# Bitcoin – part 2

*CS 161: Computer Security*

**Prof. Raluca Ada Popa**

April 29, 2020

# Announcements

- Started recording
- TA Nick on chat
- Project 3 part 2 is released and will be due on **May 3 at 11:59 pm**

# Two components

1. **Ledger:**
   1. publicly-visible,
   2. append-only, and
   3. immutable,

   log
2. **Cryptographic transactions**

   Recall:
   - Someone's cryptographic ID is PK (SK enables them to prove ownership of PK)
   - Transaction has signature from sender
   - Anyone can verify a transaction entirely based on the transaction content and the history of transactions so far

# Two components

1. **Ledger:**
    1. publicly-visible,
    2. append-only, and
    3. immutable,

    log
2. **Cryptographic transactions**

# Bitcoin's ledger

1. Hash chain / blockchain

2. Consensus via 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)**
- **Last hash essentially contains entire history**

time

| block 1: | block 2: | block 3: |
|---|---|---|
| Initial budgets:<br><br>$PK_A$ has 10 Ƀ | $TX_1$ = ($PK_A$->*$PK_B$;10 Ƀ;*<br>from initial budgets;<br>**h(block 1)** )<br>$sign_{SK_A}(TX_1)$ | $TX_2$ = ($PK_B$->*$PK_C$;5 Ƀ;*<br>$PK_B$->*$PK_B$;5 Ƀ;*<br>from $TX_1$; **h(block 2)** )<br>$sign_{SK_B}(TX_2)$ |

Given the last hash from a trusted source, one can verify the correctness of the entire history from an untrusted source

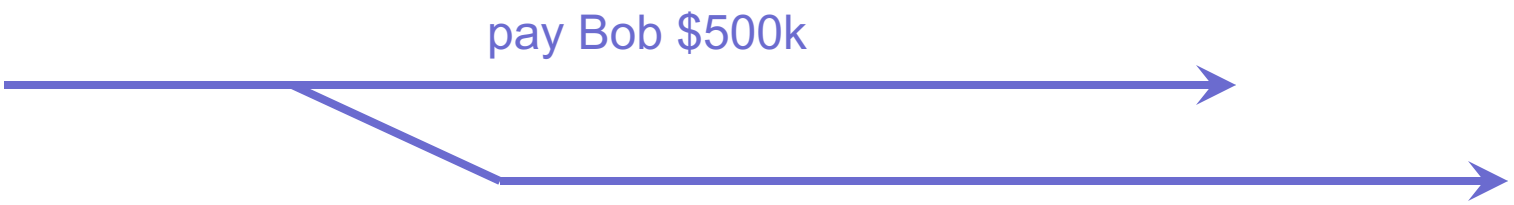
# Recall In Bitcoin:

- Every participant stores the whole blockchain
- There is no central party storing it
- 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

- Some participants can be malicious
- The majority are assumed to be honest

# Problem: fork attack, double spending

- 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.



# How do users agree on the same history?

Consensus via proof of work

# Bitcoin's ledger

1. Hash chain / blockchain

2. Consensus via proof of work

# Proof of work / Mining

- Not everyone is allowed to add blocks to the blockchain, but only certain people, called miners
- An honest miner will include all transactions it hears about after checking them
- 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 N (e.g. 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
    - Eg: Hash(block || random_number) = 000…0000453a48b244
- Currently someone in the world solves the proof of work every 10-20mins

# Propagating blocks

- Miners broadcast blocks with proof of work
- All (honest) Bitcoin nodes listen for such blocks, check the blocks for correctness, and accept the longest correct chain
- If a miner appends a block with some incorrect transaction, the block is ignored

# Consensus: longest correct chain wins

- Everyone will always prefer the longer correct chain

# Example

- An honest miner M1 stores current blockchain: b1->b2->b3
- M1 hears about transactions T
- M1 tries to mine for block b4 to include T
- Another miner M2 mines first b4 and broadcasts b4, with b3->b4
- M1 checks b4, accepts b4, and starts mining for block 5

