Do not distribute …

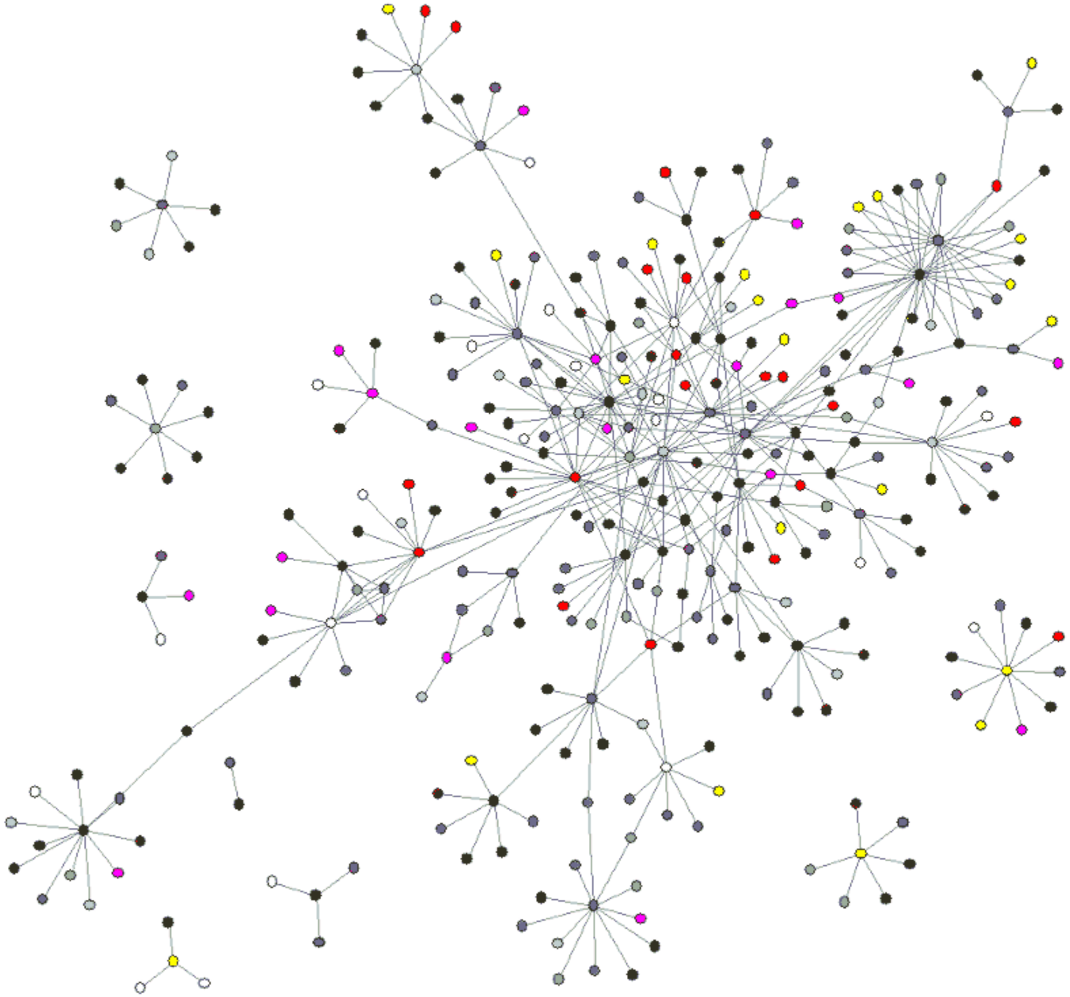
- These slides are not always prepared by me.
- Most of the content comes from the reference book
  - Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction
  - Arvind Narayanan, Joseph Bonneau,
  - Edward Felten, Andrew Miller, Steven Goldfeder
- This lecture however builds upon and uses slides from CS 3700 Networks and Distributed Systems
  - By David Choffnes available at https://david.choffnes.com/classes/cs3700fa17/

Tentative Course outline

- **PartA - Introduction, Background and Motivation**
  - Introduction, Background, Examples …
- **PartB – Core concepts focusing on Bitcoin**
  - Cryptography, Blockchain,
  - Bitcoin nuts and Bolts
  - Mining, Proof of Work and other Concensus approaches
- **PartC – Ethereum, Smart Contracts and Solidity**
  - Ethereum - The world Computer
  - Motivation, Setup, Getting Started and the Hello World
  - Writing Smart Contracts using Solidity

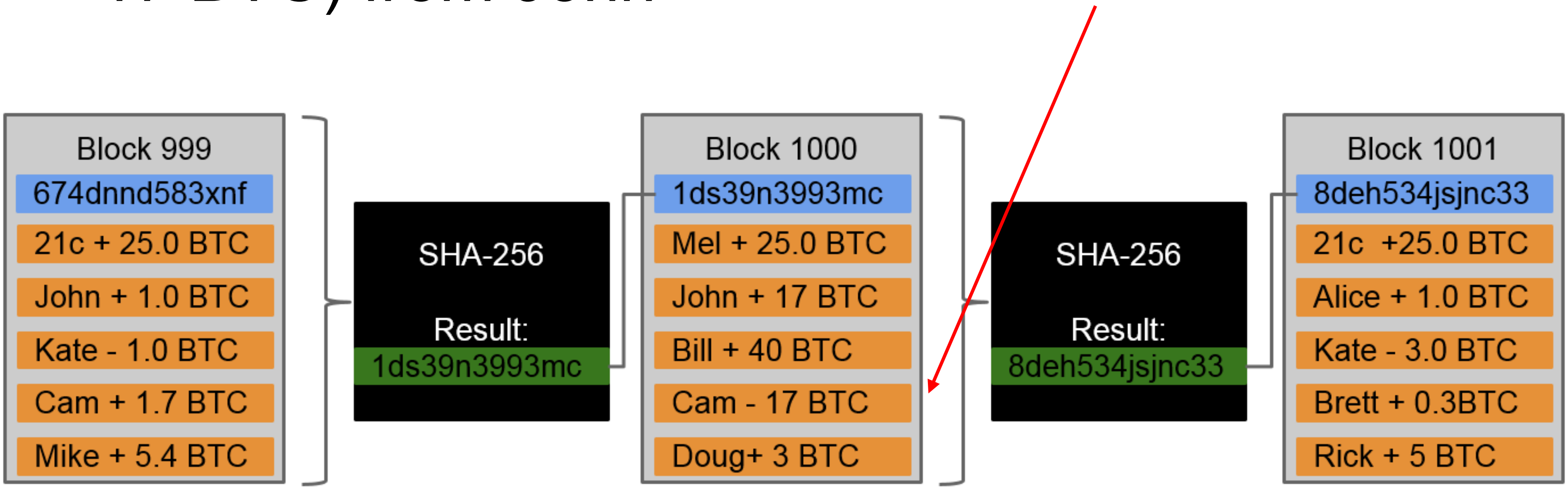
Ownership of a Digital Apple?

