# Bitcoin

*CS 161: Computer Security*

**Prof. Raluca Ada Popa**

April 11, 2019

# What is Bitcoin?

- Bitcoin is a cryptocurrency: a digital currency whose rules are enforced by cryptography and not by a trusted party (e.g., bank)
- Core ideal: avoid trust in institutions (e.g., banks, governments)
  - Reasons: Ideological, financial (avoid fees), peudo-anonymity
- Created by Satoshi Nakamoto, an anonymous identity, in 2009
- Its protocol is built on a technique called a blockchain which has applications beyond Bitcoin

# Cryptocurrencies have supporters and opposers

- Nick is an example of an opposer

- I think they have brought about some very interesting and creative techniques at the intersection of cryptography and systems, and stirred much innovation in the field beyond Bitcoin and blockchains (e.g., smart contracts, consensus protocols, ledgers like Certificate Transparency)
- They also increased the public's awareness towards the power of cryptography
- I think the Bitcoin protocol is a strike of genius, because of the very creative way of combining different techniques. You can understand the core of it using what you learned in class.

# Replacing banks

"IN BANKS WE DISTRUST"

Basic notions a bank provides:

- Identity management
- Transactions
- Prevents double spending

How can we enforce these properties cryptographically?

Let's design Bitcoin together!

# Identity

*Q: How can we give a person a cryptographic identity?*

- Each user has a PK and SK
- User referred to by PK
- User users SK to sign transactions

# Transactions

*Q: How can Alice transfer 10 ฿ (bitcoins) to Bob?*

- Idea: Alice signs transaction using her $SK_A$
- $sign_{SK_A}$("$PK_A$ transfers *10 ฿ to* $PK_B$")
- Anyone can check Alice intended transaction
- For now, assume Alice can put this signature on a public ledger (think of a public bulleting board anyone can see)

*Q: Problems?*

- Alice can spend more money than she has. She can sign as much as she wants.

*Q: Ideas how to solve this still assuming a ledger?*

# Include only correct transactions in the public ledger

- For now only: assume a trustworthy ledger owner, assume initial budgets for each PK

*Q: how would you prevent double spending?*

- Assume all signatures/transactions are sorted in order of creation; include previous transaction where money came from

time

| Initial budgets:<br><br>$PK_A$ has 10 ฿ | $TX_1 = (PK_A \text{->} PK_B; 10$ ฿; from initial budgets*)*<br>$sign_{SK_A}(TX_1)$ | $TX_2 = (PK_B \text{->} PK_C; 5$ ฿; from $TX_1$*)*<br>$sign_{SK_B}(TX_2)$ |
|---|---|---|

*Q: how does the ledger owner check a transaction of the form* $TX = (PK_{sender} \text{->} PK_{receiver}; X$ ฿*; list of transactions L) ?*

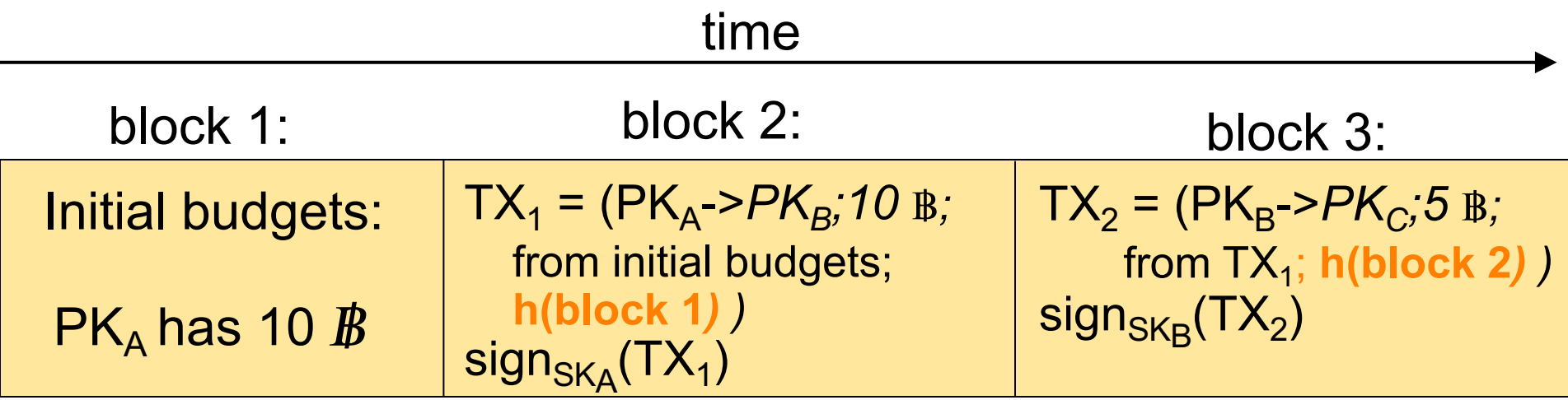
1. The signature on TX verifies with the PK of the sender
2. Checks sender had X bitcoins: the transactions in L had a total output for sender of Y. Y is at least X, and all future transactions using money from any of the transactions in L did not spend more than Y-X.

