Bitcoin
(Part 2)

Ken Calvert
Keeping Current Seminar
12 February 2014

Outline

I. Recap
   - what, why, technical guts (briefly)

II. Ecosystem
   - how to get them, what to do with them

III. Valuing
   - what determines value?

IV. Issues
   - potentially troubling aspects

V. Future
   - interesting directions, predictions (not mine)

I. Recap: What is Bitcoin?

a) A Cryptocurrency
b) Open-source software released in 2008
c) A peer-to-peer infrastructure for recording payments
d) A method of achieving distributed consensus
e) all of the above

I. Recap: What is Bitcoin?

a) A Cryptocurrency

b) Open-source software released in 2008

c) A peer-to-peer infrastructure for recording payments

d) A method of achieving distributed consensus

e) all of the above

Stated goals:

- Decentralized trust (bypass "the establishment")
- Anonymity

I. Recap: What is Bitcoin?

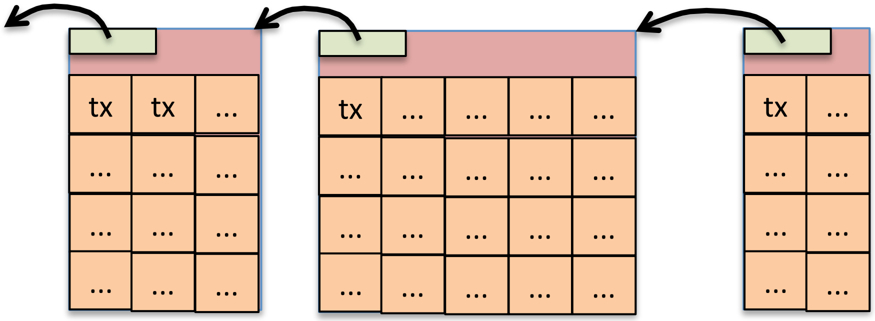
- A Cryptocurrency
  - Security of the bitcoin protocol is based on cryptographic primitives (digital signatures & crypto hash functions) and proof-of-work
- Open-source software released in 2008
  - Now maintained by the "Bitcoin community"
- A peer-to-peer infrastructure for creating a shared ledger (record) of transactions
  - "Anyone can play"
  - But special hardware needed to make it pay

I. Recap: How it works

Block chain: consensus record of valid transactions (txs) submitted to the system

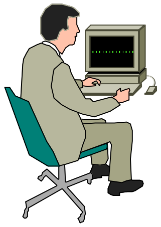
- Each block contains tx data + add'l info (header)
- Each header depends on tx data + previous block's header
- Each header has a property that is expensive to compute

⇒ Immutable, transparent (anyone can check validity)



I. Recap: How it works

Payer



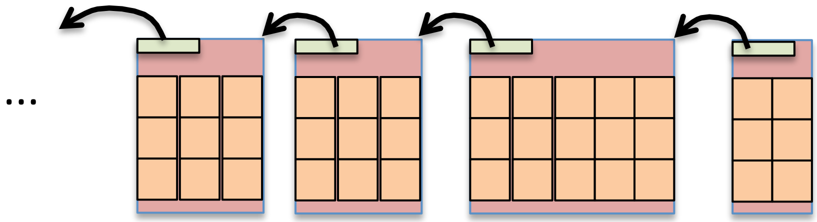
1

create pub/priv key pair
address ⇠ hash(pubkey)

Payee

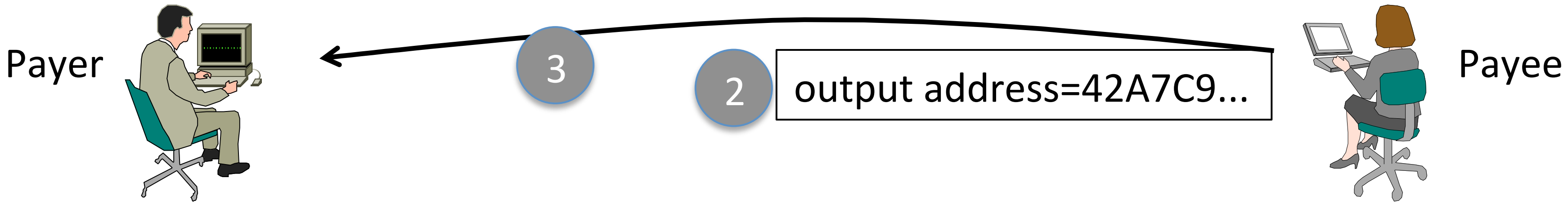
Transaction: transfer a quantity of bitcoins

- Inputs: pointer to previous tx output + proof of ownership
  - previous output: not used as input in any other tx
  - proof of ownership: digital signature
- Outputs: address + conditions of transfer
  - address: hash of public key
  - typical conditions of transfer: present pub key matching hash, sign tx with corresponding private key



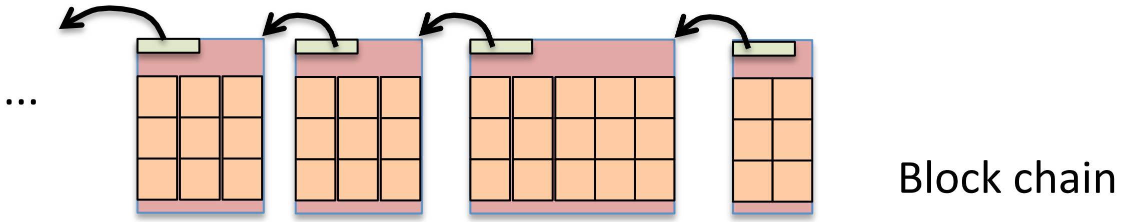
Block chain

I. Recap: How it works

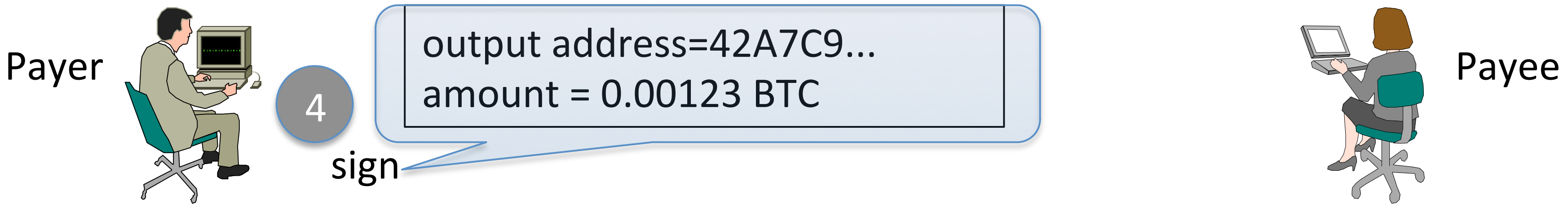


Transaction: transfer a quantity of bitcoins

- Inputs: pointer to previous tx output + proof of ownership
  - previous output: not used as input in any other tx
  - proof of ownership: digital signature
- Outputs: address + conditions of transfer
  - address: hash of public key
  - typical conditions of transfer: present pub key matching hash, sign tx with corresponding private key