Decentralized Ledgers



Bitcoin Blockchain

Example: In block 1000, Cam buys a car (for 17 BTC) from John



Who developed Bitcoin?

- Satoshi Nakamoto

Towards Decentralized P2P Currency

What is Currency?

- Medium of exchange
  - May or may not have intrinsic value (e.g. gold)
- Store of value
  - Allows one to store “value” rather than objects
  - Facilitates lending, debt, investing, and other financial innovations

Is it money?

1.:
2.
3.:
SCARCE

$20!
$20!
$20!
1¢!
1¢!
1¢!
1¢!
UNIFORM

FIELD TRIP!
PORTABLE

LOOKIN' GOOD!
THANKS
DURABLE

GOT CHANGE?
WE ARE CHANGE!
DIVISIBLE

WANNA TRADE PLACES?
ACCEPTABLE

Physical Currency

- Ancient coinage was based on precious metals
  - Largely obviated the problem of counterfeiting
    - A “fake” gold coin is still made of gold
  - Lack of advanced mining techniques limited inflation

Physical Currency

- Paper bearer tokens began to replace coinage around 600 BC
  - Easier to carry, mint large denomination bills
  - Paper was exchangeable for a commodity, e.g. the gold standard

Physical Currency

“U.S. dollars are not backed by anything other than the faith of the fools who accept it as payment and of other fools who agree in turn to accept it as payment from them. ”

Almost all of U.S. dollars, about 90 percent, are purely abstract — they literally do not exist in any tangible form.

Physical Currency

- Modern physical currency is called fiat
  - Not linked to a hard commodity, based on trust
  - Why does fiat currency have “value”?
    - Social contract – everyone accepts the currency, therefore it has value
    - Centralized power – the government has the power to enforce taxation, and they accept currency as a means to pay taxes

Physical Currency - Advantages

- Easily portable
- Cannot double-spend
  - Spend the same piece of paper >1 times
- Cannot repudiate payment
  - Once you’ve given the paper, you can’t get it back
- Semi-anonymous

Physical Currency - Disadvantages

- Easy to steal
- Hard to monitor/tax transactions
- Requires trust in the centralized issuing authority
- Doesn’t work online

What About Electronic Currency?

- Credit cards, Paypal, Online transfers
  - Bank account store the amount of money held by each individual/company
  - Transactions move money between parties

- Advantages? Works online!
- Disadvantages
  - Requires trust in the issuing authority and third-parties
  - Privacy, Transaction costs, centralized operations and control on transactions…

Towards Non-fiat Electronic Currency

- Goal: e-cash without a centralized issuing authority
  - Store and transfer value without a reliance on commodities or central banks
  - Anyone can join the system and be party to transactions
- Bitcoin was, arguably, the first viable non-fiat electronic currency

Why is P2P Currency Hard?

- The most obvious challenge is determining ownership
  - Who owns a given unit of currency?
- Without strong ownership…
  - Forgery – a user can mint arbitrary currency
  - Double spending – how do you validate and enforce transactions?
  - Theft – impossible to separate true and false claims about ownership

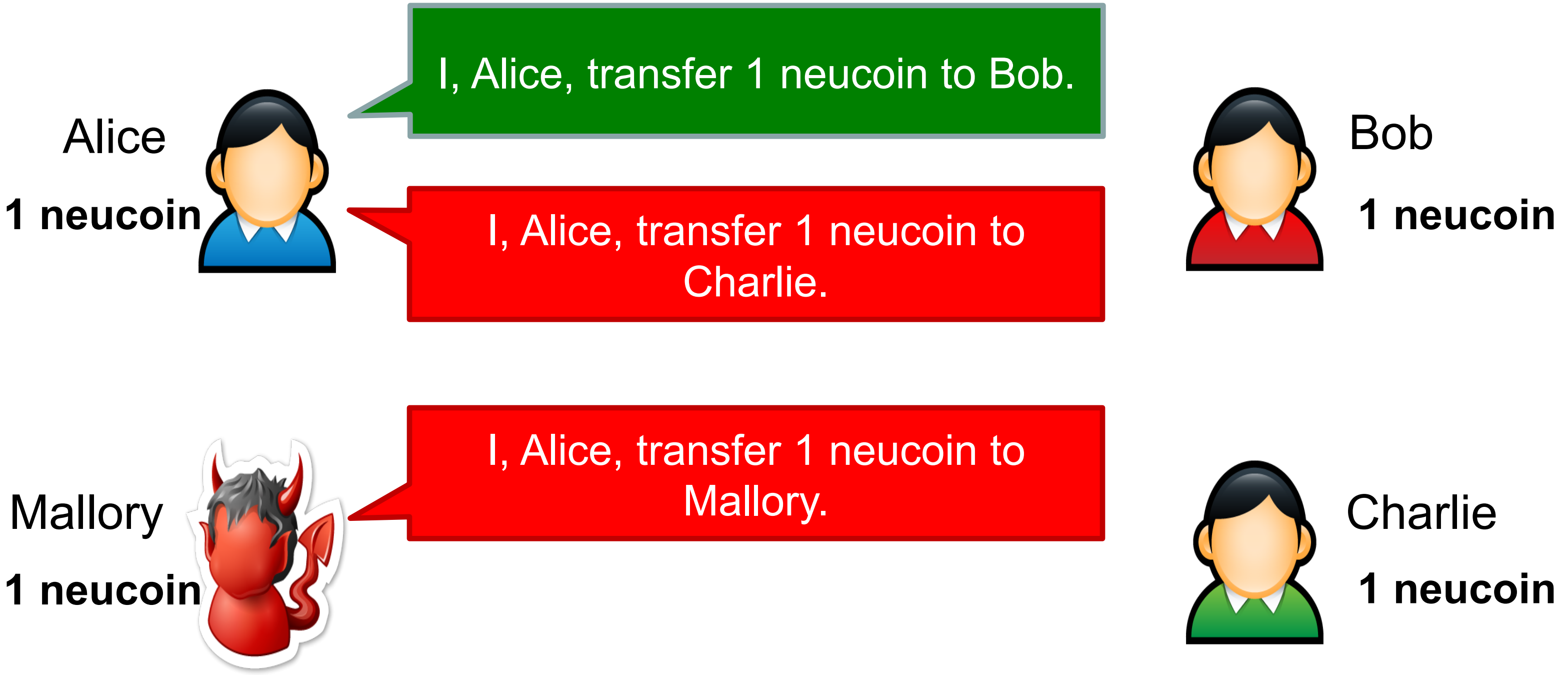
- Rest of lecture: build up design of Bitcoin
  - Let’s call our hypothetical currency *neucoin*