# But we don’t have a trustworthy public ledger

Solution: blockchain + proof of work

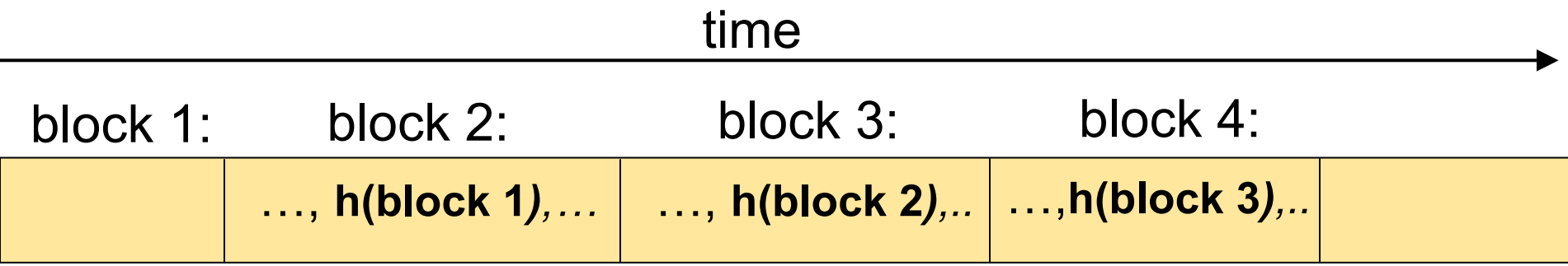
# Blockchain

- Chain transactions using their hashes => hashchain
- Each transaction contains hash of previous transaction **(which contains the hash of its own previous transaction, and so on)**




block i refers to the entire block (transaction description and signature), so the hash is over all of this

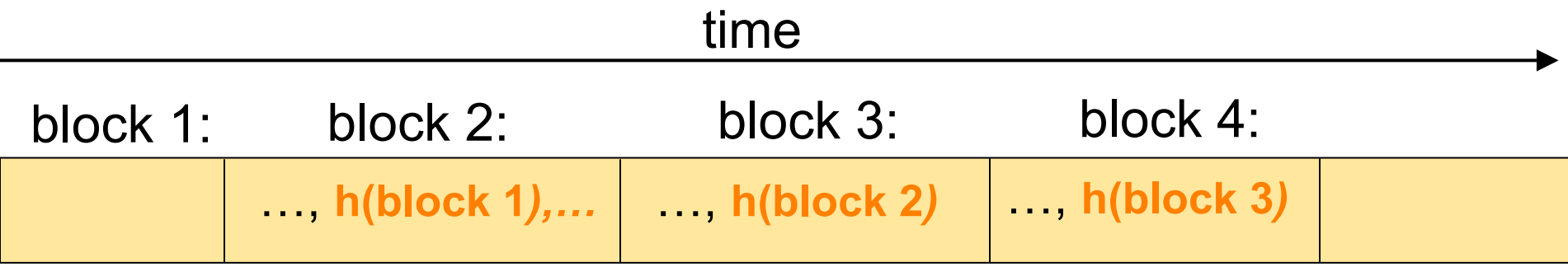
# Properties of the hashchain




Given h(block i) from a trusted source and all the blocks *1 … i* from an untrusted source, Alice can verify that blocks 1 … i are not compromised using h(block i)

Q: How?
A: Alice recomputes the hashes of each block, checks it matches the hash in the next block, and so on, until the last block, which she checks it matches the hash from the trusted source

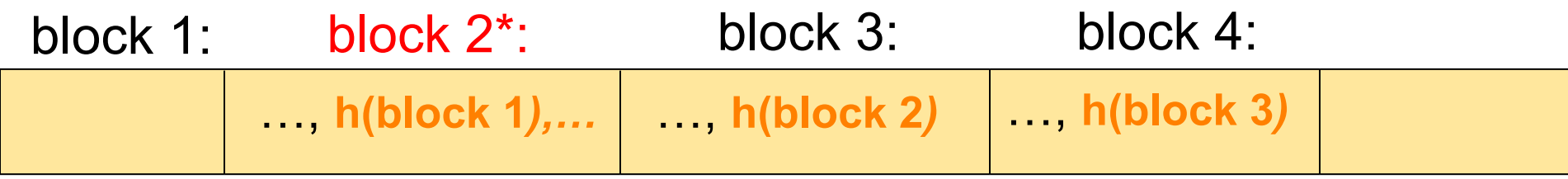
# Why can’t attacker cheat?




