

E-Payment Systems and Cryptocurrency Technologies Spring Semester, 2021

<https://course.ie.cuhk.edu.hk/~ftec4004>

Prof. Wing C. Lau

wclau@ie.cuhk.edu.hk

<http://www.ie.cuhk.edu.hk/~wclau>

Introduction to Bitcoin and Blockchain

Acknowledgements

- The slides used in this lecture are mostly adapted from the following sources. The copyrights and contribution of the original authors are hereby acknowledged and recognized:
 - ◆ Sherman S.M. Chow, IERG5590 Advanced Blockchain, CUHK, 2020.
 - ◆ Foteini Baldimtsi, CS795 Blockchain Technologies, George Mason University, 2017, http://www.baldimtsi.com/teaching/cs795_sp17
 - ◆ Stefan Dziembowski, University of Warsaw, <https://www.crypto.edu.pl/dziembowski-talks>
 - ◆ ©2016 by Stefan Dziembowski. Permission to make digital or hard copies of part or all of this material is currently granted without fee *provided that copies are made only for personal or classroom use, are not distributed for profit or commercial advantage, and that new copies bear this notice and the full citation.*

Outline

- How does Bitcoin work ?
- How to use a Blockchain to record Bitcoin transactions ?
- How to prevent “double-spending” of electronic money ?
- How to reconcile among different views of the state of a blockchain ?
- Other mechanisms for maintaining a distributed ledger

Why blockchain Technologies?

Blockchain technology: the future of the banking sector

11 January, 2017

01/12/2016 10:17  Leer en [Español](#)

A survey by Euromoney reveals that the idea that blockc
media imposition, but a reality accepted in the sector.

Share this content:      

The importance of the blockchain: The second generation of the internet



By *Nick Hammond*

The Blockchain Matters More Than The President

By [The Foundation for Economic Education](#) · on January 19, 2017 2:35 pm · in [Politics](#)

Why blockchain Technologies?

Blockchain technology of the banking

01/12/2016 10:17 [Leer en Español](#)

A survey by Euromoney reveals that blockchain is still a media imposition, but a reality accepted by the industry.

Share this content: [Twitter](#) [Facebook](#) [LinkedIn](#) [Pinterest](#)

Report: Blockchain Technology Market to Reach \$7.7 Billion by 2024

Jan 20, 2017 6:10 PM EST by Jessie Willms



Blockchain is the
second
of the internet

The Blockchain Matters More Than The President

By [The Foundation for Economic Education](#) · on January 19, 2017 2:35 pm · in [Politics](#)

All Payment Technologies we have covered so far in the course

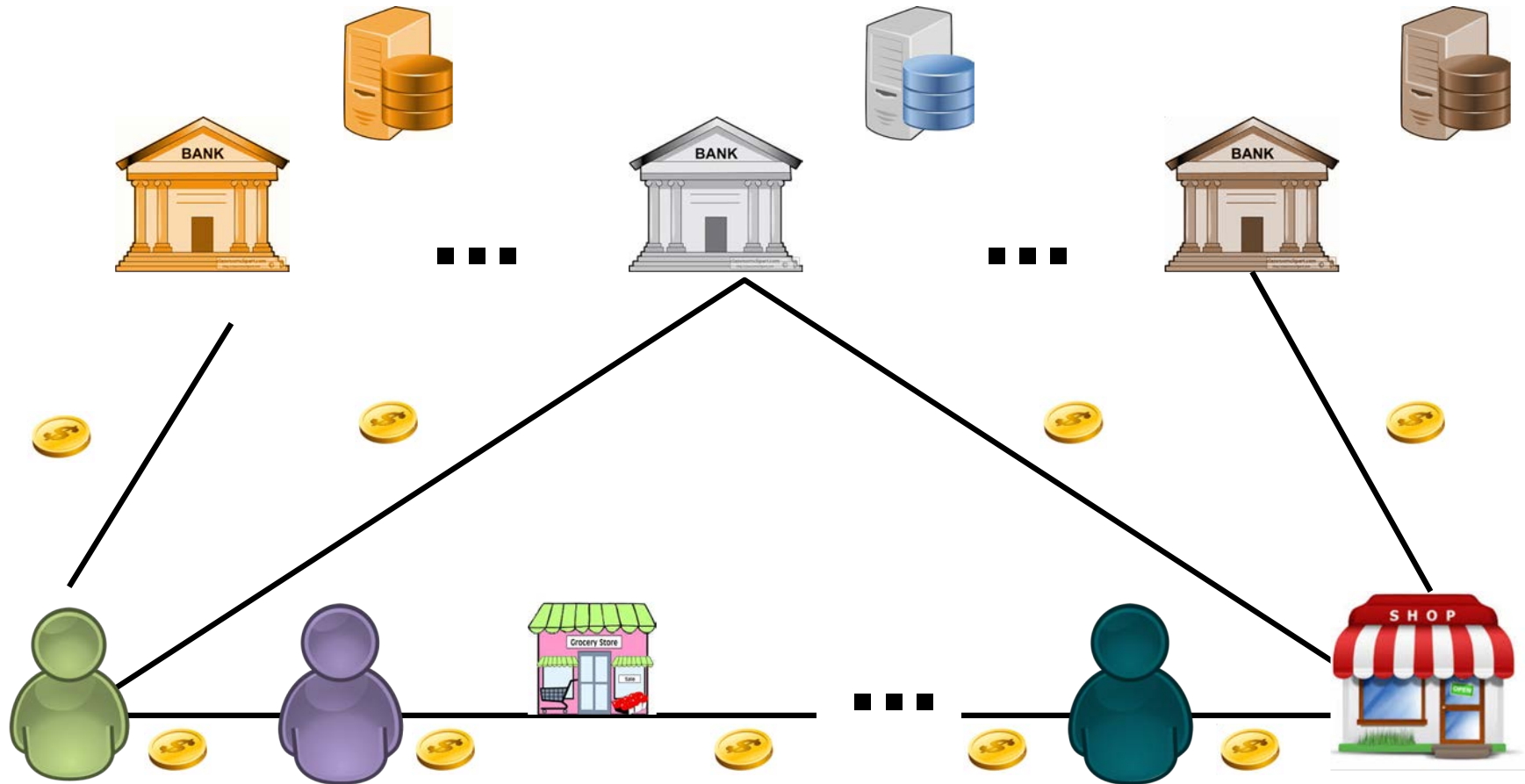


Common characteristic?

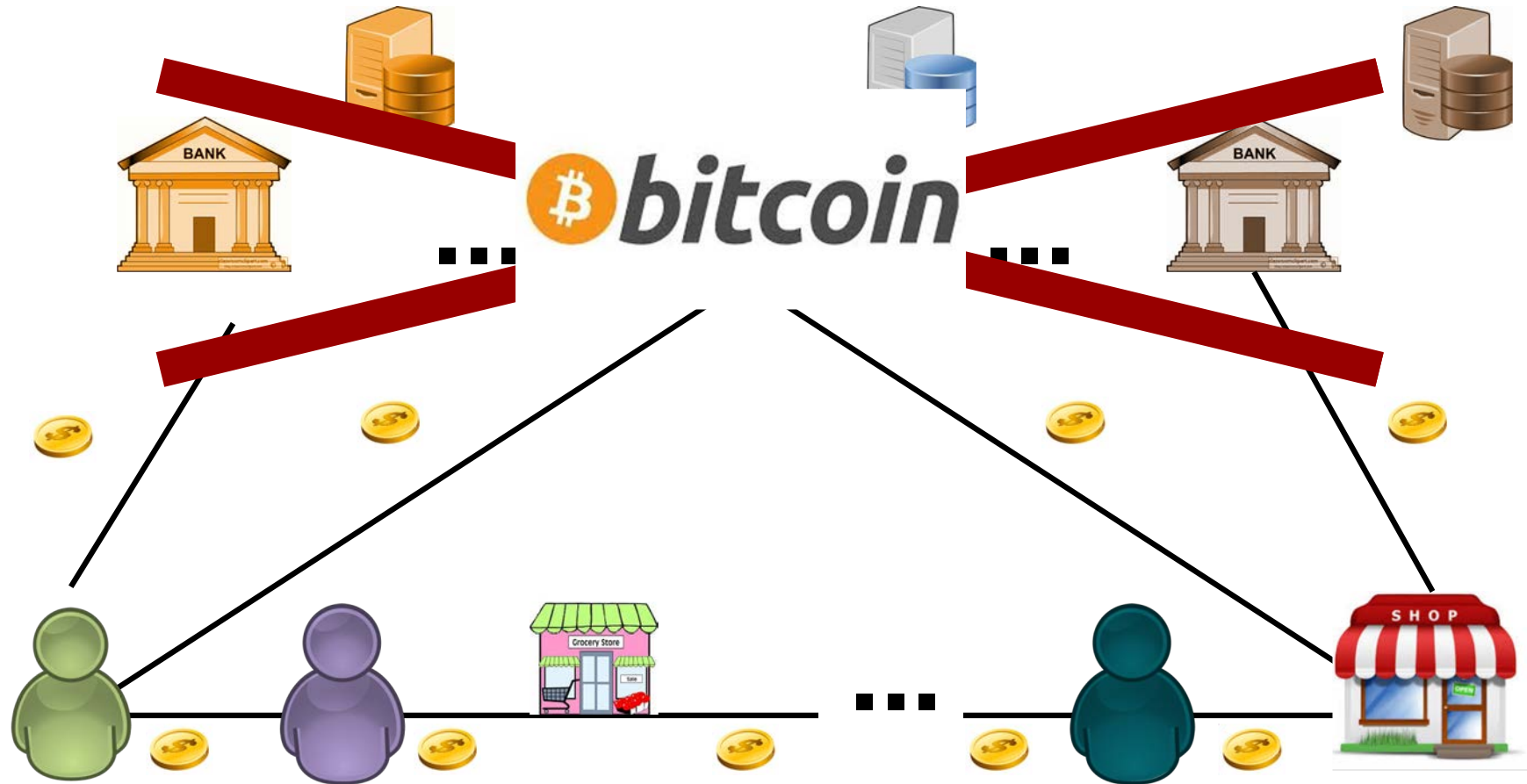
Trust to some financial institution(s)



Common types of payments

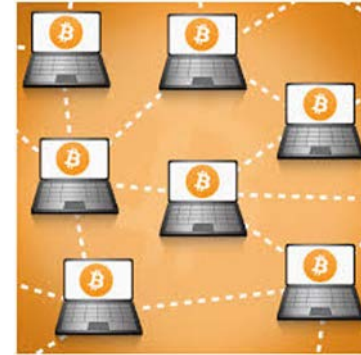


The Bitcoin Revolution



The Bitcoin Revolution

Decentralized peer to peer payment system which works as currency: has units of value which can be exchanged for “real money”.



Proposed by Satoshi Nakamoto in 2008



Really “no trusted server”?

The client software is written by people who are in power to change the system.

They contain so-called **checkpoints** (more on this later).

For example, this is the list of “desktop clients”:

The most popular client.

(open source)

The developers: Wladimir J. van der Laan, Gavin Andresen, Jeff Garzi, Gregory Maxwell, Pieter Wuille



Bitcoin
Core



MultiBit



Armory



Electrum



mSIGNA



Blockchain
.info



Green
Address



Hive

How to update the protocol if there is no governing body?

- Updates have a form of **Bitcoin Improvement Proposals (BIPs)**.
- The Bitcoin community has a **mechanism to vote on BIPs** (weight of the vote **on is proportional to the voter's computing power**),
- the voting **process** is organized centrally:

(“People wishing to submit BIPs, first should propose their idea or document to the mailing list. After discussion they should email Luke Dashjr <luke_bipeditor@dashjr.org>. After copy-editing and acceptance, it will be published here.”)

Why should I care about Bitcoin?

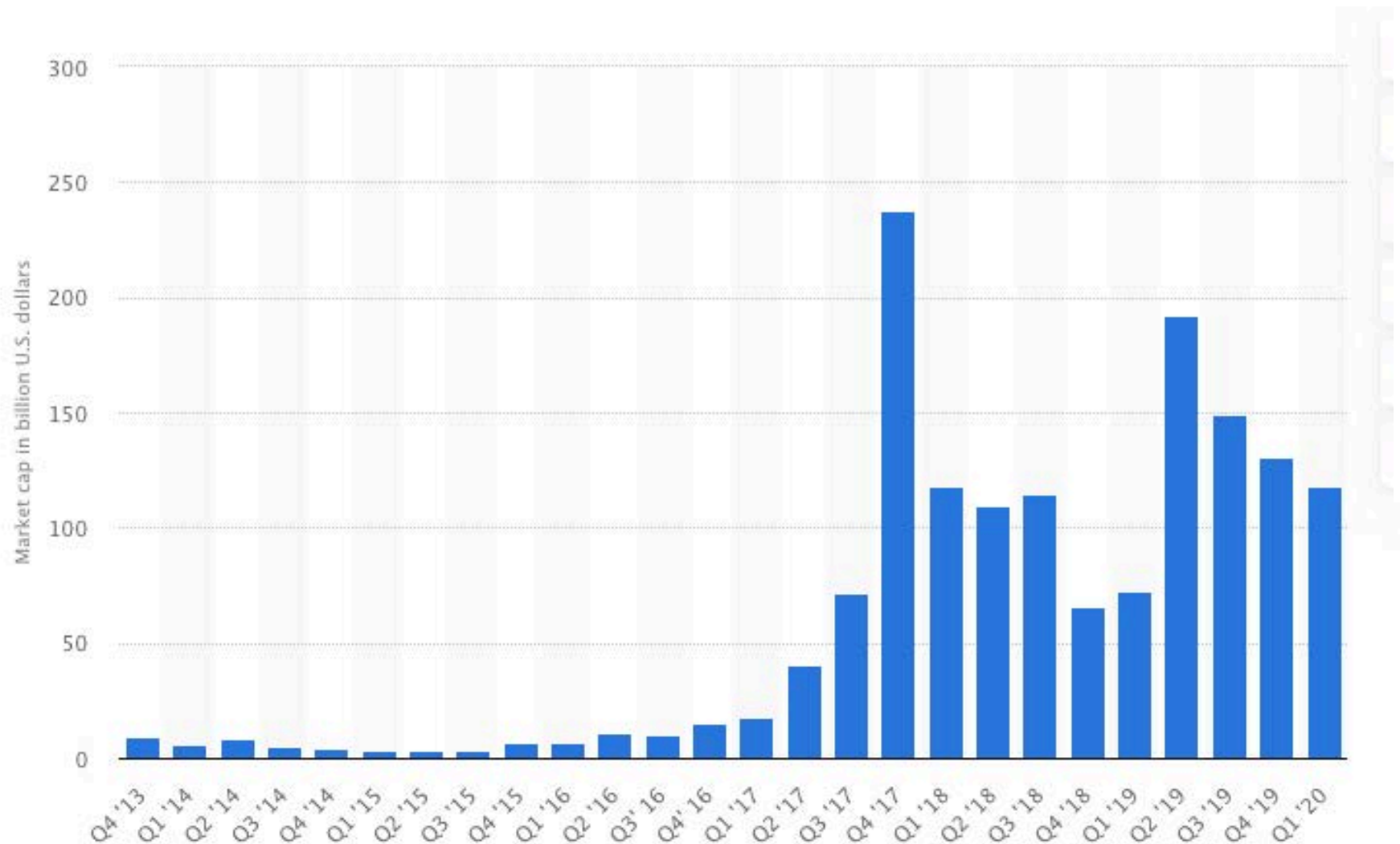
- 1) Very small fees (~ 0.1\$)
- 2) Not too slow transactions (10 - 60 minutes)
- 3) Accepted by thousands of businesses, even has bitcoin ATMs !

The image is a side-by-side comparison of two money transfer services. On the left, the Western Union logo is at the top. Below it, the text reads "Send warm wishes today." and "FOR ONLY \$5/\$50 TRANSFER FEE SEND UP TO". A blue button says "Find Agent Location »". At the bottom, it says "moving money for better". On the right, the Bitcoin logo and "bitcoin" text are at the top. Below it, the text reads "Send warm satoshis today." and "FOR ONLY \$0.01/\$ANY TRANSFER FEE SEND UP TO ANY AMOUNT". An orange button says "Pick Your Wallet »". At the bottom, it says "moving money far better". The background of the right side shows a full moon and Santa Claus flying across the sky.

The image is titled "Who Accepts Bitcoin?". It features a grid of logos for various companies and organizations that accept Bitcoin. The logos are arranged in two rows of four. The first row includes Girl Scouts, OkCupid, Zynga, and Overstock.com. The second row includes Etsy, Reddit, WordPress, and Foodler. A Bloomberg logo is in the bottom right corner.

Bitcoin Market Capitalization

Bitcoin Market Capital: ~ 118 Billion USD (2020Q1) vs. 14B USD in 2016Q1



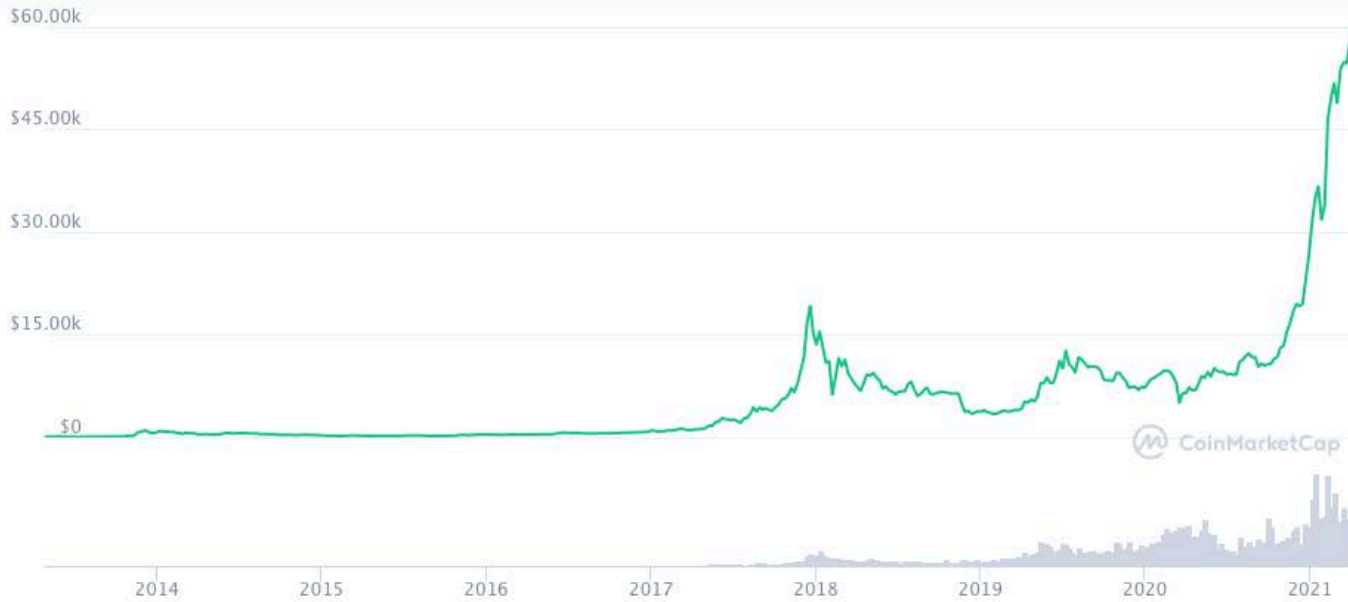
Bitcoin Market Capitalization

Just surpassed 1.1 Trillion USD in Apr 2021 vs. 14B USD in 2016Q1
~ 10x compared to 2020Q1

 Bitcoin BTC

Price: **\$58,975.66** ▲ 1.04%

[Add to Main Watchlist](#) ☆



BTC Price Statistics

Bitcoin Price Today

Bitcoin Price **\$58,975.66**

Price Change 24h **\$607.11**
▲ 1.04%

24h Low / 24h High **\$57,694.83 / \$59,891.30**

Trading Volume 24h **\$61,474,282,339.03**
▲ 26.40%

Volume / Market Cap **0.05586**

Market Dominance **55.69%**

Market Rank **#1**

Bitcoin Market Cap

Market Cap **\$1,100,535,478,251.98**
▲ 0.99%

USD BTC

Want more data? [Check out our API](#)

How do you feel about Bitcoin today?