Requirements and Expectations

- No centralized control
  - Central banks, governments, police
- No "strong identities"
  - ID cards, passports
  - Ideally, we would like anonymity (like physical paper cash)
- Entirely electronic
  - Not backed by commodities

- Clear ownership of each neucoin
  - Cannot generate money you don't have
  - Cannot double spend
  - Cannot steal arbitrarily
  - No repudiation

Motivating Example



Alice

1 neucoin

I, Alice, transfer 1 neucoin to Bob.

I, Alice, transfer 1 neucoin to Charlie.

Bob

1 neucoin

Mallory

1 neucoin

I, Alice, transfer 1 neucoin to Mallory.

Charlie

1 neucoin

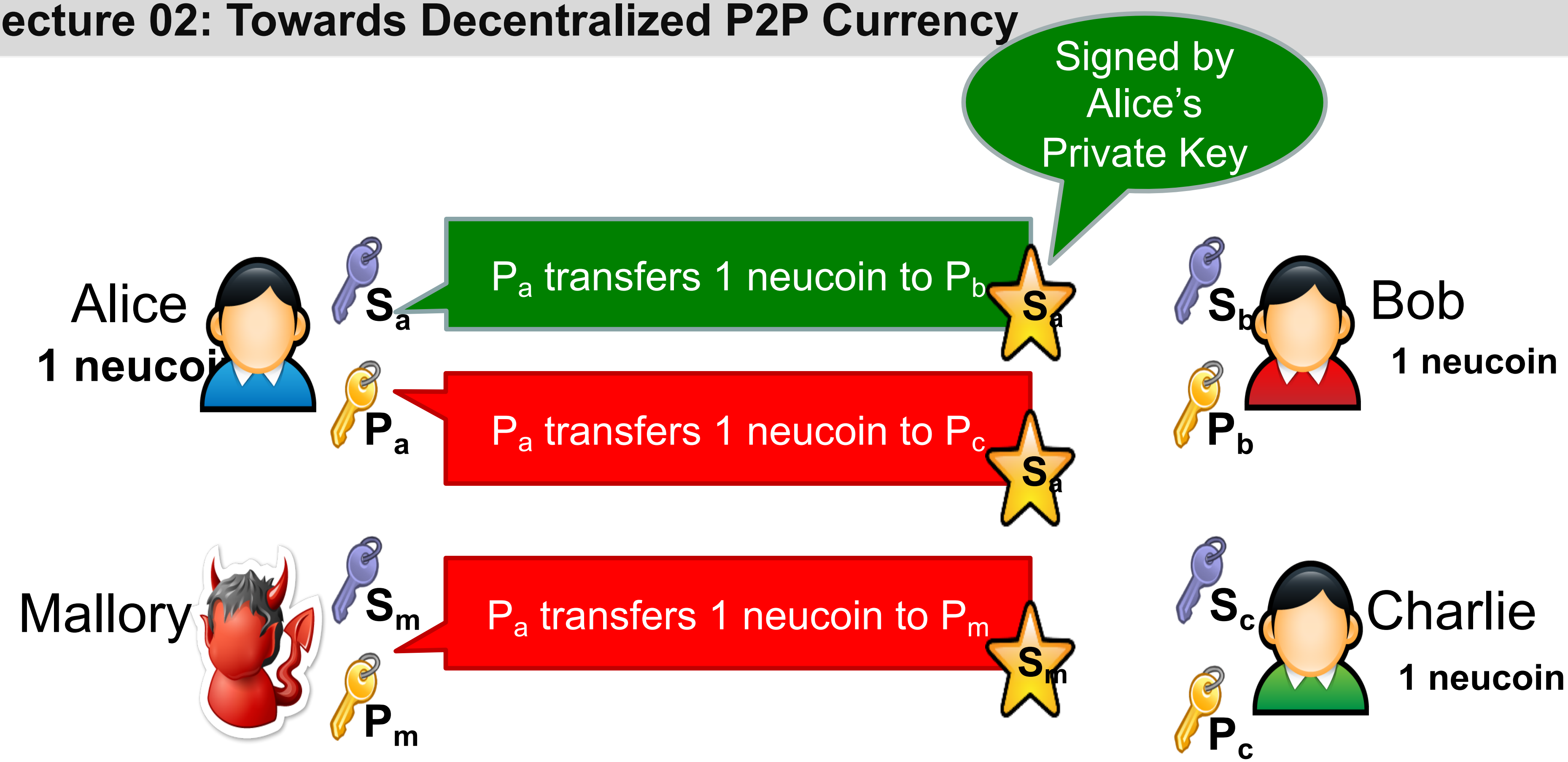
Can transactions be forged? Can neucoins be stolen?
Can users double spend?