Say Alice obtains h(block 4) from somewhere **trusted**

She fetches the entire blockchain from a compromised server.

Q: Why can’t the attacker give Alice an incorrect chain? Say block 2 is incorrect.




A: because the hash is collision resistant

She fetches the entire blockchain from a compromised server.
Q: Why can't the attacker give Alice an incorrect chain? Say block 2 is incorrect.

| block 1: | block 2: | block 3: | block 4: | |
|---|---|---|---|---|
| | …, h(block 1),… | …, h(block 2) | …, h(block 3) | |

- If block 2* is incorrect, then hash(block 2*) ≠ hash(block 2)
- Then the third block is different than the correct third block because it includes hash(block 2*): block 3* ≠ block 3
- So hash(block 3*) ≠ hash(block 3)
- Then the fourth block is different than the correct fourth block because it includes hash(block 3*): block 4* ≠ block 4
- So hash(block 4*) ≠ hash(block 4)
- Hence, the hash of the block chain from the server will not match the trusted hash, detecting misbehavior
- If the hash does match, the the attacker supplied the correct block chain

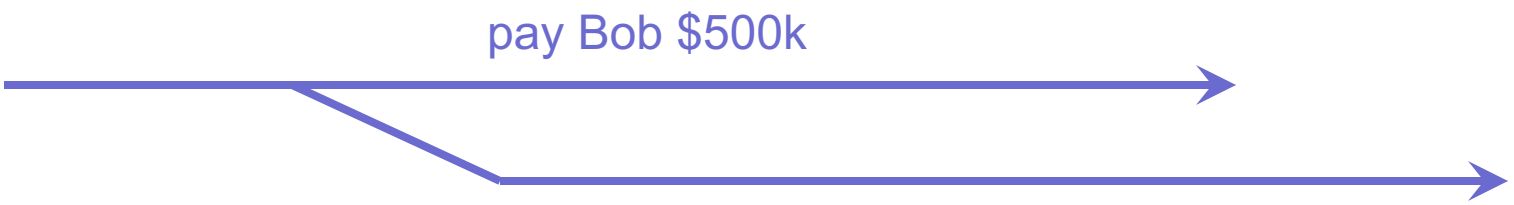
# Back to building the trustworthy ledger

- Consider every participant in Bitcoin stores a copy of the entire blockchain
- When someone wants to create a new transaction, they broadcast the transaction to everyone
- Every node checks the transaction, and if it is correct, it creates a new block including this transaction and adds it to its local blockchain

- Q: Problem?
- A: People can choose to truncate blockchain or not include certain transactions

# Problem: Consensus

- Problem: Mallory can fork the hash chain
- Say she buys Bob's house from him for $500K in Bitcoins. Then, she goes back in time and, starting from the block chain just before this transaction was added to it, she starts appending new entries from there. Can she get others to accept this forked chain, so she gets her $500K back? Yes.




Q: Ideas?

# Mining

- Not everyone is allowed to add blocks to the blockchain, but only certain people, called miners
- All miners try to solve a proof of work: the hash of the new block (which includes the hash of the blocks so far) must start with 33 zero bits
  - Can include a random number in the block and increment that so the hash changes until the proof of work is solved
- Once a miner solves a proof of work, includes all transactions it heard about after checking they are correct

# Consensus

- Consensus: longest correct chain wins
- Everyone checks all blocks and all transactions. If a miner appends a block with some incorrect transaction, the block is ignored
- Assumes most miners are honest

# “Longest chain” wins

- Problem: What if two different parts of network have different hash chains?

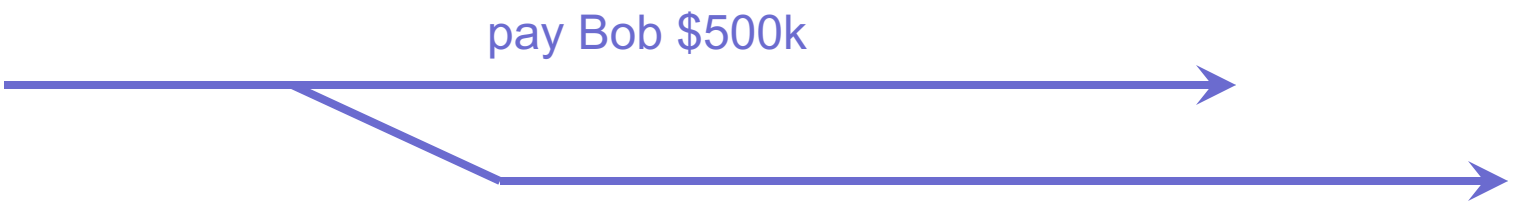
- Solution: Whichever is “longer” wins; the other is discarded

