Warning!

None of the information in this talk should be construed as legal or financial advice!
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
The only place where people buy 64 watermelons and nobody wonders why.
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!
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, Unobtainium, Quatloo, BunnyCoin, and other Altcoins
- Outlook
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
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.
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

=> Chocolate demo!

See also:
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.

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

### Home

<table>
<thead>
<tr>
<th>Height</th>
<th>Age</th>
<th>Transactions</th>
<th>Total Sent</th>
<th>Relayed By</th>
<th>Size (kB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>362950</td>
<td>1 minute</td>
<td>826</td>
<td>4,698.38 BTC</td>
<td>BitFury</td>
<td>731.55</td>
</tr>
<tr>
<td>362949</td>
<td>3 minutes</td>
<td>2437</td>
<td>7,458.34 BTC</td>
<td>F2Pool</td>
<td>976.24</td>
</tr>
<tr>
<td>362948</td>
<td>12 minutes</td>
<td>1</td>
<td>25.00 BTC</td>
<td>F2Pool</td>
<td>0.26</td>
</tr>
<tr>
<td>362947</td>
<td>13 minutes</td>
<td>964</td>
<td>8,804.23 BTC</td>
<td>Eligius</td>
<td>270.95</td>
</tr>
<tr>
<td>362946</td>
<td>43 minutes</td>
<td>1502</td>
<td>9,022.41 BTC</td>
<td>AntPool</td>
<td>911.61</td>
</tr>
<tr>
<td>362945</td>
<td>53 minutes</td>
<td>462</td>
<td>4,429.11 BTC</td>
<td>BTCChina Pool</td>
<td>226.82</td>
</tr>
</tbody>
</table>

### Latest Transactions

- 49c7ae3c06c0eeb0182e58e1d2...
- a7611a13c7b798b64a5786c...
- 4f85e1a6078f61a23cdeacde...
- 92c14b0d8c6fbde4e9917154...
- 767fc0ca8083f90e227b9f72...

- < 1 minute 47.87207621 BTC
- < 1 minute 2.67086557 BTC
- < 1 minute 0.61044466 BTC
- < 1 minute 0.019915 BTC
- < 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
- XCP Weekly Update #5 with Robert Ross
- Lets Talk Bitcoin 21 minutes ago
# The Blockchain – Block Detail

## Block #362950

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

## Hashes

<table>
<thead>
<tr>
<th>Hash</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous Block</td>
<td>000000000000000000000019ccc6318d7fd639fccc50e72fa1ee716130f095097b3b3</td>
</tr>
<tr>
<td>Next Block(s)</td>
<td>0000000000000000000000000a22e05371ede898456d6dcf3132bb67b1c136d050a1c743</td>
</tr>
<tr>
<td>Merkle Root</td>
<td>103d5a2bca6ceff6d6b52ae258267dafa1b1f5db8658f90875f34730f76e3cb</td>
</tr>
</tbody>
</table>

Network Propagation (Click To View)
# The Blockchain — Transaction Detail

## Transactions

<table>
<thead>
<tr>
<th>Transaction ID</th>
<th>Amount</th>
<th>Address Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>647b687343d17d0f9a2b5dd3a44378086d1fb60e826b7e0b7091e7b0fd738cb</td>
<td>25.10629534 BTC</td>
<td>1FeDtFhARLxjKp... (Bitfury)</td>
</tr>
<tr>
<td>75d0615c6e2d681b22794de626056d8cb7983b907a81189374bae18485f1c3c</td>
<td>25.10629534 BTC</td>
<td></td>
</tr>
<tr>
<td>1M4ns5xm894Veua32a8JWnGpiDwctMLg2U</td>
<td>28.79999671 BTC</td>
<td>18TLHSV51qfXWGV6t2xtXWAwSYeVdqZkYwm 1A83RevgCXuFsnuczGqF/UZQzX1Qh3b8Mw</td>
</tr>
<tr>
<td>51e2e600f94191b11bde7c1c453d27f18ea287d4f1669b413ac10a60ae6e377a</td>
<td>29.99999671 BTC</td>
<td></td>
</tr>
<tr>
<td>1AFcVIE1N8jo59pkCqizmHnVefP4mK6P8</td>
<td>1 BTC</td>
<td>3HUceWjsUHHuXhx8DcH5PnajwxfR6hwvh</td>
</tr>
<tr>
<td>194cca05e7b80f484829228ba54f8af4166c1e77a47e5c9aa48ab70e112b854cc</td>
<td>0.9988 BTC</td>
<td></td>
</tr>
<tr>
<td>1699Ui1xtkykJPYhA3ktXZE1Ydpzhpxpu4x</td>
<td>0.9988 BTC</td>
<td>19Bgr19D7qczLknLWa9akmRJmLcZz92Z</td>
</tr>
</tbody>
</table>
The Blockchain — Hashes

To be, or not to be

03c6691ebdd161363457e3c73a8ed44186536cf9

Carola F. Berger, Bitcoin and other cryptocurrencies, ATA56
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

| 7cdbgab6e2d681b22794de62c6056d8cb7983b907a811893d74bae18485f1c3c | 18TLHSVs1qHXWG6t2xtXWAOsYVeVdQzkYwm - (Unspent) |
| 1M4sn5xm894Veua32a8JWnGpiDwctMLg2U (30 BTC - Output) | 1A83RevgCXuFsnuczcGQfUZQzX1Qh3bBMw - (Unspent) |