Introducing Cryptography

Alice
S_a
P_a
S_b
P_b
Bob

- Each entity in neucoin is defined by a public/private keypair
  - Knowledge of private key gives ownership of neucoins
- Coins are transferred from one public key to another public key

Lecture 02: Towards Decentralized P2P Currency



Signed by Alice’s Private Key

Alice

1 neucoi

S_a

P_a

P_a transfers 1 neucoin to P_b S_a

P_a transfers 1 neucoin to P_c S_a

Mallory

S_m

P_m

P_a transfers 1 neucoin to P_m S_m

Bob

1 neucoin

S_b

P_b

Charlie

1 neucoin

S_c

P_c

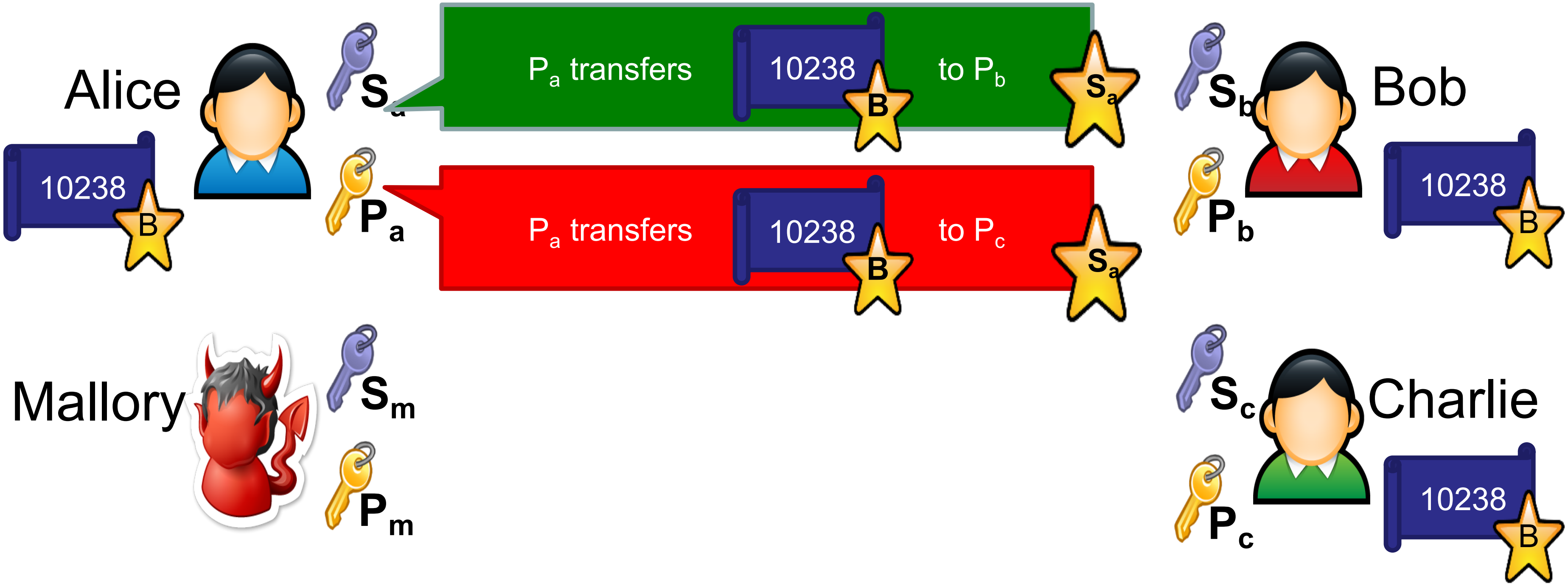
Can transactions be forged? Can neucoins be stolen?
Can users double spend?

Preventing Double Spending

- How do we prevent users from minting arbitrary neucoins?
- Add a trusted third-party that issues serial numbers
  - Also known as a bank
  - Let's assume bank is trusted, and has a well known public key

10238
B
26671
B
00392
B

Lecture 02: Towards Decentralized P2P Currency



Can transactions be forged? Can neucoins be stolen?

Can users double spend?