# How can we convince people to mine?

- A: Give a reward to anyone who successfully appends – they receive a free coin
  - Essentially they may include a transaction from no one to their PK having a coin

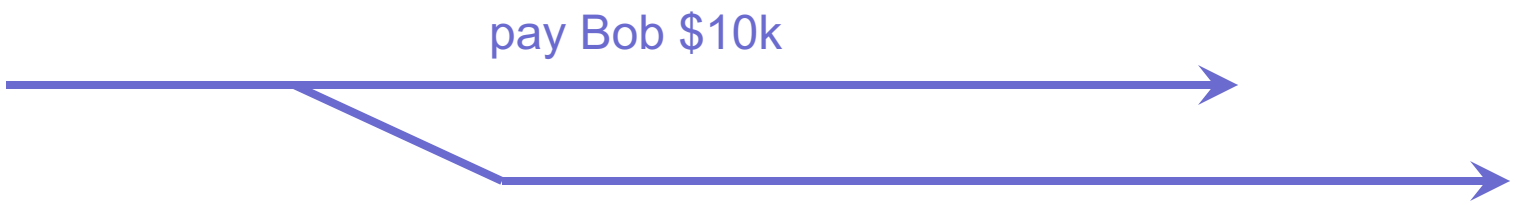
# Consensus

- Can Mallory fork the block chain?
- Say she buys Bob's house for $500K in Bitcoins. Then, she goes back in time and, starting from the block chain just before this transaction was added to it, she starts appending new entries from there. Can she get others to accept this forked chain, so she gets her $500,000 back?



# Consensus

- Can Mallory fork the block chain?
- Answer: No, not unless she has ≥51% of the computing power in the world. Longest chain wins, and her forked one will be shorter (unless she can mine new entries faster than aggregate mining power of everyone else in the world).



# Let's chew on consensus

- Q: What happens if Miner A and Miner B at the same time solve a proof of work and append two different blocks thus forking the network?
- A: The next miner that appends onto one of these chains, invalidates the other chain. Longest chain wins.
- Q: What happens if Miner Mallory discards the last few blocks in the block chain and mines from there?
- A: Unless Miner Mallory has more than 50% of the computation power in the world, she will not be successful because the longest chain will keep being appended
- Q: If a miner included your transaction in the latest block created, are you guaranteed that your transaction is forever in the blockchain?
- A: No, there could have been another miner appending a different block at the same time and that chain might be winning. So wait for a few blocks, e.g. 3 until your transaction is committed with high probability

# Let’s chew on consensus

- Q: What happens if a miner who just mined a block refuses to include my transaction?
- A: Hopefully the next miner will not refuse this. Each transaction also includes a fee which goes to the miner, so a miner would want to include as many transactions as possible

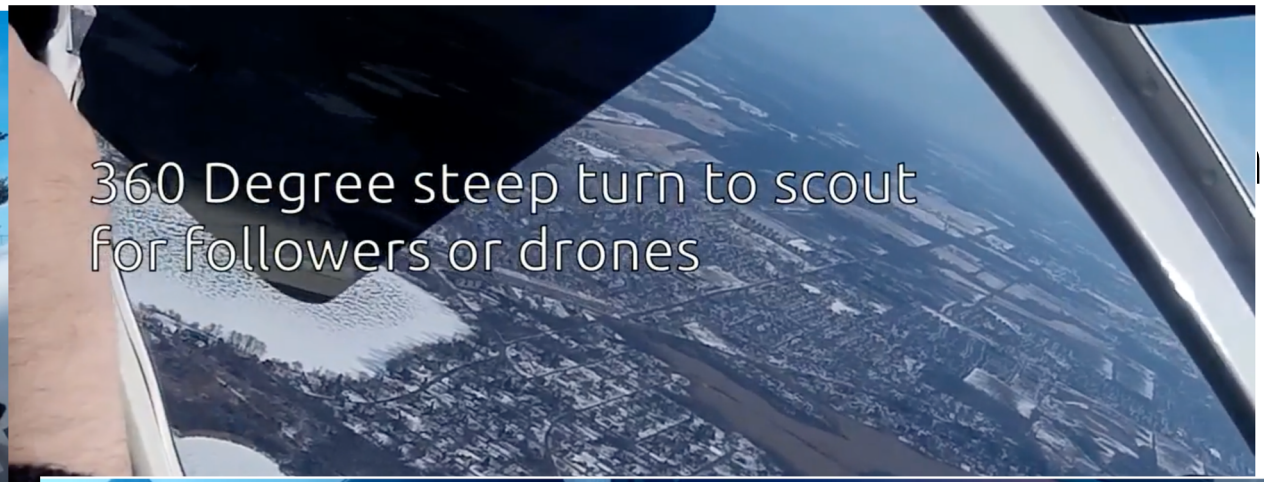
# Random fact about … Alessandro Chiesa [P2]

