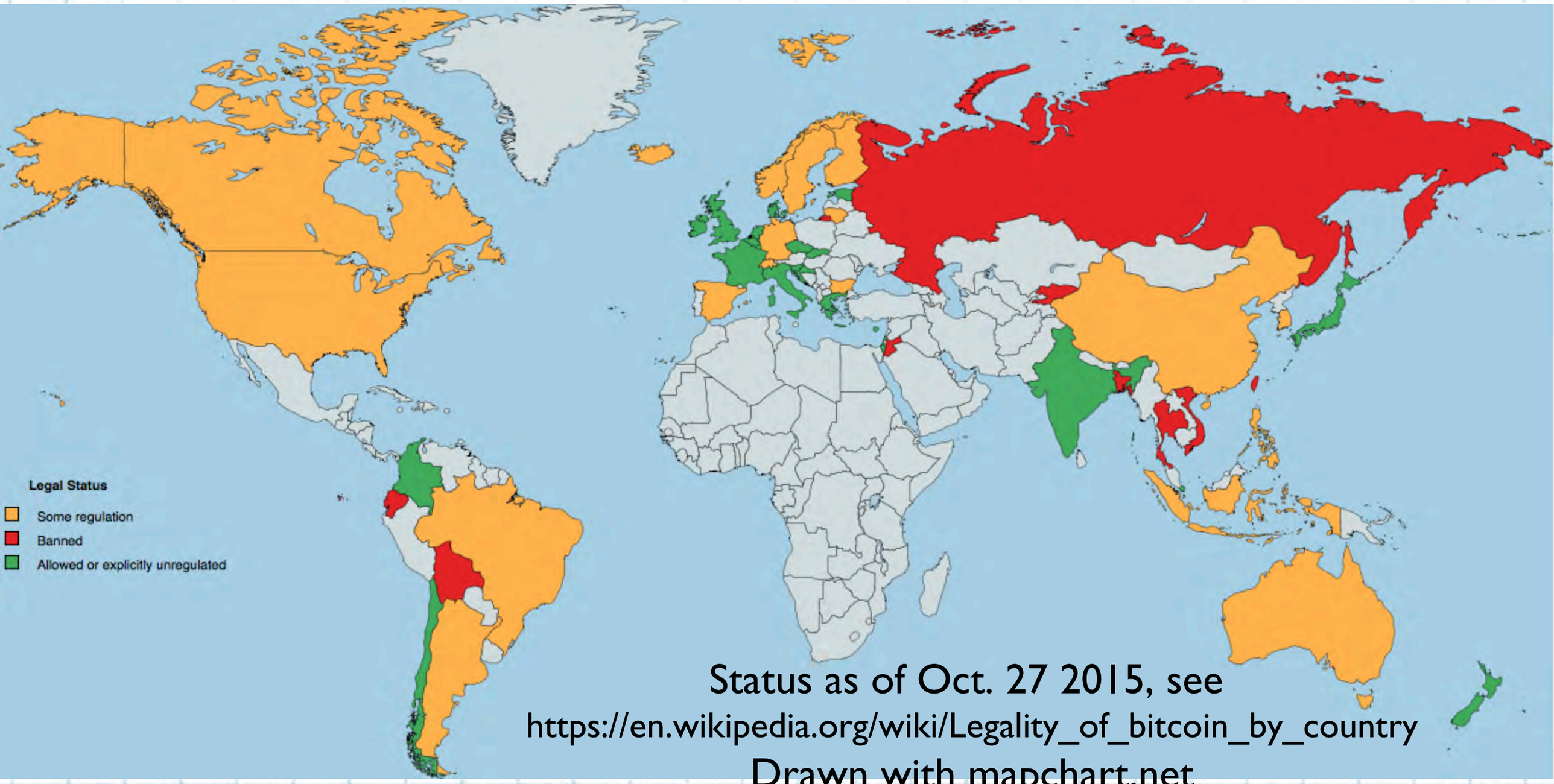
The only place where people
buy 64 watermelons
and nobody wonders why.

# Math

The only place where people
buy 64 watermelons
and nobody wonders why.


Warning!
None of the information
in this talk should be construed
as legal or financial advice!
quickmeme.com

# Legal Status




Status as of Oct. 27 2015, see
https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country
Drawn with mapchart.net

# Outline

- Introduction – What is Bitcoin?
- Bitcoin transactions and mining
- The blockchain
- Wallets and faucets
- Dogecoin, Ethereum, Unobtanium, Quatloo, BunnyCoin, and other Altcoins
- Outlook