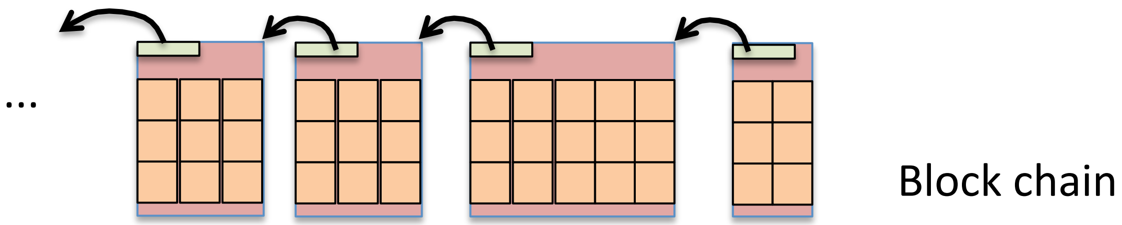
I. Recap: How it works



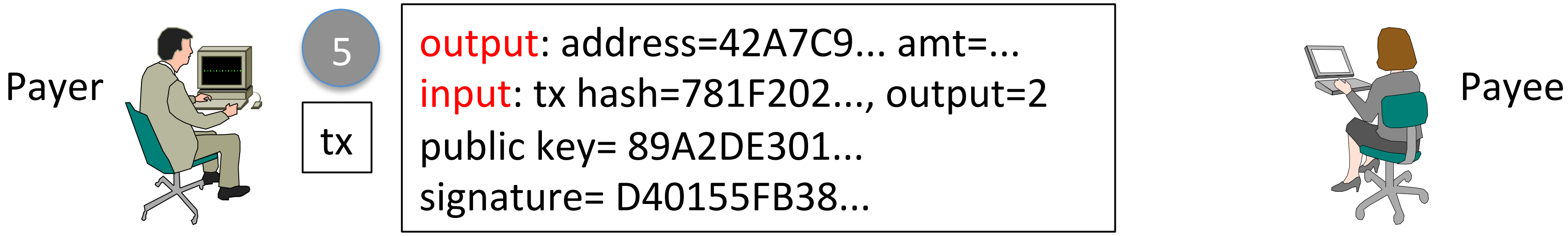
output address=42A7C9...
amount = 0.00123 BTC

Transaction: transfer a quantity of bitcoins

- Inputs: pointer to previous tx output + proof of ownership
  - previous output: not used as input in any other tx
  - proof of ownership: digital signature
- Outputs: address + conditions of transfer
  - address: hash of public key
  - typical conditions of transfer: present pub key matching hash, sign tx with corresponding private key



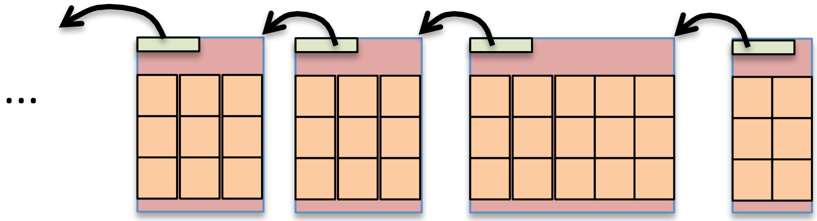
I. Recap: How it works



output: address=42A7C9... amt=...
input: tx hash=781F202..., output=2
public key= 89A2DE301...
signature= D40155FB38...

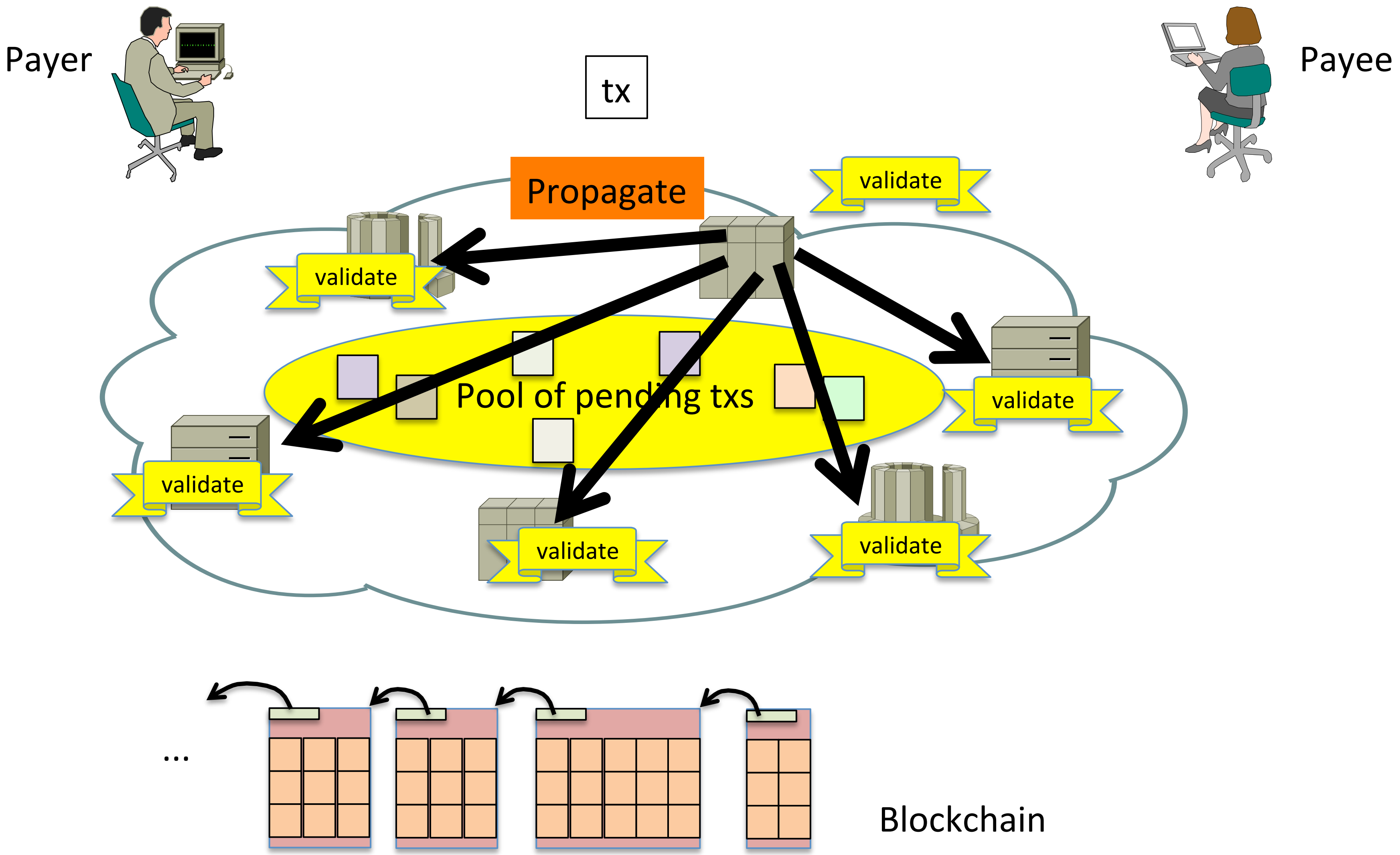
Transaction: transfer a quantity of bitcoins

