History and Concerns
Innovation and Technology
Analytics & Statistics
New Services

António Roldão, Ph.D. CQF.
About Me

MUSE.AI

python

Web Canvas

Imperial College London

GALILEO

GIOVE

http://anton.io
@roldao
Experimental Technology

$6 billion experiment!!
Brief History

- before — hashcash, eGold, b-money, ...

- 2008/Aug — bitcoin.org registered
- 2008/Oct — white paper published
- 2008/Nov — source code available
- 2009/Jan — genesis block mined (+9d to 1\textsuperscript{st} transaction)
- 2009/Oct — 1\textsuperscript{st} exchange rate: 1BTC = 0.0007639 USD
- 2010/Feb — 1\textsuperscript{st} exchange is born (Bitcoin Market)
- 2010/May — 10,000 BTCs spent on pizza
- 2011/Apr — First put option sold (#bitcoin-otc)
- 2011/Jun — Bitcoin reaches $10 on MtGox
- 2012/Jul — Bitcoin Start-up Incubator launched (BoostVC)
- 2013/Jul — Winklevoss Bitcoin Trust filed
- 2013/Aug — Texas judge ruled Bitcoin as Currency
- 2013 — BTC Ticker on all major business sites
- 2014 — Major corps accept Bitcoin (Dell, Expedia, MS, Time,..)
- 2015/Nov — EU Rules no VAT
Knowledge vs. Public Perception

Do you think the government should allow people to use Bitcoin to purchase goods and services or not?

Source: Reason-Rupe Survey
Media Coverage
Concerns - Ponzi Scheme / Tulip Mania
Confusing Media Circus
Concerns - Conspiracy Theories

or should one say Dorian Nakamoto?!
Concerns - Illicit Activities / Drugs
“The Federal Reserve simply does not have authority to supervise or regulate bitcoin in any way.” – Janet Yellen
Concerns - Others

- NotReversible
- KeyLoss
- ComplexMaths
- NotPhysical
- LimitedSupply
- NoAccountability
- Bitcoin2.0
- MoneyLaundering
- Misinformation
- BrokenSHA256
- SlowTransactions
- Scalablility
- BrokenECDSA
- NotaCurrency
- NoTaxes
- Hackers
- NoInflation
- Volatile
- Trust
The Problem
The Bitcoin Solution Allows:

- Creation of digital assets / tokens
- Proof of ownership
- Transfer of ownership
- Uniqueness of ownership
- Creation of accounts at will
- Direct exchange between participants without a third party!!
Other Related Aspects:

- Micro-payments*
- Payment freedom
- Frictionless transactions
- No central point of failure
- Public and transparent ledger
- Fast transactions across borders
- No central point of manipulation
- No risk of physical possession/loss
- Well understood and mathematical
- The gold standard in crypto-currencies
- Very low fees, some times even zero fees
- Anyone/Thing can open/close an account
- Human2Human/Machine2H/H2M/M2M Business
- ...

*currently, with some important limitations.
How Does Bitcoin Work?
Key Concepts – Hashes 1/2

Hashing functions

```
In [1]: 2**256
Out[1]: 115792089237316195423570985008687907853269984665640564039457584007913129639936L

In [2]: import hashlib
   ...: sha256 = hashlib.sha256()
   ...: sha256.update('')
   ...: sha256.hexdigest()
Out[2]: 'e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855'
```
Key Concepts – Hashes 2/2

- Obfuscating passwords (e.g. /etc/shadow)
- Cyclic Redundancy Checks (e.g. md5 on downloaded files)
- Verification of file authenticity (e.g. kernel source code)
- Compression of data (e.g. deduplication on git / ZFS/ ...)
- Bucketing data (e.g. database sharding)

... 

- Integrity of chain of events (e.g. merkle root / blockchain)
- Calibrating compute power for Proof of Work!

- Proof of prior existence without disclosure
Key Concepts – Digital Signature Algorithms

RANDOM GENERATOR

PRIVATE KEY

PUBLIC KEY
## Key Concepts – Public Ledger

<table>
<thead>
<tr>
<th>Time</th>
<th>Account</th>
<th>Inputs</th>
<th>Outputs</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>addr1</td>
<td>20</td>
<td>-</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>addr2</td>
<td>100</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>3</td>
<td>addr1</td>
<td>-</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>addr1</td>
<td>20</td>
<td>-</td>
<td>30</td>
</tr>
<tr>
<td>5</td>
<td>addr2</td>
<td>-</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>addr2</td>
<td>2</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>addr3</td>
<td>5</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>addr3</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>addr1</td>
<td>5</td>
<td>-</td>
<td>35</td>
</tr>
</tbody>
</table>

... All Transactions...
Key Concepts – P2P Networks
Key Concepts – “Script” Language

- Non-Turing complete (i.e. no loops)
- Stack-based
- Forth-like syntax (e.g. hint of the creators age!)
- Each stack evaluates to True or False
- Allows embedding of data (e.g. messages)
- Built-in cryptographic and hashing functions (e.g. SHA256, RIP160)
- Allow for non-trivial conditions such as multi-signature, etc.
Key Concepts – Network Effects & Game Theory