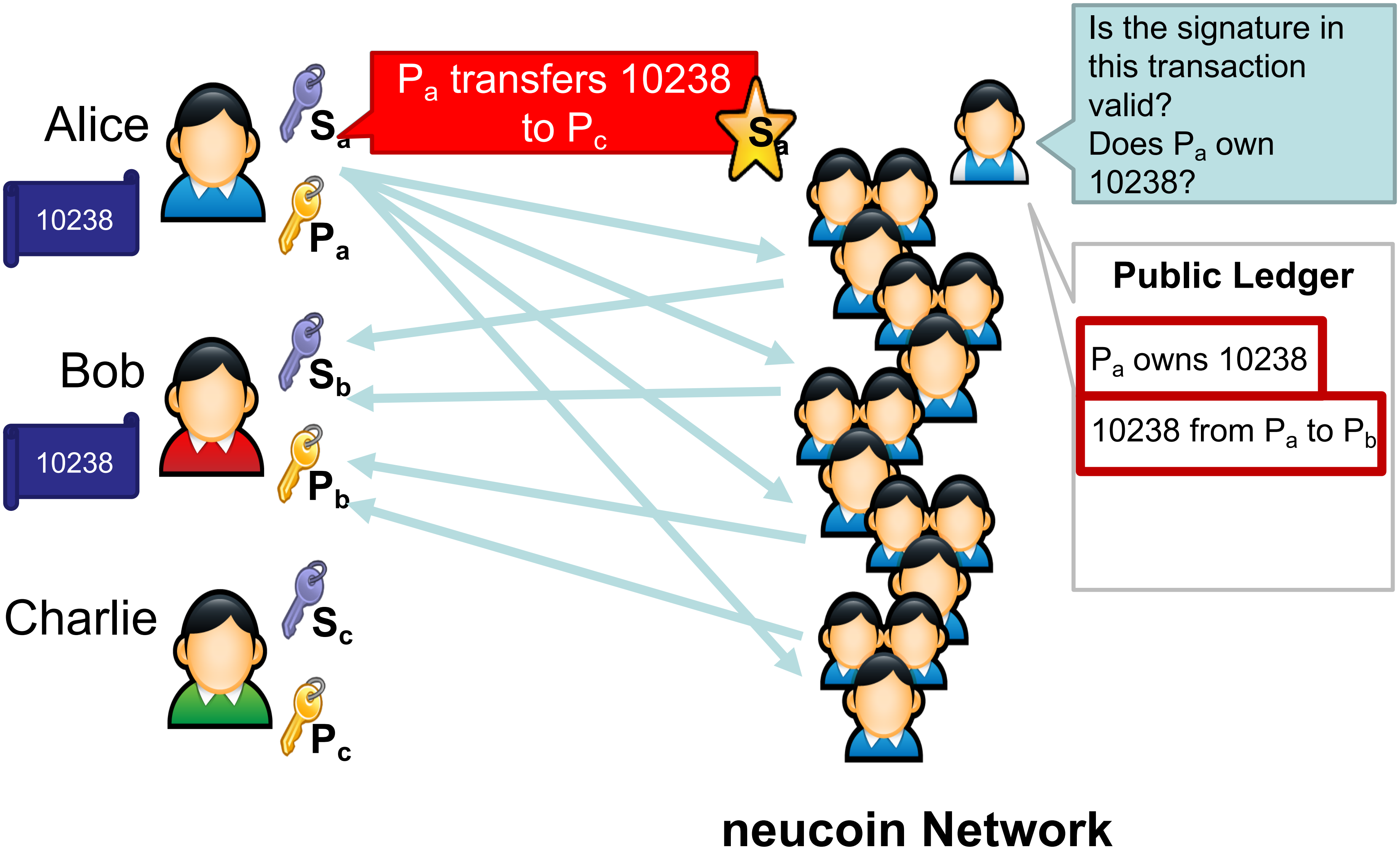
Preventing Double Spending

- What if the trusted bank also tracked who owns each neucoin?
  - Bank would have a ledger, serve as official record of ownership
  - Charlie can contact the bank, verify that Alice owns a given coin
- Problems?
  - Centralized ledger totally defeats the purpose of neucoin

Preventing Double Spending

- Instead, the network is the bank
  - Participants in neucoin collectively keep track of **all transactions**
  - Known as the public ledger
  - To verify that Alice isn’t double spending, Charlie can check the public ledger

Lecture 02: Towards Decentralized P2P Currency



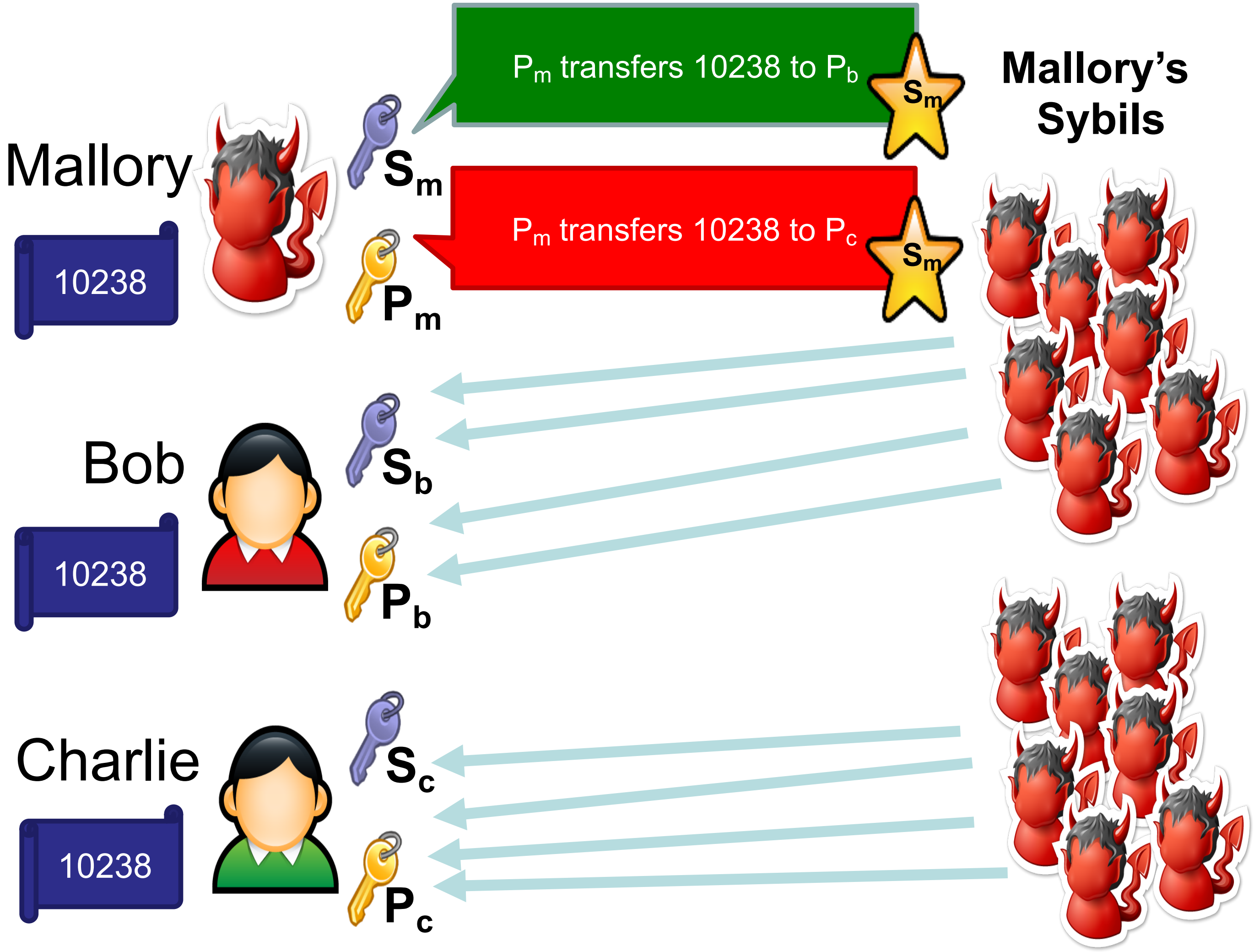
Bitcoin at a High-Level

- Bitcoin is a P2P network of nodes (Bitcoin clients)
  - Each node keeps a log (ledger) of all Bitcoin transactions, ever
  - This log is known as the blockchain
- Transactions are broadcast to nodes in the P2P network
  - Nodes validate transactions
    - Correct signatures and correct ownership of coins
  - Valid transactions are added to the blockchain and broadcast to other peers
  - Transaction is considered accepted once it appears in the blockchain
- Ultimate goal: all transactions are known and agreed upon by the network
  - In other words, we want global consensus of ordered events in log
  - Sound familiar?