Vote to see community results



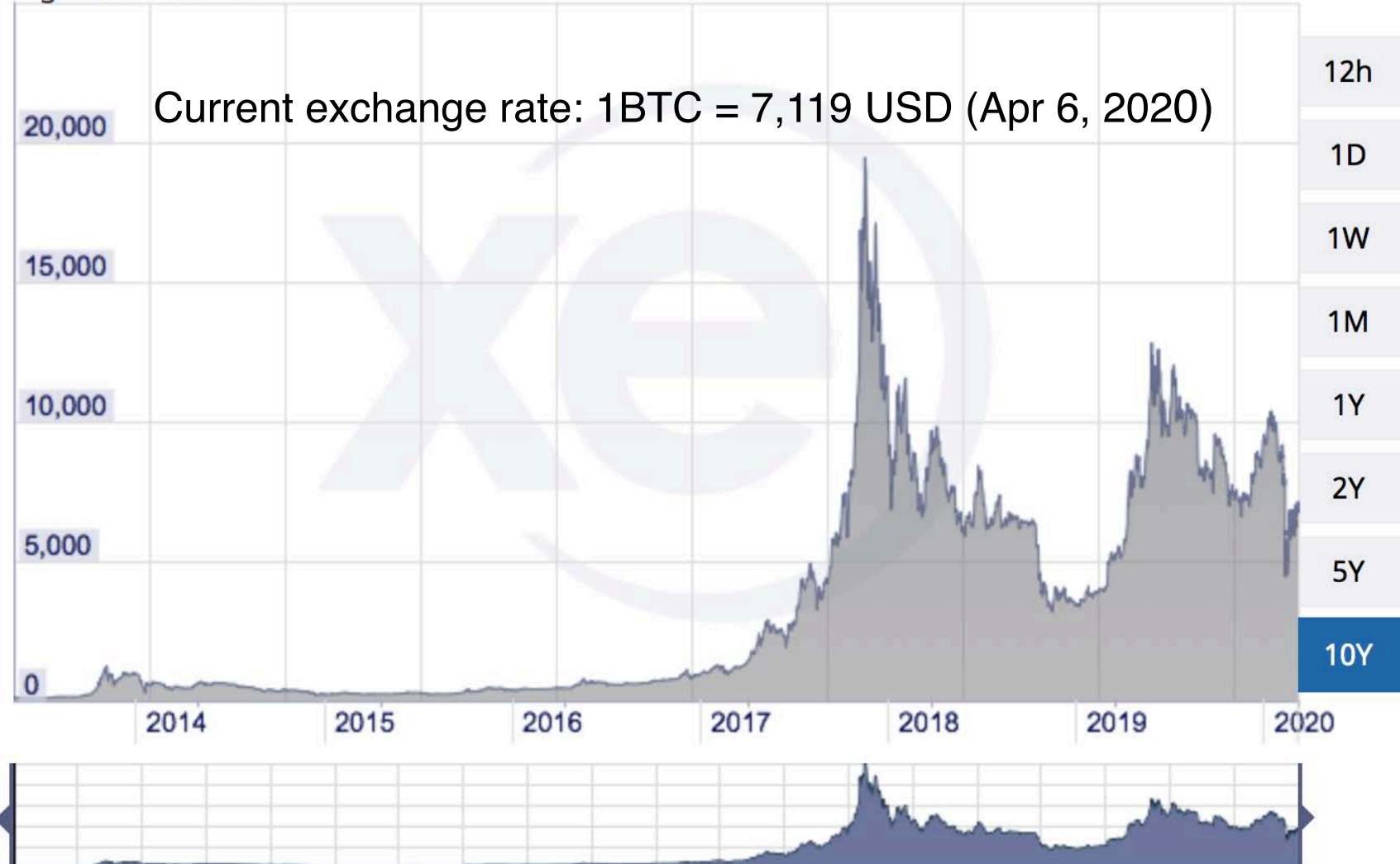
Good



Bad

Bitcoin Exchange Rate

7 六月 2013 00:00 UTC - 6 四月 2020 10:02 UTC **XBT/USD** close:**7089.74985** low:**68.67510**
high:**19447.68573**



📄 XBT - Bitcoin ▼



🇺🇸 USD - 美元 ▼



Bitcoin Exchange Rate

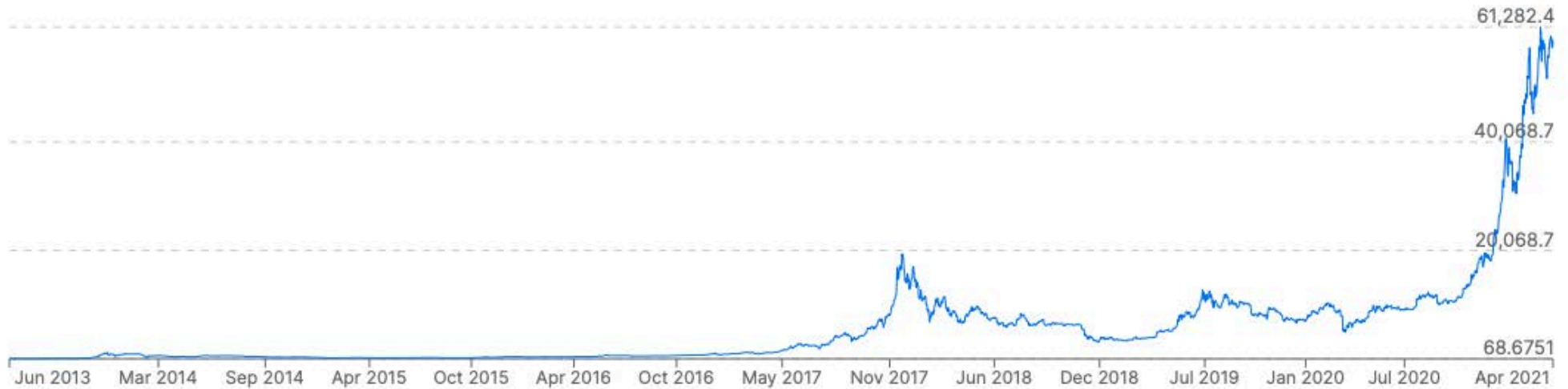
Current exchange rate: 1 **BTC** = 58,826.6 USD (Apr 6, 2021)

XBT to USD Chart

Bitcoin to US Dollar

● 1 XBT = 58,826.6 USD Apr 6, 2021, 04:43 UTC

12H 1D 1W 1M 1Y 2Y 5Y **10Y**



Jun 7, 2013, 00:00 UTC - Apr 6, 2021, 04:42 UTC
XBT/USD close: 58,826.6 low: 68.6751 high: 61,282.4

Why did Bitcoin become so popular ?



- Ideological reasons (crypto-anarchism).

- Good timing (in 2008 the “quantitative easing” in the US started).



Drugs 486
Cannabis 82
Dissociatives 18
Ecstasy 64
Opioids 8
Other 15
Precursors 13
Prescription 92
Psychedelics 83
Stimulants 38
Apparel 77
Art 0
Biotic materials 0

messages 0 | orders 0 | accou

Search

browsing drugs



- Seeming anonymity (anonymous enough for trading illegal goods?)

Bitcoin \approx “Real Money” ?

Bitcoin value comes from the fact that:

“people expect that other people will accept it in the future.”

Enthusiasts:



It's like all the other currencies

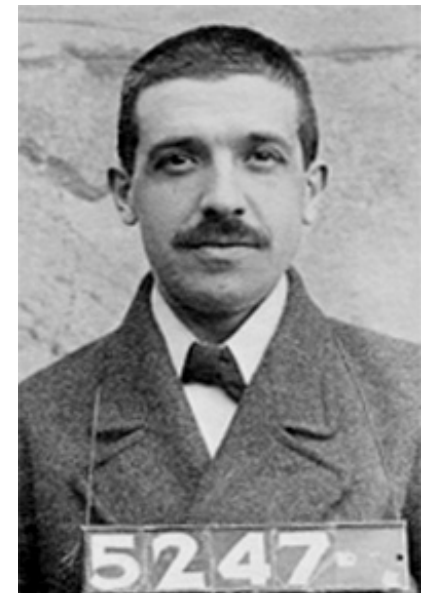
Skeptics:



P. Krugman A. Greenspan



It's a Ponzi scheme



Carlo Pietro Ponzi

The Economist (Nov 1st, 2017)

The Economist

Greater fool theory

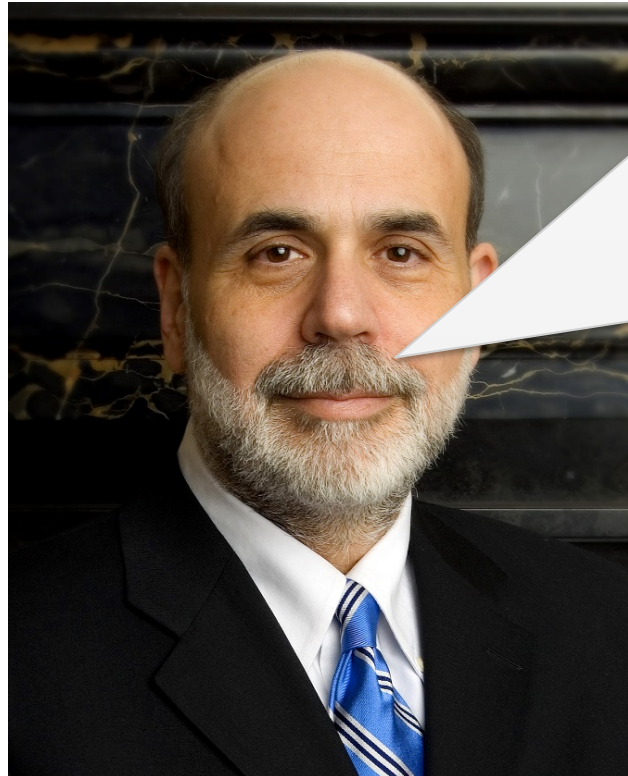
The bitcoin bubble

There may be good reasons for buying bitcoin. But the dominant reason at the moment is that it is rising in price

“People are buying Bitcoin because they expect other people to buy it from them at a higher price; the definition of the greater fool theory.”



Some economists are more positive



Ben Bernanke

While these types of innovations **may pose risks** related to law enforcement and supervisory matters, there are also areas in which they may hold long-term promise, particularly if the innovations **promote a faster, more secure and more efficient payment system.**

Overview of Bitcoin Technology




Bitcoin leverages a Combination of techniques from

- Cryptography and security
- Distributed Systems
- Economics

Bitcoin Users

Permissionless: Anyone can participate in the Bitcoin network: just generate your key public-private key pair, *no need to register with any authority*

public key
(secret)
private key




Alice

Address

PK: hUK67H9fyg

SK: z4Pxc2kKn3



“Unspent Transaction (UTX)”: A user can have multiple such key pairs, each is “unspent”



Bob

PK: p2Pkn7frT

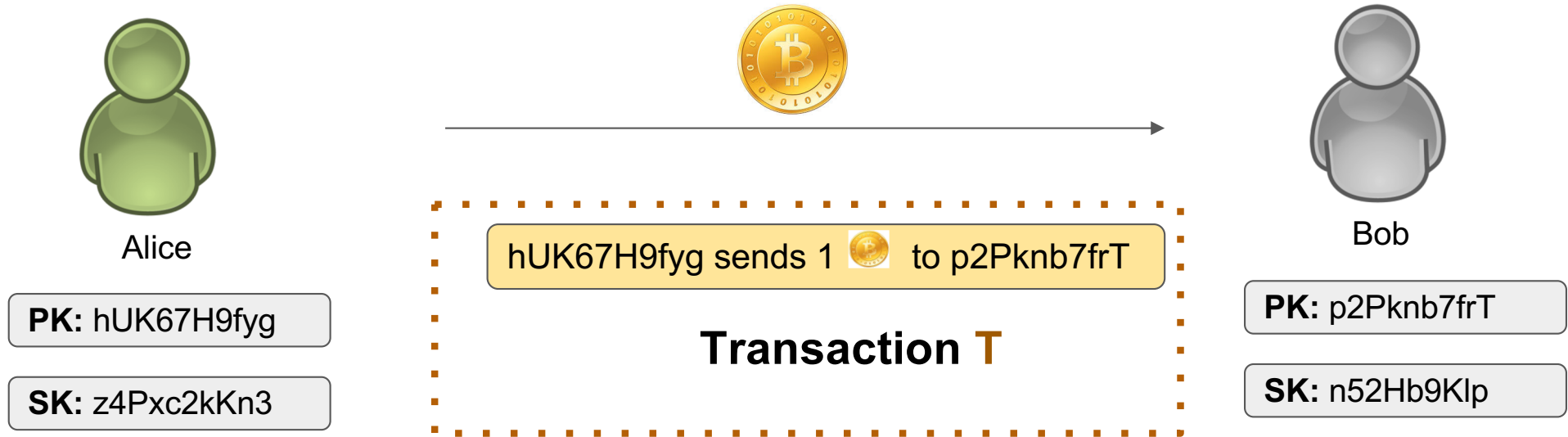
SK: n52Hb9Klp

Why not just call it money ?

- 1) The amount of “bitcoin” that will ever be created is fixed => no inflation
- 2) The Blockchain of Bitcoin does not *directly* keep the total balance of your account ; instead, it tracks the Unspent Transaction Outputs (UTXOs) of yours (to contrast with the account model of Ethereum) ; more later in the course

Bitcoin Transactions

Transactions are authorized/ authenticated based on digital signatures



1. **PK of the Alice and Bob serve as the sender/ recipient addresses**

2. **Transaction T Signed by Alice's SK!**

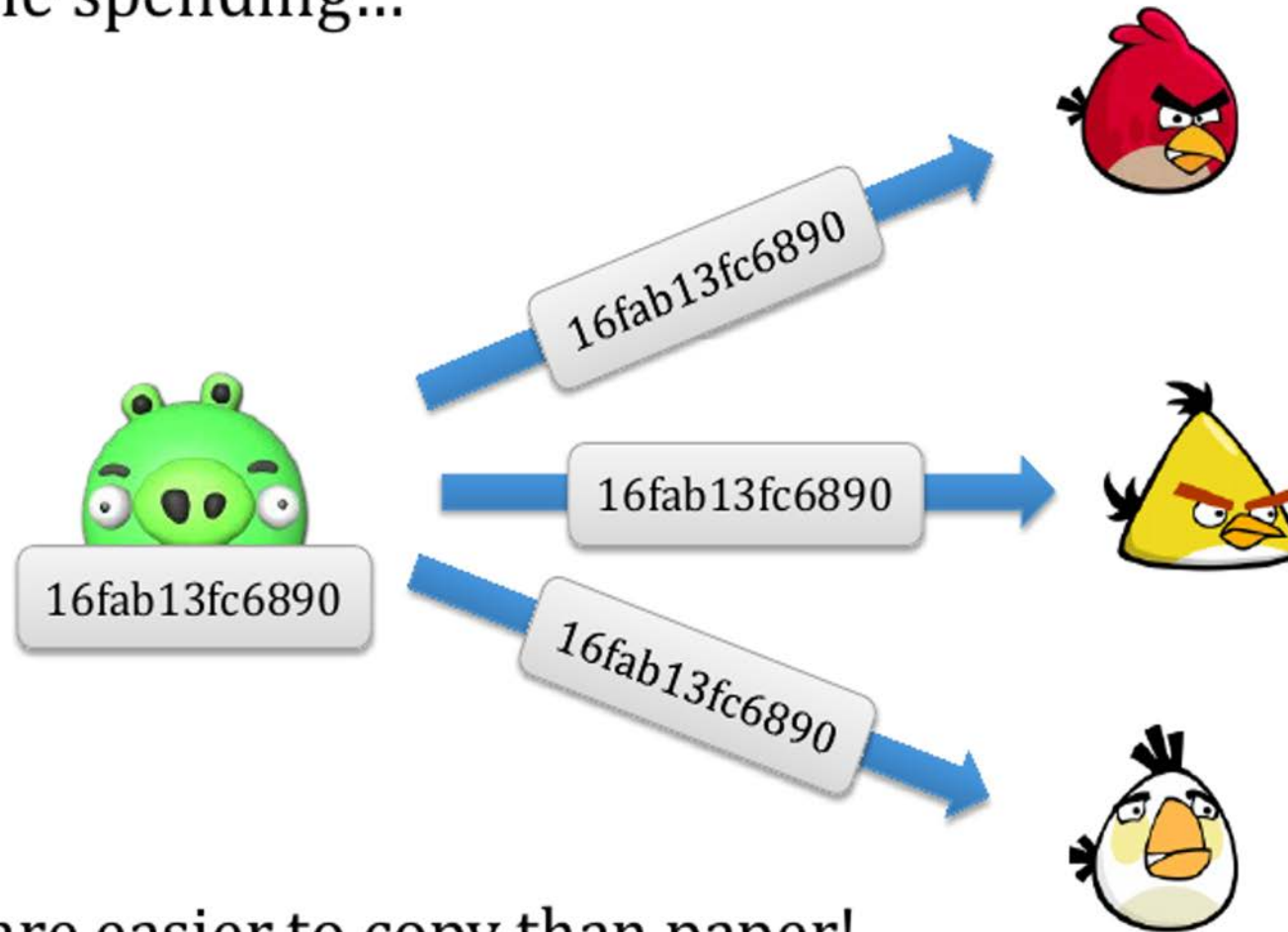
3. **A transaction is valid only if the signature verifies**



Note: In reality, a bitcoin address is not the same as a public key. Instead, bitcoin addresses are derived from a public key using one way hash function => This saves storage space in the blockchain.

Biggest challenge with digital money

Double spending...



Bits are easier to copy than paper!

Main idea to prevent Double Spending

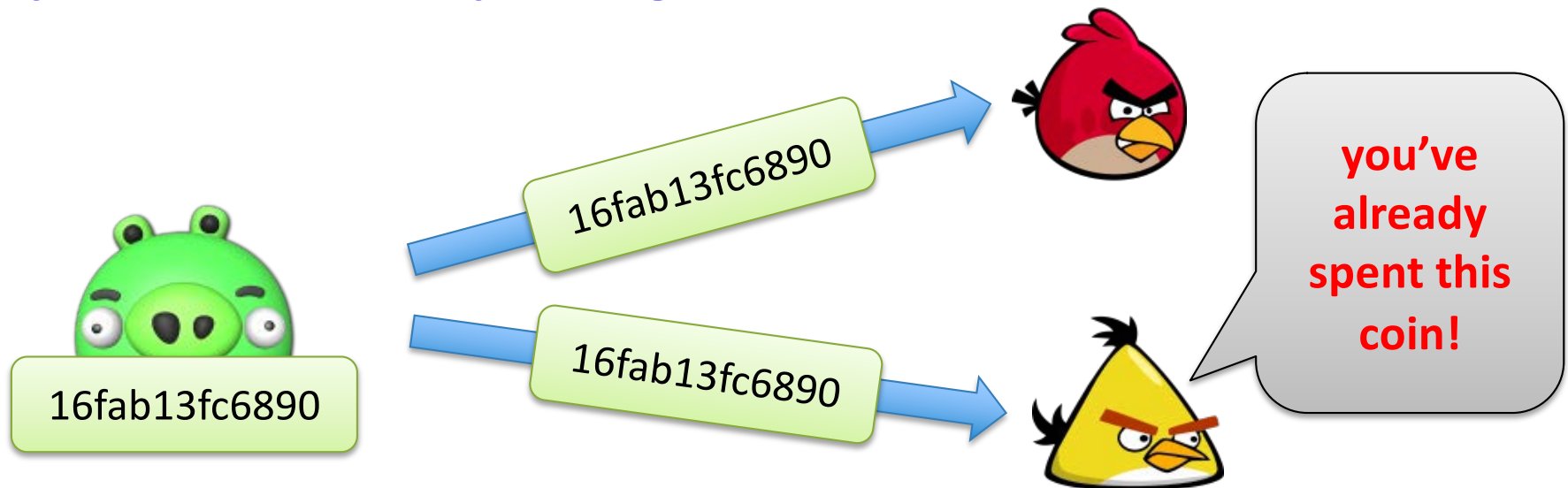
The users emulate a **public append-only (non-reversible) bulletin-board (aka Public Ledger)** containing a list of transactions.

A transaction is of a form:

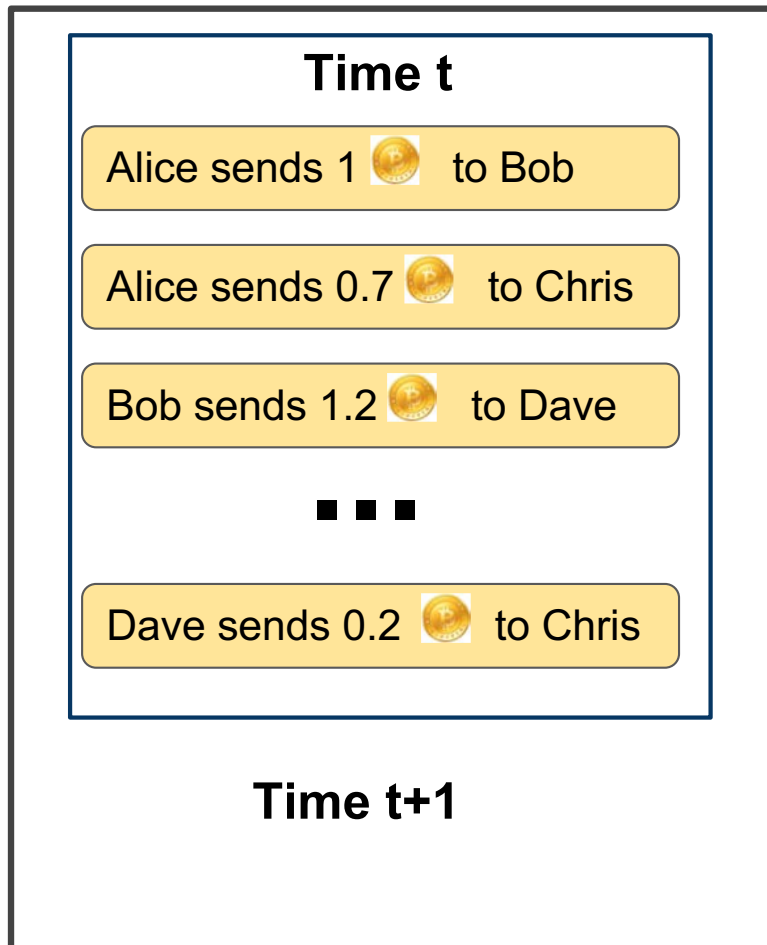


“User P_1 transfers a coin #16fab13fc6890 to user P_2 ”

This prevents double spending.