- Interests are aligned for everyone to cooperate
- Positive Network effects
- Only valuable if intact
- Need to cooperate to keep its value
- 51% Attacks benefit no-one
- ...
Details – Transactions 1/2
Details – Transactions 2/2

- 2 types: Coinbase, and Standard
- Outputs typically “lock” coins to the owner of some key
- Can embed messages (e.g. timestamp)

- Coinbase
  - 1\textsuperscript{st} transaction of a mined block
  - Brings coins into existence
  - Allows miners to claim mining fees

- Standard
  - Outputs cannot exceed inputs
  - Excess Inputs will be added to Coinbase as mining reward
  - Chain of transactions necessarily begins at a Coinbase
Details - Storing Transactions
Details – Block 1/3
Details – Block 2/3

- 1st block is named genesis
- All other blocks reference previously mined block
- System calibrates difficulty to mine one every ~10mins
- At the beginning, each block generated 50 BTCs
- Every 210,000 blocks (~4 years) this value halves
- Currently at 25 BTCs/block
- Block size is currently fixed at 1 MB*
- 1 MB translates to ~7 Transactions per Second

*Bitcoin XT – includes patches to upgrade to 8 MB once 75% are voting to change from 2016.
Details – Computing a Block Hash

```python
In [1]: from hashlib import sha256
    # Block 288888
    hex_next_block = (
        # Version
        "02000000" +
        # Prev block
        "d5776392209a5211166c137c6645b0c07610c64bff39a3350000000000000000000000" +
        # Merkle root
        "adf3233d0c6de7739cd3c9c3ebc8f0513831e935f49d637ead4afcf9c1b622cd" +
        # Time
        "ecee1553" +
        # Difficulty
        "26200119" +
        # Nonce
        "6a14f276"
    )
    bin_next_block = hex_next_block.decode('hex')
    hash = sha256(sha256(bin_next_block).digest()).digest()
    hash[::1].encode('hex_codec')
```

Out[1]: '00000000000000000000000456b9cd160ccf4d6b7341dc9aae04f98e5120fa5a73a3'

https://blockchain.info/block-height/288888
Details - Blockchain

Genesis

PREVIOUS HASH + NONCE + MERKLE ROOT

HASH

THIS BLOCK's HASH

PREVIOUS HASH + NONCE + MERKLE ROOT

THIS BLOCK's HASH

Previous SHA256
SHA256

Difficulty

Nonce SHA256
SHA256

Merkle Root

Hash

Hash

Hash

Hash

Hash

Transaction

Transaction

Transaction

Transaction
Mining
Mining - Pools
Mining – Pools Contribution

source: https://blockchain.info/pools
Bitcoin Mining
Mining Fees and Rewards

- Miners are incentivized in two ways: Fees and Rewards
- Fees are discretionary amounts set by the sender
- Rewards are given at the discovery of each block
  - (until 2136-10-11 10:15:05)
- Transaction may be free if
  - Less than 1kB
  - Outputs >0.01 BTCs
  - Priority is large enough
- each additional 1k should include a fee of 0.1mBTCs

Source: https://en.bitcoin.it/wiki/Transaction_fees
Analytics & Statistics
Discovering Bitcoin’s Fair Price?

1 Bitcoin = \( f_{\text{cost}}(\text{Energy} + \text{Equipment} + \ldots) \)
- Hardware performance varies widely
- Energy depends on country
- Difficulty level

Other Interesting questions
- How will diminishing coinbases affect fees?
- Will mining make energy generation more efficient or more expensive for day-to-day use?
- Will mining drive innovation for faster and cheaper electronics or make high-end chips more expensive?
Mining Efficiency

- **CPU**: >1Mh/s, ~5khps/W
- **GPGPU**: >1Gh/s, ~2Mhps/W
- **FPGA**: >1Gh/s, ~10Mhps/W
- **ASIC**: >10Gh/s, ~235Mhps/W

source: [https://en.bitcoin.it/wiki/Mining_hardware_comparison](https://en.bitcoin.it/wiki/Mining_hardware_comparison)
FPGA Spaghetti Monster

source: http://www.bitcoinminingrigs.com/
Professionalized Mining
Hash Rates

Source: blockchain.info

[Chart showing the increase in hash rates from 2009 to 2015. The y-axis represents Hash Rate GHash/s, and the x-axis represents years from 2009 to 2015. The hash rate increases significantly over the years.]
Difficulty Rates
Ledger Storage