- Inputs: pointer to previous tx output + proof of ownership
  - previous output: not used as input in any other tx
  - proof of ownership: digital signature
- Outputs: address + conditions of transfer
  - address: hash of public key
  - typical conditions of transfer: present pub key matching hash, sign tx with corresponding private key



Block chain

I. Recap: How it works



Payer

Payee

tx

Propagate

validate

validate

validate

validate

validate

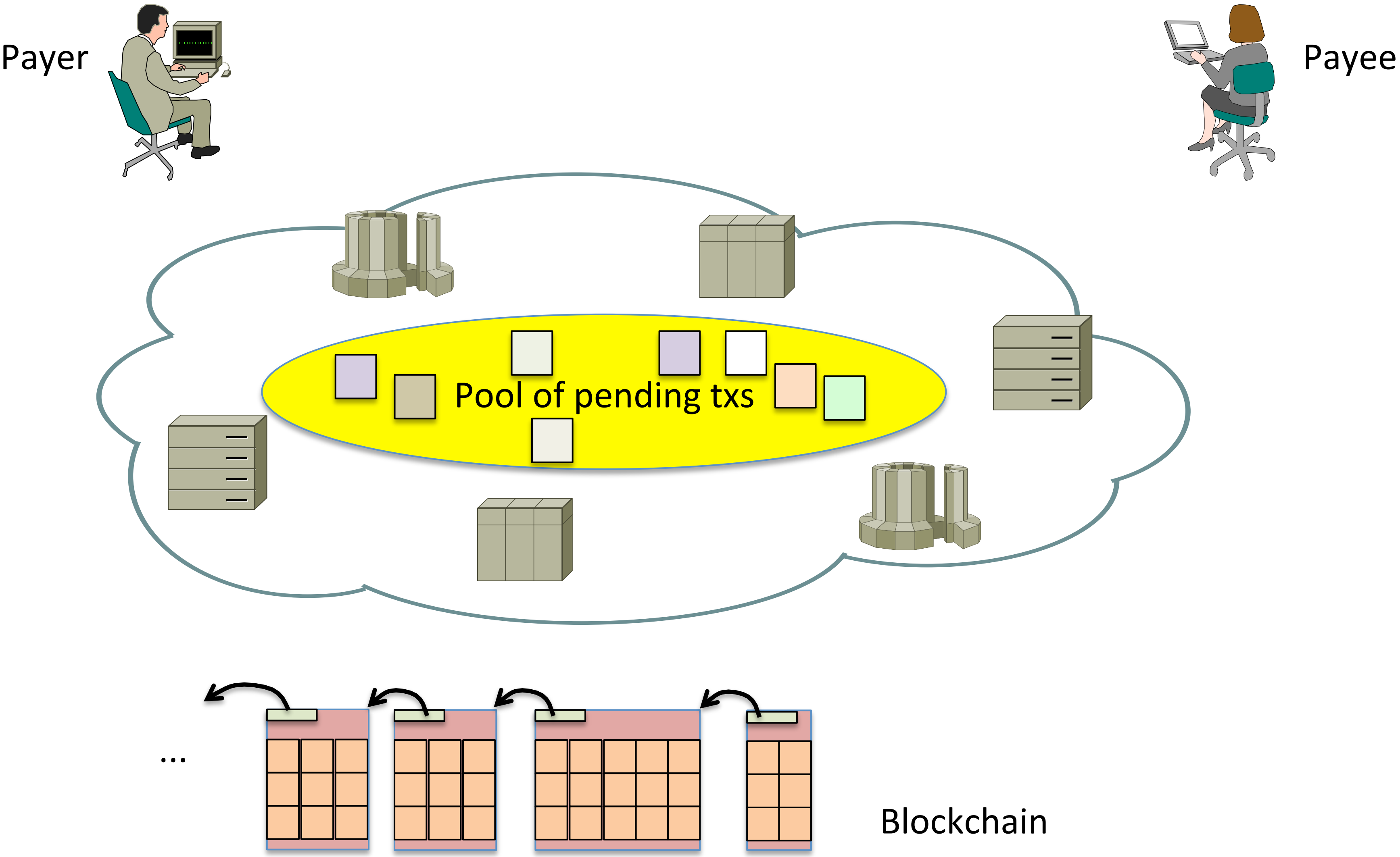
validate

Pool of pending txs