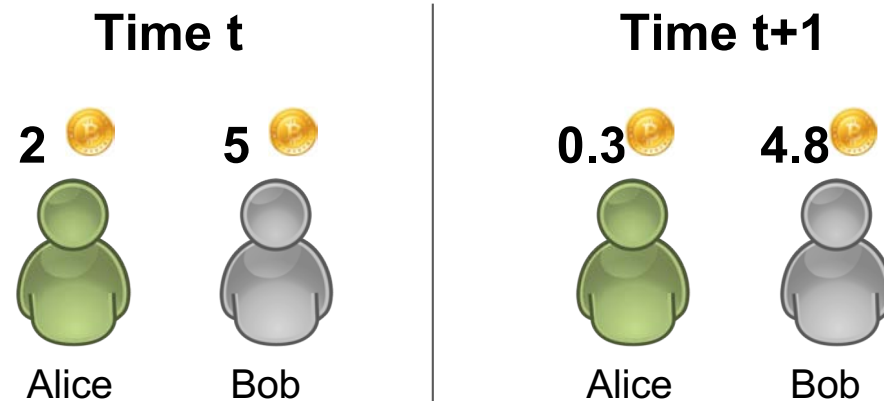


Transaction table: the Bitcoin Blockchain



Stores every transaction and checks users balances

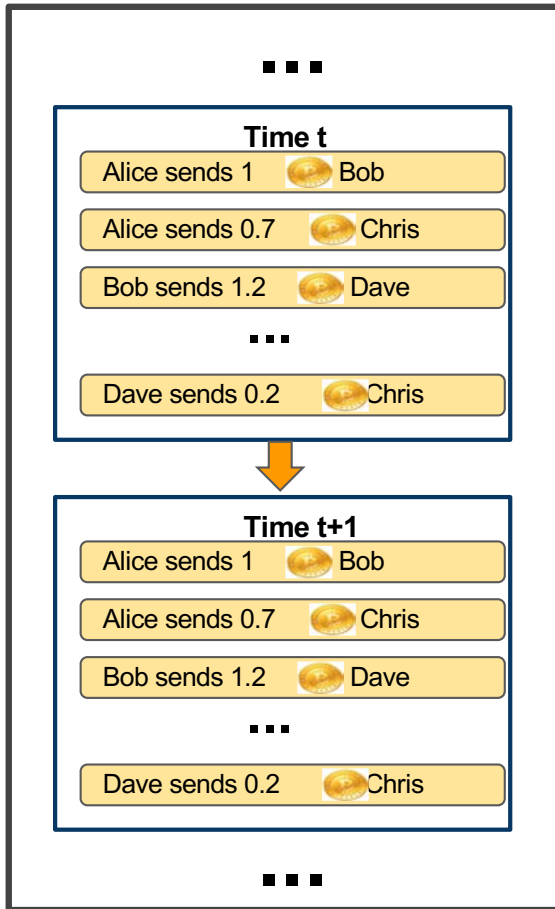
Example:



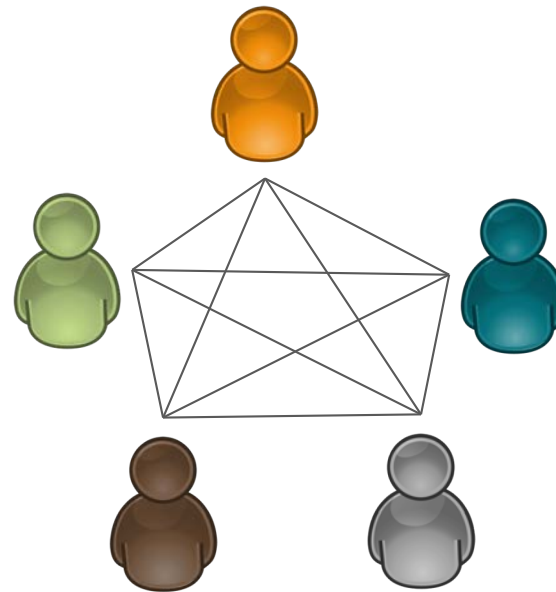
Required properties:

- Append only
- Cannot revise existing blocks
- Distributed

Who maintains the Bitcoin Blockchain?



~~In traditional payment systems
that would be a financial
institution~~



Miners: special
type of user

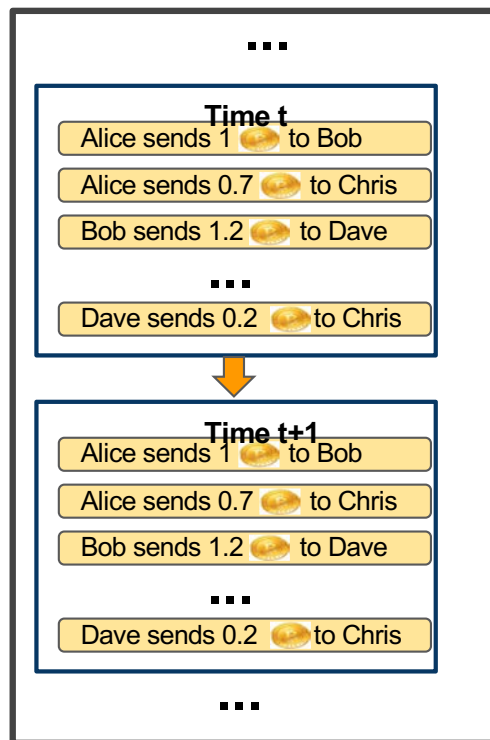
peer-to-peer

Who maintains the Bitcoin Blockchain?

Every transaction is broadcasted to all users

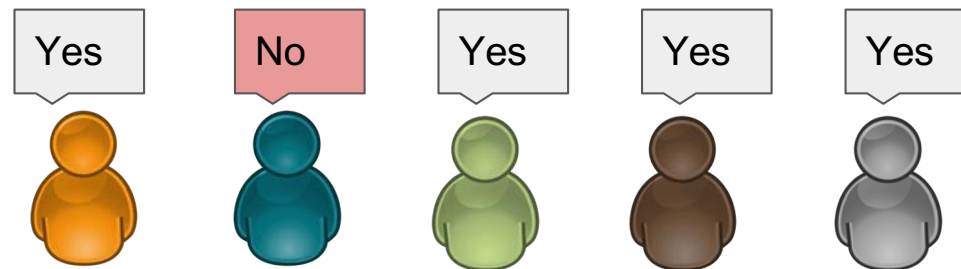


Distributed Ledger



Is this the right view of the blockchain?

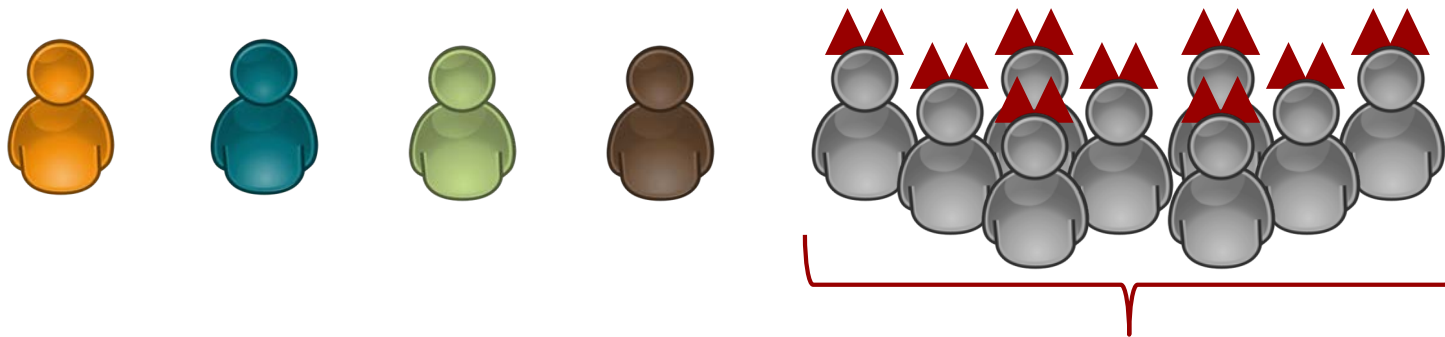
Voting -> majority wins



1. Works well only if users are all honest but this is not the case in practice!
2. Worse still, "Sybil" aka fake identities can be created "for free" in a Permissionless network

The Sybil problem

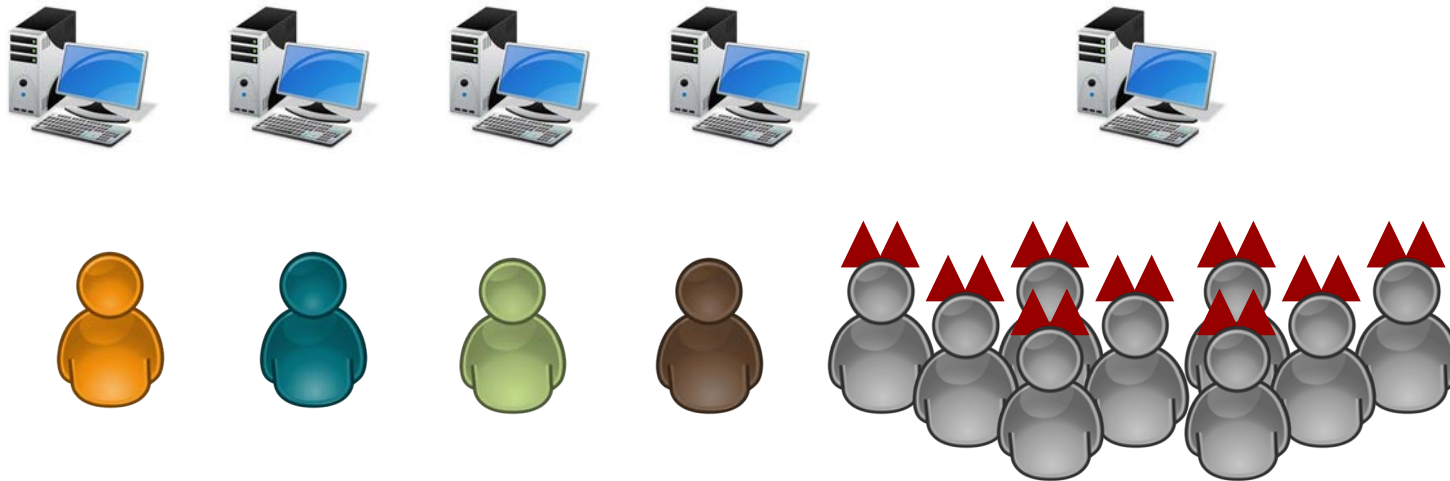
What does majority mean in a system that everyone (including anonymous user) is free to participate?



Sybil: Multiple identities belonging to the same (malicious) user

Bitcoin's solution

Majority is defined as the majority of **computational power!**



This works because Sybil creation doesn't increase attackers computational power !!

How to check majority of computational power ?



Majority is defined as the majority of **computational power!**

Sybil creation **doesn't increase** attackers computational power ;)

Proof of Work

“Measures” a user’s computational power by how much time is needed for solving a “puzzle”

- the puzzle should be difficult to solve
- but, a solution should be easily verifiable

In Bitcoin, it is based on the

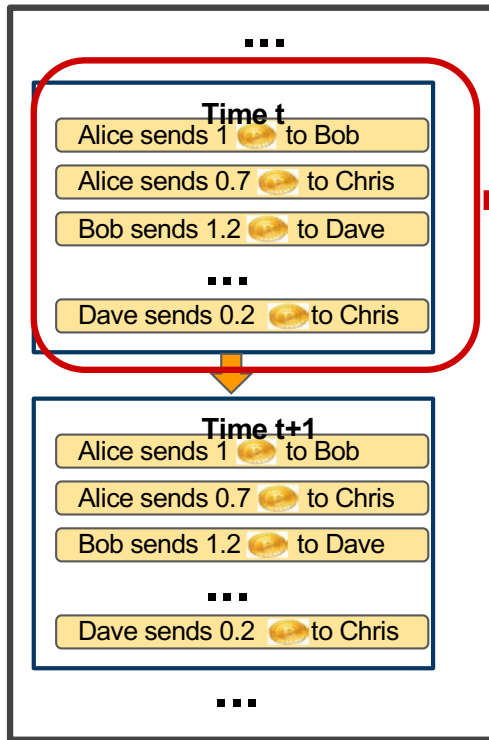
cryptographic hash functions

$$H(x) < D$$

Puzzle: Given D find x !



How to add a block to the blockchain?

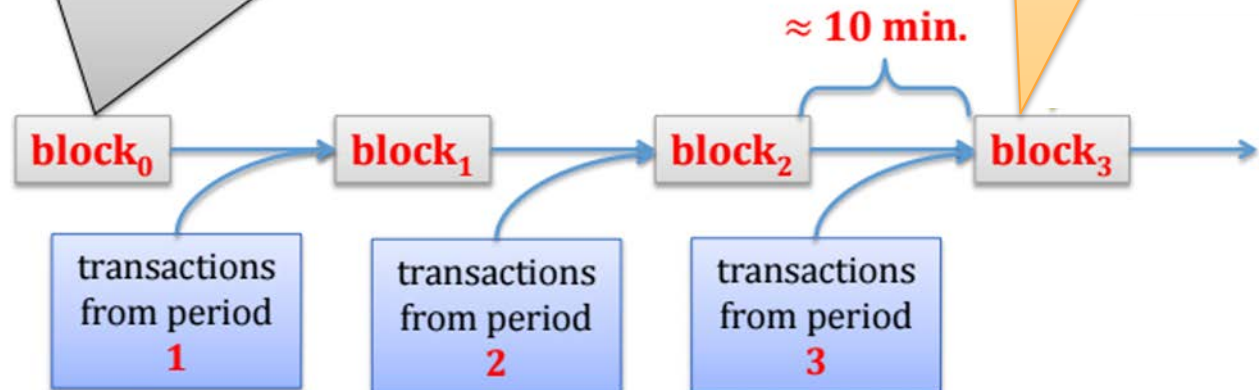


1 block

A block is added every 10 minutes and has size < 1MB

block size
< **1MB**,
which
translates to
max
7 trans./sec.

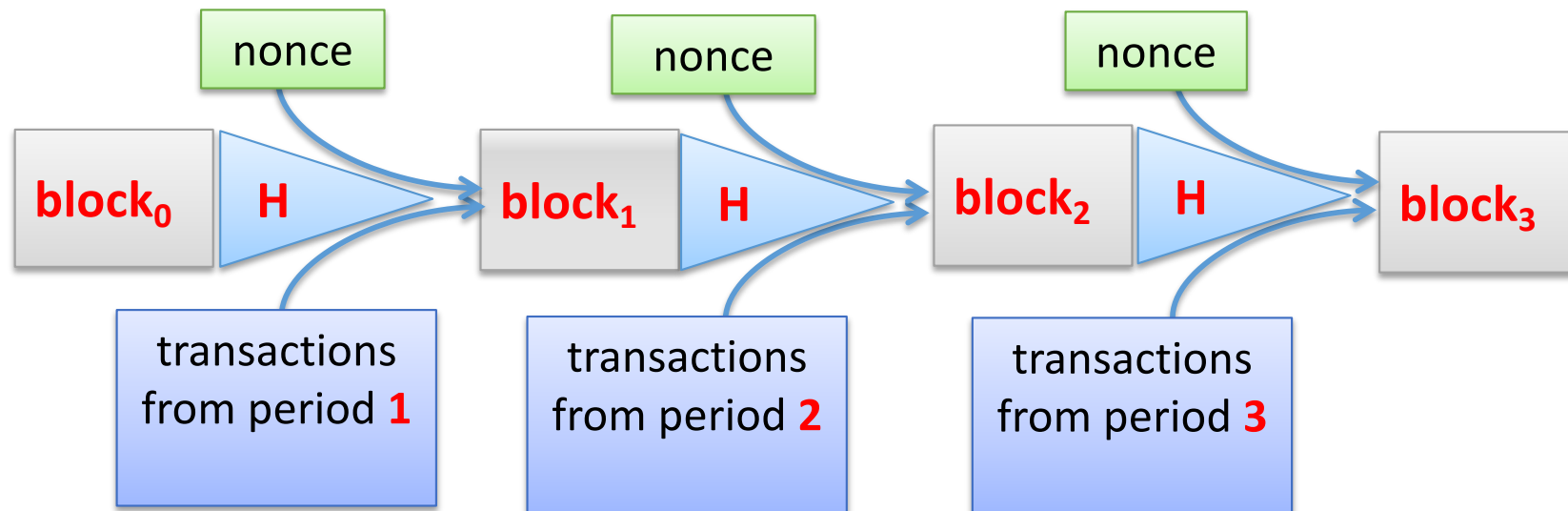
the "genesis block" created by Satoshi on 03/Jan/2009



How are the PoWs used?

H – hash function

more concretely in Bitcoin: H is **SHA256**.



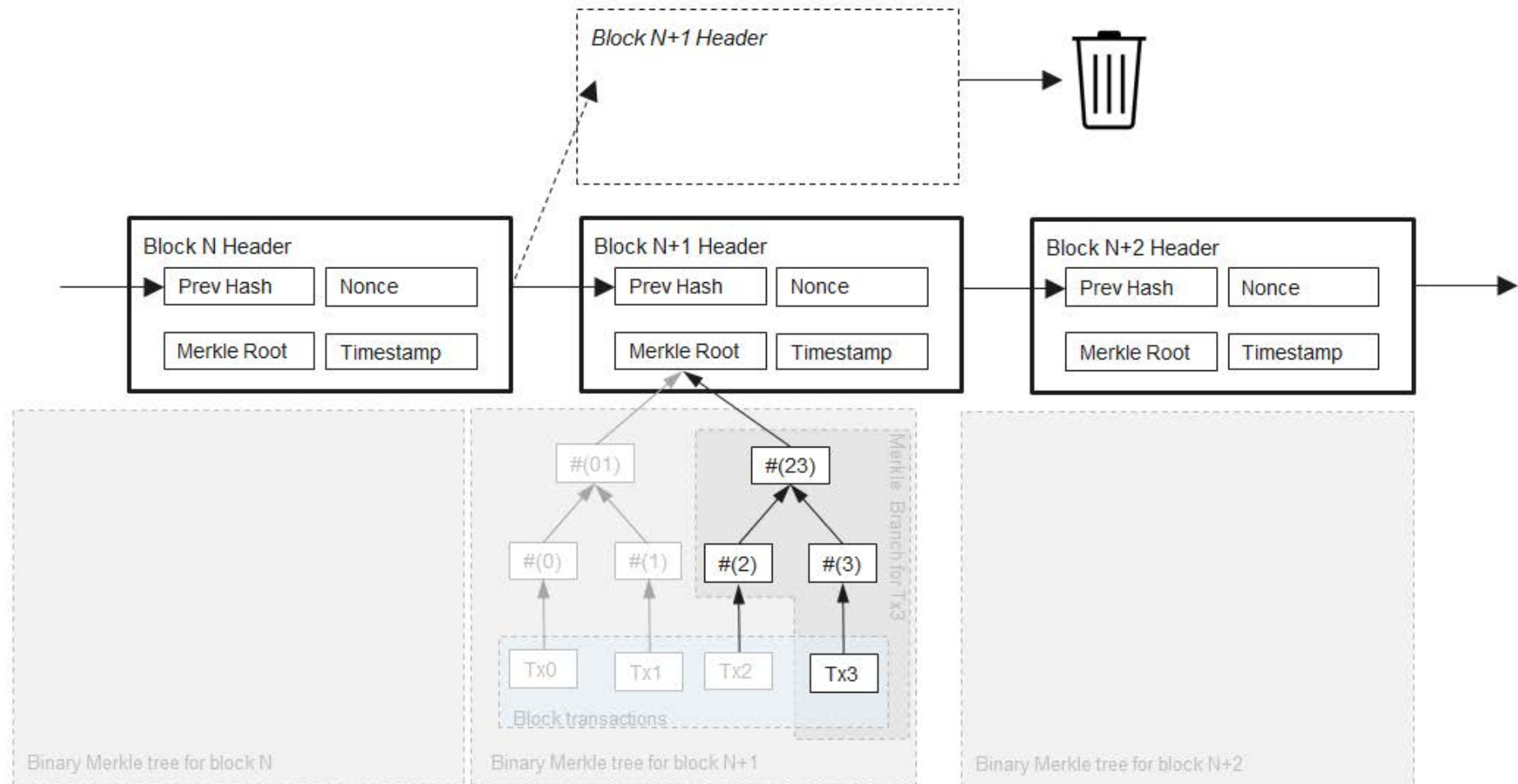
Main idea: to extend the chain one needs to find **nonce** such that **$H(\text{nonce}, H(\text{block}_i), \text{transactions})$** starts with some number **n** of **zeros**

“hardness parameter”

How it looks in real life

Height	Timestamp	Transactions	Size
414902	Jun 5, 2016 5:01:20 PM	386	171361
414901	Jun 5, 2016 4:58:57 PM	304	114339
414900	Jun 5, 2016 4:57:25 PM	1004	428715
414899	Jun 5, 2016 4:50:43 PM	739	384667
414898	Jun 5, 2016 4:45:29 PM	1388	999990
414897	Jun 5, 2016 4:41:19 PM	2187	999945
414896	Jun 5, 2016 4:23:42 PM	2743	998020