# Example (cont'd)

- M1 now has blockchain

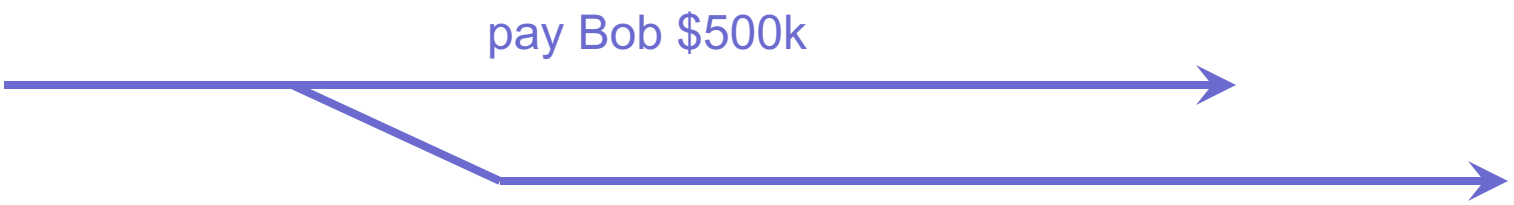
  b1->b2->b3->b4
- M1 hears that some miners are broadcasting b1->b2->b3->b4'->b5'
- M1 checks this new chain, and then accepts this new chain, essentially discarding b4

# Assumption

- Assumes more than half of the computing power is in the hands of honest miners
- So honest miners will always have an advantage to mine the longest chain

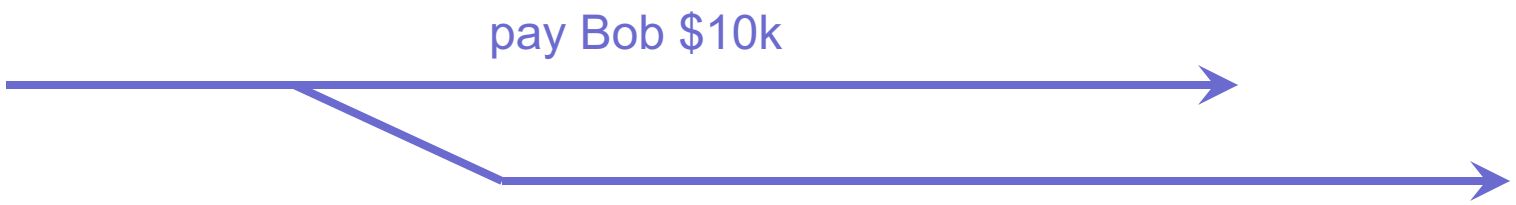
# Consensus

- 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).



# “Longest chain” wins

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

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

# 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

# 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

- Q: What happens to a miner's reward if his block was removed because an alternate longer chain appears?
- A: The miner lost their reward. Only the transactions and rewards on the longest chain "exist".

# 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: 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, though you can never be sure.