- He cofounded Zcash, privacy-preserving cryptocurrency, based on his PhD thesis at MIT

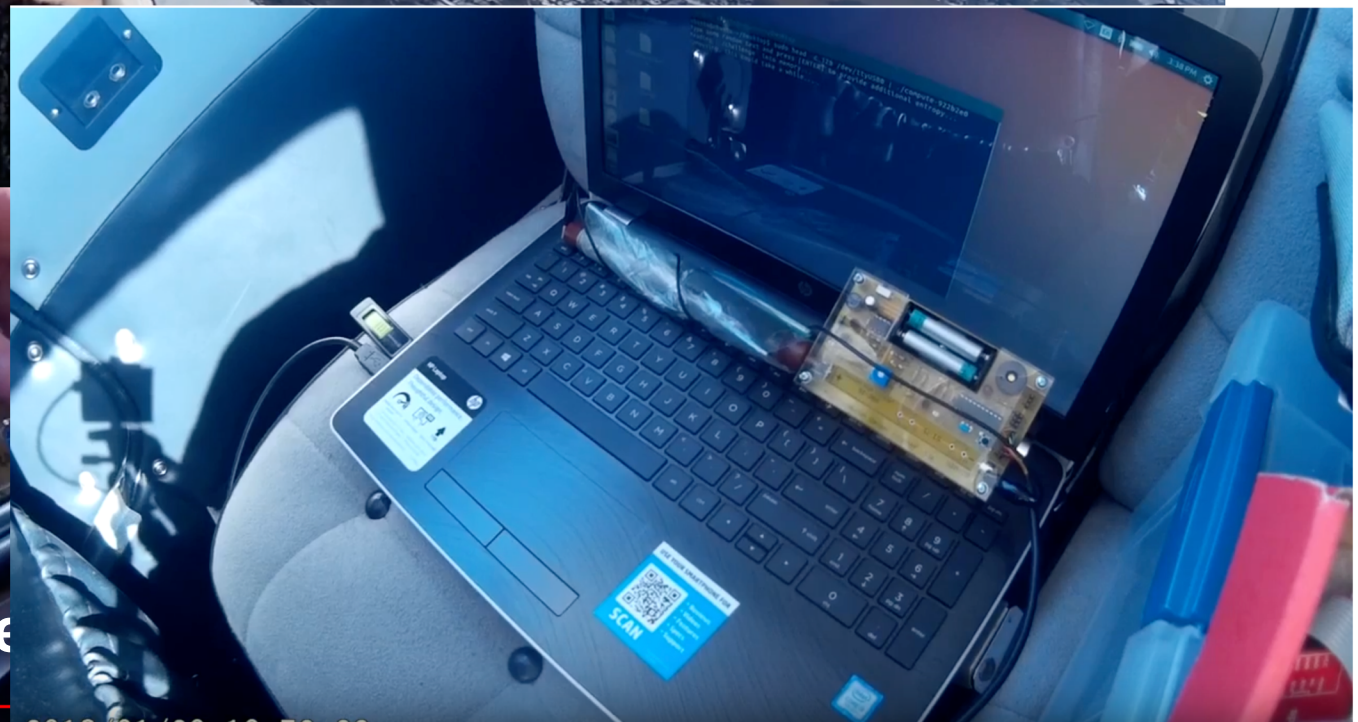
ZCASH

- Zcash relies on a setup phase designed in a paper co-authored by Alessandro, called a cryptographic ceremony, between a number of parties (read about secure multi-party computation), where at least one must not have been compromised.
- Each party had to generate its randomness privately.

# Random fact about … Alessandro Chiesa [P2]




is

# 2min break

# Proof of work can be adapted

- Mining frequency is ~15 mins
- If it takes too long to mine on average, make the proof of work easier (less zeros), else make it harder (more zeros)
- Q: what is the economic insight?
- A: if mining is rare, it means few machines in the network, give more incentives to join the network