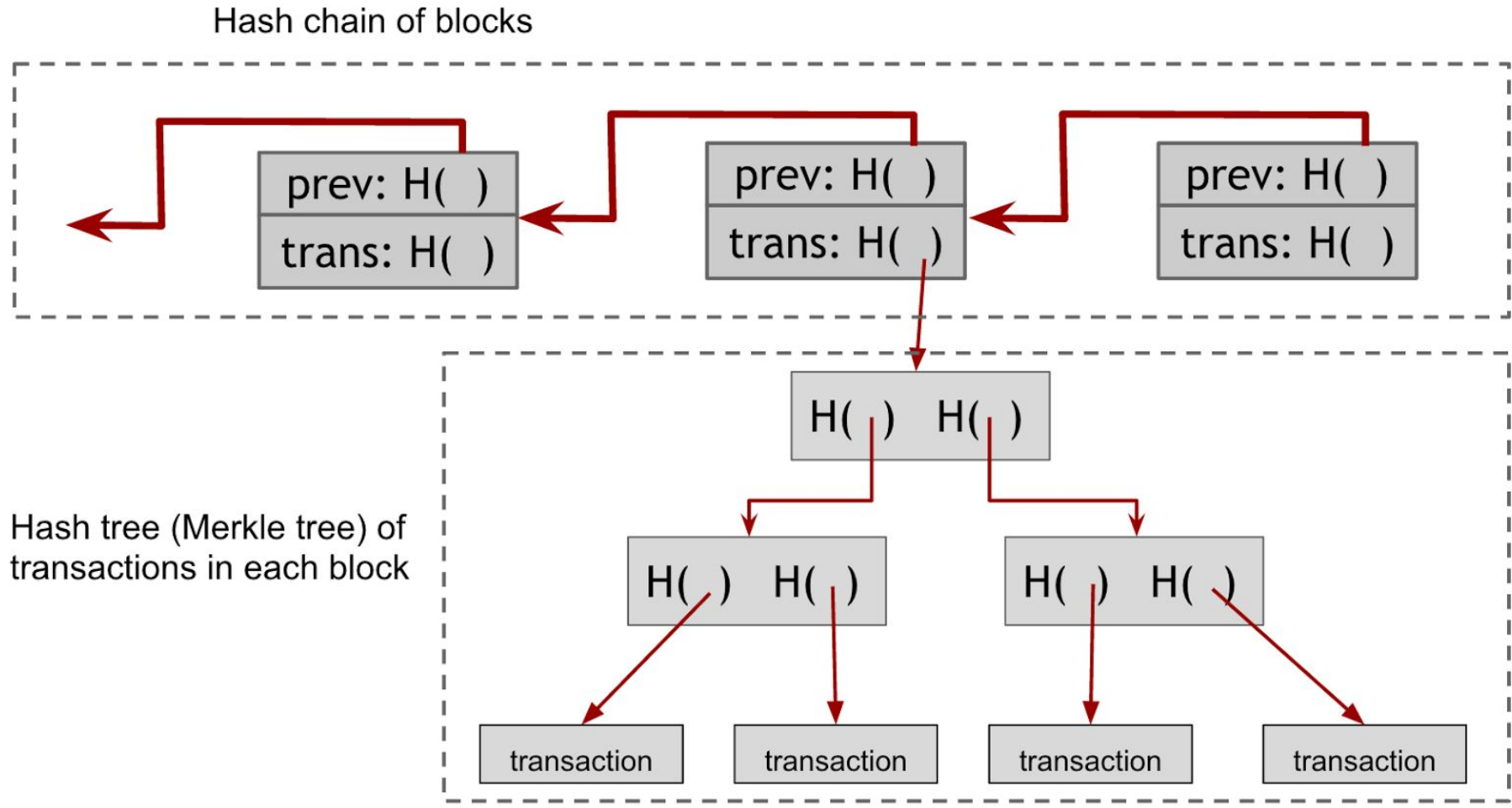
Actual data-structure of the Bitcoin Blockchain



Source: <https://ethereum.stackexchange.com/questions/268/ethereum-block-architecture>

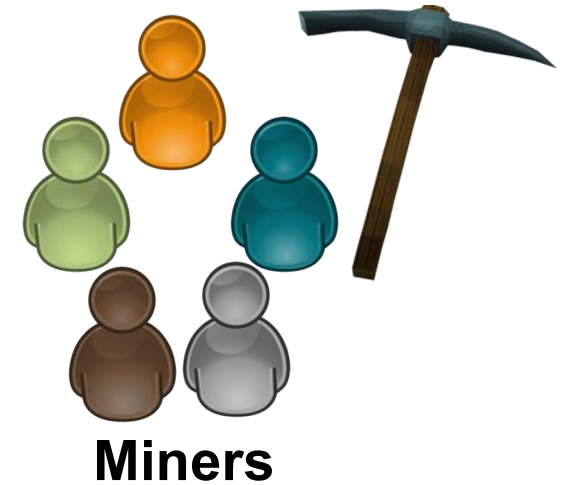
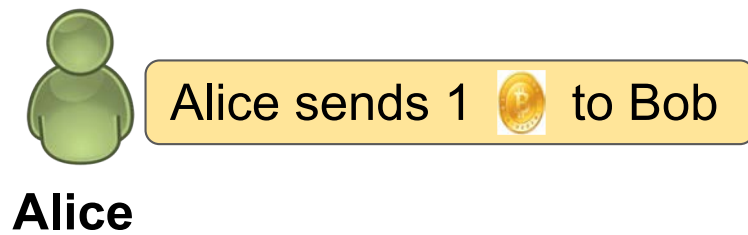
Note: The actual Bitcoin blockchain contains two different hash structures. The first is a hash chain of blocks that links the different blocks to one another. The second is internal to each block and is a Merkle Tree of transactions within the blocks.

Actual data-structure of the Bitcoin Blockchain



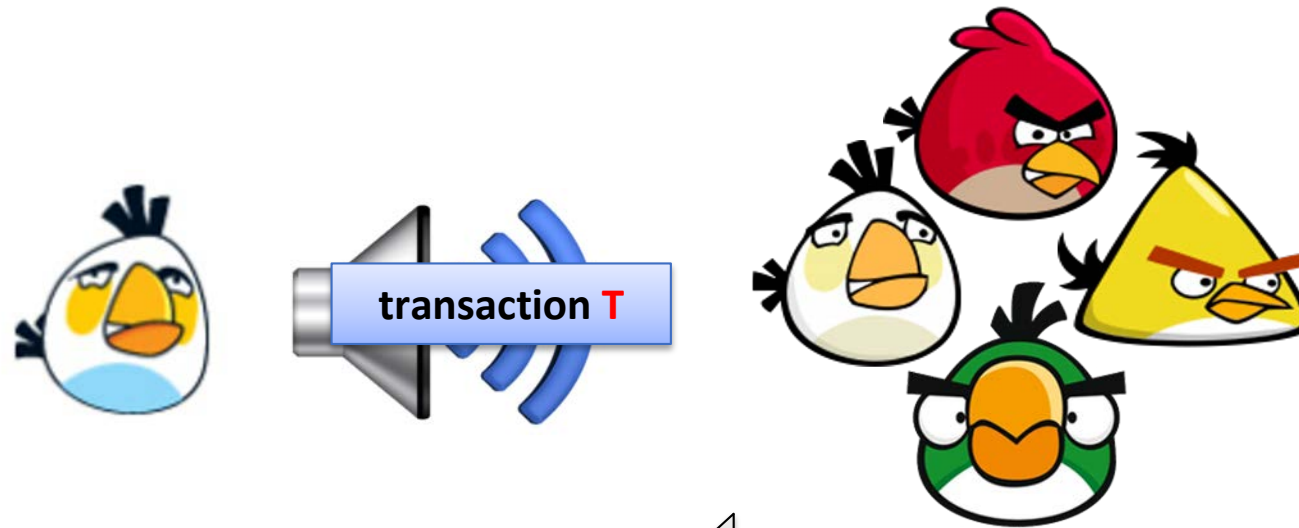
Note: The actual Bitcoin blockchain contains two different hash structures. The first is a hash chain of blocks that links the different blocks to one another. The second is internal to each block and is a Merkle Tree of transactions within the blocks.

How to add a transaction to a block ?



How to post on the Bulletin-board ?

Just broadcast (over the internet) your transaction to the miners.



And hope they will **add it to the next block**

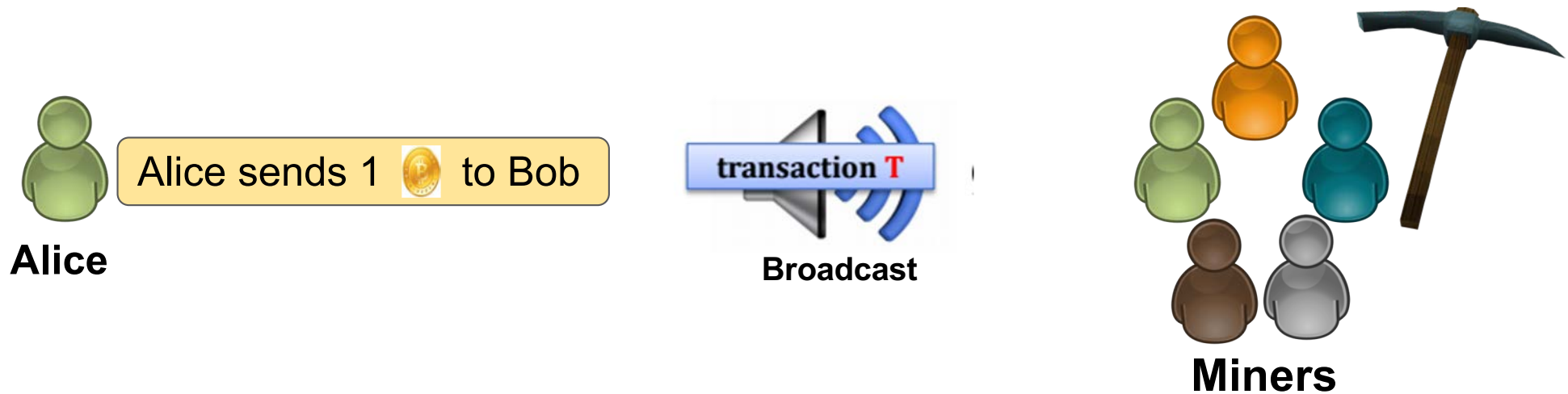
the miners are incentivized to do it.

Important:

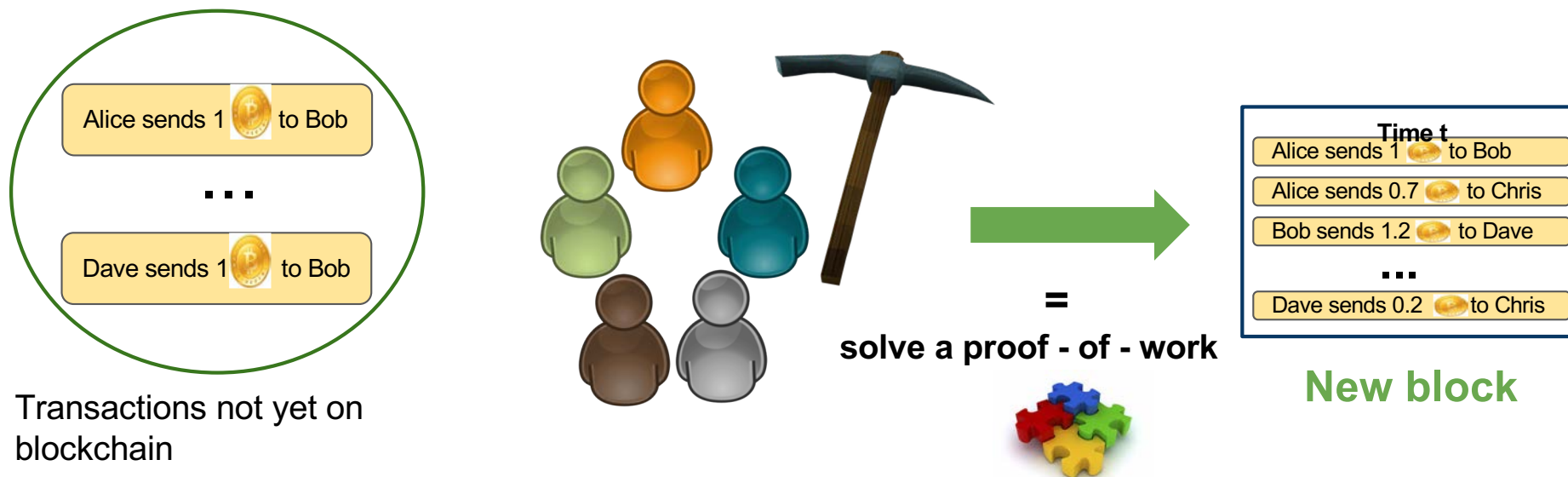
They **never add an invalid transaction** (e.g. double spending)

a chain with an invalid transaction is **itself not valid**, so no rational miner would do it.

How to add a transaction to a block ?



Miners compete on who will make the next block




Main principles

1. It is **computationally hard** to extend the chain.

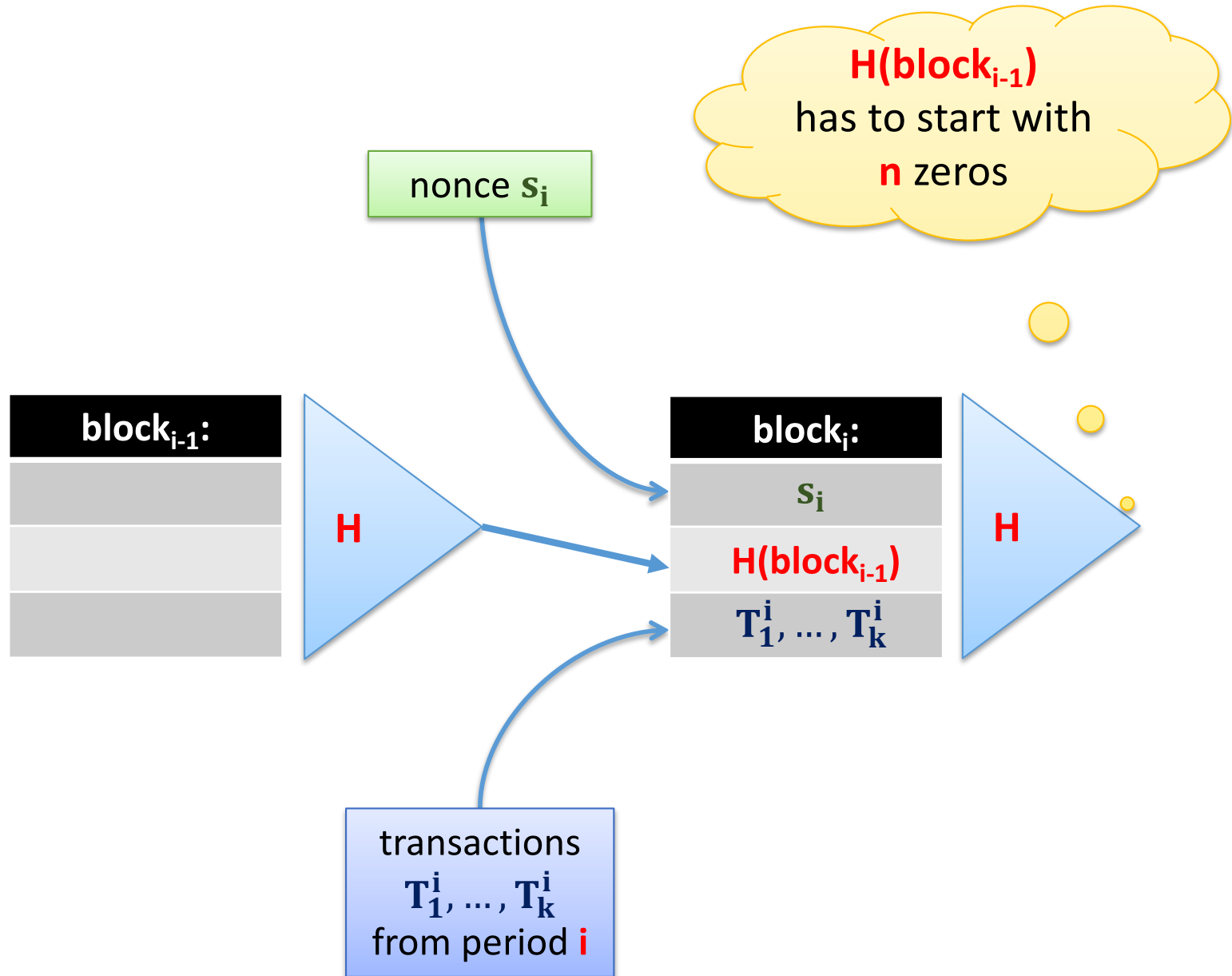
1. Once a miner finds an extension he **broadcasts it to everybody**.

1. The users will always accept “**the longest chain**” as the valid one.



the system
incentivizes
them to do it

In more details:



The hardness parameter is periodically changed

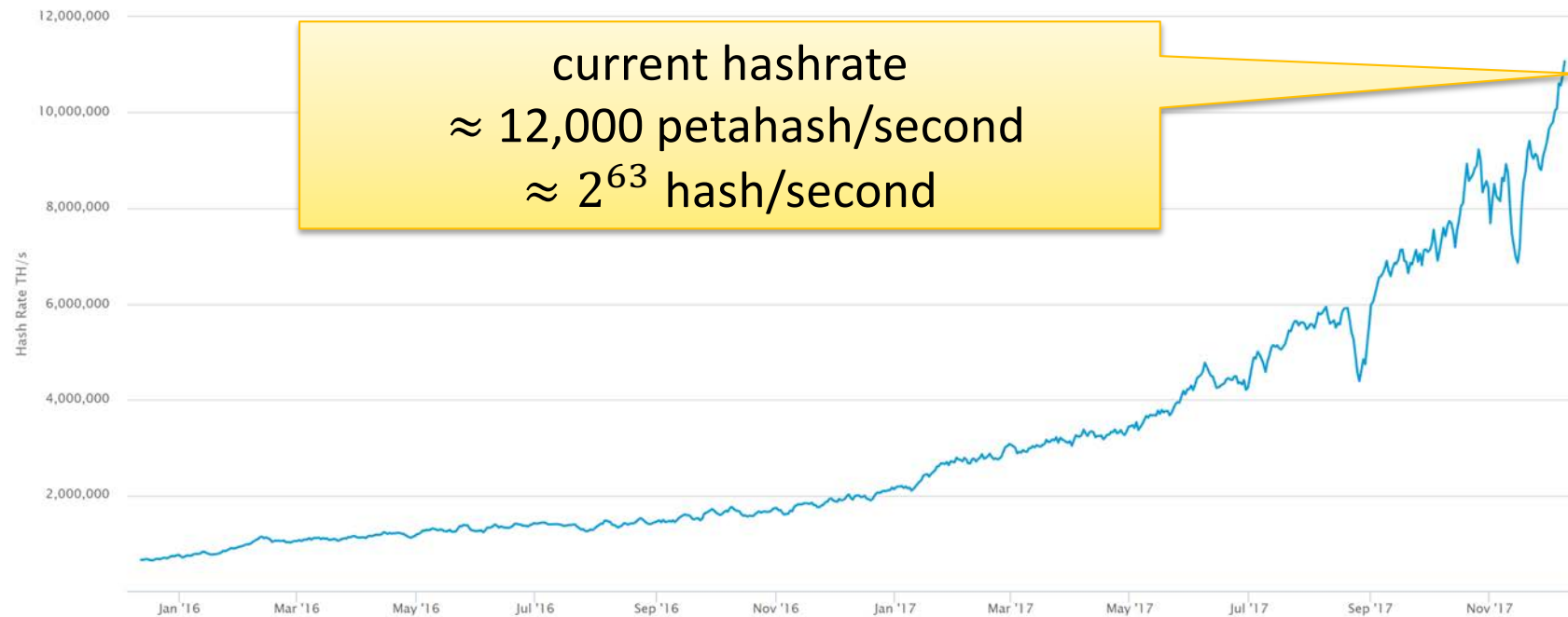
- The computing power of the miners **changes**.
- The miners should generate the new block **each 10 minutes** (on average).
- Therefore the hardness parameter **is periodically adjusted** to the mining power
- This happens once each **2016 blocks**.
- **Important**: the hardness adjustment is **automatic**, and depends on how much time it took to generate last 2016 blocks.

this is possible since every block contains a **time-stamp** produced by the miner who mined it



“Hashrate” = number of hashes computed per second

total hashrate over the past few years:

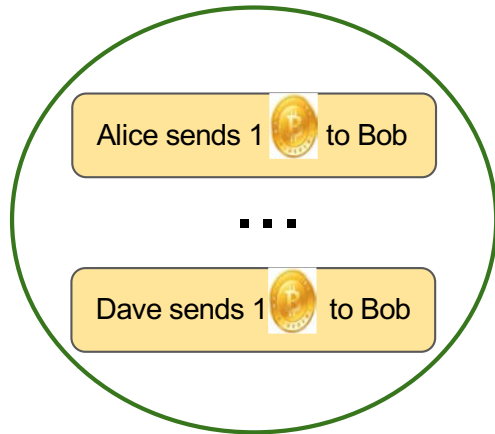


Dec 2015: 500 petahash/second

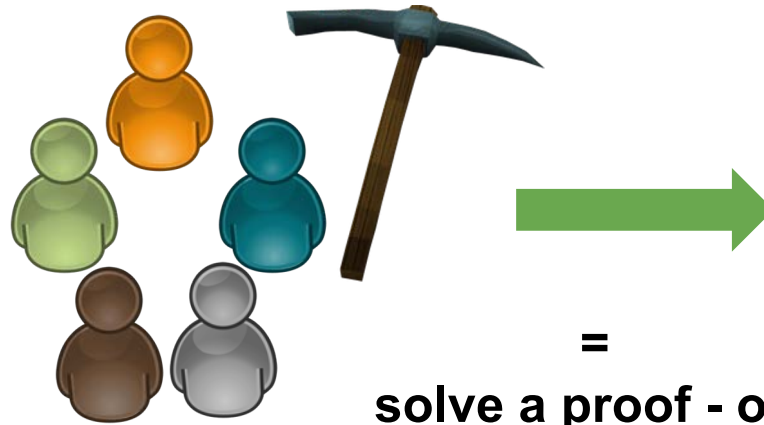
Dec 2016: 2,000 petahash/second

Dec 2017: 12,000 petahash/second

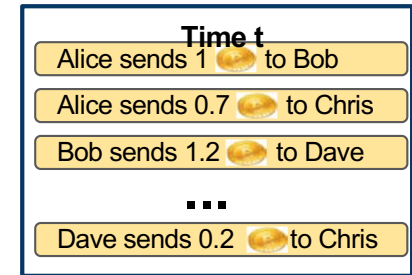
Creating a new block



Transactions not yet on blockchain



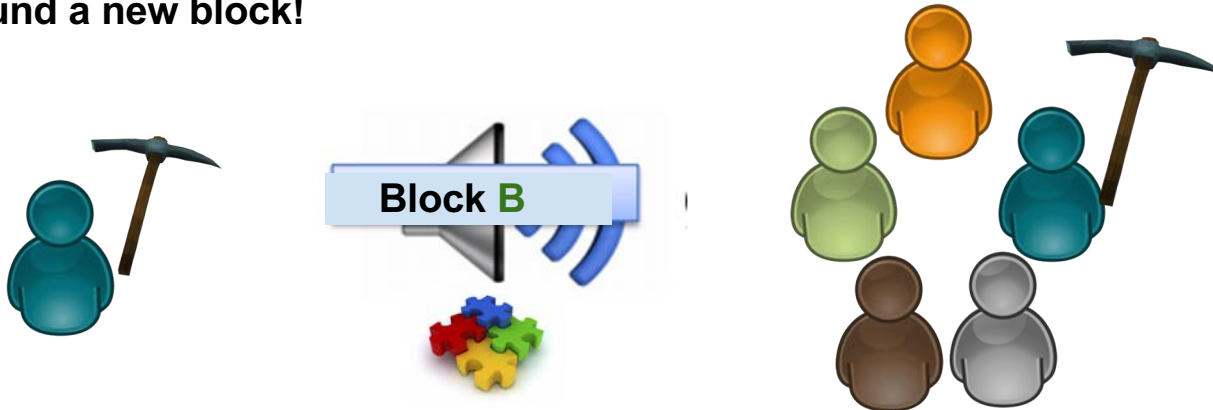
=
solve a proof - of -
work



New block

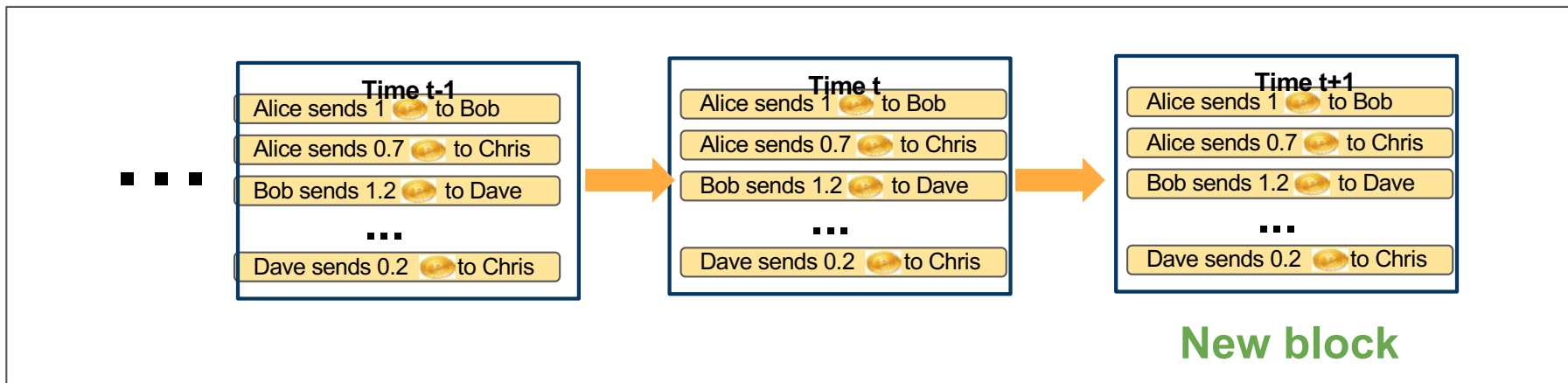
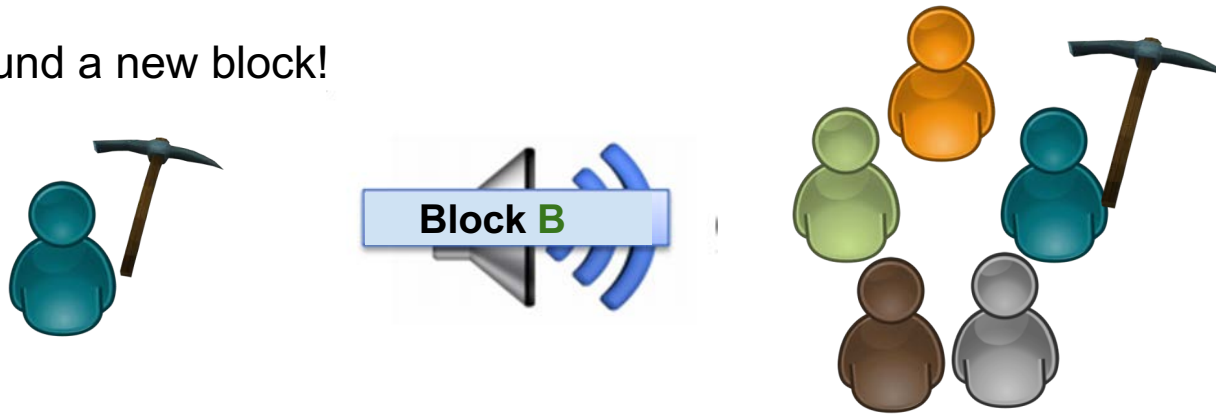


I found a new block!



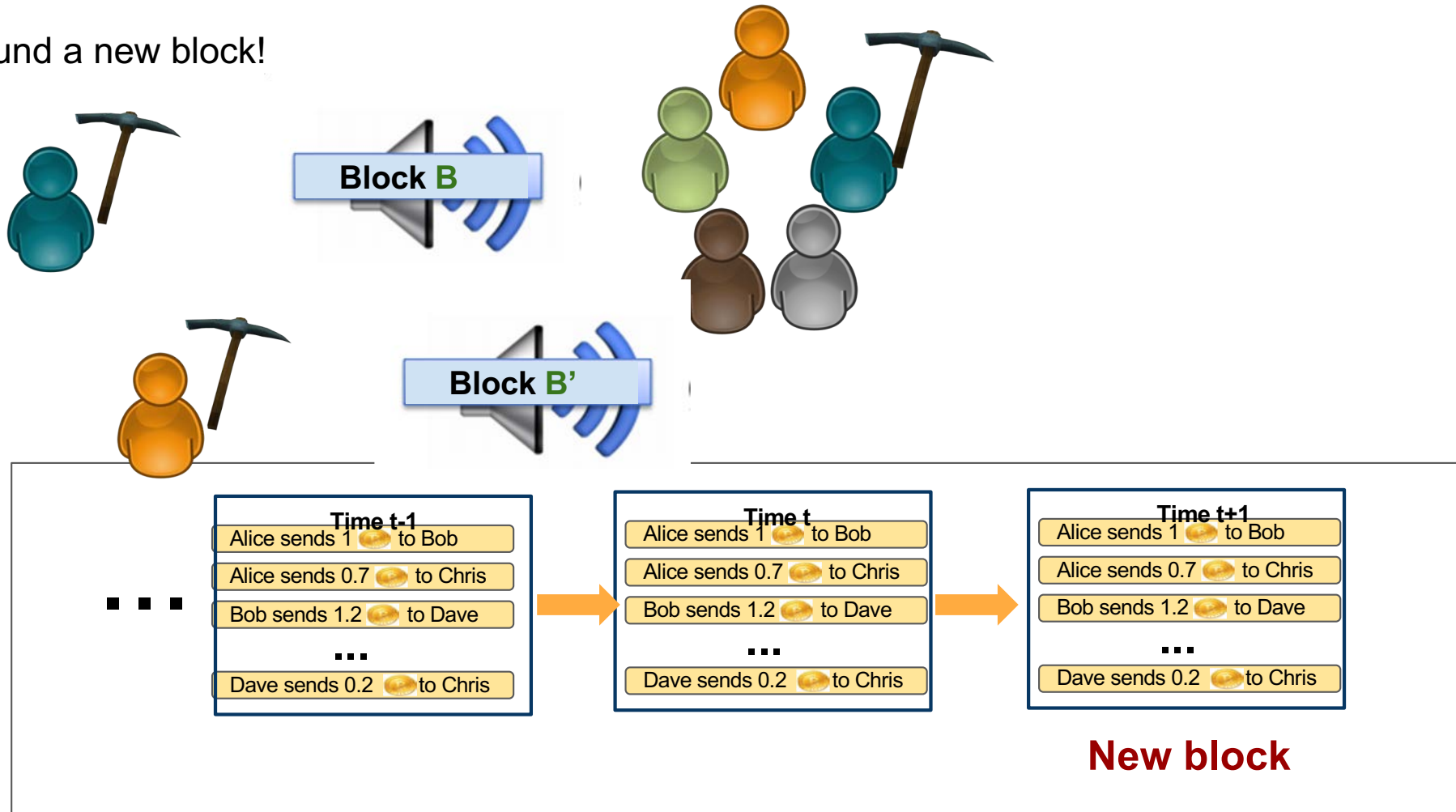
Creating a new block

I found a new block!



Creating a new block

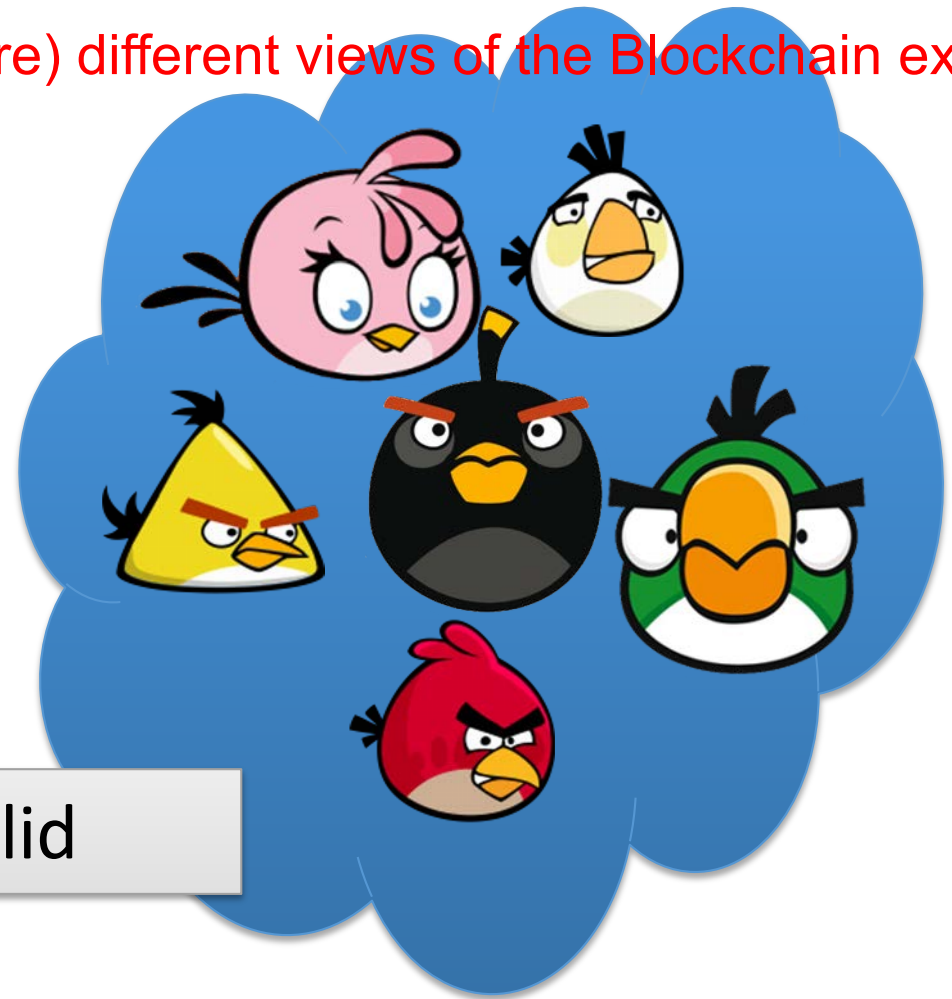
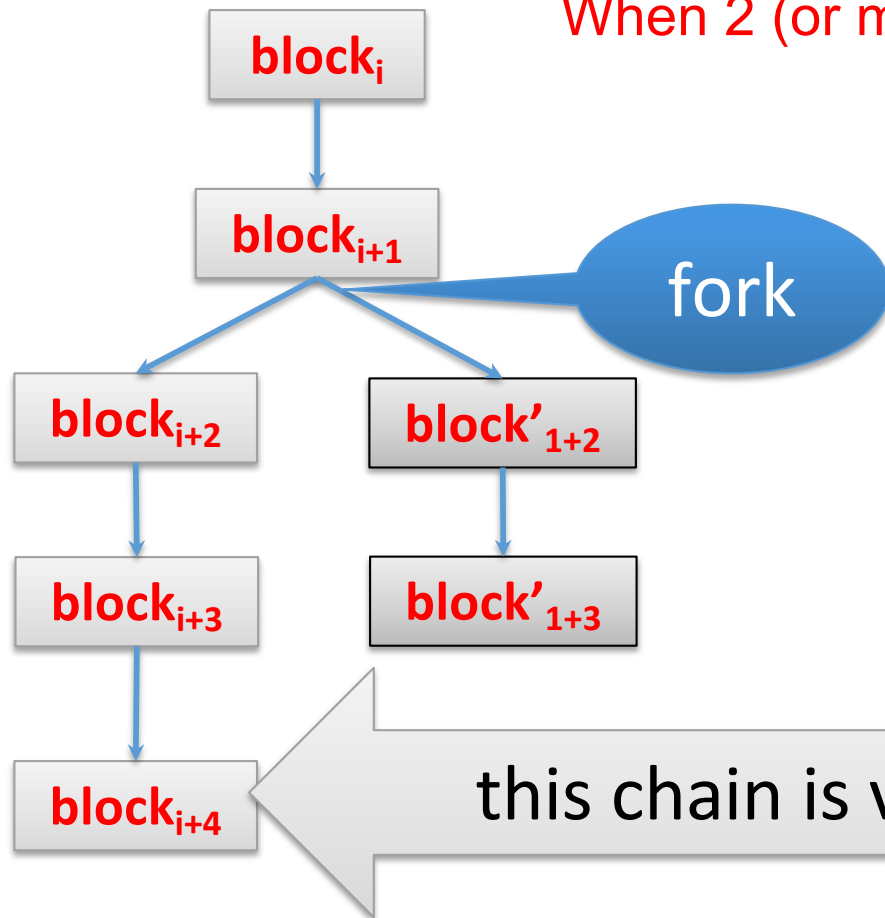
I found a new block!



What if there is a “fork”?

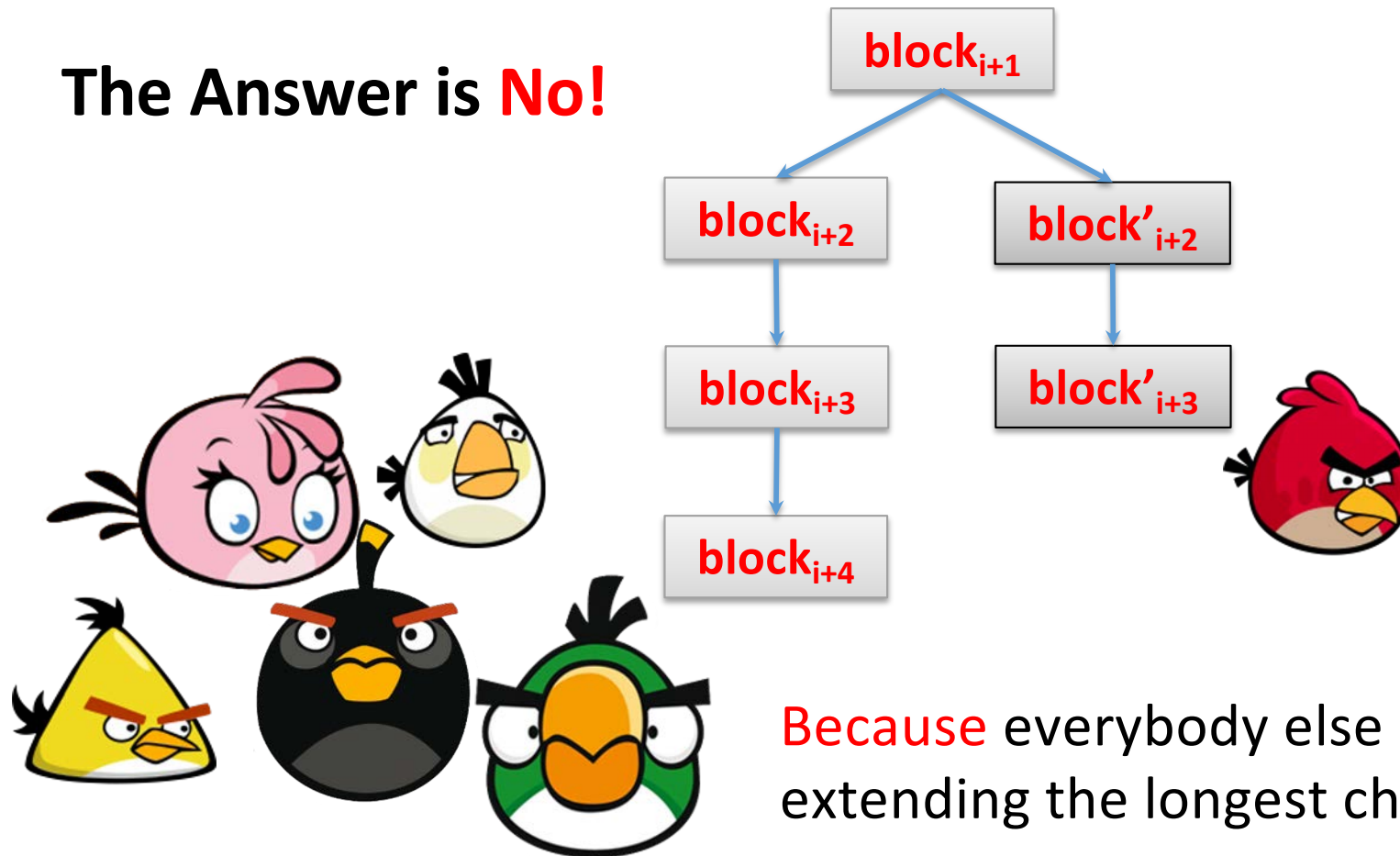
Rule: Only the “**longest**” chain counts.
But how long ? (more later)

When 2 (or more) different views of the Blockchain exist



Does it make sense to “work” on a shorter chain?

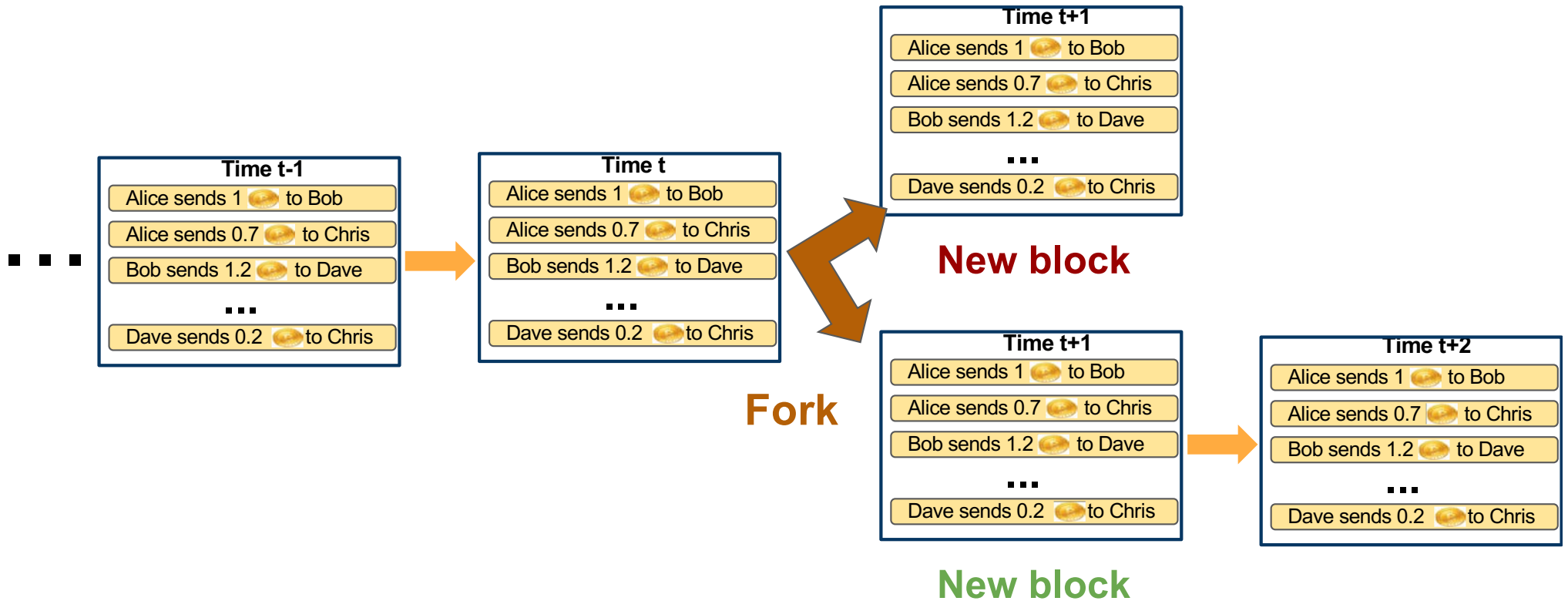
The Answer is **No!**



Because everybody else is working on extending the longest chain.

Recall: we assumed that the majority follows the protocol.

Rule: Longest chain wins



Consequences

The system should quickly **self-stabilize**.

If there is a fork then one branch will quickly die.