# 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

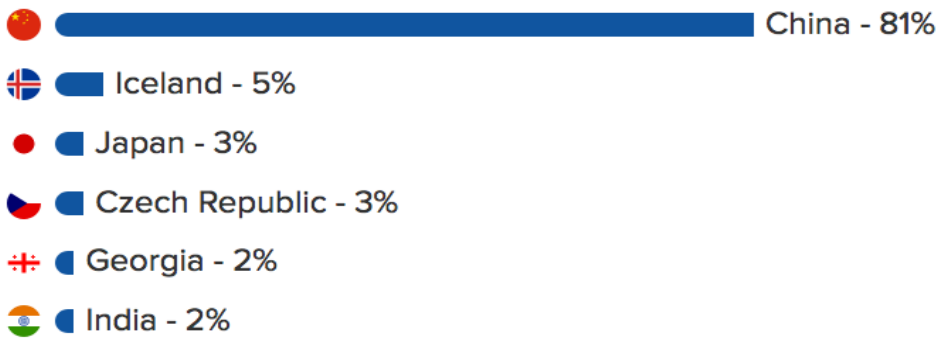
# Watch the blockchain live

- https://blockchain.info/

# Mining pools

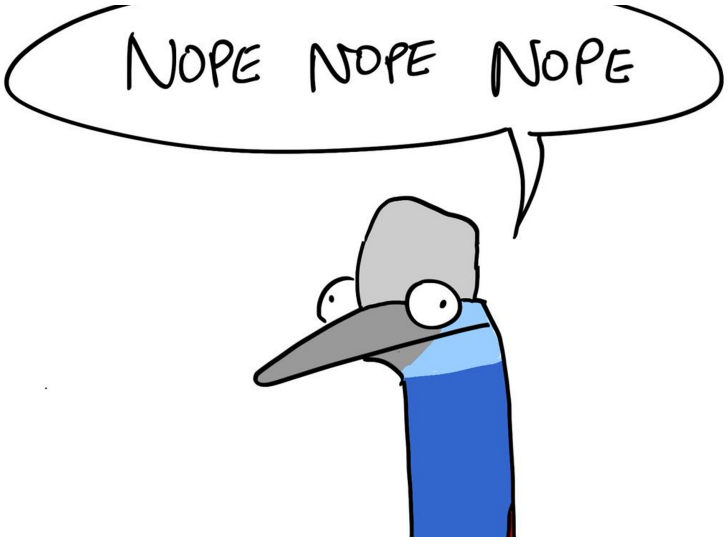
- It used to be easy to mine in early days, but now it is too hard for a regular person to mine, they need too much compute
- But you can contribute your cycles to a mining pool, which is a group of many machines with good success of mining on average
- Receive a more predictable income based on the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

Top mining countries




(the ranking is influenced by price of electricity)

