

# **CPSC 3640/5400: Decentralized Payments, Contracts, and Finance for Humans and AI**

## **Lecture 3: Bitcoin Ledger**

---

Instructor: Prof. Fan Zhang

Yale University

Fall 2026

## Bitcoin-based Liquid Network says \$320 million withdrawn in hack

By Reuters

September 7, 2026 12:05 AM EDT · Updated September 7, 2026



- <https://mempool.space/tx/c103de95817b43f2df635ec6f35ff126ca26a7c6d20570c4b01866b2b3e69a19>

# Crypto in the news

HOME > THREATS

## Liquid Network Hackers Return Most of \$320M Bitcoin Haul

Liquid Network hackers returned 3,400 BTC after draining \$320 million from its federation wallet, but about \$47 million in Bitcoin remains outstanding.

WRITTEN BY

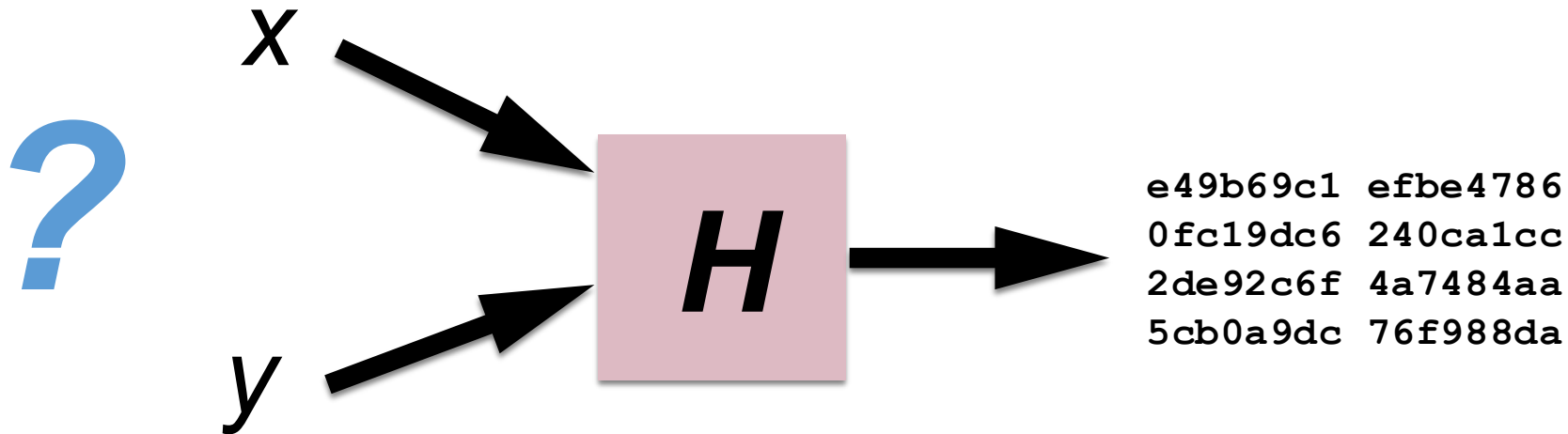


**JOSEPH OFONAGORO**

SEP 8, 2026 · 3 minute read

# Recall: Collision Resistant Hash Functions

It is hard to find  $x \neq y$  such that  $H(x) = H(y)$



- Note: Collisions must exist for any CRH (why?)
- CRH requires that **it is hard to find one**
- How hard? E.g.,  $2^{128}$  steps –  $10^{13}$  year at  $10^{18}$  steps/second, longer than universe's age

# A simple way to think about hash functions

If  $(x, y)$  is in storage,  
return  $y$ .

Otherwise, sample random  
 $y \in \{0, 1\}^{256}$ , store  $(x, y)$ ,  
return  $y$ .