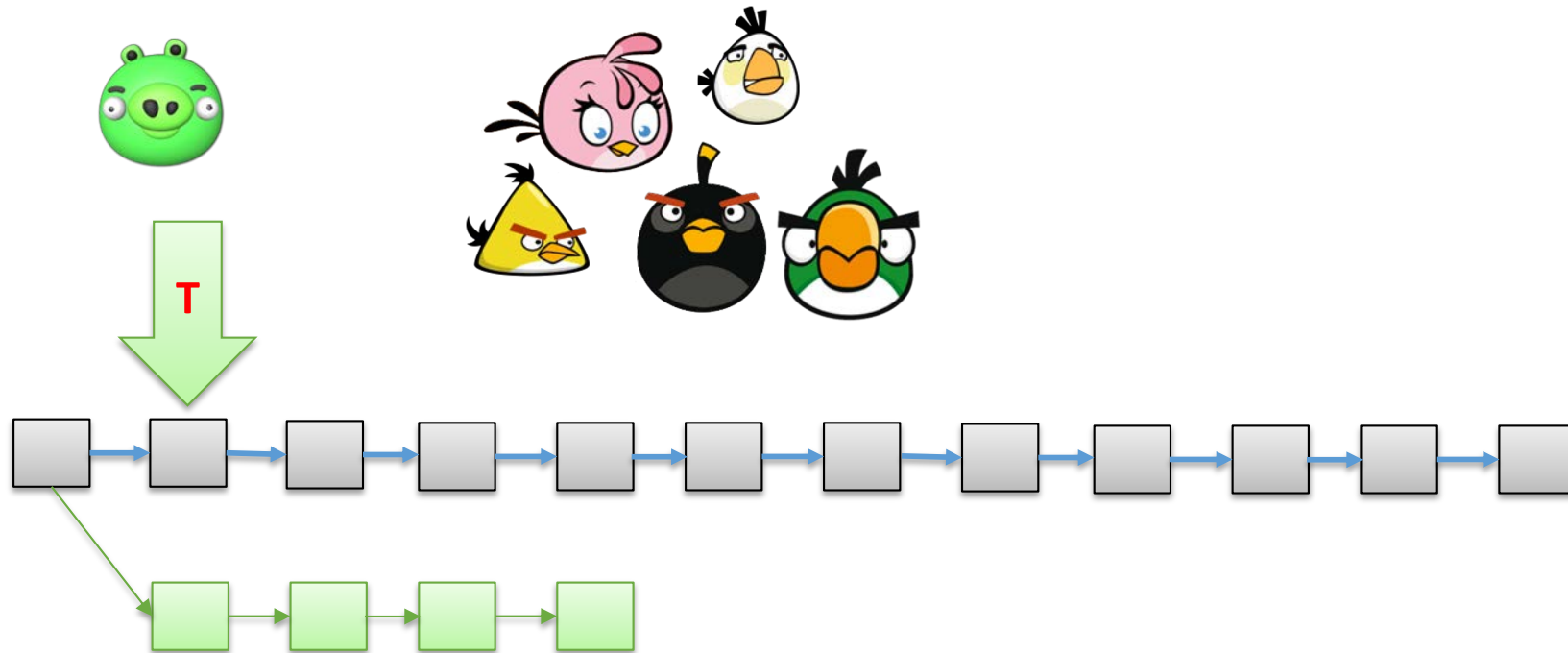
Problem: what if your transaction ends up in a “dead branch”?

Recommendation: to be sure that it doesn't happen **wait 6 blocks**.



≈ 1 hour

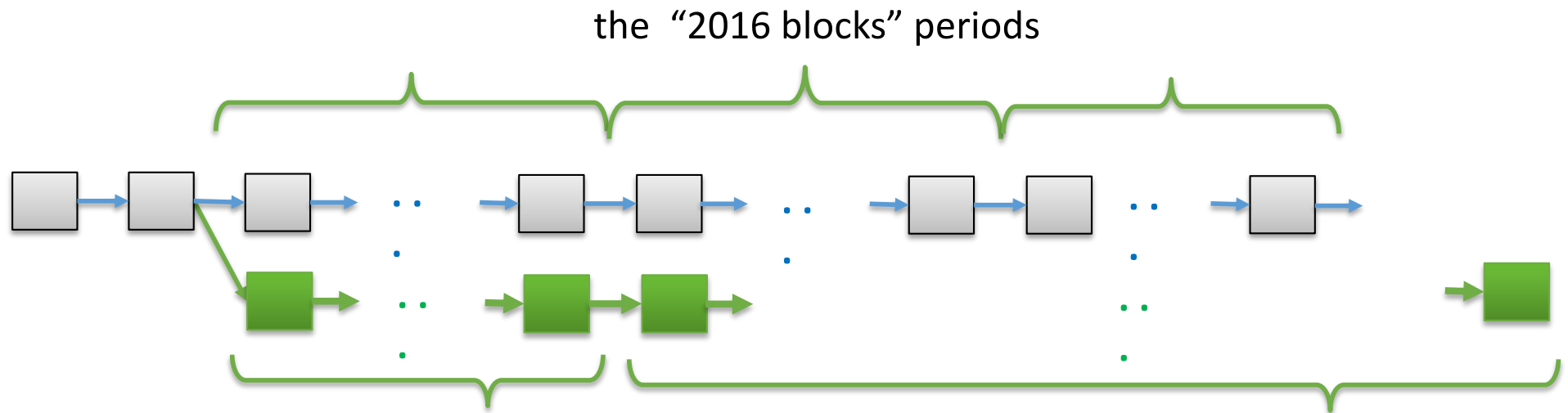
Can transactions be “reversed” ?



To reverse a transaction, an adversary has to create a “fork in the past”. This looks very hard if he/she has a minority of computing power (the honest miners will always be ahead of him).

It gives the security, but also a “shortcoming” of decentralization

Since hardness is adjusted thus the following attack might be possible



the adversary
forks the chain:



(1)
he computes (secretly)
another chain with
fake time-stamps
(indicating that it took
a lot of time to
produce it)

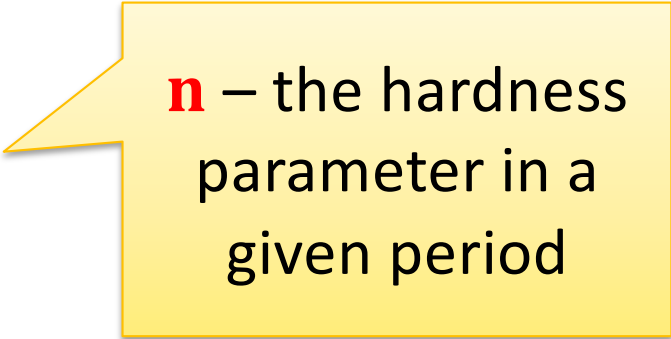


(2)
the difficulty drops
dramatically, so he
can quickly produce a
chain longer than the
valid one, and publish
it.

Therefore

In Bitcoin it's not the **longest chain** but the **strongest chain** that matters.

The **strength of each block** is 2^n .



n – the hardness parameter in a given period

The **strength of the chain** is the sum of hardnesses of each block in it.

How are the miners incentivized to participate in this game?

Short answer: they are paid (in Bitcoins) for this.

Can I become a Bitcoin miner ?

Yes, but it is very competitive and capital intensive ! =>
Gang-up together can help



Special hardware



Huge mining pools

Where does the money (reward) come from?

A miner who finds a new block gets a “reward” in **BTC**:

≈ 4 years

- for the first **210,000** blocks: **50 BTC**
- for the next **210,000** blocks: **25 BTC**
- for the next **210,000** blocks: **12.5 BTC**,

and so on...

Was here between July 2016 to May 13, 2020
Most recent Reward-Drop ETA date: May 13, 2020

Note: $210,000 \cdot (50 + 25 + 12.5 + \dots) \rightarrow 21,000,000$

This is how it looks in detail

“generation transaction”

“coinbase”

Transaction ²	Fee ²	Size (kB) ²	From (amount) ²	To (amount) ²
0ac34c9949...	0	0.173	Generation: 25 + 0.05974785 total fees	1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY: 25.05974785
2055f19a51...	0.0002	0.259	1Kpv8JEcWLhUqi4q8dnrwxiaZPKL4KUoeR: 179.9998	1HCukLGfkCfKCryXT73hj2SyVAC9kzRGkC: 105 15zBXYeXbtJ5xs48arouP7BHQ4AQ5xfZa: 74.9996
66815aff01...	0.001	0.258	1dice6DPtUMBpWgv8i4pG8HMjXv9qDJWN: 0.35	15GPjviasjMD8QJvMTs5qYsB8wtQLQGBtP: 0.00175 1HZHBnH2FbHNWieMxAh4xBPfgfuxW15UPt: 0.34725

More details

Each block contains a transaction that **transfers the reward** to the miner.

Advantages:

1. It provides **incentives** to be a miner.
2. It also makes the miners interested in **broadcasting new block** asap.

This view was challenged in a recent paper:

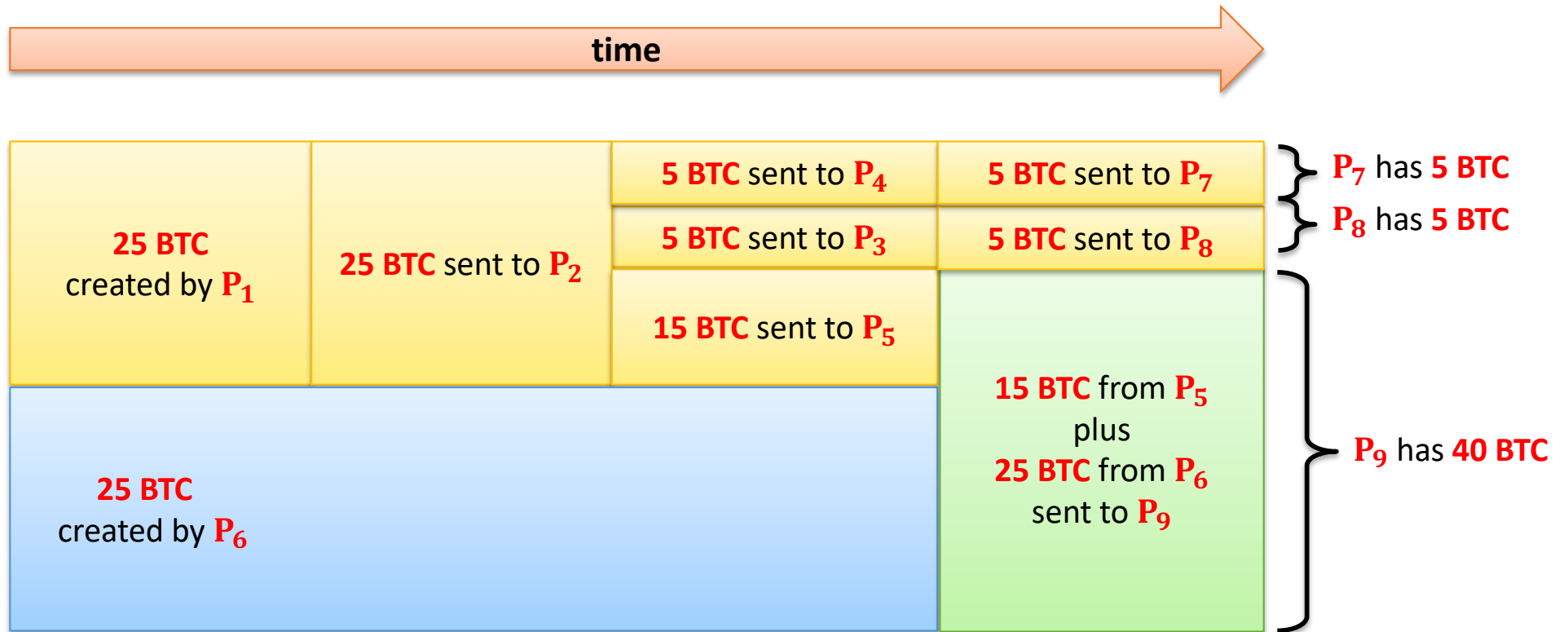
Ittay Eyal, Emin Gun Sirer

Majority is not Enough: Bitcoin Mining is Vulnerable

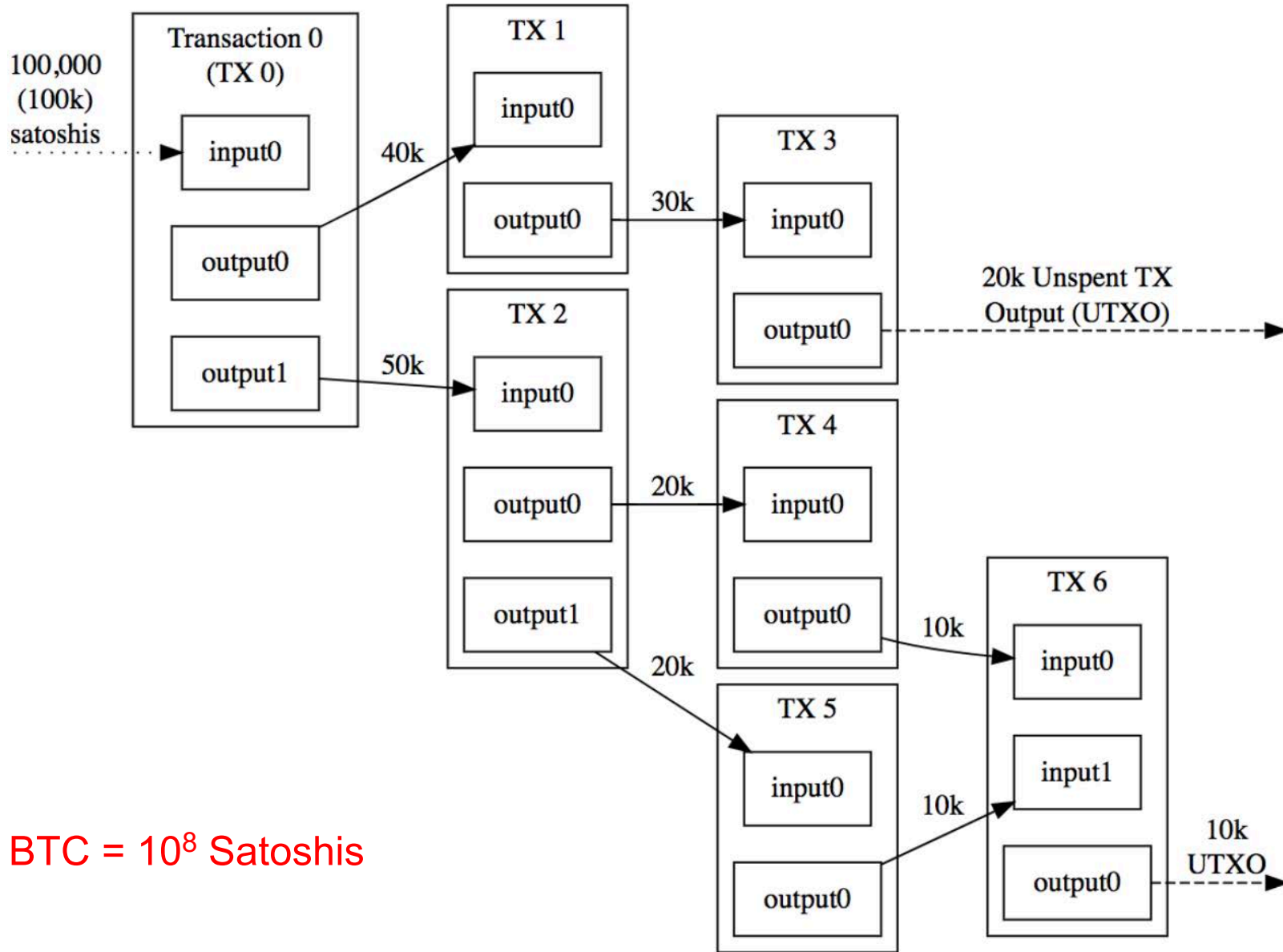
Bitcoin's money mechanics

Bitcoin is “transaction based”.

Technically: there is no notion of a “coin” in Bitcoin.



The Unspent Transaction Outputs (UTXOs) model



1 BTC = 10^8 Satoshis

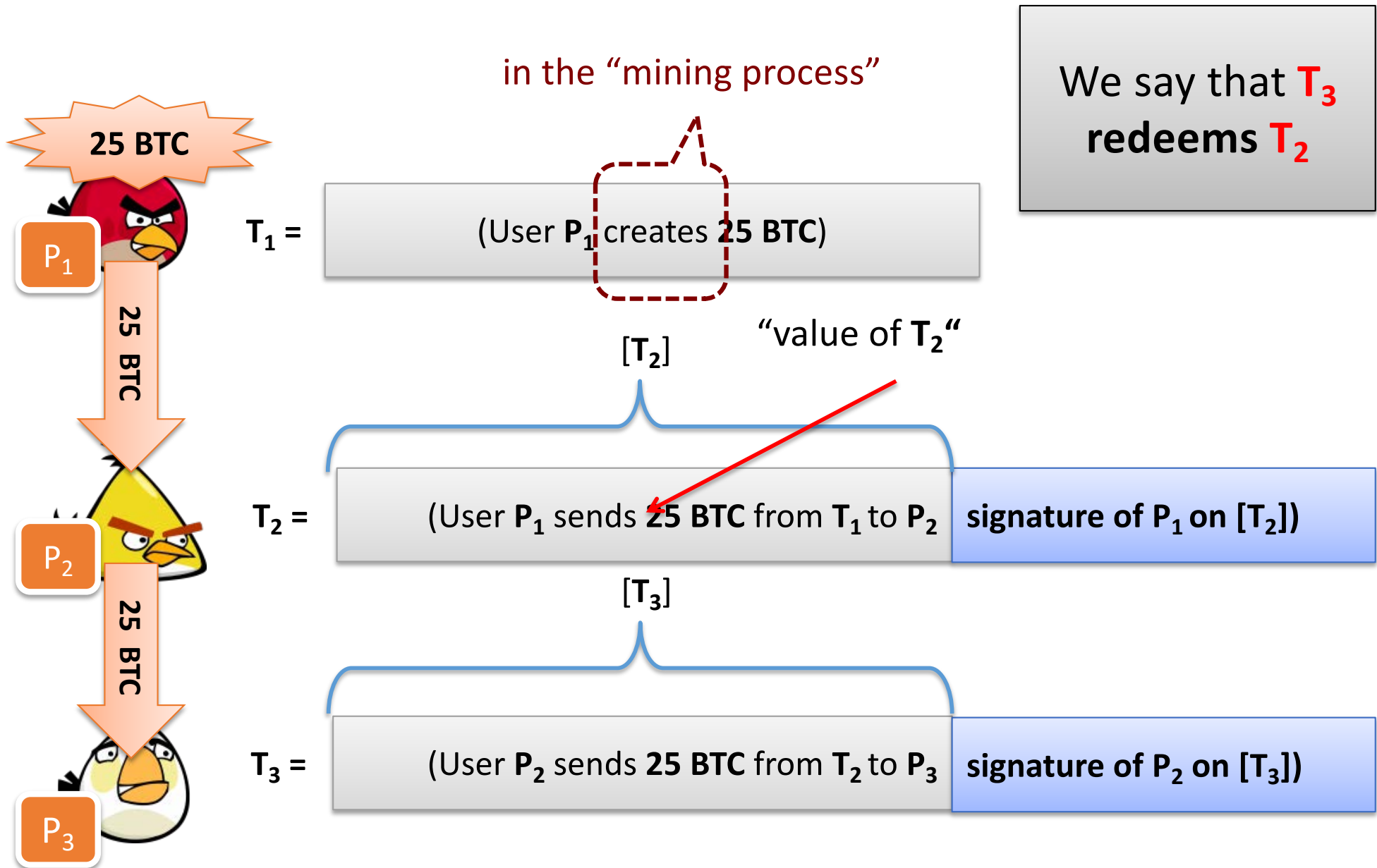
Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Note: Sum of UTXOs input to a transactions = Sum of UTXOs output from a transaction + Fees

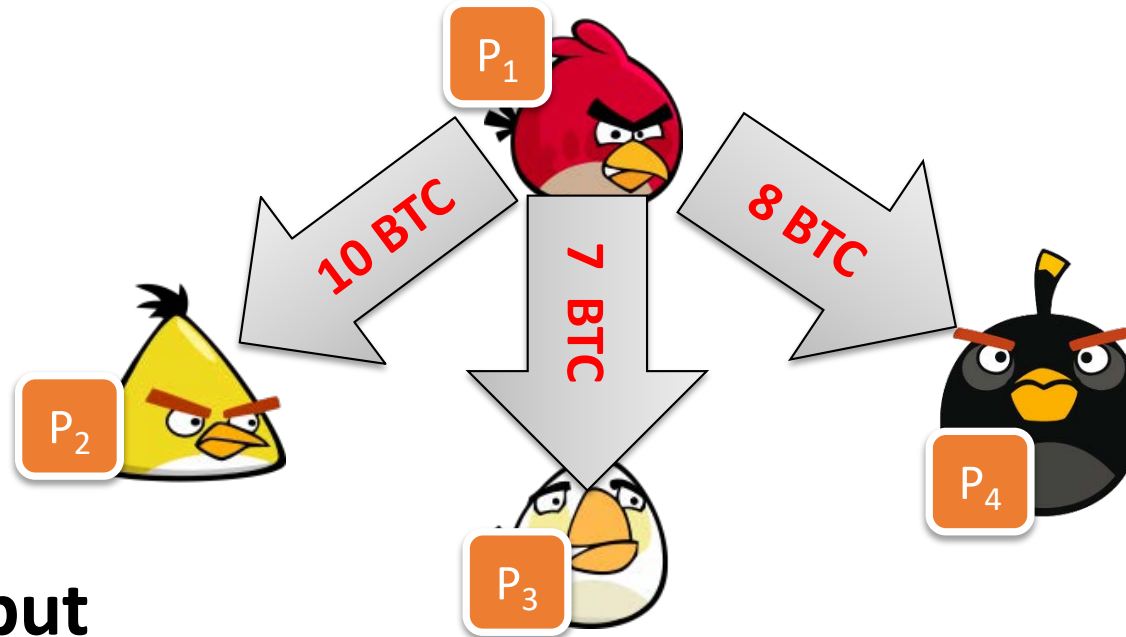
The Unspent Transaction Outputs (UTXOs) model

- In Bitcoin, each transaction spends *Output from prior transactions (aka UTXO) as input of the current transaction* and generates **new** (Unspent) Transaction Outputs that can be spent by the owner in the future.
transactions
- A user's wallet is responsible for keeping track of a list of UTXOs associated with **all addresses (public keys)** owned by the user.
- When the user wants to spend some Bitcoins, e.g. to pay for something, the wallet is responsible to use *one or more* of the user's existing UTXOs to cover the bill and may receive some *change* back (in form of **new UTXOs**).
- Each UTXO can only be spent once, since, once spent, this UTXO is removed from the pool.
- The current set of UTXOs (i.e. all UTXOs in the world) are kept by each participating node in a full-synchronized manner.
- The UTXO model enables more scalable operations as it allows multiple UTXOs to be processed in a parallel manner.
- The UTXO model also enhances privacy (not complete anonymity) as users can use new addresses (public key) for each transaction (to receive the "change" in a transaction in form of new UTXOs

Transaction syntax – simplified view



How to “divide money”?