# Introduction – Monetary Exchange

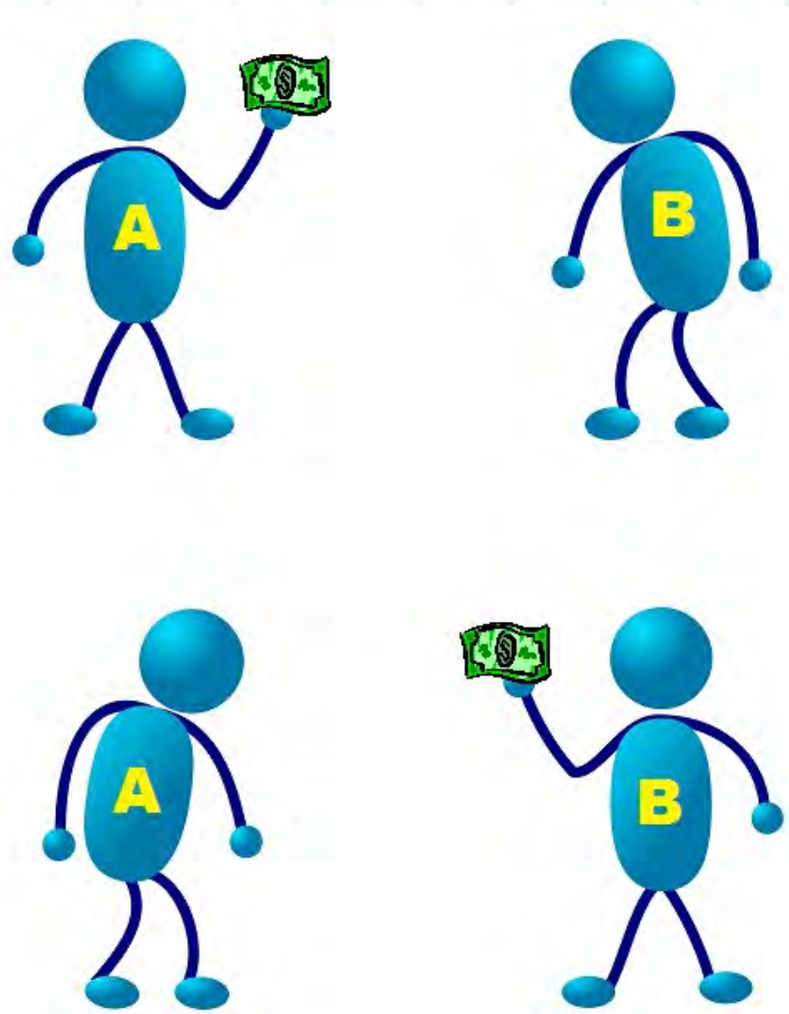
1. Check that the sender actually possesses the required amount of money.

2. Deduct the amount to send from the sender's account.

3. Transmit the specified amount of money to the recipient.

4. Update the recipient's balance with the transmitted amount.

Cash exchange



# Introduction – Monetary Exchange

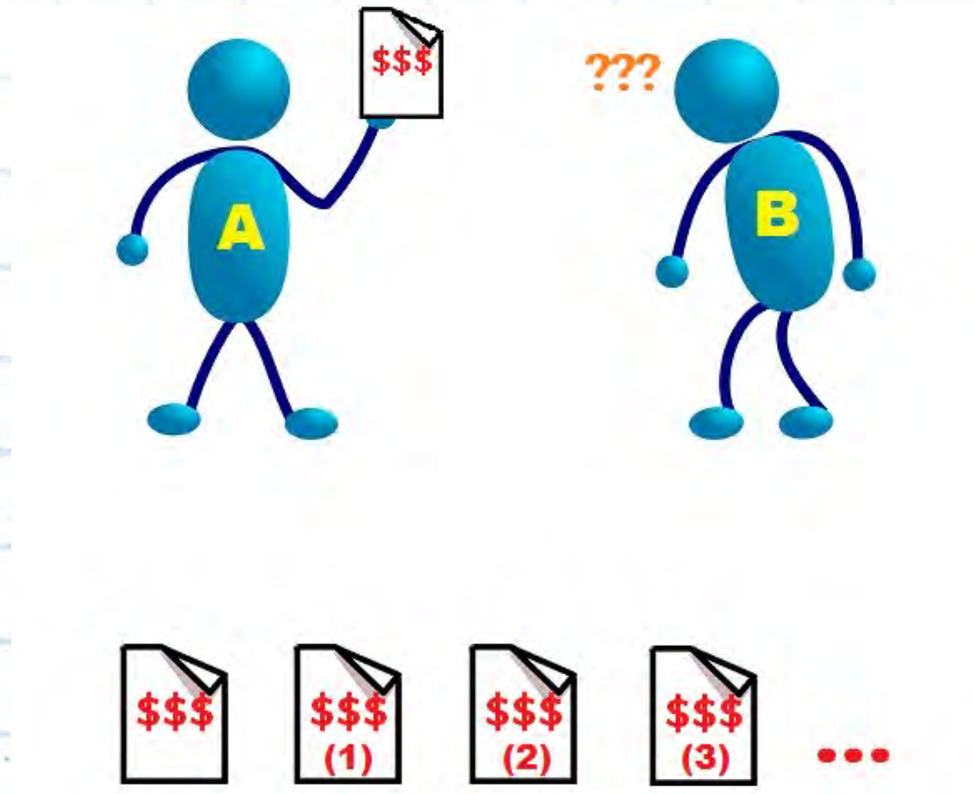
1. Check that the sender actually possesses the required amount of money.

2. Deduct the amount to send from the sender's account.

3. Transmit the specified amount of money to the recipient.

4. Update the recipient's balance with the transmitted amount.

Electronic exchange?