An *imaginary* global  
function available to  
everyone in the world

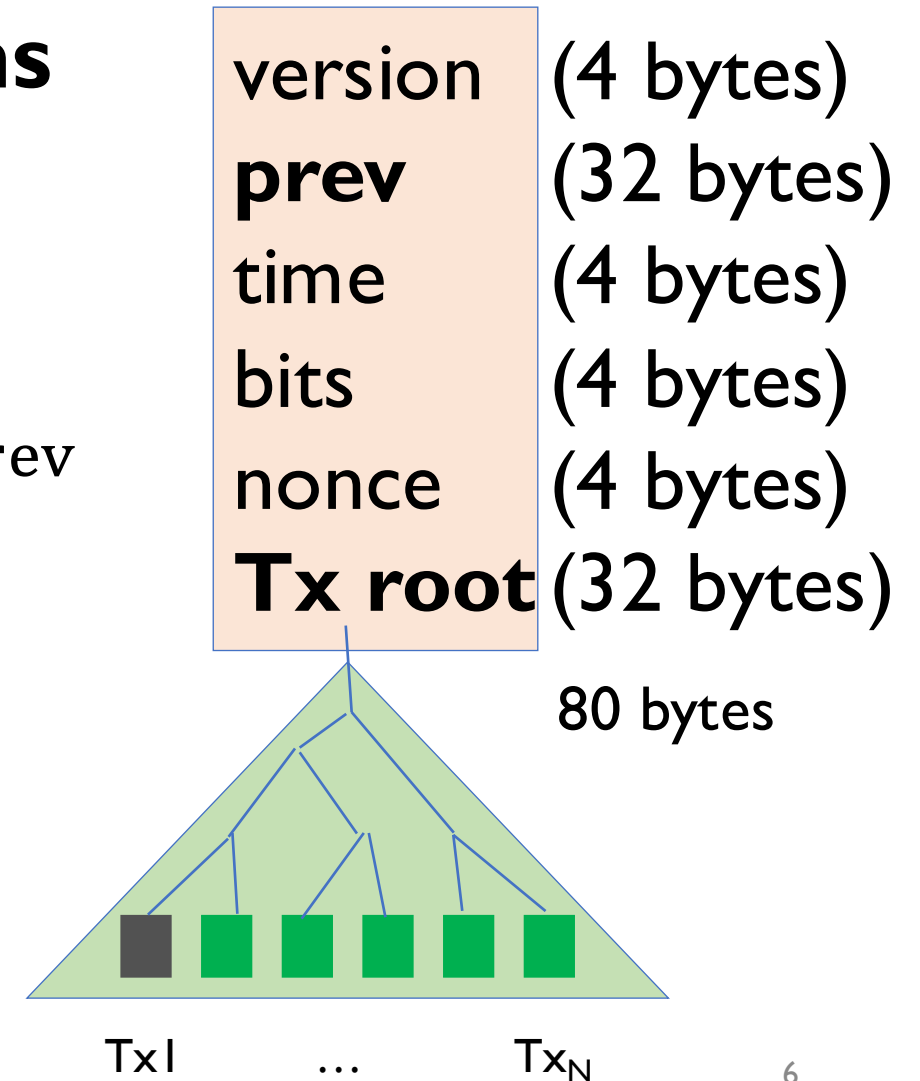
$x$

$y$

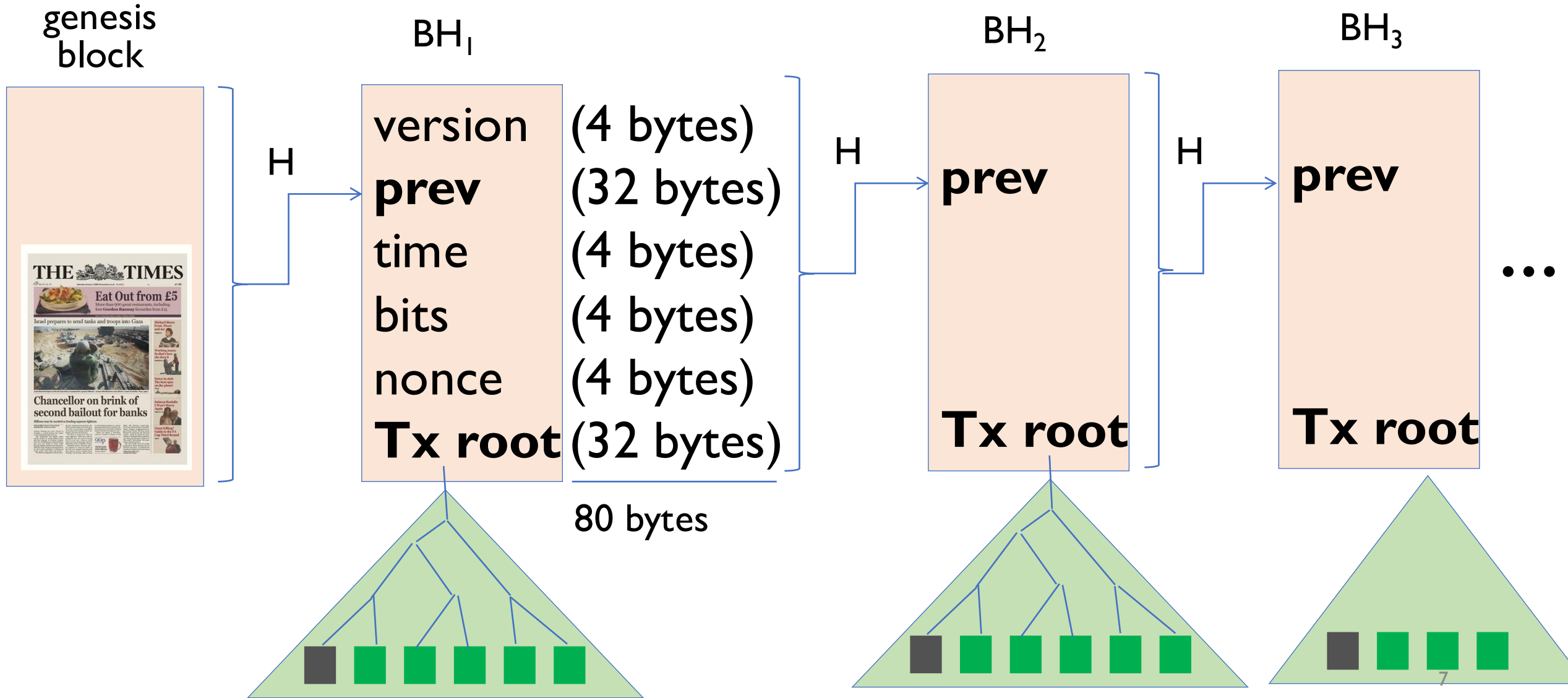
- Random Oracle model (ROM)
- RO can't be realized in practice, but real-world CRHs *come close*