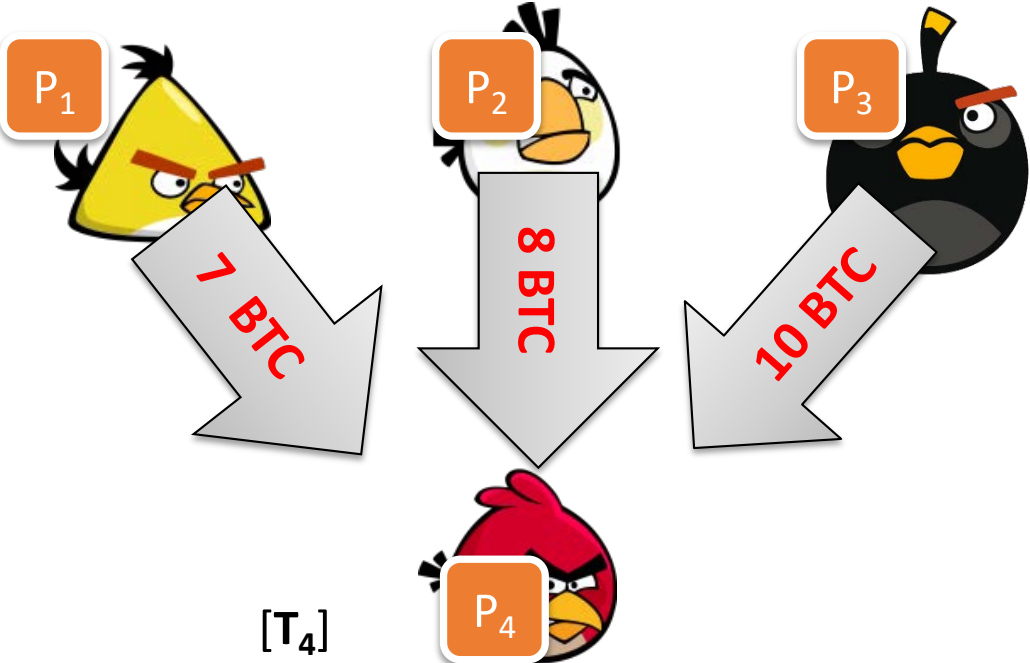
Multi-output
transactions:

$T_2 =$ $[T_2]$

(User P_1 sends 10 BTC from T_1 to user P_2 ,
User P_1 sends 7 BTC from T_1 to user P_3 ,
User P_1 sends 8 BTC from T_1 to user P_4)

signature of P_1 on $[T_2]$

Multiple inputs



T₄ =

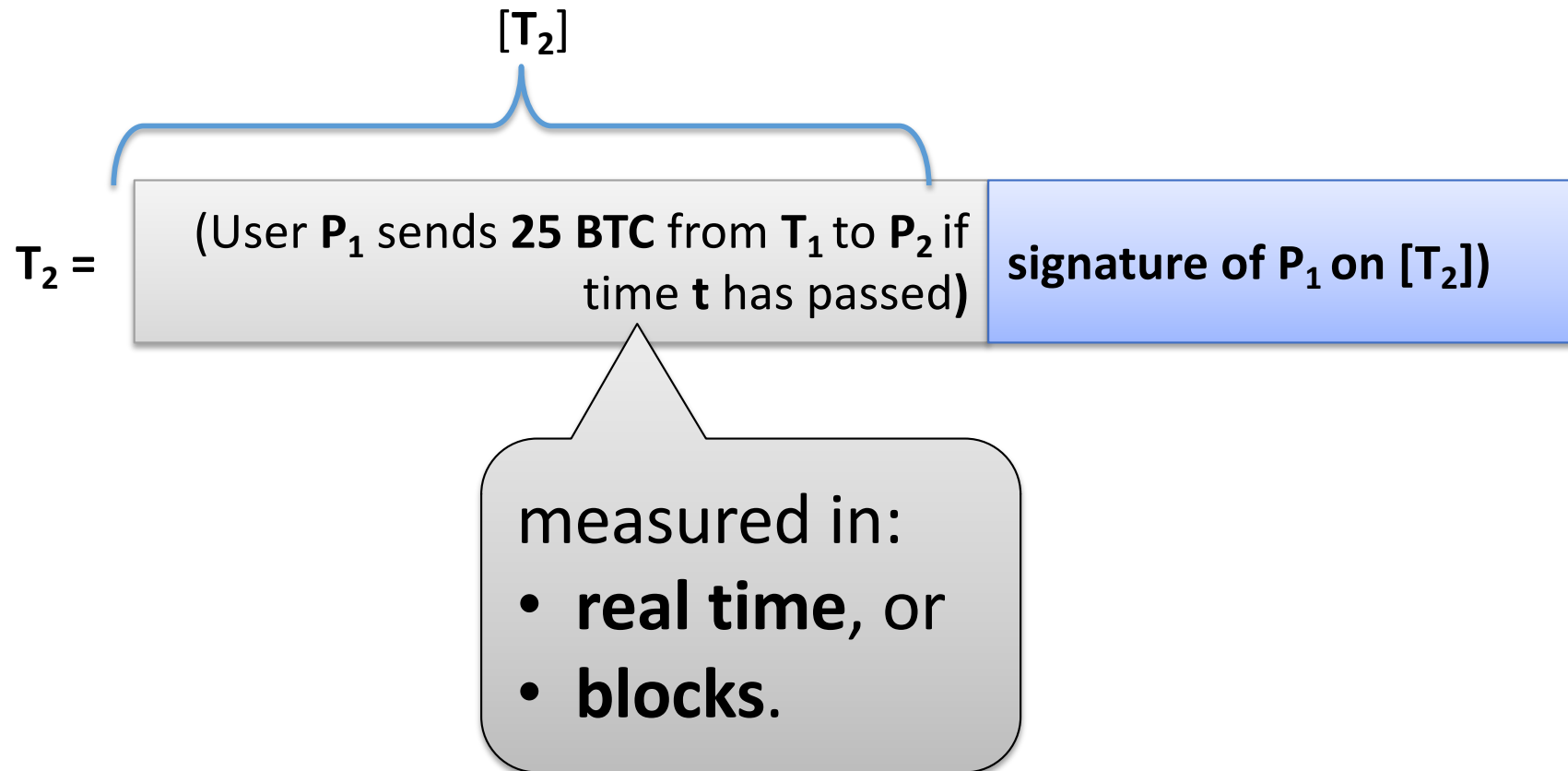
(User P₁ sends 10 BTC from T₁ to user P₄,
User P₂ sends 7 BTC from T₂ to user P₄,
User P₃ sends 8 BTC from T₃ to user P₄)

signature of P₁ on [T₄],
signature of P₂ on [T₄],
signature of P₃ on [T₄])

all signatures need to be valid!

Time-locks

It is also possible to specify time **t** when a transaction becomes valid.



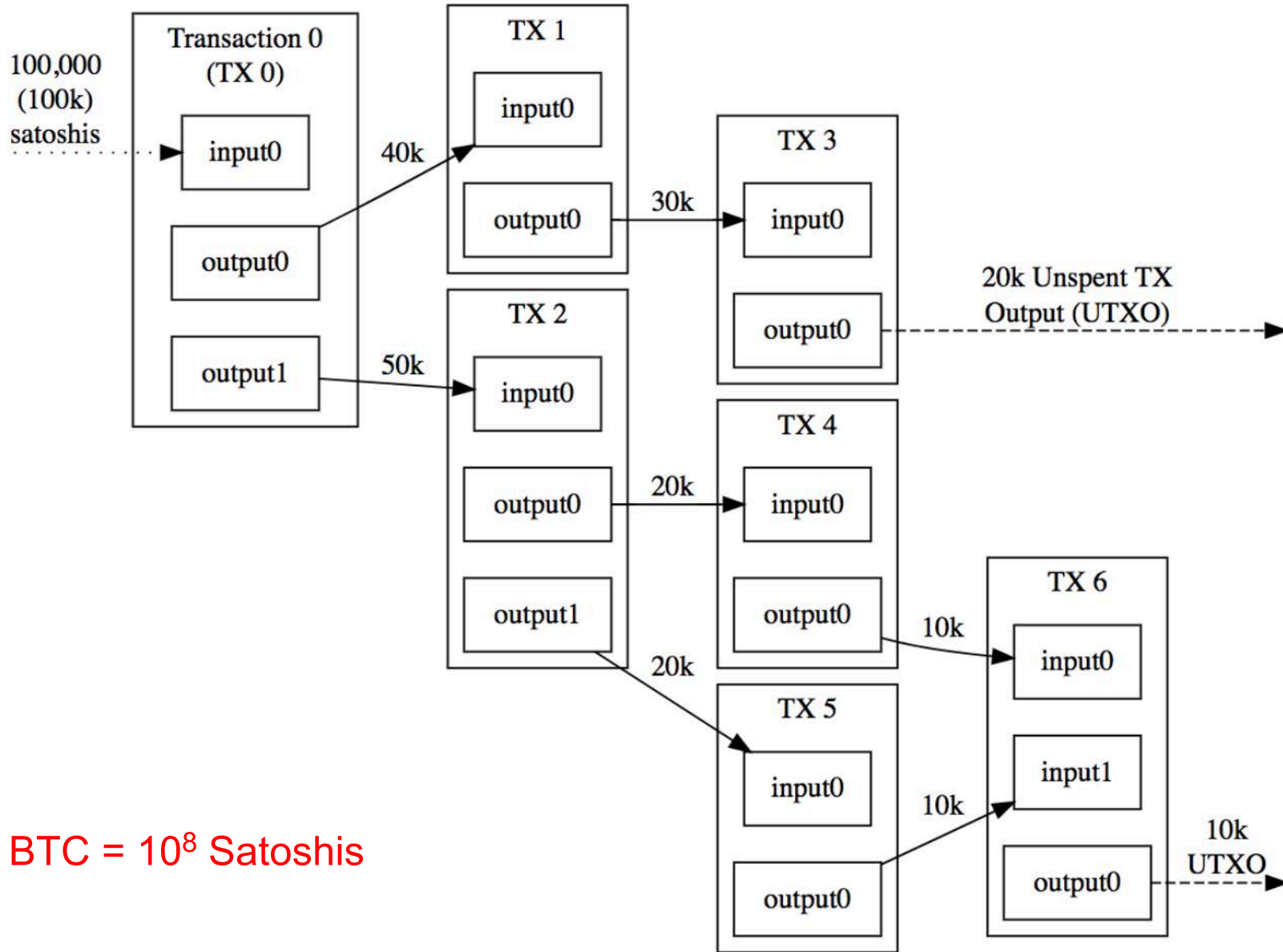
Generalizations

1. All these features can be combined.
2. The total value of **in-coming transactions** can be larger than the value of the **out-going transactions**.

(the difference is called a “**fee**” and goes to the miner)

1. The condition for redeeming a transaction can be more general (the so-called “**strange transactions**”)

The Unspent Transaction Outputs (UTXOs) model



1 BTC = 10^8 Satoshis

Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Note: Sum of UTXOs input to a transactions = Sum of UTXOs output from a transaction + Fees

Transaction-based Ledger similar to that of Bitcoin

1	Inputs: \emptyset Outputs: 25.0→Alice	
2	Inputs: 1[0] Outputs: 17.0→Bob, 8.0→Alice	SIGNED(Alice)
3	Inputs: 2[0] Outputs: 8.0→Carol, 9.0→Bob	SIGNED(Bob)
4	Inputs: 2[1] Outputs: 6.0→David, 2.0→Alice	SIGNED(Alice)

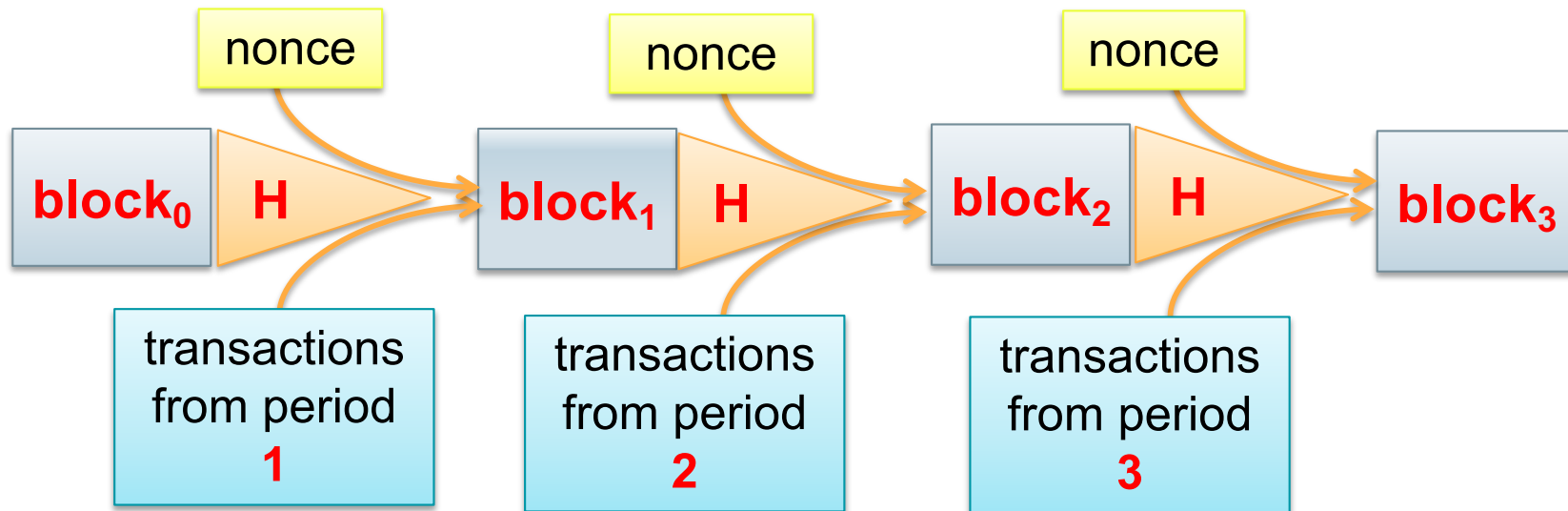
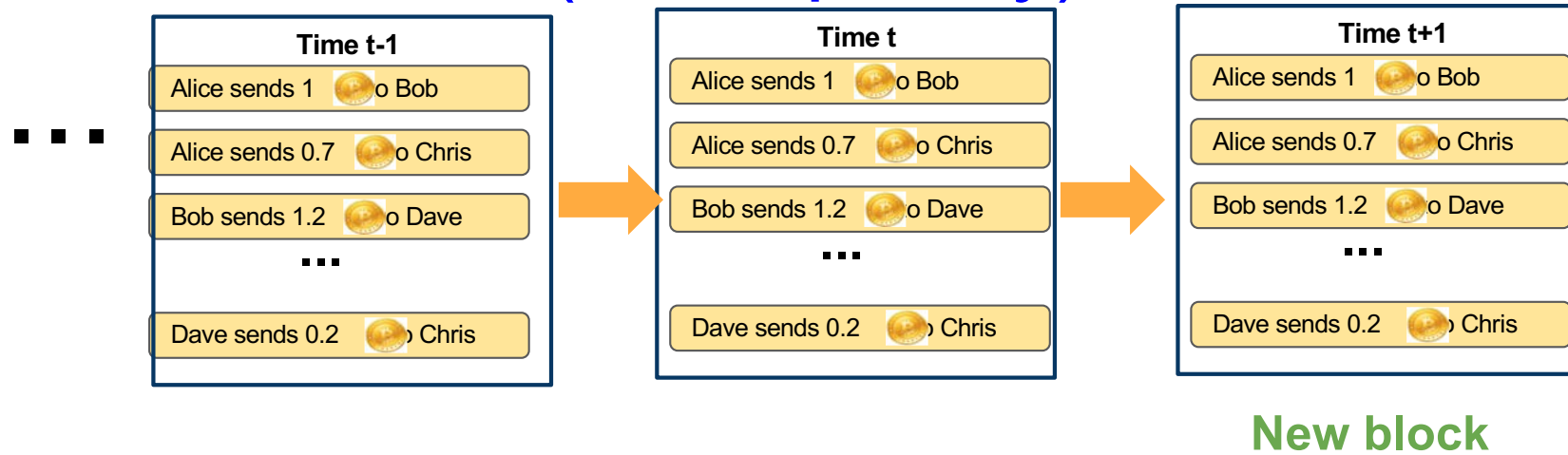
An actual Bitcoin Transaction



For another example, see:

<https://www.blockchain.com/btc/tx/9ac80e922402c01b23d46d10a07389eecffb27056e2759f3dfe259bc7a7a6d50?page2=2>

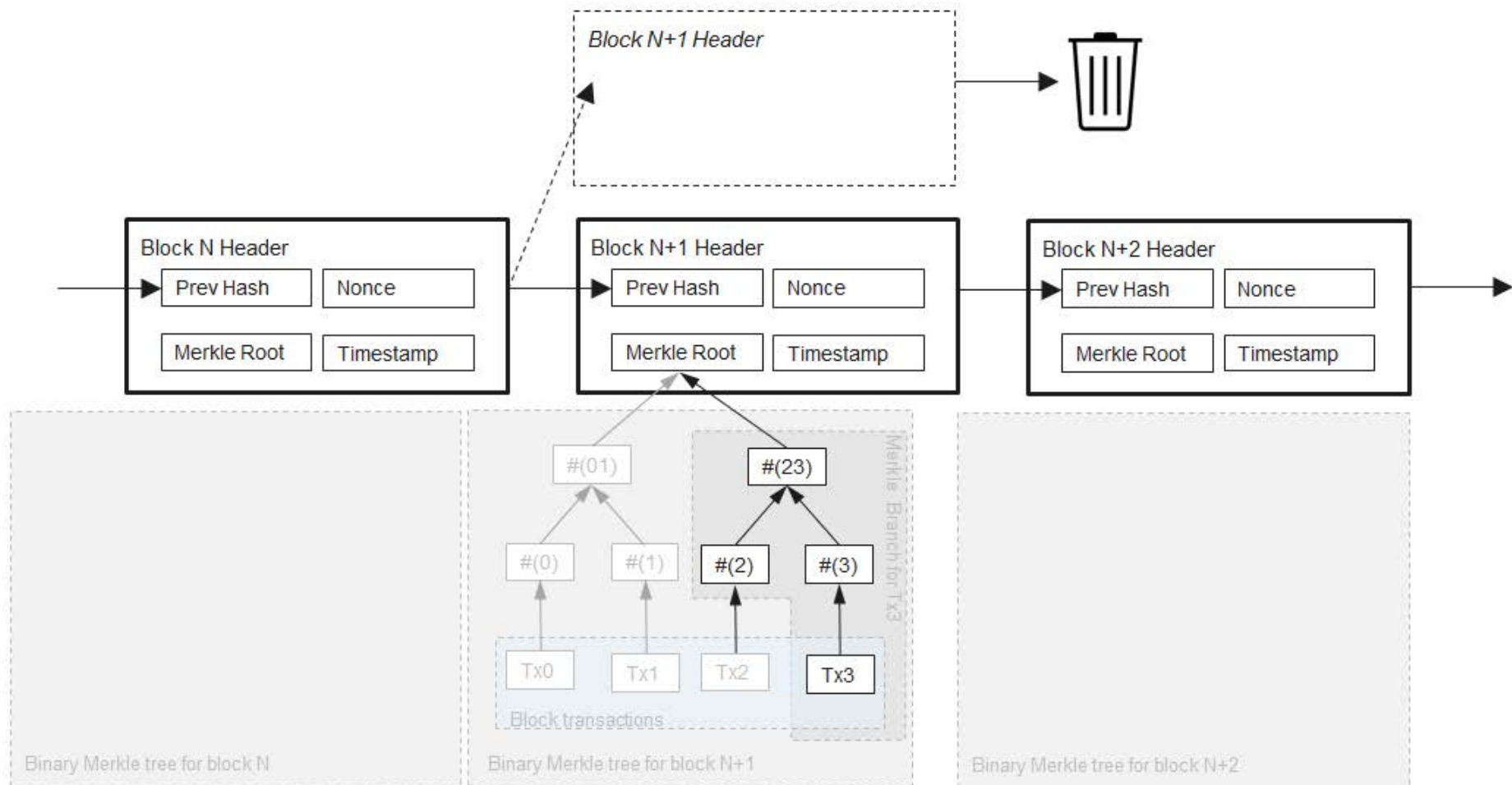
Recap: How the Bitcoin Blockchain looks like (conceptually):



H – hash function

more concretely in Bitcoin: **H** is **SHA256**.