…

Blockchain

I. Recap: How it works



Payer

Payee

Pool of pending txs

…

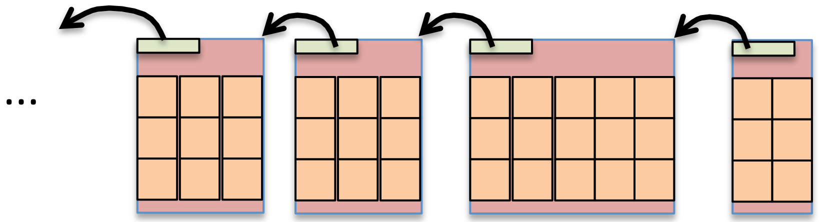
Blockchain

I. Recap: How it works

Mining: adding transactions into the block chain

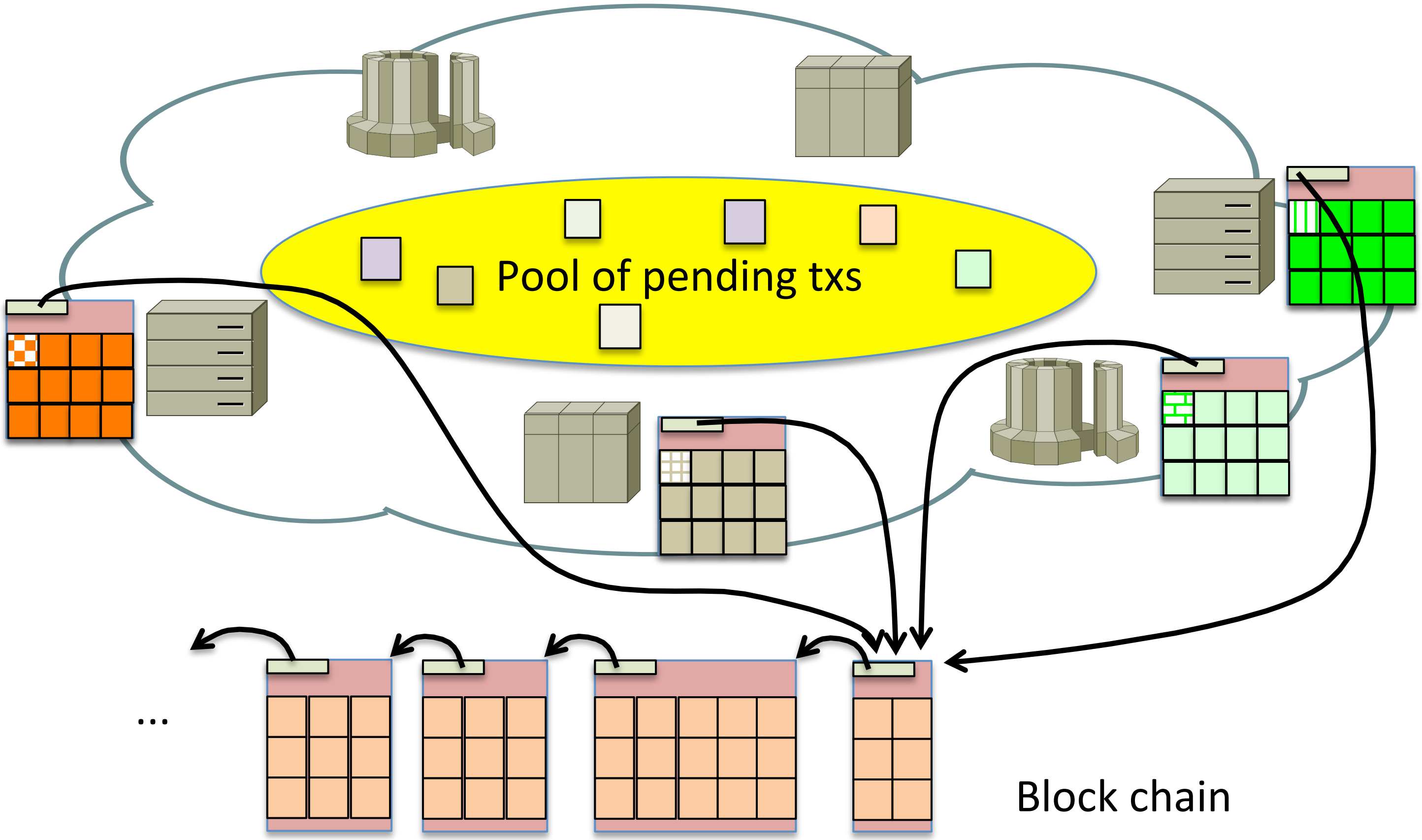
Peers ("miners") build the chain of transactions:

- Validate transactions
- Group txs into blocks
- "Solve" blocks by tweaking them until their header has the required property (hash(header) < target)
- Propagate newly-solved blocks to peers
- Validate blocks received from peers