# Is Bitcoin anonymous?



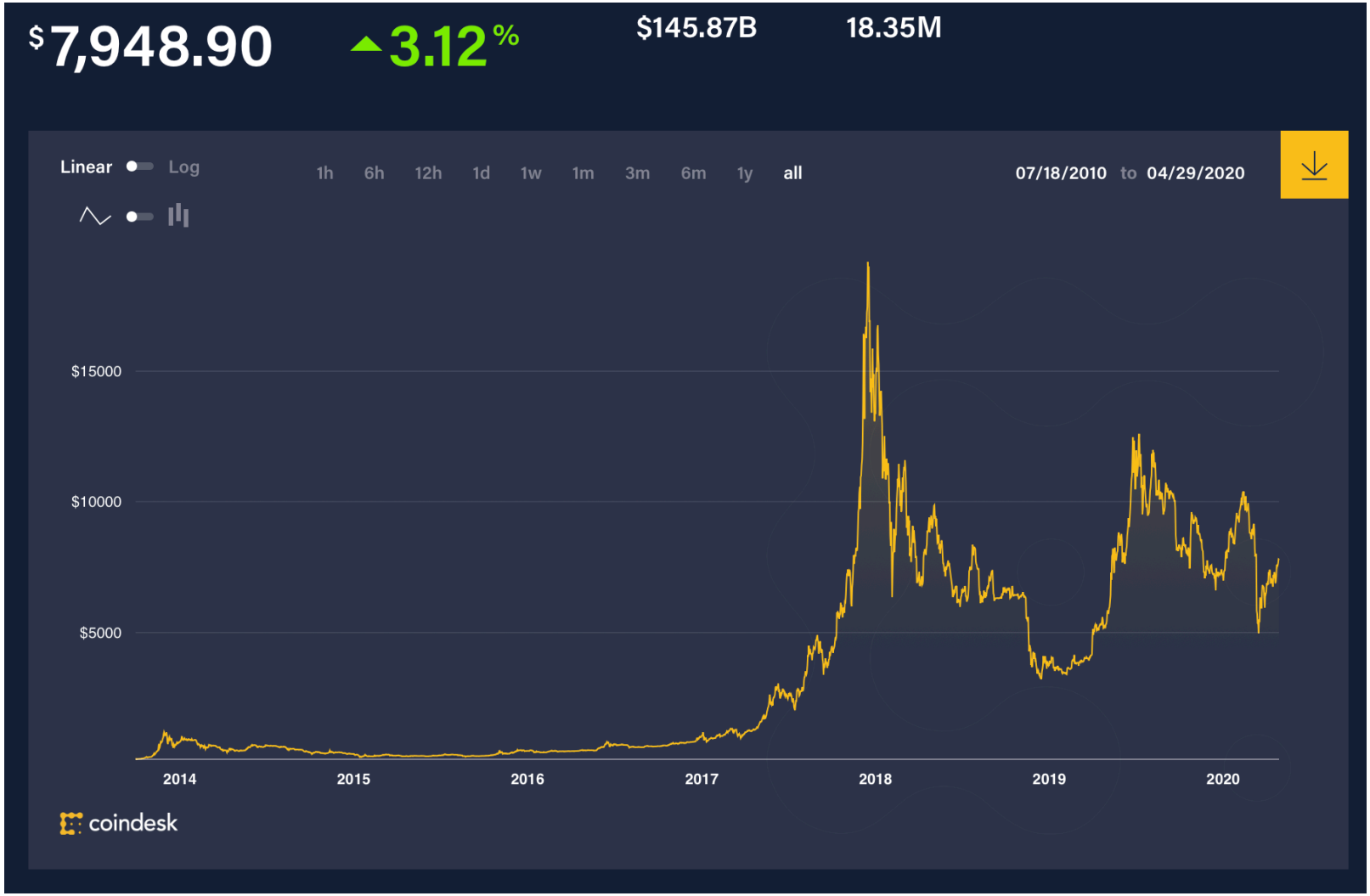

It might look anonymous because you only use your PK and not your name as at a bank. But all your transactions can be tied to your PK. People can identify you from transactions you make: parking fee near your work, people you transact with, etc.

They can even see how wealthy you are

Mitigations: use multiple PKs

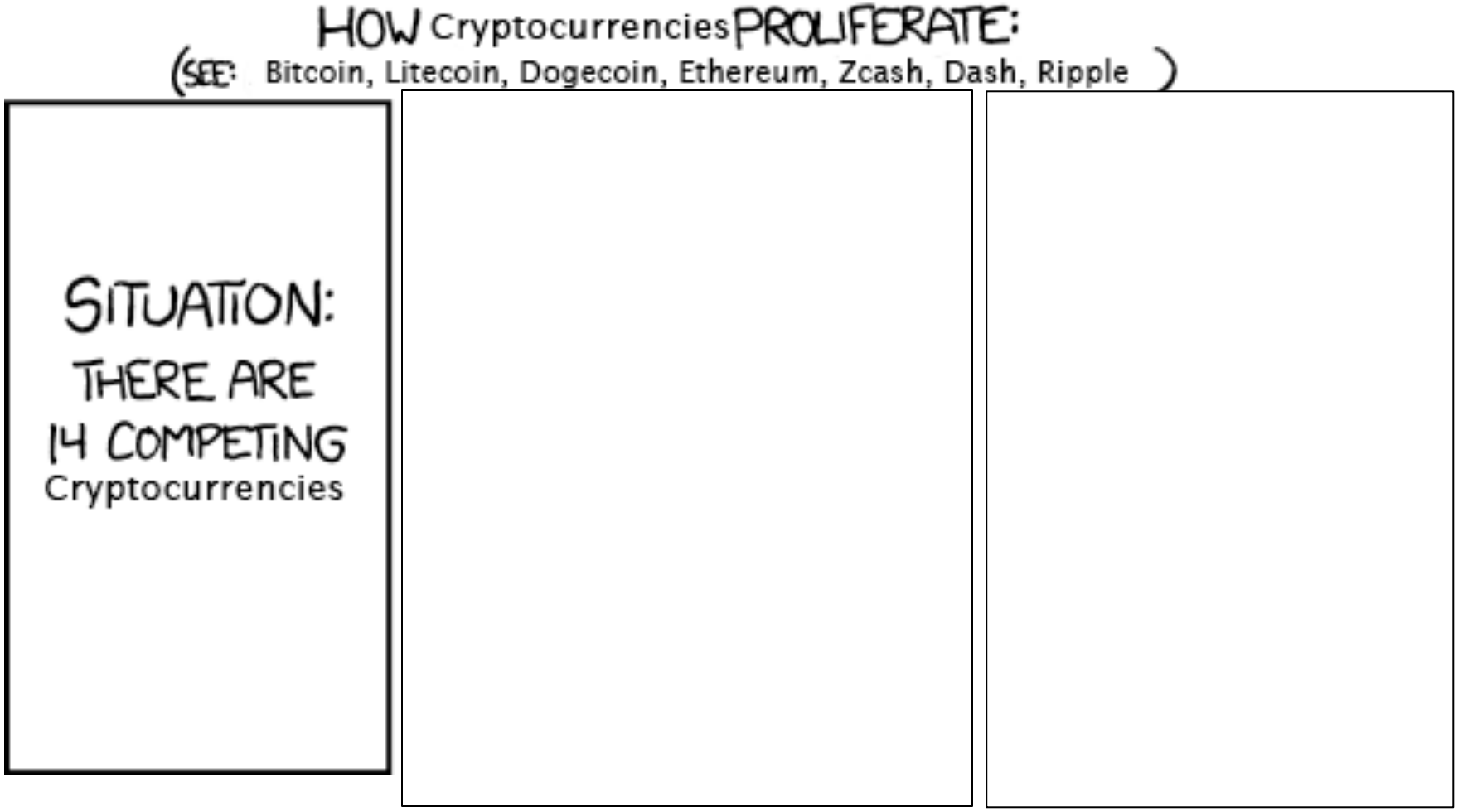
Solution: Zcash, anonymous version of Bitcoin