# The Bitcoin ledger: chain of blocks

- Block = **header** and **transactions**
- Some important fields are
  - prev: hash of the previous block  $h_{\text{prev}}$
  - Nonce [What is nonce?]
  - Tx root [what is tx root]



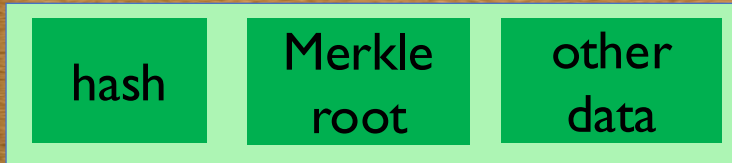
# The Bitcoin ledger : chain of blocks



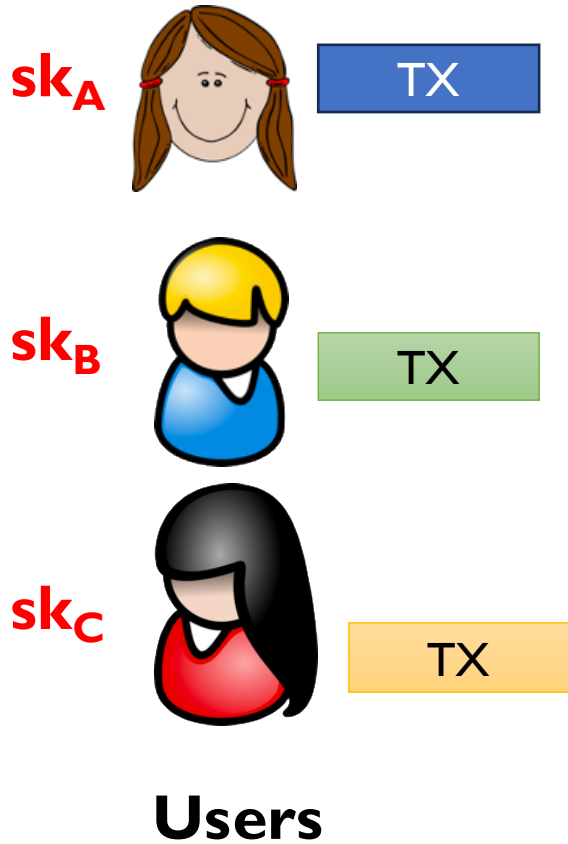
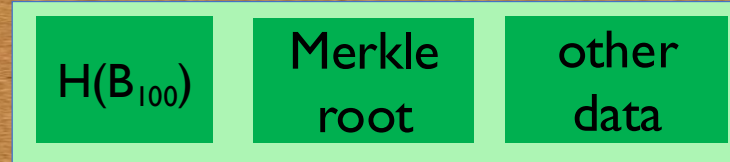
**How is a Bitcoin block  
created.**

# blockchain

Block 100



Block 101



**Miners**

block header



## Miners:

- Select, Order & Validate transactions
- Keep mining for the next block

# How is a Bitcoin block created

- This picture shows miners acting in unison, but under the hood, miners act **individually**
  - No central coordinator or global knowledge (other than genesis)
  - Each miner has a local copy of the chain
  - Messages from users and other miners may be delayed
  - anyone (literally) can be a miner
  - some miners may be malicious (e.g., not following protocol)
- Bitcoin's consensus protocol ensures that these local copies are consistent despite all these.