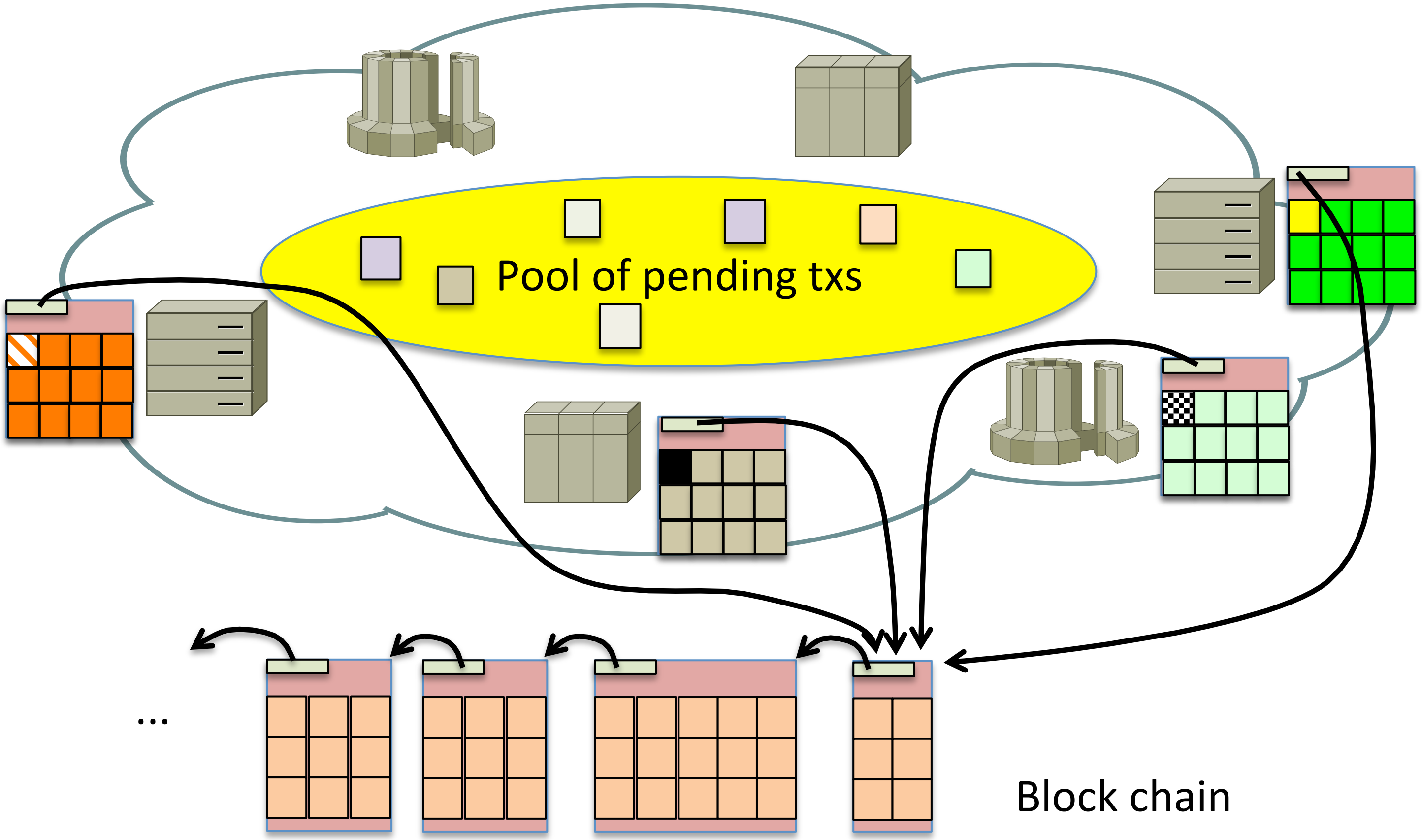


Block chain

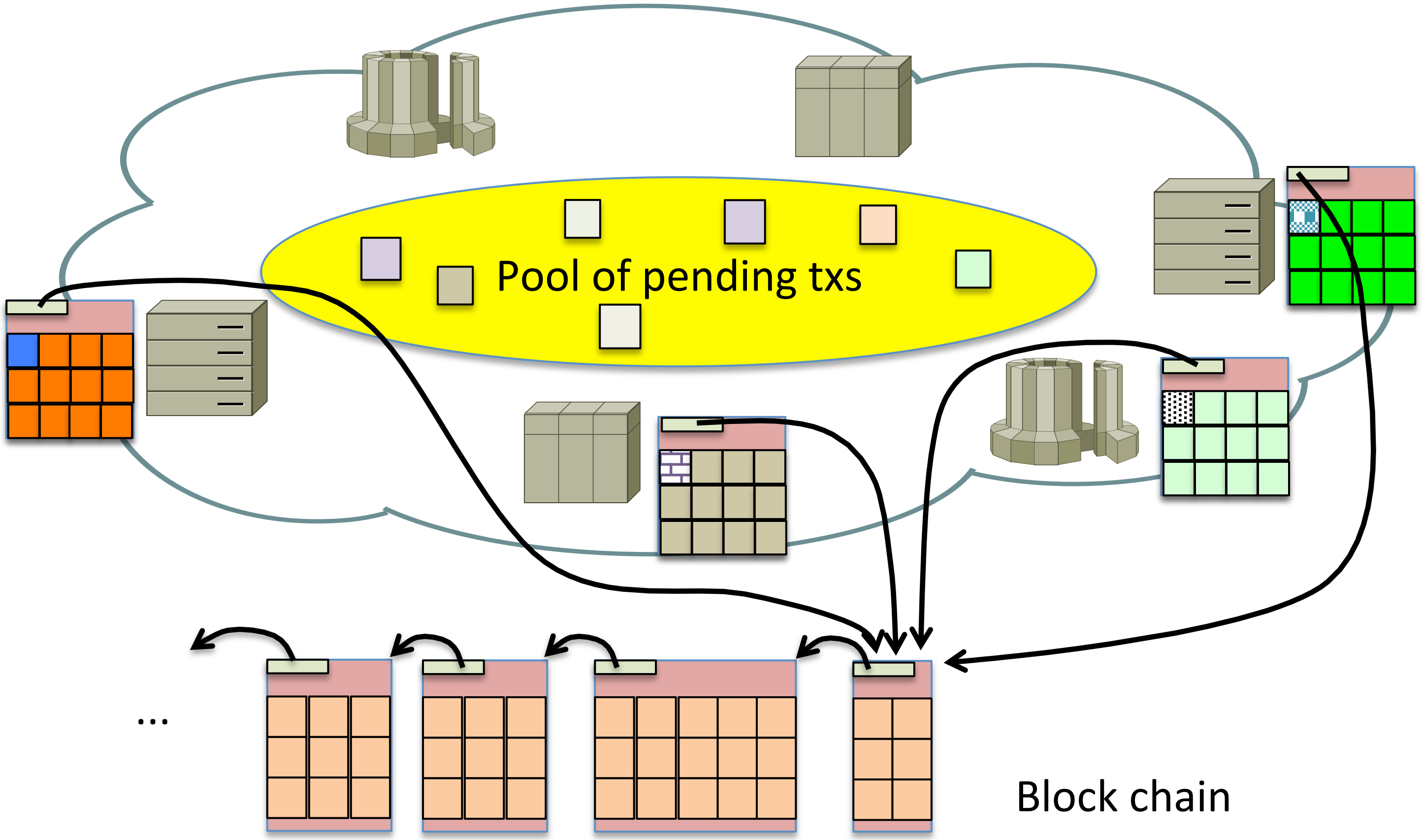
I. Recap: How it works



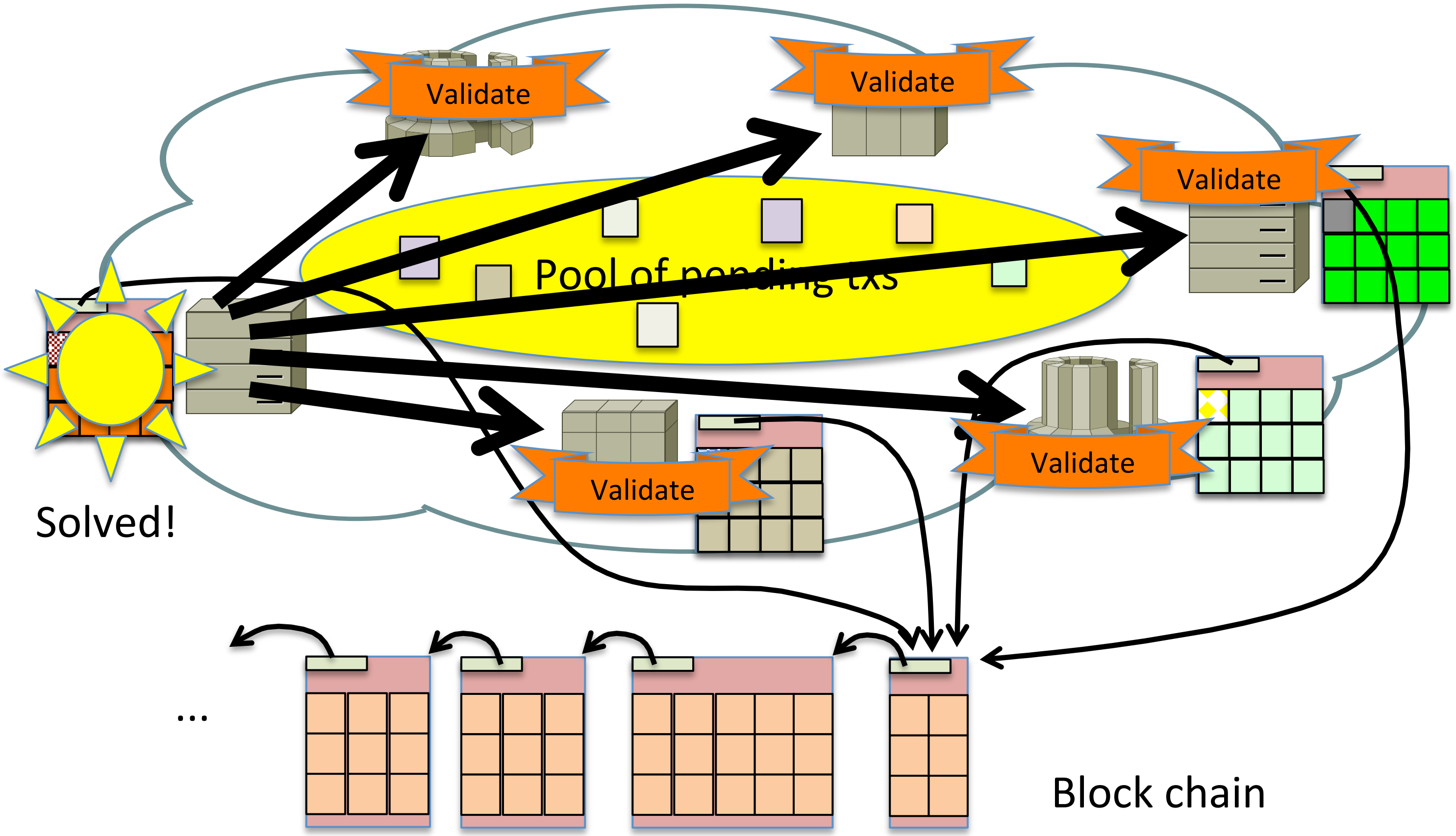
I. Recap: How it works



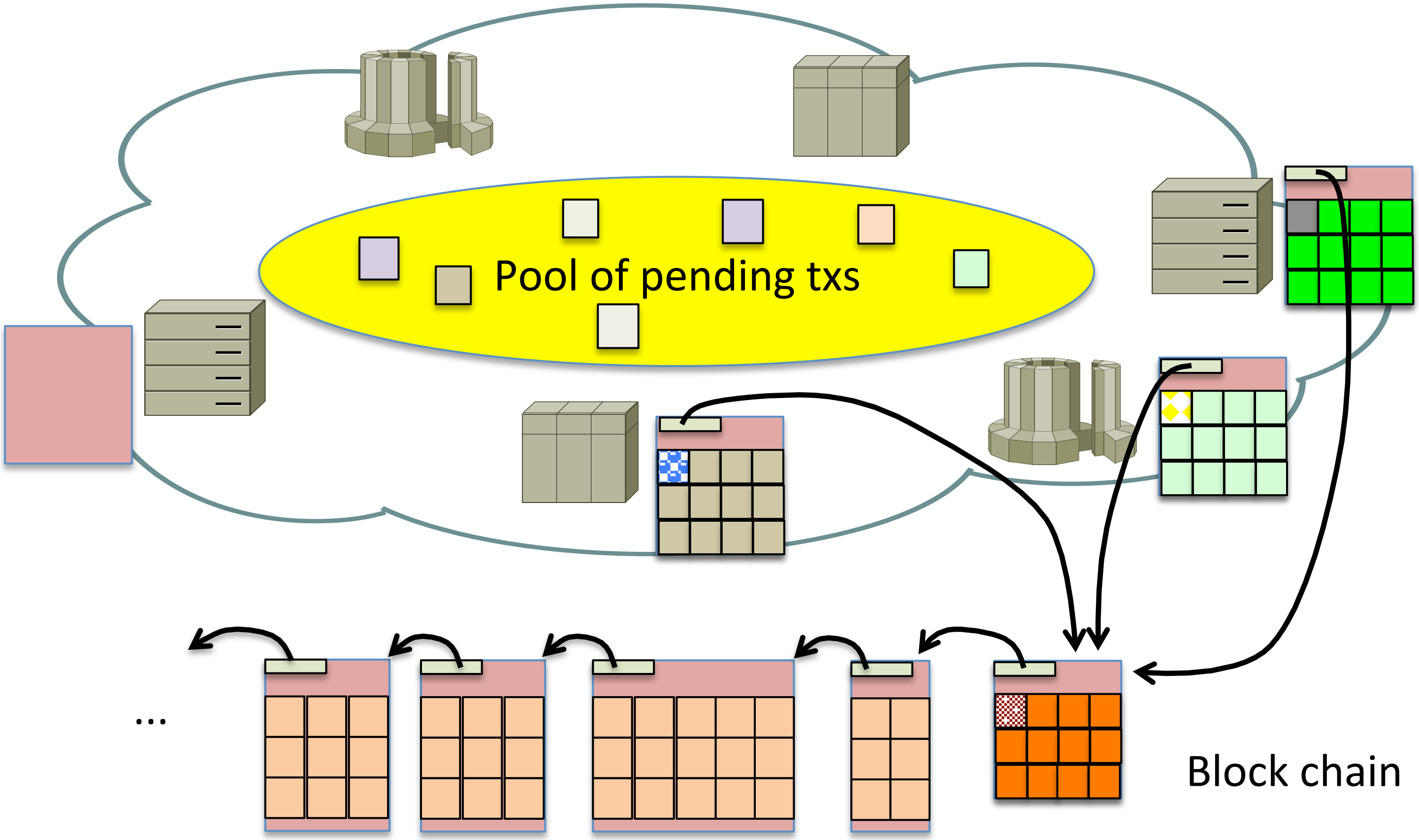
I. Recap: How it works



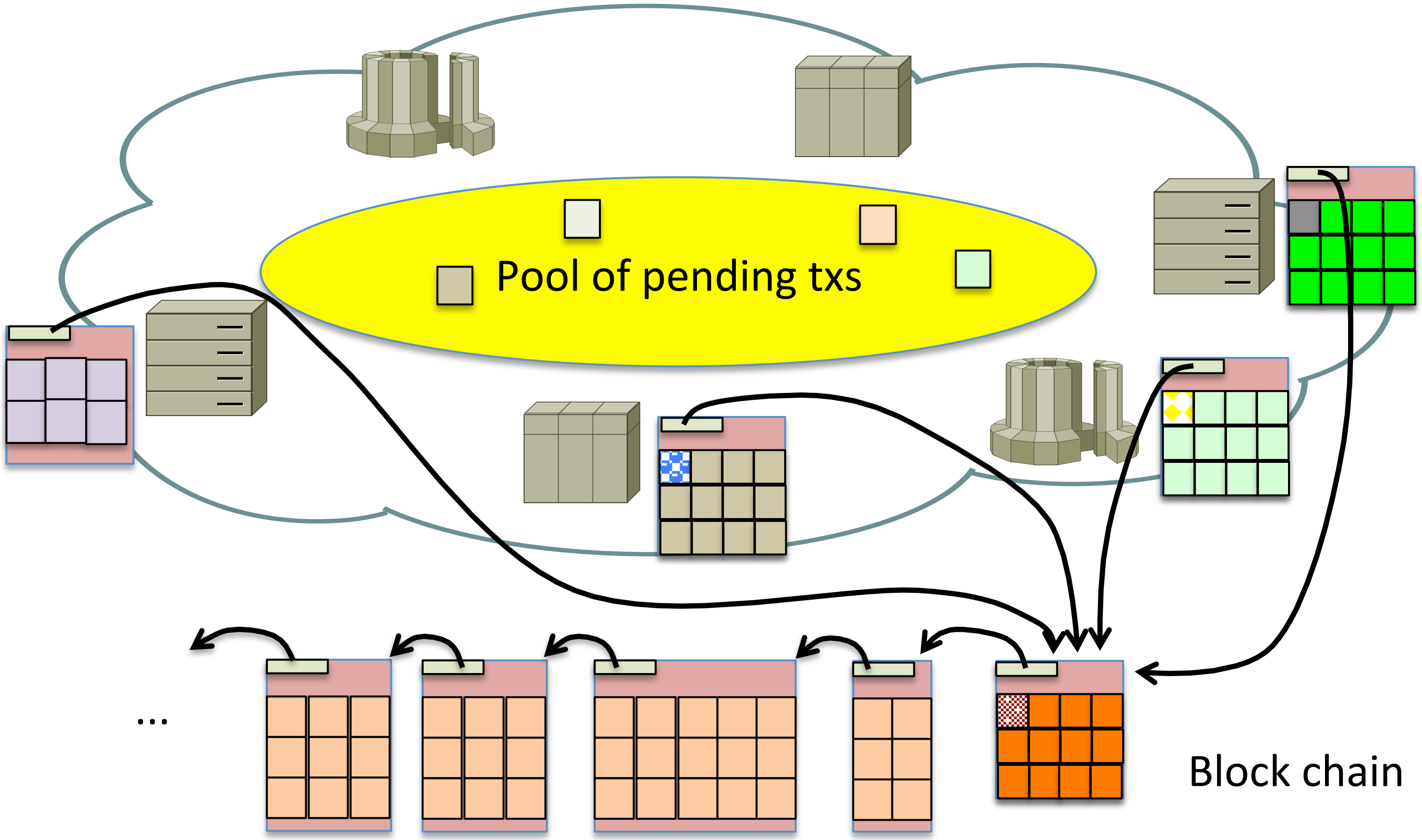
I. Recap: How it works



I. Recap: How it works



I. Recap: How it works



I. Recap: How it works

What motivates miners?

- "Coinbase" transaction:
  - First transaction in each block has no inputs
  - Miner that "solves" the block controls its outputs
  - Reward for solving the block