Challenges

- There are numerous aspects to consider
- Let us consider following challenges for the time being
  - How to defend agains sybill attacks ?
  - What is the incentive for users to keep blockchain consistent ?

Sybil Attack



- Classic attack that all P2P systems are vulnerable to
- Mallory can introduce many fake nodes into the network
- N/2 respond to Bob, N/2 respond to Charlie
- Implication: one node = one vote doesn't work

Proof-of-Work

- Need to tie voting to a resource that is hard to obtain
  - In the past, we would have used a commodity (e.g. gold)
  - Identity (e.g. passports) would work, but defeats the purpose

- Key idea: tie voting to control of **computational resources**
  - To add a transaction to the ledger, you must present a proof-of-work
  - Proof-of-work can be generated by solving a cryptopuzzle

Proof-of-Work

- Why is this a good idea?
  - Cryptopuzzles prove that a node expended significant effort
  - Obviates the need for Sybil prevention
    - E.g. one machine pretending to be 100 Sybils doesn’t magically get 100x CPU power

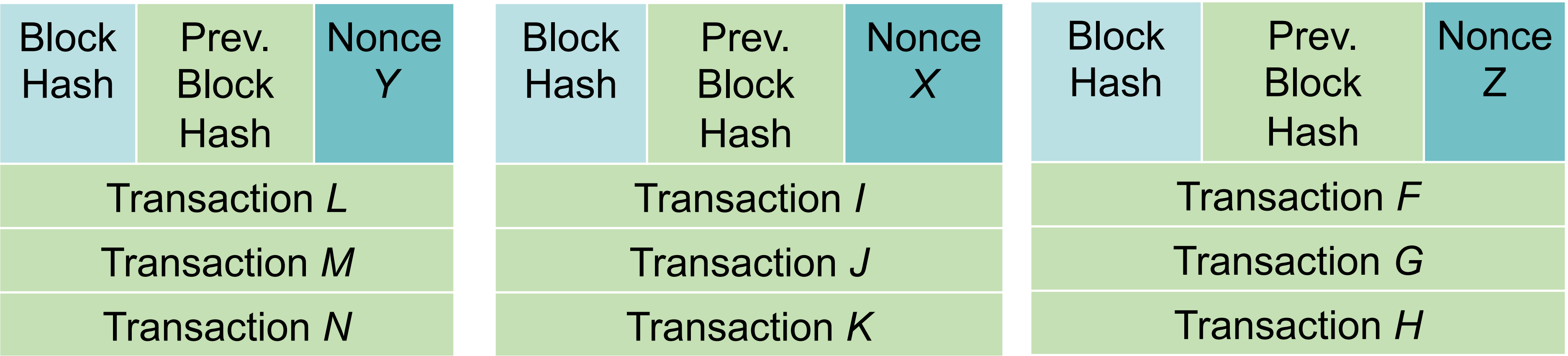
Proof-of-work in Bitcoin

- Key idea: a node can only add an entry to the blockchain if it solves a cryptopuzzle
  - Other nodes can easily validate new blocks to ensure the puzzle has been solved
  - Changes “one node/one vote” to “one CPU/one vote”
    - To dominate the network, Mallory must control significant CPU resources

Proof-of-work in Bitcoin

- Implementing proof-of-work in Bitcoin
  - Nodes receive transactions, group them into blocks
  - Nodes attempt to solve a cryptopuzzle based on the **previous block** and the **new block**
    - Blocks are linked, hence the name blockchain

Mining Blocks



Block Hash | Prev. Block Hash | Nonce *Y*

Transaction *L*

Transaction *M*

Transaction *N*

Block Hash | Prev. Block Hash | Nonce *X*

Transaction *I*

Transaction *J*

Transaction *K*

Block Hash | Prev. Block Hash | Nonce *Z*

Transaction *F*

Transaction *G*

Transaction *H*

- Block hash = Hash(Prev Block Hash | Nonce X | <Transactions>)
- Nonce *X* is the number chosen to make the *block hash* < *target*
  - Changing the nonce changes the output of the hash function unpredictably
  - All nodes are competing to identify a nonce that solves the puzzle
- Creation of new blocks is known as mining

Building the Blockchain

- At any given time, all nodes are searching for the next block
  - Searching == trying different nonces to solve the puzzle
  - Hoping to get lucky, identify nonce *X* such that *block hash* < *target*
- Once a node discovers a block, it broadcasts it to other peers
  - Other nodes validate (easy, simply recompute the hash)
  - Nodes begin working on the next block (with the new block as Prev)

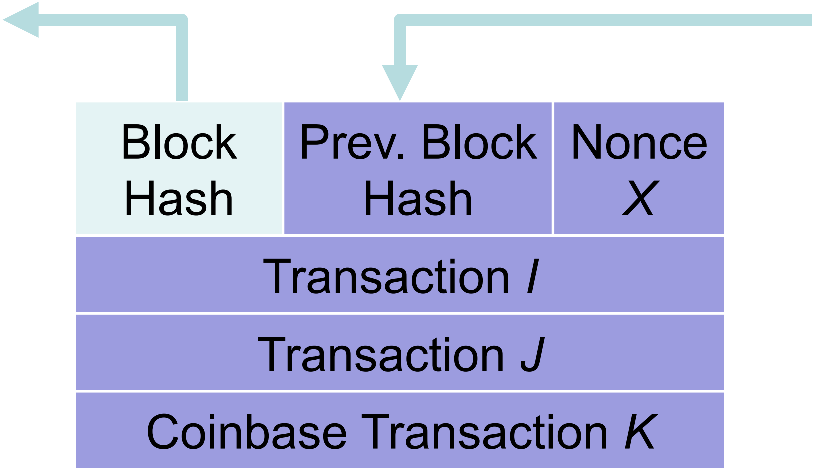
Incentive for Miners

- What is the incentive for users to act as Bitcoin nodes?
  - Computing hashes is CPU intensive
  - Bandwidth of communication with peers and users
  - Storage cost of storing the entire blockchain

Creation of New Coins

- Bitcoin solves the incentive problem in two ways
  - Transactions may include a transaction fee
    - Paid to whoever “wins” first, i.e. mines a block that includes the transaction
  - New blocks mint new coins
    - Node who wins “mines” a fixed amount of coins as a prize
      - This is why it’s called mining
    - Current reward is 12 BTC
    - Called a coinbase transaction