# Introduction – Monetary Exchange

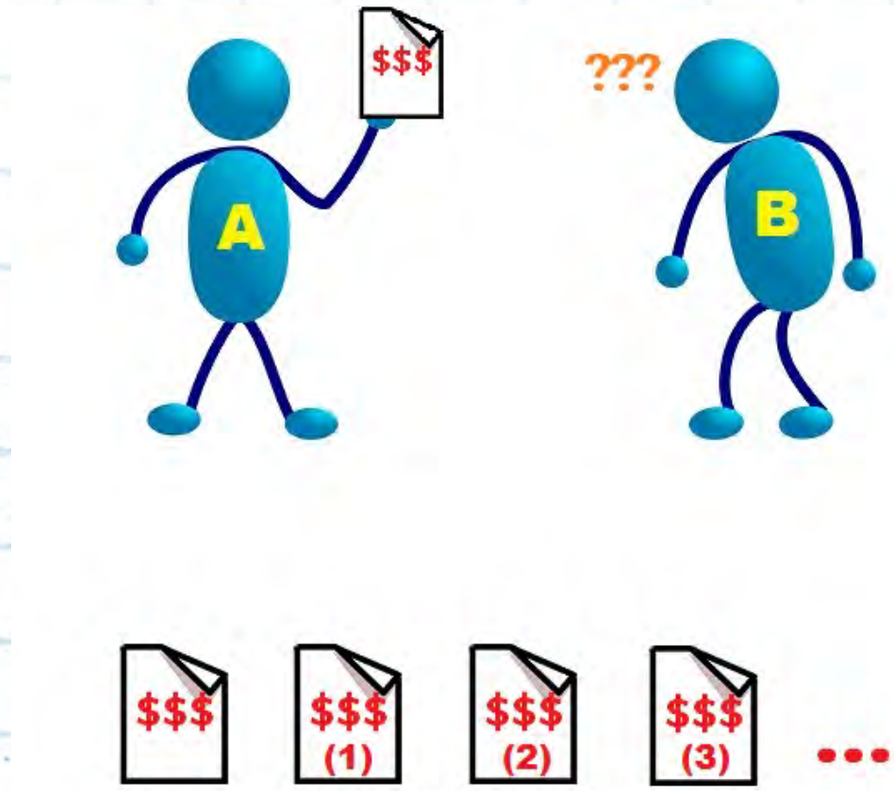
1. Check that the sender actually possesses the required amount of money.

2. Deduct the amount to send from the sender's account.

3. Transmit the specified amount of money to the recipient.

4. Update the recipient's balance with the transmitted amount.

Electronic exchange?




**Always requires a trusted intermediary!!!**

# Introduction – Monetary Exchange Without a Trusted Intermediary

Rai stones, island of Yap (Micronesia) Picture by Eric Guinther, Wikipedia

# Introduction – Monetary Exchange Without a Trusted Intermediary

The solution: the Bitcoin protocol, proposed by **Satoshi Nakamoto** in "*Bitcoin: A Peer-to-Peer Electronic Cash System*,"
https://bitcoin.org/bitcoin.pdf

# Introduction – Monetary Exchange Without a Trusted Intermediary

The solution: the Bitcoin protocol, proposed by **Satoshi Nakamoto** in "*Bitcoin: A Peer-to-Peer Electronic Cash System*," https://bitcoin.org/bitcoin.pdf

**=> Chocolate demo!**

See also: http://www.cfbtranslations.com/bitcoin-part-1-byzantine-generals-and-pseudonyms-or-what-is-bitcoin/