  - Amount of reward decreases every 210,000 blocks

    ⇒ total supply of bitcoins is finite

    (~21×10^6)
- Transaction fees:
  - Excess inputs of any tx can be added to coinbase tx's outputs

I. Recap: How it works

Target value (hex) as of 1/22/14:
0000000000000002666000000000000000000000000000000000000000000000
Target value as of 2/11/14:
0000000000000001A36E00000000000000000000000000000000000000000000

- Block header hash must begin with 64 0 bits
  - Requires computing ~2^{63} hashes
- Target adjusted periodically (biweekly)
  - Goal is for the network to solve a block approximately every 10 minutes
  - So: Network-wide hash rate ≈ 1.5×10^{16} hash/s
  - With 120K nodes ⇒ 125 GHash/sec/node (!)
- Most mining nowadays uses special h/w

II. Ecosystem

- Wallets:
  - User-facing software
  - Accept and store “coins” (unused outputs)
  - Create transactions to transfer coins (signing)
- Exchanges:
  - Buy and sell bitcoins (currency conversion)
  - Maintain user accounts (store bitcoins for you)
- Merchants:
  - Accept bitcoins as payment
- P2P network:
  - Miners build & maintain the block chain

III. Valuing

(Warning: I am not an economist.)

What determines the value of a currency?