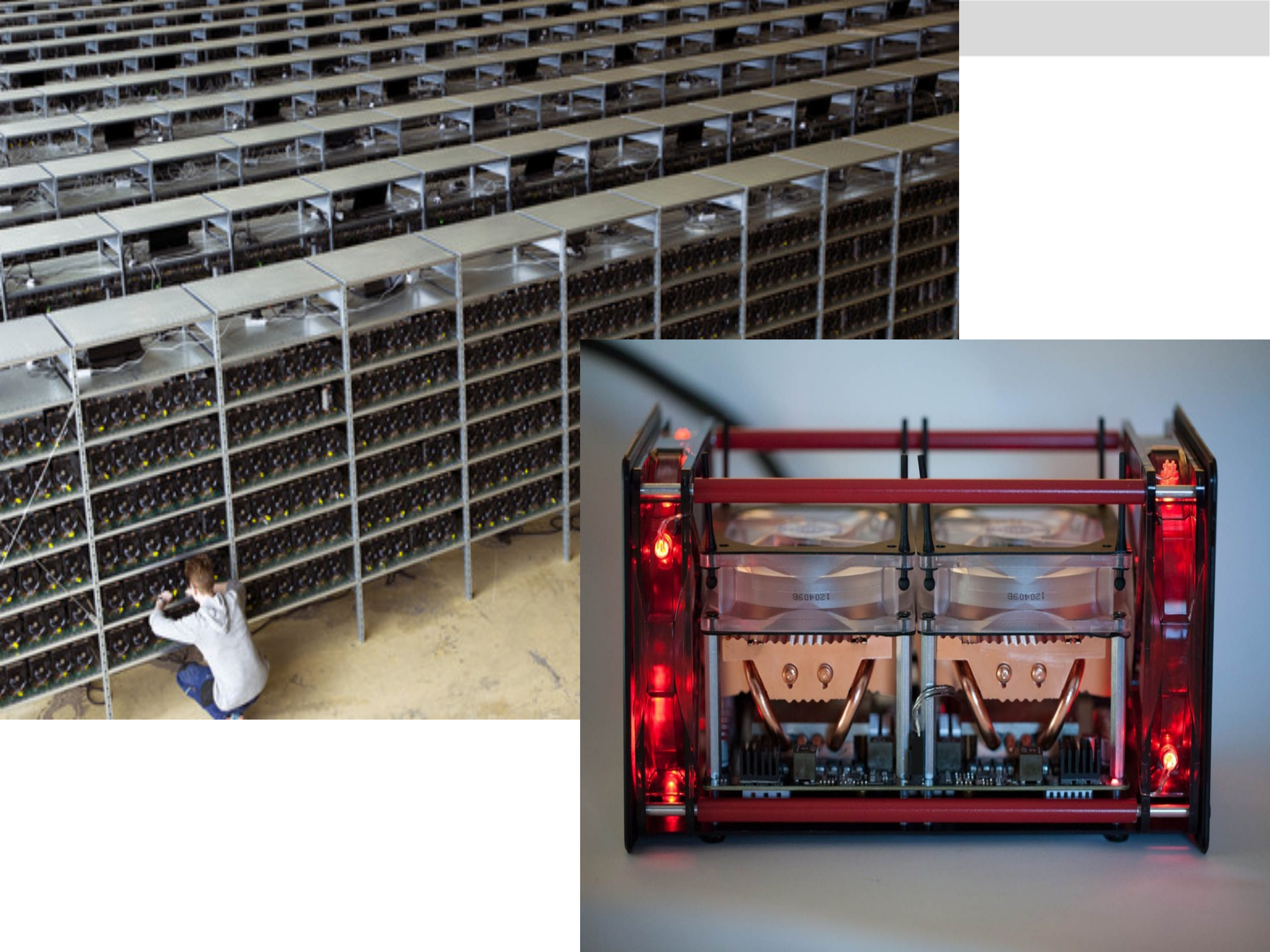
Coinbase Transactions



- Elegantly solves several problems
  - How are bitcoins minted?
  - Who gets newly minted coins?
- Reward for mining halves every 210,000 blocks
  - Currently 12 BTC, was 50 BTC until 2012, 25 until 2016
  - Will become 0 in year 2140; 21 million total bitcoins
  - At this point, only transaction fees will incentivize miners