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
</tr>
<tr>
<td>Received Time</td>
</tr>
<tr>
<td>Included In Blocks</td>
</tr>
<tr>
<td>Confirmations</td>
</tr>
<tr>
<td>Relayed by IP</td>
</tr>
<tr>
<td>Visualize</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inputs and Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Input</td>
</tr>
<tr>
<td>Total Output</td>
</tr>
<tr>
<td>Fees</td>
</tr>
<tr>
<td>Estimated BTC Transacted</td>
</tr>
</tbody>
</table>

Scripts | Hide scripts & coinbase |
Wallets and Faucets – Bitcoin Wallet

Balances
Available: [redacted] BTC
Pending: 0.00000000 BTC
Total: [redacted] BTC

Recent transactions

Encrypted and locked
Synchronization status
Wallets and Faucets – Bitcoin Wallet

![Bitcoin Core - Wallet](image)

- **Pay To:** Enter a Bitcoin address (e.g. 1NS17iog9jJgTHD1VXjvLCEnZuQ3rJDE9L)
- **Label:** Enter a label for this address to add it to your address book
- **Amount:**BTC

**Transaction Fee:** 0.00015748 BTC/kB  
Choose...

**Balance:** BTC
Getting BTC - Bitcoin Exchange Rate

Market Price (USD)
Source: blockchain.info

Carola F. Berger, Bitcoin and other cryptocurrencies, ATA56
Faucets = websites, where you can get BTC for “free,” usually by watching ads (warning – anti-virus programs are strongly recommended!)

Usually only a few Satoshi = 0.00000001 BTC

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

List of faucets:
## Altcoins

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
<th>Available Supply</th>
<th>Volume (24h)</th>
<th>% Change (24h)</th>
<th>Price Graph (7d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$4,747,586,452</td>
<td>$321.10</td>
<td>14,785,475 BTC</td>
<td>$41,826,500</td>
<td>-0.57 %</td>
<td><img src="https://via.placeholder.com/150" alt="Price Graph" /></td>
</tr>
<tr>
<td>2</td>
<td>Litecoin</td>
<td>$168,397,130</td>
<td>$3.92</td>
<td>42,964,260 LTC</td>
<td>$5,736,820</td>
<td>-1.98 %</td>
<td><img src="https://via.placeholder.com/150" alt="Price Graph" /></td>
</tr>
<tr>
<td>3</td>
<td>Ripple</td>
<td>$156,298,050</td>
<td>$0.004714</td>
<td>33,156,211,683 XRP</td>
<td>$255,296</td>
<td>-1.21 %</td>
<td><img src="https://via.placeholder.com/150" alt="Price Graph" /></td>
</tr>
<tr>
<td>4</td>
<td>Ethereum</td>
<td>$72,519,611</td>
<td>$0.975311</td>
<td>74,355,370 ETH</td>
<td>$924,801</td>
<td>-9.94 %</td>
<td><img src="https://via.placeholder.com/150" alt="Price Graph" /></td>
</tr>
<tr>
<td>5</td>
<td>Dogecoin</td>
<td>$14,358,167</td>
<td>$0.000141</td>
<td>101,619,804,175 DOGE</td>
<td>$164,071</td>
<td>-1.52 %</td>
<td><img src="https://via.placeholder.com/150" alt="Price Graph" /></td>
</tr>
<tr>
<td>6</td>
<td>Dash</td>
<td>$14,298,373</td>
<td>$2.41</td>
<td>5,943,836 DASH</td>
<td>$67,670</td>
<td>-5.74 %</td>
<td><img src="https://via.placeholder.com/150" alt="Price Graph" /></td>
</tr>
<tr>
<td>7</td>
<td>Stellar</td>
<td>$10,954,581</td>
<td>$0.002265</td>
<td>4,837,356,606 STR</td>
<td>$15,985</td>
<td>8.72 %</td>
<td><img src="https://via.placeholder.com/150" alt="Price Graph" /></td>
</tr>
</tbody>
</table>

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

---

Carola F. Berger, Bitcoin and other cryptocurrencies, ATA56
# Altcoins

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>75</td>
<td>Electronic G...</td>
<td>$281,739</td>
<td>13,571,710</td>
<td>$273</td>
<td>9.96 %</td>
</tr>
<tr>
<td>76</td>
<td>TileCoin</td>
<td>$273,824</td>
<td>100,000,000</td>
<td>$92</td>
<td>3.74 %</td>
</tr>
<tr>
<td>77</td>
<td>Unobtanium</td>
<td>$271,947</td>
<td>196,194</td>
<td>$529</td>
<td>-4.55 %</td>
</tr>
<tr>
<td>78</td>
<td>CannabisCoin</td>
<td>$270,388</td>
<td>77,165,665</td>
<td>$556</td>
<td>0.07 %</td>
</tr>
<tr>
<td>79</td>
<td>UnionCoin</td>
<td>$265,240</td>
<td>8,388,608</td>
<td>$445</td>
<td>-5.20 %</td>
</tr>
<tr>
<td>80</td>
<td>Flycoin</td>
<td>$264,791</td>
<td>164,928</td>
<td>$849</td>
<td>-22.02 %</td>
</tr>
<tr>
<td>81</td>
<td>Nas</td>
<td>$257,170</td>
<td>10,000,000,000</td>
<td>$58</td>
<td>-0.44 %</td>
</tr>
<tr>
<td>82</td>
<td>SolarCoin</td>
<td>$254,288</td>
<td>34,180,042</td>
<td>$19</td>
<td>10.86 %</td>
</tr>
<tr>
<td>83</td>
<td>Qora</td>
<td>$251,706</td>
<td>10,000,000,000</td>
<td>$21</td>
<td>2.91 %</td>
</tr>
<tr>
<td>84</td>
<td>SkyNET</td>
<td>$244,193</td>
<td>894,223</td>
<td>$29</td>
<td>-5.85 %</td>
</tr>
</tbody>
</table>
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
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