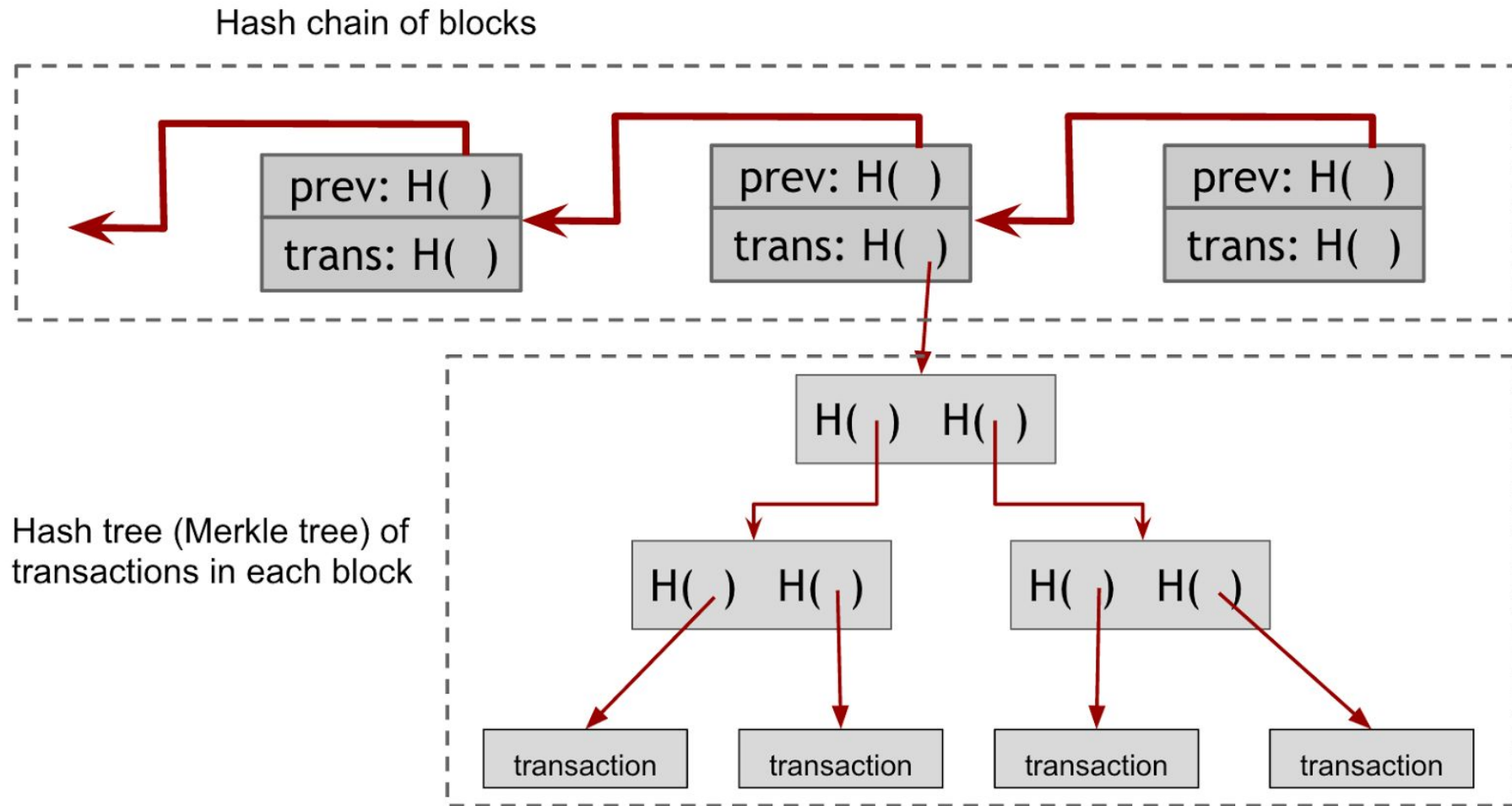
Actual data-structure of the Bitcoin Blockchain



Source: <https://ethereum.stackexchange.com/questions/268/ethereum-block-architecture>

Note: The actual Bitcoin blockchain contains two different hash structures. The first is a hash chain of blocks that links the different blocks to one another. The second is internal to each block and is a Merkle Tree of transactions within the blocks.

Actual data-structure of the Bitcoin Blockchain



Note: The actual Bitcoin blockchain contains two different hash structures. The first is a hash chain of blocks that links the different blocks to one another. The second is internal to each block and is a Merkle Tree of transactions within the blocks.

Mining pools

Miners create cartels called

the mining pools

This allows them to reduce the variance of their income.

Note:

The **total hashrate** of the
Bitcoin system as of 5.11.2014

$$\frac{283,494,086 \text{ GHash / s}}{1,700 \text{ GHash / s}} \approx 166,761 = 3.17 \cdot \underbrace{(365 \cdot 24 \cdot 6)}_{\text{number of blocks in 1 year}}$$

The **hashrate of the Achilles Labs AM-1700
miner** (1095 USD)

The user has to wait on average over **3 years** to mine a block
(**even if the difficulty does not increase!**)

Big picture

The mining pools are **operated centrally** or are designed in a **p2p** way.

Some of the mining pools **charge fees for their services**.

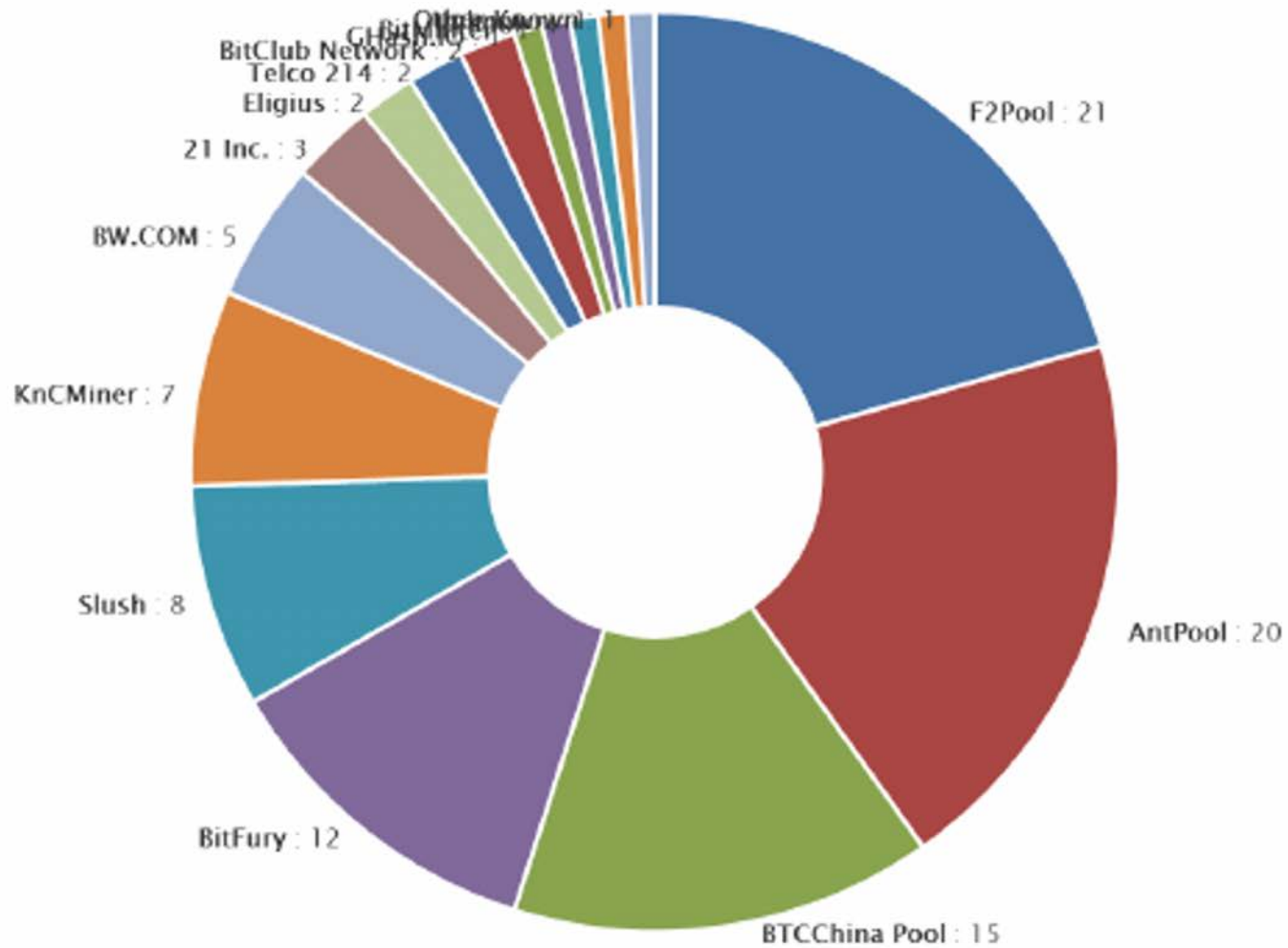
E.g. if the operator got **25 BTC** from mining then he will share
25 BTC - fee among them
(and keep the **fee** to himself)

In other words:

- the **expected revenue** from pooled mining **is slightly lower** than the expected revenue from solo mining,
- but the **variance is significantly smaller**.

Tricky part: how to prevent cheating by miners? How to reward the miners?

Popular Mining Pools



Problems with Bitcoin's Proof-of-Work (PoW)

1. **high energy consumption**



costs money



bad for
environment

2. advantageous for people with **dedicated hardware**



Some Alternatives to Proof-of-Work (PoW)

Proof-of-stake



Proof-of-knowledge

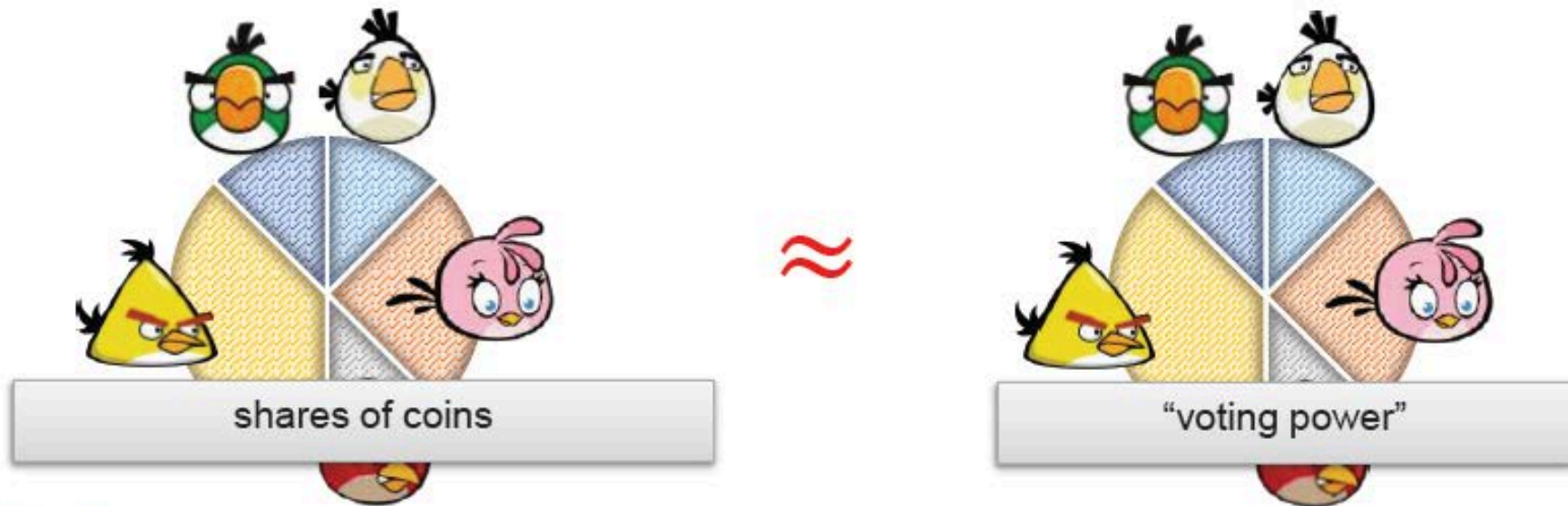


Proof-of-space*



Proof-of-Stake (PoS)

The “voting power” depends on how much money one has.



Justification: people who have the money are naturally interested in the stability of the currency.

Currencies: BlackCoin, Peercoin, NXT, etc.

• **Problem:**

1. How to **distribute initial money**?
2. How to **force coin owners to mine**?

A potential speculative attack on PoStake coins

[Nicolas Houy, It Will Cost You Nothing to 'Kill' a Proof-of-Stake Cryptocurrency, 2014]



I am going to destroy your currency by buying **> 51%** coins and gaining the voting majority

I buy the coins now (cheaply)

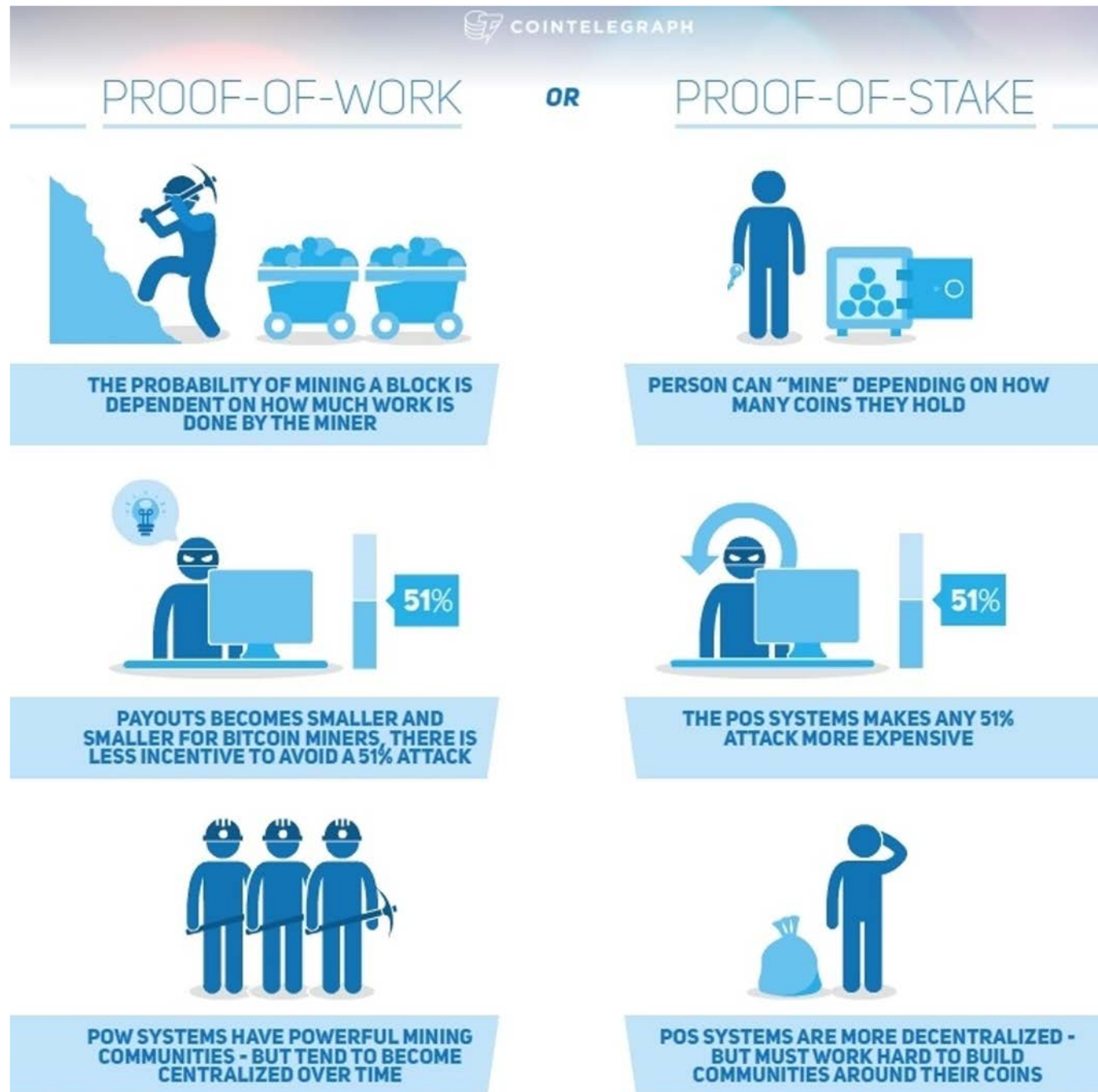
if I believe that he succeeds then I should sell at **any non-zero price**

shall I sell him my coins?

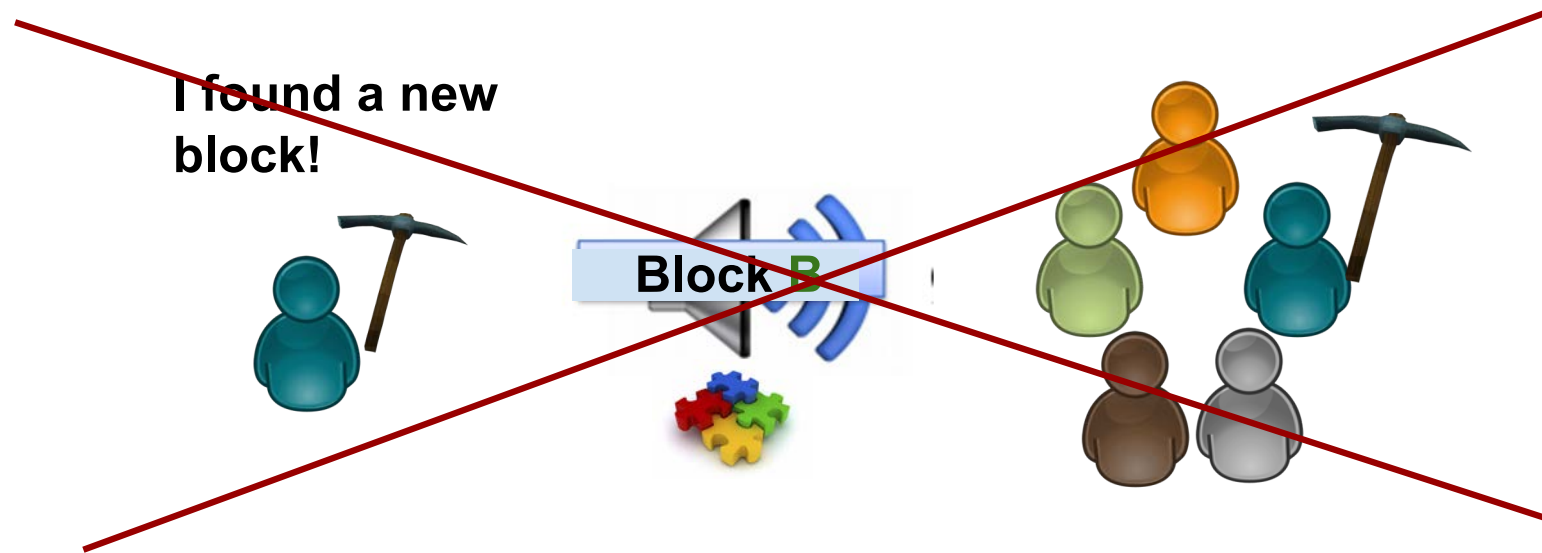
if everybody thinks this way then the coin price will quickly go close to **zero**



Proof-of-Work (PoW) vs. Proof-of-Stake (PoS)



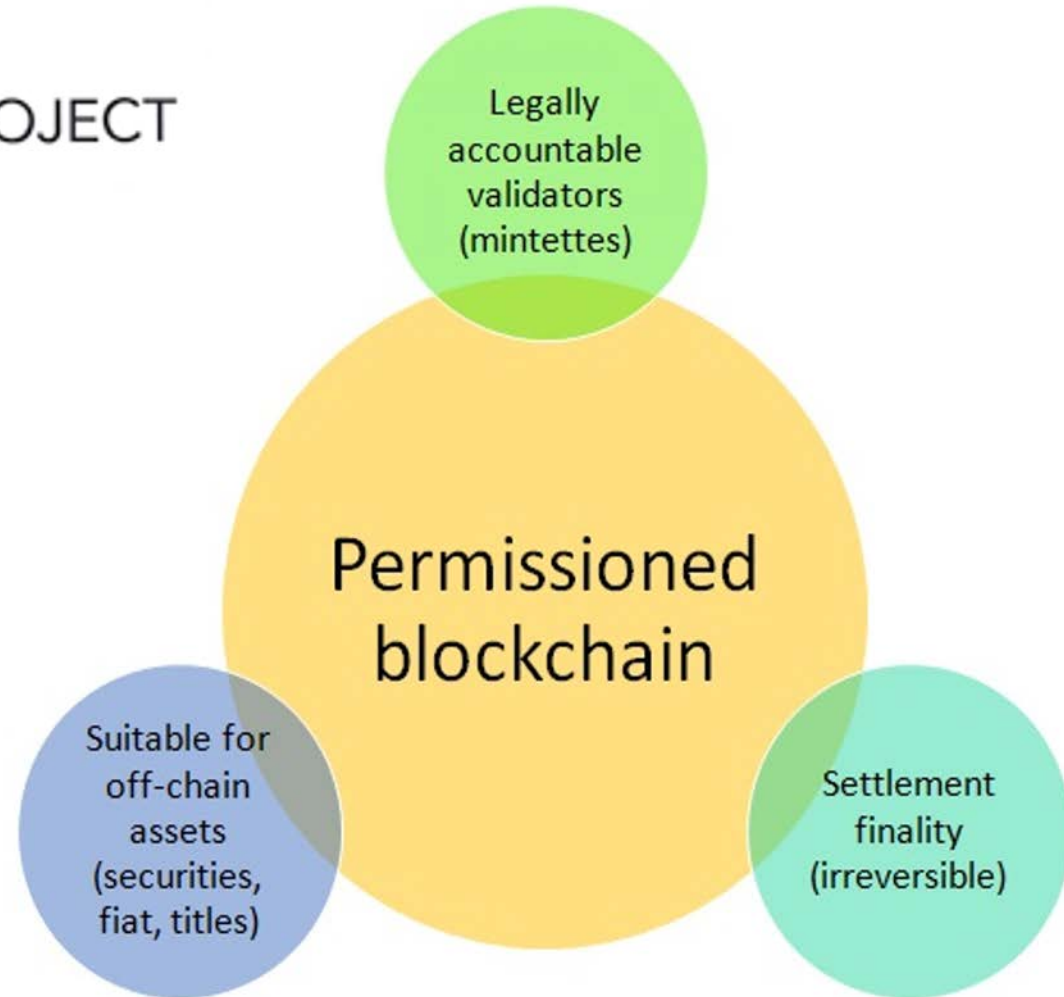
Proof of Knowledge



Proof of knowledge



HYPERLEDGER PROJECT



Conclusions

- Bitcoin can be seen as an innovative solution for the Distributed Consensus Problem, namely, to have the community to agree on the rightful owner of a piece of digital money in a **Decentralized**, and **Anonymous** way !
- Due to its fully decentralized nature, i.e. trust no one and trust no government, it is difficult for Governments and conventional Financial Institutions to regulate Bitcoin
 - ◆ It is therefore a threat to Governments' control on monetary matters
 - ◆ It has been widely used for criminal financial activities, e.g. money laundry, as ransom for blackmail, payment for various illegal trades like drug trafficking, etc.
- Consumers can easily get burnt by technical and non-technical problems/ scams/ bugs due to the lack of regulations and government overseeing.