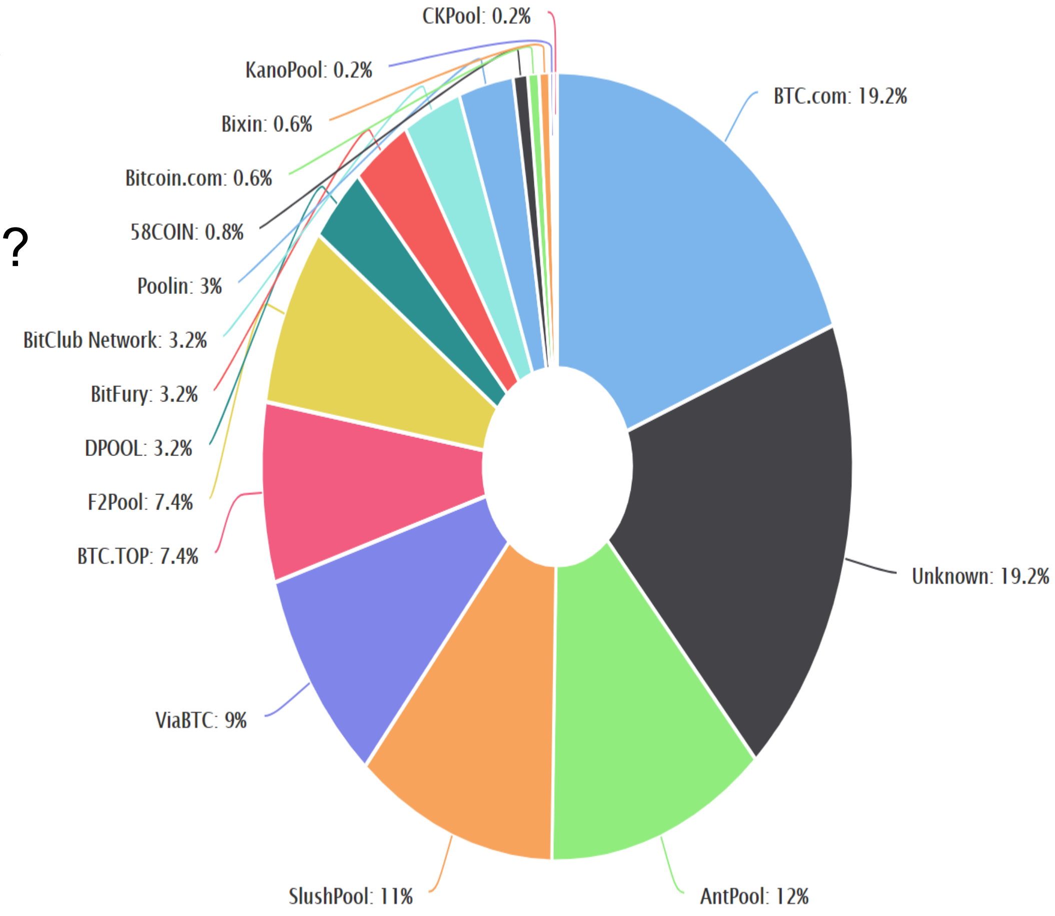
Mining

- In theory, anyone can download bitcoin and start mining
  - Your node will search for blocks
  - But in practice, you will *never win*
- Arms race: CPU < GPU < FPGA < ASICs
  - Real miners use thousands of chips custom designed to solve cryptopuzzles
  - Much faster and more power efficient than general purpose hardware
- Many miners operate in Iceland (cheap power and free cooling)



Mining Pools

- Problem: Bitcoin is a lottery
  - You are extremely unlikely to win
  - Can we make it more “fair”?
    - Nodes “get out” what they “put in”?
- Solution: mining pools
  - Groups of nodes that work together
  - Split proceeds when any node finds the next block (more fair)
- Lots of mining pools today
  - Instances of pools with >25% of total hash power have existed

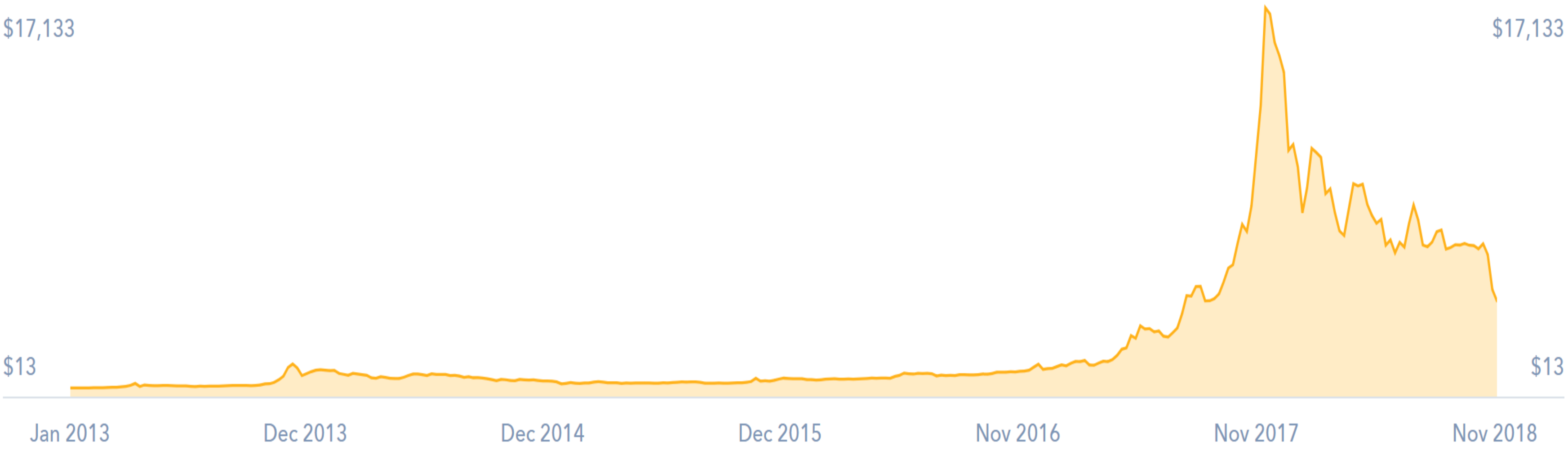


Is Bitcoin Secure?

- Can I fake a transaction? (i.e. steal your bitcoins)
  - No, you would need access to the victim's private key
- Can I edit the blockchain? (i.e. remove or modify old transactions)
  - No, all blocks are linked by their hashes
  - Changing historical block B_t would require changing all blocks *[*B_t*,* $B_{current}$*]*
- Can I repudiate a transaction? (i.e. deny that I paid you)
  - No, all of your transactions are signed by your private key
  - Plus, you can't go back and change previous blocks
- Can I mint money out of thin air?
  - Yes, but only through legitimately solving a cryptopuzzle (i.e. a coinbase txn)
  - All peers can validate that your block (and the minted coins) are correct

Lecture 02: Towards Decentralized P2P Currency

- BTC to USD exchange rate has been very volatile over time
  - All-time high: $17,133
  - Current: around $12000
- Several “bitcoin millionaires” exist
  - Mined a bunch of coins back in 2009



Altcoins

- P2P + cryptopuzzles + blockchain + incentives is a general formula
  - Can be applied to other distributed systems problems besides currency
  - Bitcoin is open-source
- Led to the creation of dozens of alternate coins
  - Litecoin – faster mining rate and scrypt instead of SHA-256 (harder to design ASICS)
  - Filecoin – designed for storing files in the blockchain
  - Namecoin – designed as a replacement for DNS
  - Etherium – distributed virtual machine + smart contracts

Quote of the day

- *He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.*

Chinese proverb

Do not distribute …

- These slides are not always prepared by me.
- Most of the content comes from the reference book
  - Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction
  - Arvind Narayanan, Joseph Bonneau,
  - Edward Felten, Andrew Miller, Steven Goldfeder

- This lecture however builds upon and uses slides from CS 3700 Networks and Distributed Systems
  - By David Choffnes available at https://david.choffnes.com/classes/cs3700fa17/