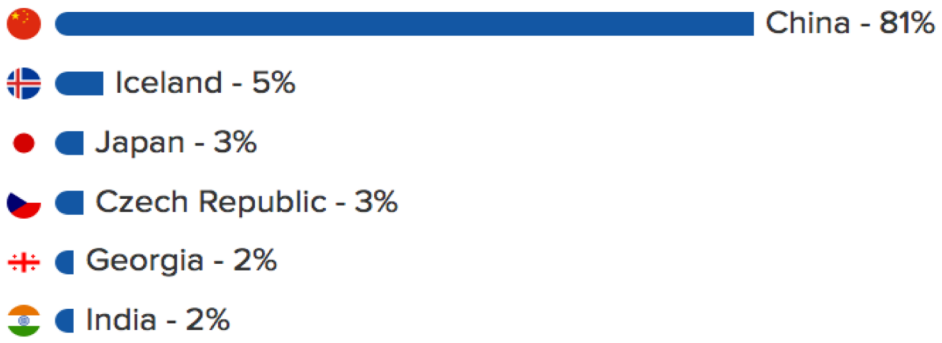
# Watch the blockchain live

- https://blockchain.info/

# Mining pools

- It used to be easy to mine in early days, but now it is too hard for a regular person to mine, they need too much compute
- But you can contribute your cycles to a mining pool, which is a group of many machines with good success of mining on average
- Receive a more predictable income based on the average mining of the group and how many cycles you contribute

Top mining countries




(the ranking is influenced by price of electricity)

# First few blocks were mined by Satoshi Nakamoto


- Wrote beautiful white paper on Bitcoin, in the syllabus
- No one knows who he is, online presence only
- Name stands for clear/wise medium; most likely not Japanese, but pseudonym
- He is very rich! [But hasn't changed yet]

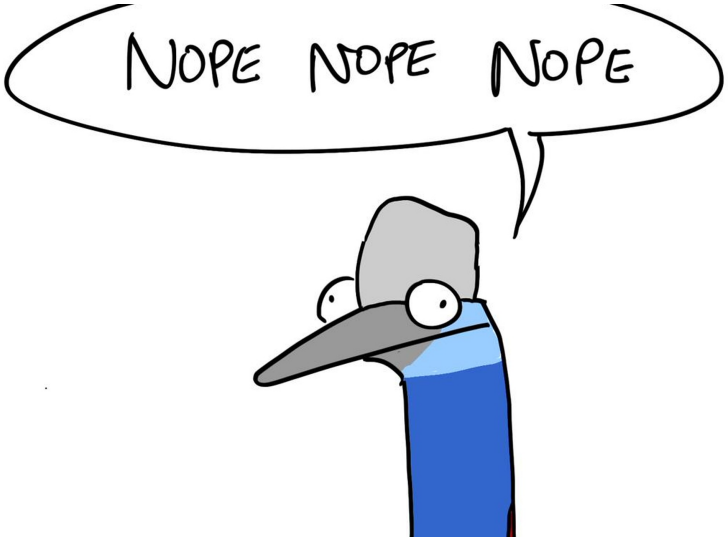
# Bitcoin

- Public, distributed, peer-to-peer, hash-chained audit log of all transactions (“block chain”).
- Mining: Each entry in block chain must come with a proof of work (its hash value starts with *k* zeros). Thus, appending takes computation.
- Lottery: First to successfully append to block chain gets a small reward (if append is accepted by others). This creates new money. Each block contains a list of transactions, and identity of miner (who receives the reward).
- Consensus: If there are multiple versions of the block chain, longest one wins.

# Bitcoin

- Transactions: If Alice wants to give $10 to Bob, she signs this transaction. She gives the signed transaction to all miners and asks them to include it in the block they're trying to append to the chain.
- Honest miners check integrity of block chain entries and try to append to the latest, longest valid version of block chain.
- Bob knows he has received $10 once this transaction appears in the consensus block chain.