- What you can buy with it! (liquidity)
  - E.g., dollars, euros, T-shirts, cars, ...
- Faith:
  - That it will retain its value

    E.g., that your transaction will not disappear from the block chain
  - That it will continue to be usable to buy things

III. Valuing

Some back-of-the-envelope calculations:

(thanks to Brian Wesbury, First Trust Advisors)

- Assume all 21M Bitcoins are available
- Money Supply (US dollars everywhere)
  - M2 (Fed metric) ≈ $11 Trillion
  - 11 x 10^{12} / 2.1 x 10^{7} = 5.24 x 10^{5}

    ⇒1 BTC ≈ $524K (if BTC replaced $ entirely, in the US)
- Liquidity (what you can buy)
  - Current US GDP ≈ $17 trillion (total value of production)
  - Assume Bitcoins accepted in 0.01% of all transactions (very liberal!)
  - 17 x 10^{12} x 10^{-4} / 2.1 x 10^{7} ⇒1 BTC ≈ $80

IV. Issues

- Volatility
- Security
- Protocol
- Trust
- Energy
- Anonymity

IV. Issues: Volatility

- A problem for bitcoin as investment
- Off about 15% this week...
- “Bitcoin has the volatility of hot C4 plastique sitting over an open flame. ... Its value moves faster than you can, and the size of these price moves makes heroin street pricing look like cotton on the commodities exchange.” – Mark Anderson, Strategic News Service

IV. Issues: Security

- Bitcoin ≃ tx id + public/private key pair
  - Generally: one key per transaction (!)
- Lose private key ⇒ bye-bye bitcoins!
- Where will you store them?
  - Exchange?
    - So much for not having to trust "banks"
  - Laptop? Phone? Printed on paper?
    - QR codes

IV. Issues: Protocol

- Persistent forks in the block chain
  - Different “solved” blocks arrive at different parts of the network in different orders ⇒ ambiguity as to which is the “last” block
  - Persists until one branch “wins” (extends further)
  - Forks may persist for unbounded time
  - March 2013 incident (caused by protocol update)
- Scalability
  - Record of unspent txs must be maintained
  - Max 2.1×10^{15} Satoshis (smallest unit) in circulation

IV. Issues: Protocol

- Protocol weaknesses

  Example: “Transaction Malleability”

  - Signature does not cover entire transaction
  - Some (insignificant) fields can be changed after signing
    - This changes the hash (=tx id), but not semantics

  Attack:

  1. Buy bitcoins at exchange
  2. modify tx (new id) and rebroadcast it yourself
  3. (if) mod’d tx gets into block chain → you have coins!
  4. first tx will not get into chain → complain to exchange
  5. exchange searches, fails to find original tx id → refund!

2 of 3 largest exchanges (Mt. Gox, Bitstamp) suspended withdrawals this week because their code did not deal with this problem (!)

IV. Issues: Trust

- Banks are heavily regulated
  - They have years of experience maintaining trust
  - Agencies set standards: FDIC, SEC, ...
- Bitcoin "community" ... not so much
- Theory: as long as honest nodes control majority of compute power, system is trustworthy
- Practice:

  See practically any bitcoin forum...

  See theories about this week's Mt. Gox freeze...

IV. Issues: Trust

- Theory: Decentralized, peer-to-peer, anyone can play
- Practice: mining is mainly in the hands of large players with significant capital investment
  - What regulations or laws govern them?
  - Nothing in the protocol guarantees that your transactions will enter the block chain

IV. Issues: Energy

- Bitcoin mining takes a large amount of computation
  - Perform a complex calculation enough times to roll over a 64-bit counter every 10 minutes!
- This requires a lot of electricity
  - KnC Jupiter ASIC: 600W/500 GH/s
  - Assume network hash rate = 2 x 10^{16} H/s
  - $(6\mathrm{x}10^{2})$ x $(2\mathrm{x}10^{16})$ / $5\mathrm{x}10^{11}$ = 24 Megawatts
- Assume $.10/KwH ⇒ $240/block, or ~ $10/BTC
  - Not to mention transaction validation, storage, communication, ...

IV. Issues: Anonymity

- Bitcoin is anonymous – in theory
  - In practice, not so much
  - It has been shown possible to trace ownership
- Ongoing tension between viewpoints:
  - More accountability ⇒ more trust
  - More anonymity ⇒ more trust
- Note: Government stances run the gamut
  - India: Bitcoin is illegal (also Russia this week)
  - Denmark: law explicitly says "we don't care"

V. Futures

- Hardware wallets
- "Altcoins"
- Other uses of the Bitcoin approach
- A high-profile bet on the future of bitcoin

V. Futures: Hardware Wallets

- Best way to store bitcoins?
  - Strong access control
  - Tamper-proof
  - Trackable?
- Several startups in this area
- Potentially useful for other things...

V. Futures: Altcoins

- Use the Bitcoin protocol (or similar) to start your own currency
- What prevents these things from springing up like mushrooms? (Nothing!)
  - At the end of US Civil War: ~50 different scripts in circulation
- From altcoins.com:

  Namecoin, Peercoin, Devcoin, Ixcoin, Freicoin, Deutsche eMark, Litecoin, Novacoin, Tagcoin, ...

V. Futures: Other uses

Bitcoin provides a way to create a stable (more or less) public record of transactions that obeys a published protocol (policy)

- Anyone can verify that the record is consistent with the protocol
  - "Incorruptible"
- Record is backed by the services of miners
  - Compensated for their service with "shares" of the enterprise
  - Buying bitcoin ≈ buying shares

V. Futures: Other uses

Bitcoin provides a way to create a stable (more or less) public record of transactions that obeys a published protocol (policy)

- "Distributed Autonomous Corporation" (DAC):
  - Generalize coins ➛ shares
- This system can be useful for many things:
  - Manage namespace/ID rights (e.g., DNS names)
  - Secure escrow service
  - Crowd-sourced venture capital
  - Government (?!)

IV. Futures: A wager

- Ben Horowitz, venture capitalist, bitcoin enthusiast
- Felix Salmon, economist and “bitcoin curmudgeon”
- The bet:
  - In January, 2019 the folks at “Planet Money” (NPR show) will poll a sample of Americans
  - If ≥ 10% say they have used bitcoin to buy something in the past month, Ben wins, else Felix wins
- The stakes: a pair of Alpaca socks
  - Claimed to be the first thing sold for bitcoin

Questions/Comments?