Bitcoin

The world’s first decentralized digital currency

Meni Rosenfeld
Bitcoil
Decentralized digital currency

- Used as money
- Exists as information stored on a computer
- No central issuer (run by a p2p network)

- Invented in 2008 by “Satoshi Nakamoto” (pseudonym)
- Main site: [http://bitcoin.org/](http://bitcoin.org/)
How to use?

- Install open-source client software
- Software generates “addresses”, which are like bank account numbers (e.g. 1BBsbEq8Q29JpQr4jygjPof7F7uphqyUCQ)
- To receive bitcoins, let the sender know your address
- To send bitcoins, specify receiving address and amount, and click “send”
How to use?

![Image of Bitcoin Wallet interface](image_url)

**Pay To:** Enter a Bitcoin address (e.g., LN171ag8j6hM1UXjwLCEnZU3rJDKSL)

**Label:** Enter a label for this address to add it to your address book

**Amount:**

---

29/11/2012

Written by Meni Rosenfeld
Why?

- No need for 3rd party
- Easy to send and receive money
- Almost no fees
- No single point of failure
- Secure
- Limited supply – no built-in monetary and price inflation
- International
- No chargebacks
- Usable by weak/small countries
- Pseudonymous
- Public ledger
- Advanced applications
- See also [http://www.bitcoin.org.il/](http://www.bitcoin.org.il/)
Quantitative data

- No more than 21 million bitcoins will ever exist
- So far about 10 million bitcoins have been created
- Each bitcoin is currently worth roughly $12 (started at roughly half a cent, all-time high $32)
- Bitcoin amounts can be specified with 8 decimal places (2.1 quadrillion atomic units)
- Monetary inflation rate is stepwise decaying exponential, halving roughly every 4 years
Inflation schedule
Historic price chart

Mt. Gox (USD/dwolla/SEPA)

Nov 17, 2012 – Daily

Op:11.75, Hi:11.8, Lo:11.52, Cl:11.71

Vol: 16.8K

mtgox:USD

UTC – http://bitcoincharts.com

29/11/2012
Written by Meni Rosenfeld
Bitcoin system components

- A transaction structure for specifying and changing ownership
- A p2p network for propagating, verifying and storing transaction data
- A proof-of-work system (hashing, “mining”) for:
  - Synchronizing transactions
  - Determining initial distribution of coins
Transactions

- Transactions are the fundamental building blocks of Bitcoin
- In a transaction, coins move from address A to address B
- Address A must have the necessary amount of coins
- The transaction must contain a digital signature from the private key associated with address A (ECDSA)
- In a generation transaction, coins are created
Transaction structure

Transaction

tx hash - c371a3cb284256f93b4978d3634a0757e8f08698b40e428b4a7f

Input #1
Output ref.; signature

Input #2
Output ref.; signature

Input #3
Output ref.; signature

Output #1
Receiving address; amount

Output #2
Receiving address; amount

Tx 5e082...

#2

Tx ca079...

#1

Tx d7e67...

#1

29/11/2012

Written by Meni Rosenfeld
Transaction structure

- A transaction can have any number of inputs and outputs
- An output specifies a receiving address and amount
- An input references a previous unspent output
- The total value of all inputs must be at least the total value of all outputs
- The transaction is identified by a hash of its data
- The hash must be signed by the private key corresponding to every input address
- An address is a hash of an ECDSA public key
- More generally, an output specifies a script with the conditions to allow spending it
The Network
Problem: Double spending

- Using the same output ("coin") to pay 2 different recipients
- No agreement on who is the "true" recipient
- One recipient will be out of his coins (presumably after providing some product)
- Traditional solution: Central service determining order of transactions
- Naïve decentralized solutions have vulnerabilities
Solution: The blockchain

- Transactions are grouped into blocks
- Blocks are confirmed with proof of work
- A transaction is considered final if it is included in a confirmed block
- Each block references a previous block to form a chain
- In case of conflict, the transaction with more compute power spent on confirmation wins
- Attacks require having more compute power than the rest of the network
The Blockchain

Block #208364:
00000000000004dbfec547f2b52754079bbc1663bda4c2bed043102b16451

Header
Prev. block hash: ...e3a23
Nonce: 1165787096
MetaData
Merkle Root: e3b99e1ef650306a61471b55c11c6f6088367b9110001f3d0b977d215b2b5a6

Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx

Block #208363:
...e3a23
Block structure

- Transactions are organized in a Merkle tree with a resulting root hash
- The block header consists of the Merkle root, the hash of the previous block, other metadata, and a nonce
- The block is identified by the SHA-256 hash of its header
- A block is valid only if its hash is lower than the target
Proof of work

- A block with given data and nonce has a very low probability of being valid
- Miners try different nonces and compute the resulting hash (billions of tries per second) until they match the target, and release the resulting block
- The existence of a block which includes a transaction proves that computational work has been done by a node which considers this transaction valid
- Each block references the previous one. Each transaction gets increasingly more powerful proof of work
- In case of competing branches, the one with the most proof of work is selected
Proof of work

• A transaction “buried” under several blocks is very hard to revert mistakenly or maliciously
• Reverting a transaction requires catching up with the computation of the honest network, which is unlikely without greater hashrate
• Any change to a transaction invalidates all proof of work
• Hash target is adjusted every 2016 blocks (roughly 2 weeks) so that on average one block is found every 10 minutes
Creation of coins

- Every block is allowed one special “generation transaction”
- A generation transaction has a single special input, and any number of outputs
- Value of input: New coins + tx fees
- New coins: \( 50 \times 2^{-\frac{H}{210000}} \) (starts at 50 BTC per block and halves roughly once every 4 years)
- Incentivizes securing the network by hashing
- Robust way to determine initial distribution
Questions?
Thank you

- Meni Rosenfeld
- meni@bitcoil.co.il
- https://bitcoil.co.il
- 1DdrvajpK221W9dTzo5cLoxMnxu859QN6