# Bitcoin Transactions

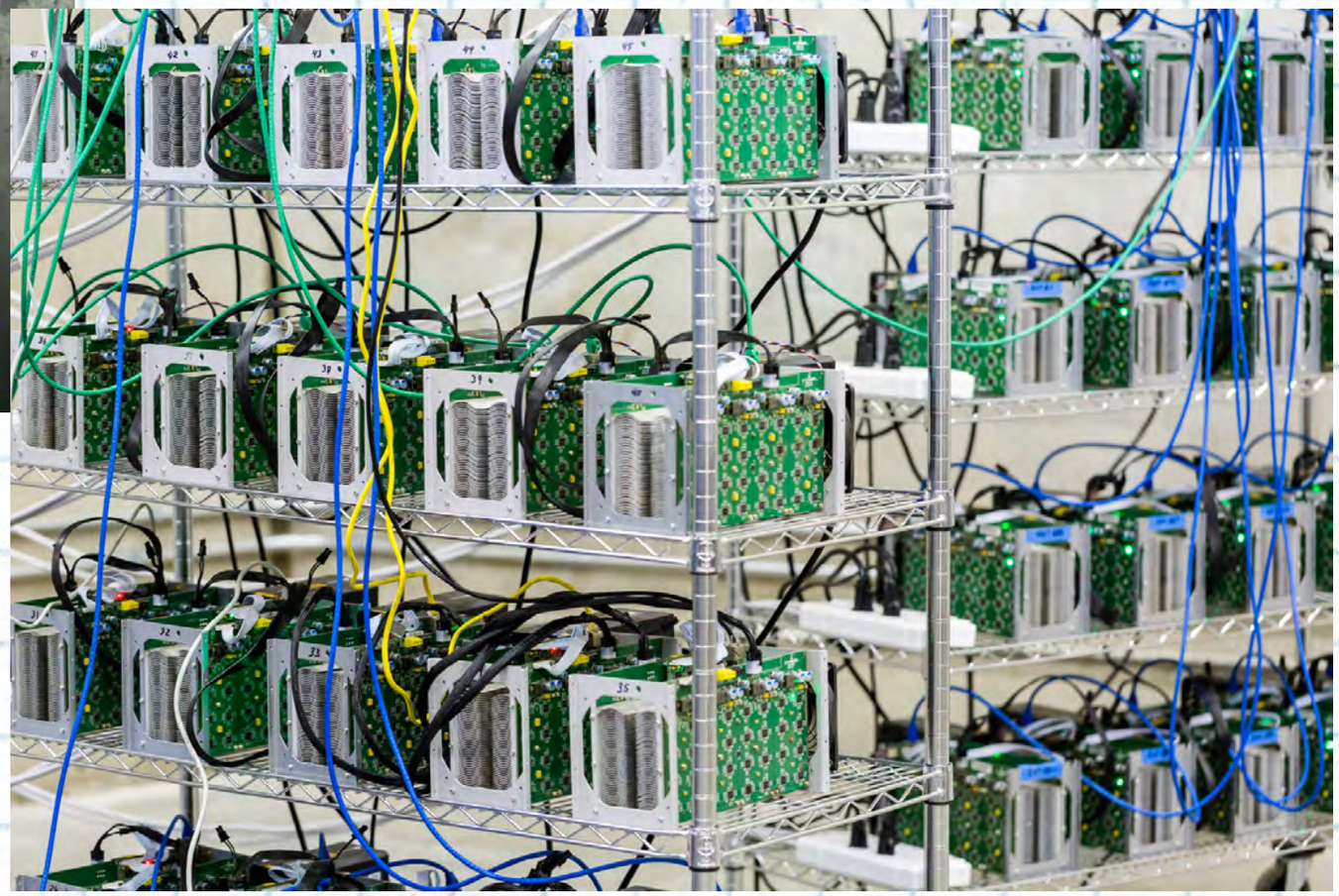
1. The ownership of Bitcoins can be publicly verified, because every Bitcoin transaction since the very first one (the so-called genesis block) is entered into a public ledger called the **blockchain**.

2. A transaction is publicly broadcast to **all nodes** in the network.

3. Double-spending is not possible, because the network decides through a process that is a bit like voting (and involves solving a complex math problem) called **mining (proof of work)**, which transactions are valid and which ones are not.

4. The transactions that are chosen as **valid are entered into the blockchain**, the public ledger, and become final..

# Bitcoin Mining – Proof of Work



# Bitcoin Mining

1. A computational problem is sent to the nodes in the Bitcoin network.
2. All unconfirmed transaction proposals are also sent to the nodes. Not every node receives the transactions in the same order.
3. The nodes attempt to compute a solution to the problem in step 1.
4. After on average 10 minutes, a solution is found by one node. The node broadcasts the solution along with its particular copy of transactions that will be the new additions to the ledger (blockchain).
5. The other nodes validate the solution and confirm the transactions.
6. After 100 confirmation the solution and associated transactions are final. The node that found the solution collects the transaction fees and a certain amount of newly “minted” Bitcoins.
7. Begin again with step 1.

# The Public Ledger – the Blockchain

A **block** consists of the following main elements:

- A timestamp
- A reference to the previous block — thus the name chain
- The transactions that are being confirmed in this block and thus being finalized and publicly broadcast
- A statement of a new complex mathematical problem to be solved for the miners

# The Public Ledger – the Blockchain

Publicly accessible at www.blockchain.info

BLOCKCHAIN info | Home | Charts | Stats | Markets | API | Wallet | Search | English

## Home Welcome to Blockchain

More...

| Height | Age | Transactions | Total Sent | Relayed By | Size (kB) |
|---|---|---|---|---|---|
| 362950 | 1 minute | 826 | 4,698.38 BTC | BitFury | 731.55 |
| 362949 | 3 minutes | 2437 | 7,458.34 BTC | F2Pool | 976.24 |
| 362948 | 12 minutes | 1 | 25.00 BTC | F2Pool | 0.26 |
| 362947 | 13 minutes | 964 | 8,804.23 BTC | Eligius | 270.95 |
| 362946 | 43 minutes | 1502 | 9,922.41 BTC | AntPool | 911.61 |
| 362945 | 53 minutes | 462 | 4,429.11 BTC | BTCChina Pool | 226.82 |

**Latest Transactions**

| | | |
|---|---|---|
| 49c7ae3c6c6aeb0182e58e1d2... | < 1 minute | 47.87207621 BTC |
| a7611a13c7b7d988b64a5786c... | < 1 minute | 2.67086557 BTC |
| f8f5e1a6078ff61a23cdeacde... | < 1 minute | 0.61044466 BTC |
| 92c140dddc6fbfde4e9917154... | < 1 minute | 0.019915 BTC |
| 767fc0ca8083fdfde227b9f72... | < 1 minute | 2.3899 BTC |

**Search**

*You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...*

Address / ip / SHA hash | Search

NEWS

BTC.sx - The Most Secure Leveraged Bitcoin Trading Platform
BTC.sx ← 1 minute ago