# Value fluctuations



# Many other cryptocurrencies

“The number of cryptocurrencies available over the internet as of 19 August 2018 is over 1600 and growing.” [Wikipedia]


HOW Cryptocurrencies PROLIFERATE:
(SEE: Bitcoin, Litecoin, Dogecoin, Ethereum, Zcash, Dash, Ripple )
SITUATION:
THERE ARE
14 COMPETING
Cryptocurrencies

# Blockchain

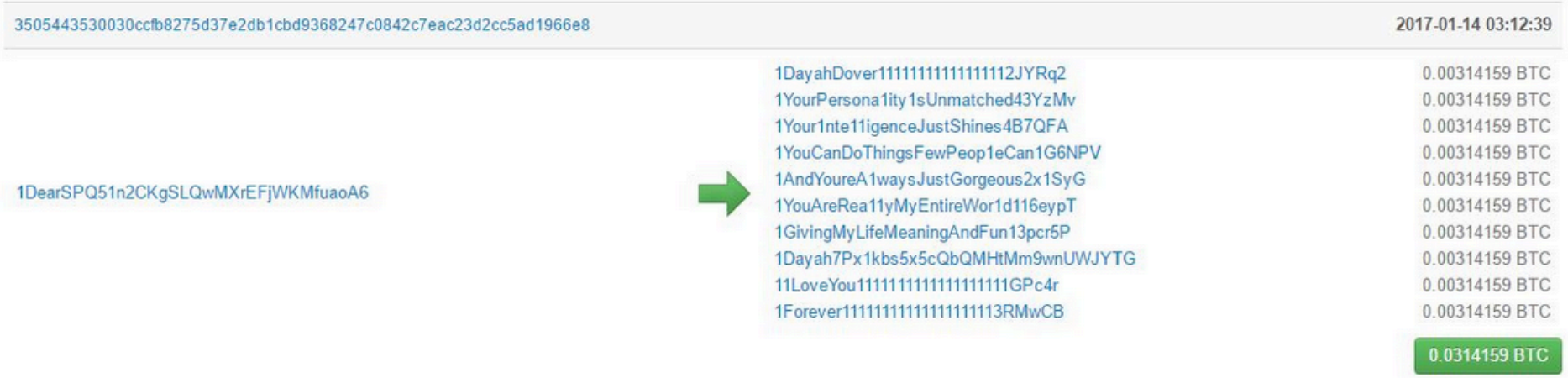
Usage of blockchain goes beyond cryptocurrencies. The idea is a ledger storing information in an immutable way that can be accessed cross organizations.

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)
- Key distribution
- **Certificate Transparency**

next time!

# Another usage of a blockchain




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

# 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 *N* 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.