# Is Bitcoin anonymous?



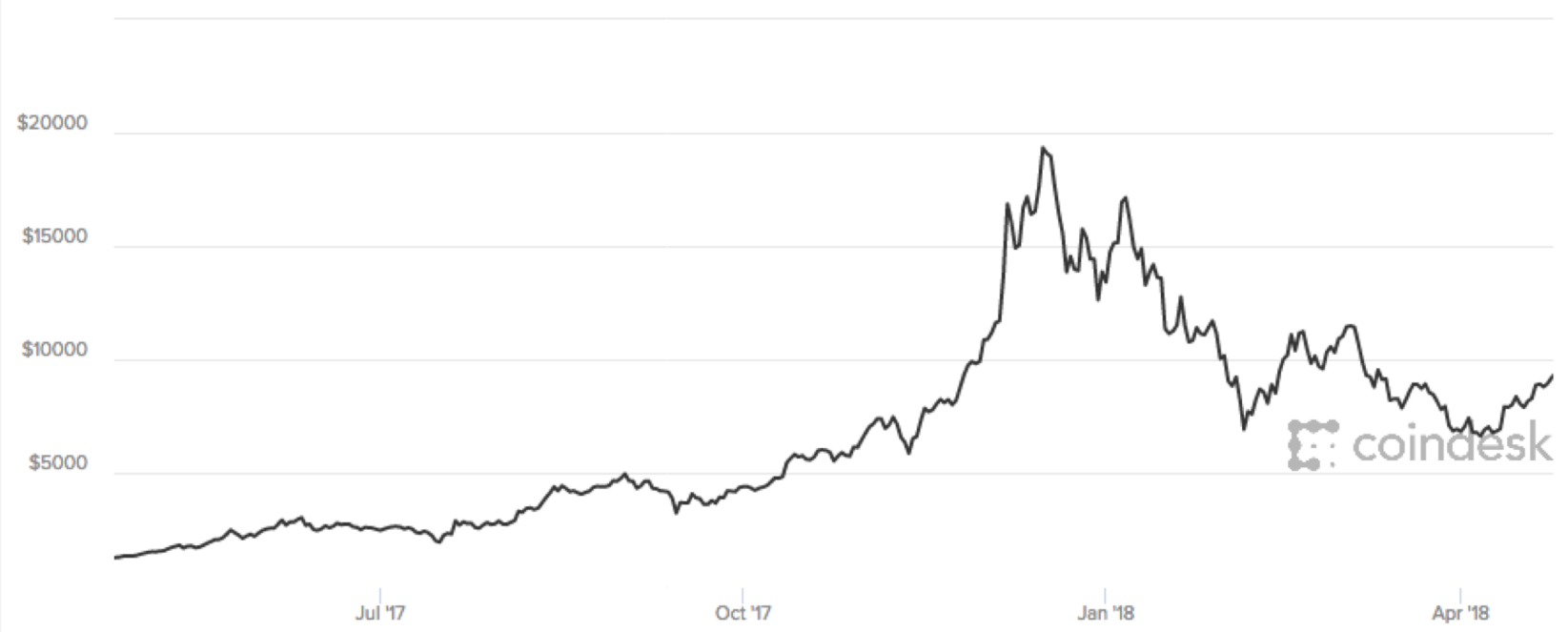

It might look anonymous because you only use your PK and not your name as at a bank. But all your transactions can be tied to your PK. People can identify you from transactions you make: parking fee near your work, people you transact with, etc.

They can even see how wealthy you are

Mitigations: use multiple PKs

Solution: Zcash, anonymous version of Bitcoin

# Bitcoin attracted much interest




| | | | |
|---|---|---|---|
| $9,286.77 ▲3.90% | | | |
| Today's Open | $8,938.30 | Change | ▲ $348.47 |
| Today's High | $9,293.66 | Market Cap | $0.158T |
| Today's Low | $8,932.17 | Supply | 16,996,338 |