XCP Weekly Update #5 with Robert Ross
Lets Talk Bitcoin 21 minutes ago

# The Blockchain – Block Detail

## Block #362950

| Summary | |
|---|---|
| Number Of Transactions | 826 |
| Output Total | 4,698.37910323 BTC |
| Estimated Transaction Volume | 651.11862874 BTC |
| Transaction Fees | 0.10629534 BTC |
| Height | 362950 (Main Chain) |
| Timestamp | 2015-06-28 18:55:50 |
| Received Time | 2015-06-28 18:55:50 |
| Relayed By | BitFury |
| Difficulty | 49,402,014,931.23 |
| Bits | 404111758 |
| Size | 731.552734375 KB |
| Version | 3 |
| Nonce | 252502466 |
| Block Reward | 25 BTC |

| Hashes | |
|---|---|
| Hash | 00000000000000000019ccc6318d7fd639fcc50e72fa1ee716130f095097b3b3 |
| Previous Block | 0000000000000000a22e05371ede898456d6dcf3132bb67b1c136d050a1c743 |
| Next Block(s) | |
| Merkle Root | 103d5a2bca6ceff6d65b52ae258267dafa1b1f5db8658f90875f34730f76e3cb |

**Network Propagation (Click To View)**

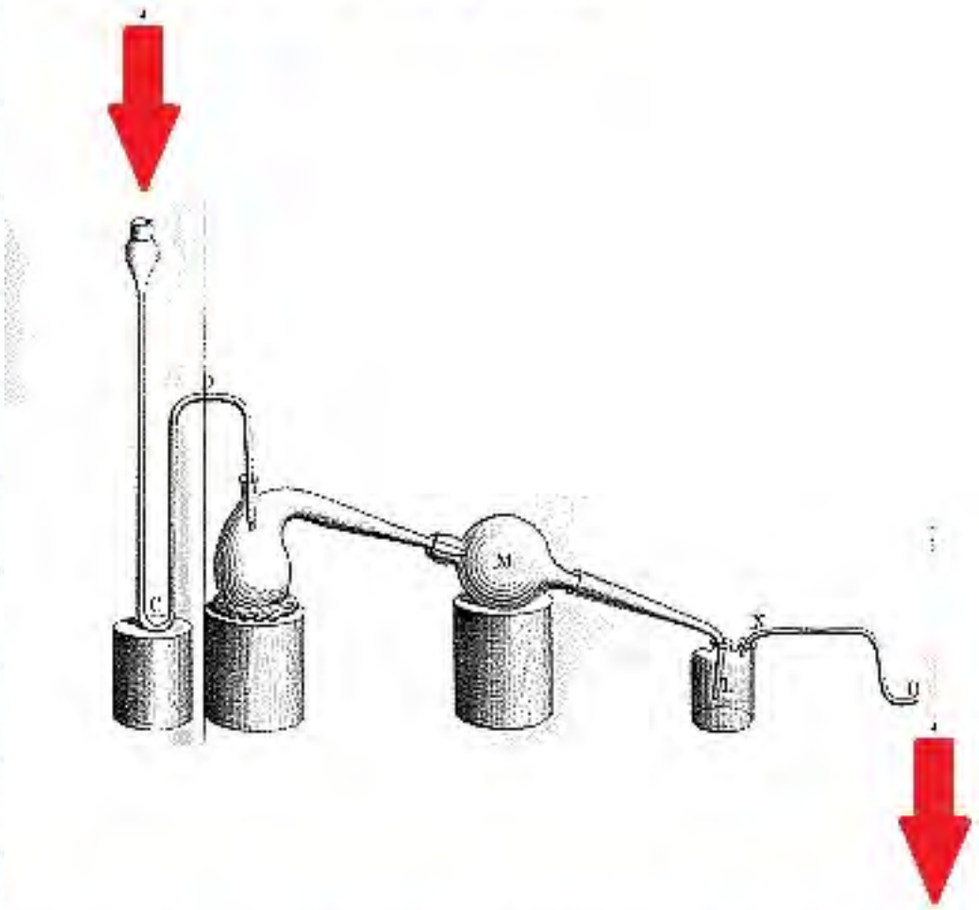
# The Blockchain – Transaction Detail

## Transactions

| | | | |
|---|---|---|---|
| 647b687343d17d0f9a2bf5dd3a44378086d1fb60e826b7e0b7091e7b0fd738cb | | | **2015-06-28 18:55:50** |
| **No Inputs (Newly Generated Coins)** | → | 1FeDtFhARLxjKUP… (Bitfury) | 25.10629534 BTC |
| | | | 25.10629534 BTC |
| 7cdbbac6e2d681b22794de62c6056d8cb7983b907a811893d74bae18485f1c3c | | | **2015-06-28 18:15:35** |
| 1M4sn5xm894Veua32a8JWnGpiDwctMLg2U | → | 18TLHSVs1qHXWG6t2xtXWAoSYeVdQzkYwm | 28.79999671 BTC |
| | | 1A83RevgCXuFsnuuczGQfUZQzX1Qh3b8Mw | 1.2 BTC |
| | | | 29.99999671 BTC |
| 51e2e600f94191b11bde7c1c453d27f18ea287d4f1669b413ac10a60ae6e377a | | | **2015-06-28 18:14:07** |
| 1AFcViE1N8jo59pkCqizmHnVTefP4mK6P8 | → | 3HUcEwjsUHHuXhx8DcH5PneJwxfiR6hwvh | 1 BTC |
| | | | 1 BTC |
| 194cca05e7b80f48429228ba54f8af4166c1e77a47e5c9aa48ab70e112b854cc | | | **2015-06-28 18:14:11** |
| 1699Ui1xtkykJPYhA3ktXZE1YdPzhxpu4x | → | 19Bgbr19D7qczLknLWa9akmRJmLcCzh92Z | 0.9988 BTC |
| | | | 0.9988 BTC |