Source: blockchain.info
Average Block Size
Blockchain Browsers

<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>289599</td>
<td>3 minutes</td>
<td>23</td>
<td>33,071.56 mBTC</td>
<td>Eligius</td>
<td>11.80</td>
</tr>
<tr>
<td>289598</td>
<td>3 minutes</td>
<td>351</td>
<td>466,711.86 mBTC</td>
<td>Slush</td>
<td>187.56</td>
</tr>
<tr>
<td>289597</td>
<td>&lt; 1 minute</td>
<td>64</td>
<td>1,042,265.53 mBTC</td>
<td>109.72.56.244</td>
<td>52.21</td>
</tr>
<tr>
<td>289596</td>
<td>11 minutes</td>
<td>110</td>
<td>466,894.30 mBTC</td>
<td>BTC Guild</td>
<td>96.82</td>
</tr>
<tr>
<td>289595</td>
<td>13 minutes</td>
<td>91</td>
<td>540,007.66 mBTC</td>
<td>GHash.IO</td>
<td>56.44</td>
</tr>
<tr>
<td>289594</td>
<td>14 minutes</td>
<td>159</td>
<td>1,312,066.81 mBTC</td>
<td>BTC Guild</td>
<td>96.83</td>
</tr>
</tbody>
</table>

Latest Transactions:
- 9630322bf... (SatoshiBONES 62.5pct) < 1 minute 3.48751 mBTC
- 30aef292f2... (SatoshiBONES 62.5pct) < 1 minute 36.82681 mBTC

Search:
You may enter a block height, address, block hash, transaction hash, hash 160, or ipv4 address.

- Blockchain
- Block Explorer
- BTCLook
- Biteasy
- Blockr.io
## Current Statistics (05.Nov.2015)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total blocks</td>
<td>382,187</td>
</tr>
<tr>
<td>Time between blocks</td>
<td>9.11 (minutes)</td>
</tr>
<tr>
<td>Terahashs/s</td>
<td>354,753</td>
</tr>
<tr>
<td>PetaFLOPS</td>
<td>5,920,057 (1st top500 ~x100)</td>
</tr>
<tr>
<td>Average transactions/h</td>
<td>8125</td>
</tr>
<tr>
<td>Average fees/h</td>
<td>1.575 BTCs / 630 USD + ~10000 USD (coinbases)</td>
</tr>
<tr>
<td>Bitcoins mined</td>
<td>14,804,274 BTCs (70%)</td>
</tr>
<tr>
<td>Market cap</td>
<td>5,834,808,906 USD</td>
</tr>
<tr>
<td></td>
<td>7,743,170,444 EUR</td>
</tr>
<tr>
<td></td>
<td>3,926,537,858 GBP</td>
</tr>
</tbody>
</table>

Source: [http://bitcoinwatch.com/](http://bitcoinwatch.com/)
Transaction Volumes

Source: blockchain.info

Transaction Volumes (USD)

Wallet Statistics

Source: blockchain.info

User Count

Open Source Libraries and Resources
Some Bitcoin Reference Sites

- Main source of information
  https://en.bitcoin.it/

- News
  http://www.coindesk.com/

- Historical data
  http://winkdex.com/

- Forum
  https://bitcointalk.org/

- Bitcoin explorer and Wallet
  https://blockchain.info/

- Twitter
  @BitcoinByte
  @BitcoinMagazine
  @LetsTalkBitcoin
  @petertoddbtc
  @jgarzik
Some Bitcoin Libs/Apps

- Source code of reference Bitcoin client
  
  `github/bitcoin/bitcoin`

- RPC-based library – not maintained anymore
  
  `github/laanwj/bitcoin-python`

- Low-level library does follows the bitcoin core
  
  `github/petertodd/python-bitcoinlib`

- Alternative to main client - relies on original net stack
  
  `github/etotheipi/BitcoinArmory`

- Out-dated but had great tools for dumping data out of db
  
  `github/gavinandresen/bitcointools`

- Trading application with SMSs alerts
  
  `github/skylarweaver/Bitcoin-Trader`

- Simple ticker that collects data from multiple exchanges
  
  `github/rgho/bitcoin_prices_python`

- Blockchain explorer
  
  `github/bitcoin-abe/bitcoin-abe`

- Automated arbitrage trading application
  
  `github/maxme/bitcoin-arbitrage`
Generating a Custom Address

```python
In [1]:
# https://github.com/cdecker/pycoin
from pycoin import wallet
import random

while True:
    seed = hex(random.randint(0, 2**126))[2:-1]
    master = wallet.Wallet.from_master_secret(seed)
    addr = master.bitcoin_address()
    if addr[1:3].lower() == 'py':
        print 'Found key'
        print '    Seed:', seed
        print '    Address:', addr
        print '    PrivKey:', master.wif()
        break
```

Found key

Seed: 22605df3c42c63c26ca3f217bf5aacc7
Address: 1PyFvWBEY5JeDNwGwaq6gAPQLmpTikd2y5
PrivKey: KxHhPATrad6vvSK5Yg8DNMo9EhREUxiBDicLvoRiVDsy2tvZH6EN
New Services
New Services Enabled

- Zero/Low commission betting (WinCoins)
- Music made of transactions (Listen to Bitcoins)
- Smart contracts (Etherium)
- Time stamping (Btproof)
- Micro-donations (Laybit)
- Tracking places of tension (Fiatleak)
- Virtual IPOs / Stock Market / Derivatives (mpex.co)
- Arbitrage between fiat and crypto currencies (btcarb)
- Machines that work for own profit/upgrades
  - e.g. self driving cars / delivery drones
- ... many many others ...
Thank you
Have a cryptic day!

http://anton.io
@roldao