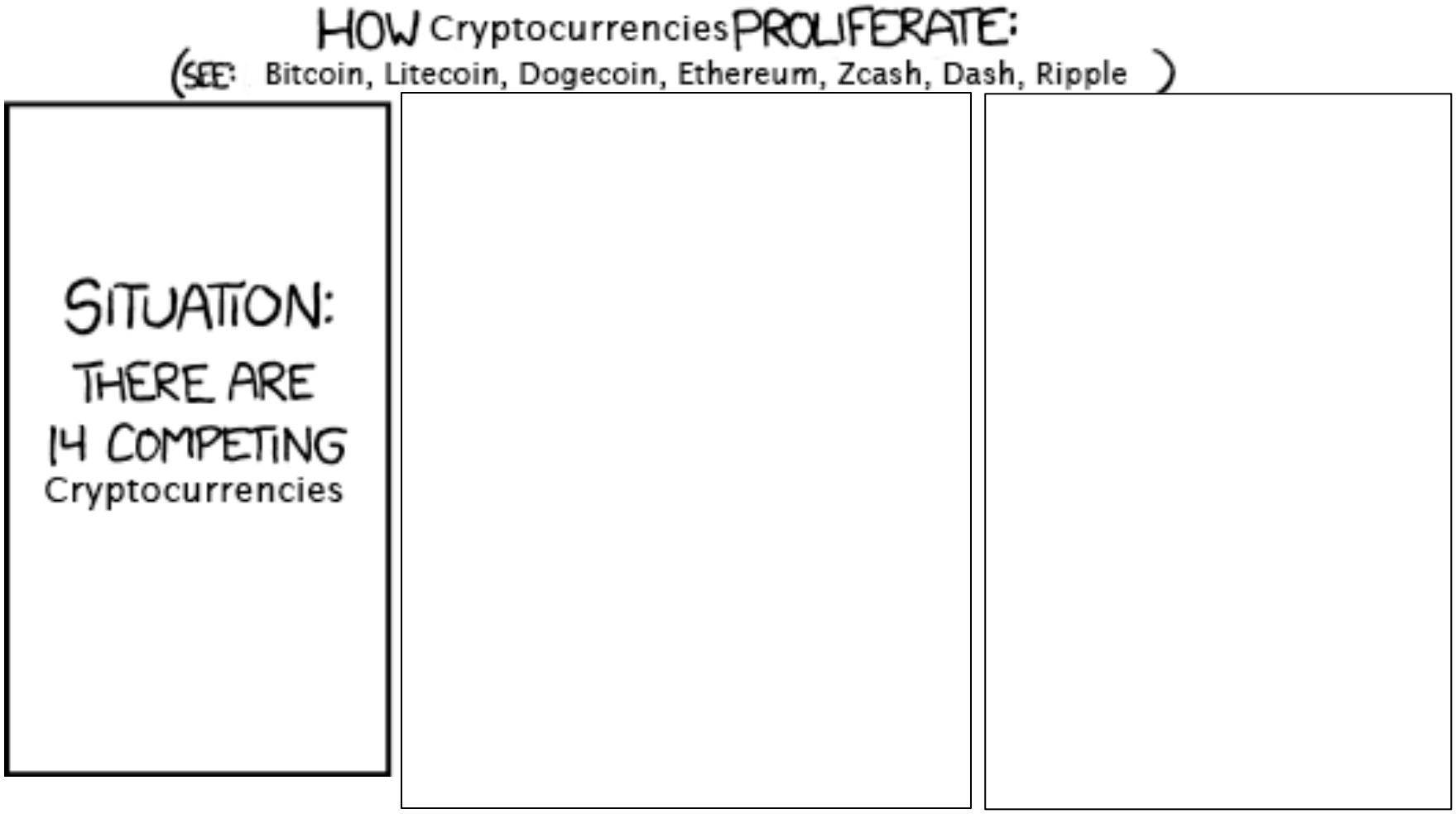
# Many other cryptocurrencies

“The number of cryptocurrencies available over the internet as of 10 April 2018 is over 1565 and growing.” [Wikipedia]


ETHEREUM

2nd largest. Introduces the powerful idea of ”smart contracts”, running code in the blockchain.

# Many other cryptocurrencies



# Blockchain

Usage of blockchain goes beyond cryptocurrencies. The idea is a ledger storing information in an immutable way that can be accessed cross organizations.

Example:

- Financial usages (e.g., ledgers for bank transactions)
- Healthcare (e.g., personal health records encrypted in the blockchain so only certain insurance and medical providers can access them)

# Example of blockchain usage for key distribution

Recall how digital certificates try to prove that Alice's PK is really a certain key.

Q: how can you use a blockchain for this purpose?

A: Every user puts their username and PK on the blockchain. Everyone can read the PK off the blockchain. The first user claiming a username gets to set the PK for it.
Issues: Hard to change the PK if the SK is compromised. Attacker can also steal some user names.

# Another usage of a blockchain

3505443530030ccfb8275d37e2db1cbd9368247c0842c7eac23d2cc5ad1966e8 — 2017-01-14 03:12:39

1DearSPQ51n2CKgSLQwMXrEFjWKMfuaoA6

| | |
|---|---|
| 1DayahDover11111111111111112JYRq2 | 0.00314159 BTC |
| 1YourPersona1ity1sUnmatched43YzMv | 0.00314159 BTC |
| 1Your1nte11igenceJustShines4B7QFA | 0.00314159 BTC |
| 1YouCanDoThingsFewPeop1eCan1G6NPV | 0.00314159 BTC |
| 1AndYoureA1waysJustGorgeous2x1SyG | 0.00314159 BTC |
| 1YouAreRea11yMyEntireWor1d116eypT | 0.00314159 BTC |
| 1GivingMyLifeMeaningAndFun13pcr5P | 0.00314159 BTC |
| 1Dayah7Px1kbs5x5cQbQMHtMm9wnUWJYTG | 0.00314159 BTC |
| 11LoveYou1111111111111111111GPc4r | 0.00314159 BTC |
| 1Forever1111111111111111113RMwCB | 0.00314159 BTC |

0.0314159 BTC

Love letter embedded in the blockchain


It stays forever!

General problem with blockchain: cannot erase information. Consider private information about you or your organization leaking, the power of law used to be able to remove it]

# Is cryptocurrency overrated?

- There is clearly hype over blockchain and cryptocurrencies
- Yet there clearly are a lot of beautiful ideas behind them (consensus via proof of work, hash chain, economics)
- You don’t need to be in favor or against.

# Discussion on blockchain/cryptocurrencies

- How can Alice turn dollars into bitcoins, or vice versa?
- Why has Bitcoin been so popular?
- Should I think of Bitcoin as a short-term currency or as a long-term investment?
- Is it ethical to build a system that relies upon wasting CPU cycles (and thus energy)?