# The Blockchain – Hashes

*To be, or not to be*



03c6691ebdd161363457e3c73a8ed44186536cf9

# The Blockchain – Hashes

Input:

**To be, or not to be**

Output of SHA-1:

**03c6691ebdd161363457e3c73a8ed44186536cf9**

# The Blockchain – Hashes

Input:

**To be, or not to be**

Output of SHA-1:

**03c6691ebdd161363457e3c73a8ed44186536cf9**

Input:

**To be or not to be**

Output of SHA-1:

**6025f94596c2445f0a776d9bac929829de3c948d**

# The Blockchain – Hashes

Input:

**To be, or not to be**

Output of SHA-1:

**03c6691ebdd161363457e3c73a8ed44186536cf9**

Input:

**To be or not to be**

Output of SHA-1:

**6025f94596c2445f0a776d9bac929829de3c948d**

Input:

**2B~not2B**

Output of SHA-1:

**5ed97a13c423c7abea25de49472f7043f156d31c**

# Blockchain – Public Key Cryptography

Private key:
Public key:

# Blockchain – Public Key Cryptography

1. A unique pair of a public and a private key is created.
2. The public key is broadcast to all recipients. The private key is kept secret.
3. All messages or (in the case of Bitcoin) transactions are encrypted with the private key, the equivalent of locking them into the mailbox above.
4. The message is then sent to the recipient(s). The message (or transaction) can be authenticated and decrypted by anyone with the public key.
5. It is (next to) impossible to fake messages (or transactions) without knowledge of the private key. Impostors are out of luck.

# The Blockchain – Transaction Detail

## Transaction View information about a bitcoin transaction

7cdbbac6e2d681b22794de62c6056d8cb7983b907a811893d74bae18485f1c3c

1M4sn5xm894Veua32a8JWnGpiDwctMLg2U (30 BTC - Output)

18TLHSVs1qHXWG6t2xtXWAoSYeVdQzkYwm - (Unspent) 28.79999671 BTC

1A83RevgCXuFsnuuczGQfUZQzX1Qh3b8Mw - (Unspent) 1.2 BTC

7 Confirmations | 29.99999671 BTC

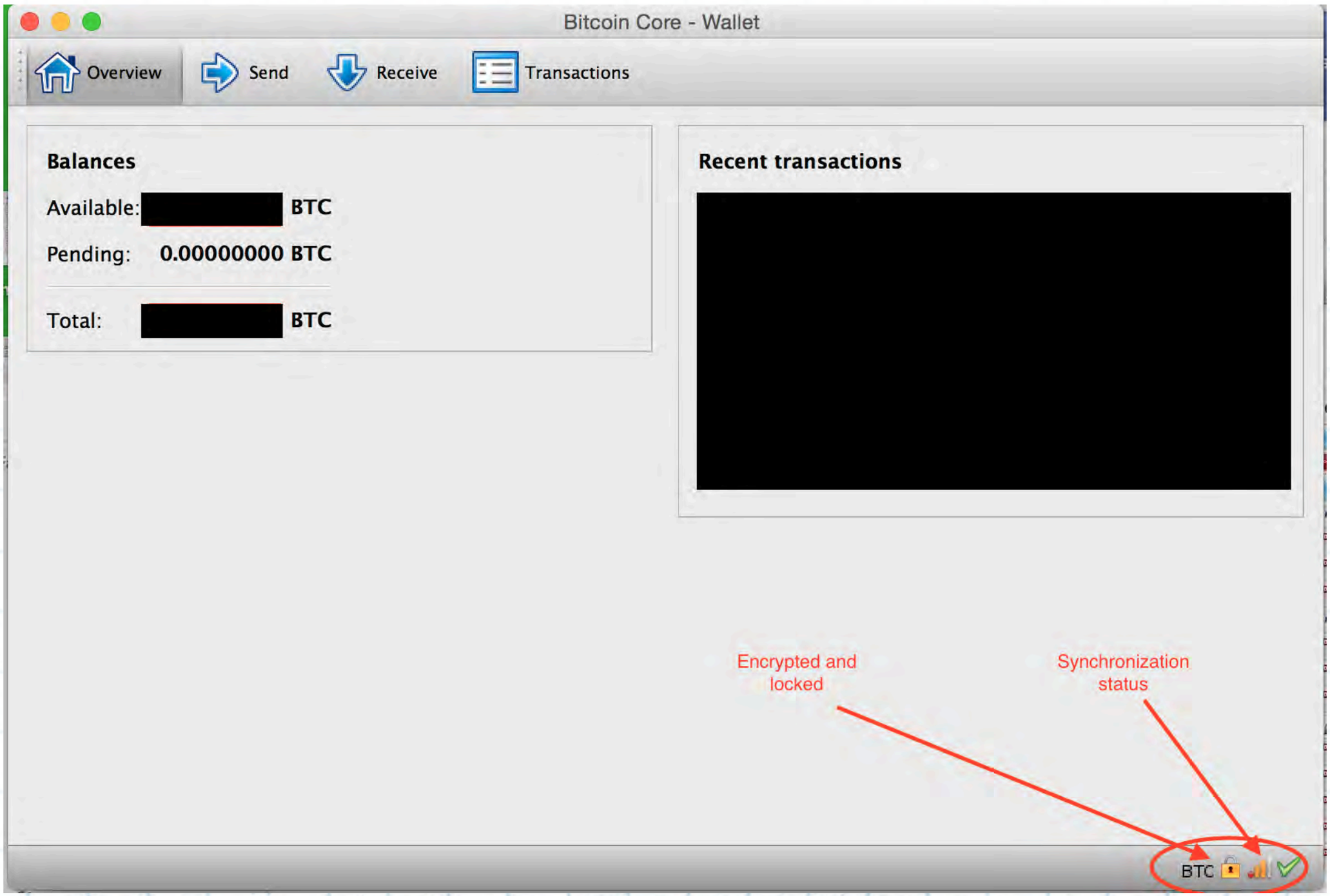
### Summary

| | |
|---|---|
| Size | 258 (bytes) |
| Received Time | 2015-06-28 18:15:35 |
| Included In Blocks | 362950 ( 2015-06-28 18:55:50 + 40 minutes ) |
| Confirmations | 7 Confirmations |
| Relayed by IP | 5.9.87.134 (whois) |
| Visualize | View Tree Chart |

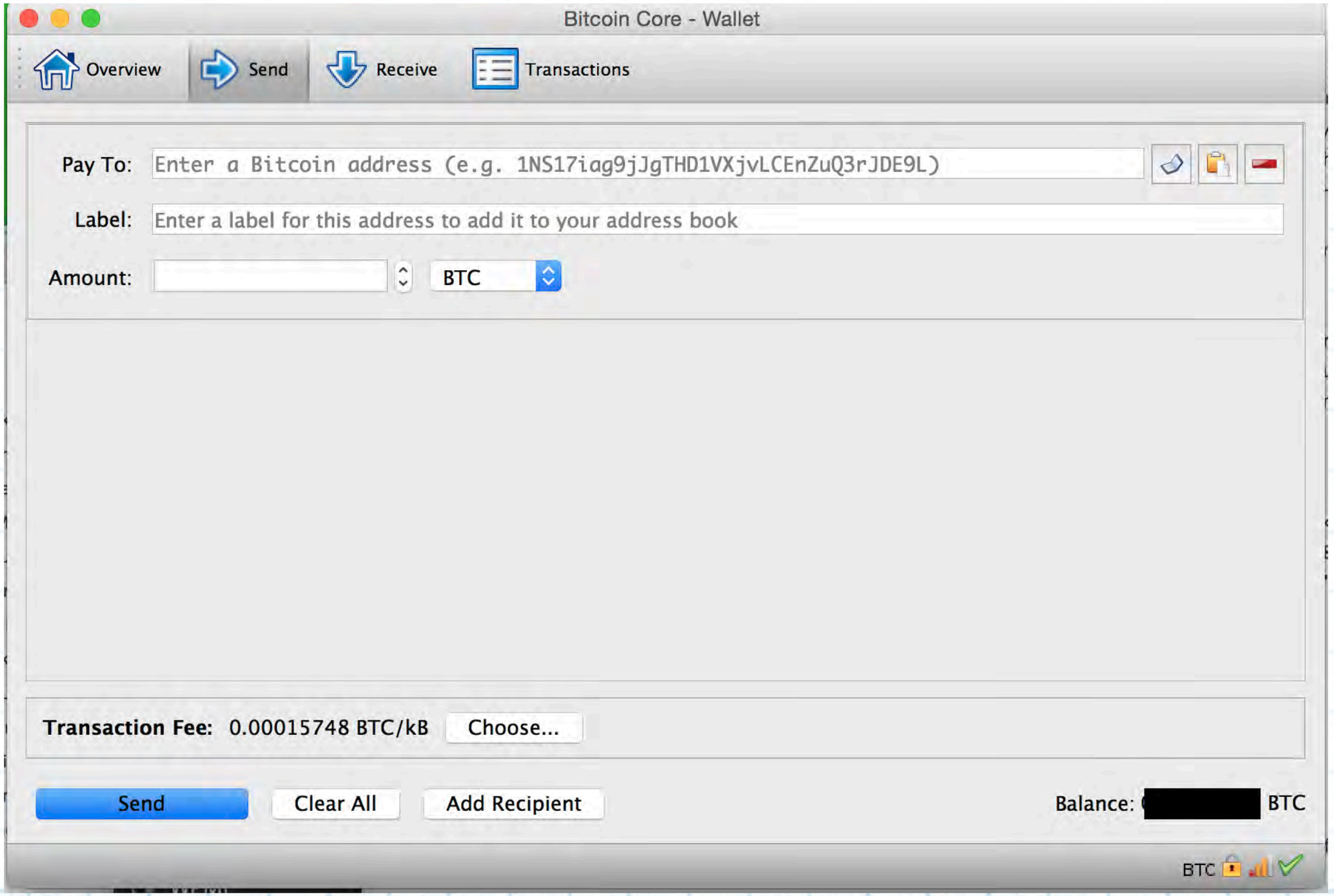
### Inputs and Outputs

| | |
|---|---|
| Total Input | 30 BTC |
| Total Output | 29.99999671 BTC |
| Fees | 0.00000329 BTC |
| Estimated BTC Transacted | 1.2 BTC |
| Scripts | Hide scripts & coinbase |

# Wallets and Faucets – Bitcoin Wallet



# Wallets and Faucets – Bitcoin Wallet



# Getting BTC - Bitcoin Exchange Rate

# Getting BTC - Faucets

**Faucets** = websites, where you can get BTC for "free," usually by watching ads (warning – anti-virus programs are strongly recommended!)

Usually only a few **Satoshis =** 0.00000001 BTC

Minimum amount in BTC transaction is currently 5430 Satoshis (0.00005430 BTC) => **micropayment** sites

List of faucets:
http://www.cfbtranslations.com/bitcoin-and-altcoin-faucets/

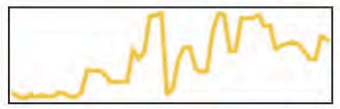
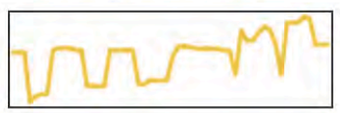
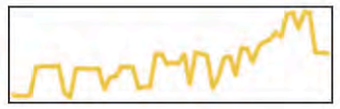
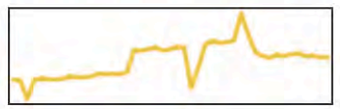
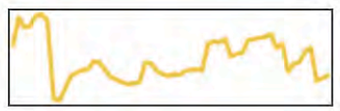
# Altcoins

All ▾ | Currencies ▾ | Assets ▾ | USD ▾ | Next 100 → | View All

| # | Name | Market Cap | Price | Available Supply | Volume (24h) | % Change (24h) | Price Graph (7d) |
|---|---|---|---|---|---|---|---|
| 1 | Bitcoin | $ 4,747,586,452 | $ 321.10 | 14,785,475 BTC | $ 41,826,500 | -0.57 % |  |
| 2 | Litecoin | $ 168,397,130 | $ 3.92 | 42,964,260 LTC | $ 5,736,820 | -1.98 % |  |
| 3 | Ripple | $ 156,298,050 | $ 0.004714 | 33,156,211,683 XRP * | $ 255,296 | -1.21 % |  |
| 4 | Ethereum | $ 72,519,611 | $ 0.975311 | 74,355,370 ETH | $ 924,801 | -9.94 % |  |
| 5 | Dogecoin | $ 14,358,167 | $ 0.000141 | 101,619,804,175 DOGE | $ 164,071 | -1.52 % |  |
| 6 | Dash | $ 14,298,373 | $ 2.41 | 5,943,836 DASH | $ 67,670 | -5.74 % |  |
| 7 | Stellar | $ 10,954,581 | $ 0.002265 | 4,837,356,606 STR * | $ 15,985 | 8.72 % |  |

Source: coinmarketcap.com (Oct. 31, 2015)

# Altcoins

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 75 | Electronic G... | $ 281,739 | $ 0.020759 | 13,571,710 EFL ** | $ 273 | 9.96 % |  |
| 76 | TileCoin | $ 273,824 | $ 0.002738 | 100,000,000 XTC * | $ 92 | 3.74 % |  |
| 77 | Unobtanium | $ 271,947 | $ 1.39 | 196,194 UNO | $ 529 | -4.55 % |  |
| 78 | CannabisCoin | $ 270,388 | $ 0.003504 | 77,165,665 CANN | $ 556 | 0.07 % |  |
| 79 | UnionCoin | $ 265,240 | $ 0.031619 | 8,388,608 UNC | $ 445 | -5.20 % |  |
| 80 | Flycoin | $ 264,791 | $ 1.61 | 164,928 FLY * | $ 849 | -22.02 % |  |
| 81 | Nas | $ 257,170 | $ 0.000026 | 10,000,000,000 NAS * | $ 58 | -0.44 % |  |
| 82 | SolarCoin | $ 254,288 | $ 0.007440 | 34,180,042 SLR * | $ 19 | 10.86 % |  |
| 83 | Qora | $ 251,706 | $ 0.000025 | 10,000,000,000 QORA * | $ 21 | 2.91 % |  |
| 84 | SkyNET | $ 244,193 | $ 0.273079 | 894,223 SKYNET * | $ 29 | -5.85 % |  |

Source: coinmarketcap.com (Oct. 31, 2015)

# Bitcoin and other Cryptocurrencies: Illegal Money or a New Global Payment Option?

## Neither!

# Bitcoin and other Cryptocurrencies: Illegal Money or a New Global Payment Option?

## Neither!

# Thank you!

**Slides at http://www.CFBtranslations.com**

# References & Further Reading

- Series of blog posts on cryptocurrencies: http://www.cfbtranslations.com/weblog/
- University of Nicosia – free online MOOC on digital currencies: http://digitalcurrency.unic.ac.cy/free-introductory-mooc (Part of an online MSc in Digital Currency (not free))
- Official Bitcoin website: http://www.bitcoin.org
- Bitcoin block chain explorer: https://blockchain.info
- Cryptocurrency market capitalization/altcoins: http://coinmarketcap.com