# How is a Bitcoin block created

Every honest miner repeatedly:

- **Set  $h_{\text{prev}}$  to the last block** (last block on the longest chain)
- **Pick a set of transactions** (up to block limit) from its *local* pending transactions, typically prioritizing higher fees.
- Builds a **block template**  $B = (h_{\text{prev}}, \text{nonce}, \text{Merkle root}, \text{txns})$
- **Search for nonce** so that  $H(B)$  has k-leading zeroes; when succeed, send B to other miners.

Block template is updated when:

Higher fee txn arrives in the mempool

Chain grows to a new tip  $h'_{\text{tip}}$

Search space is exhausted

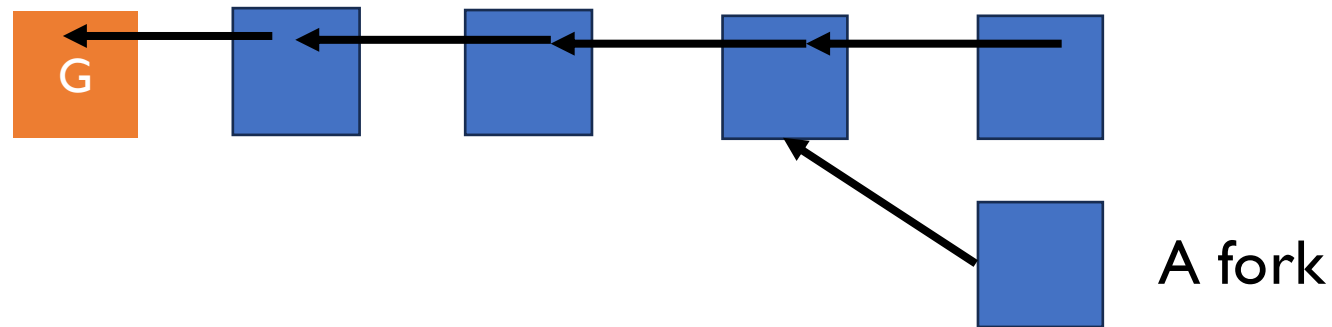
When receiving a block from other miners:

Verify PoW & all transactions

If valid, add it to the local copy of the chain

# Ideally, blocks form a chain

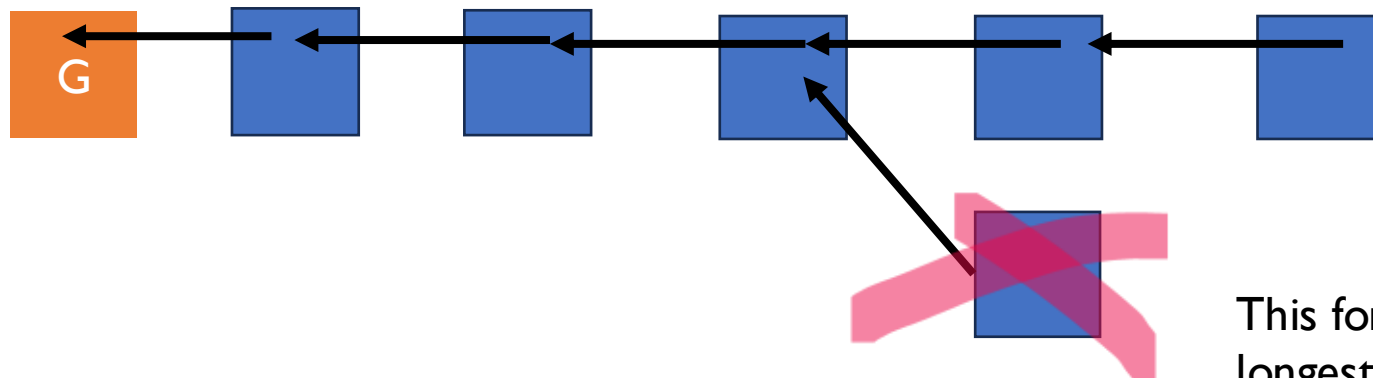
- **Genesis block G**: a special block (public knowledge)
- Invalid blocks are auto ignored by miners.
- But forks may appear **naturally** or due to **malicious reasons**



- natural reasons: e.g., two miners wins simultaneously
- malicious reasons: e.g., attacker trying to erase a TX.
- Bitcoin defends against forks using a simple **longest-chain rule**.

# Longest-chain rule

- Longest-chain rule: only follow the longest fork **[should be most-work]**
- Natural forks: the next honest miners will break the tie.
- This suggests that we must consider the last few blocks “in flux”
- For Bitcoin, it is suggested to wait for 6 confirmations.
- **Rule: a block is confirmed if a) it's on the longest chain, and b) it has at least 6 follow-ups**

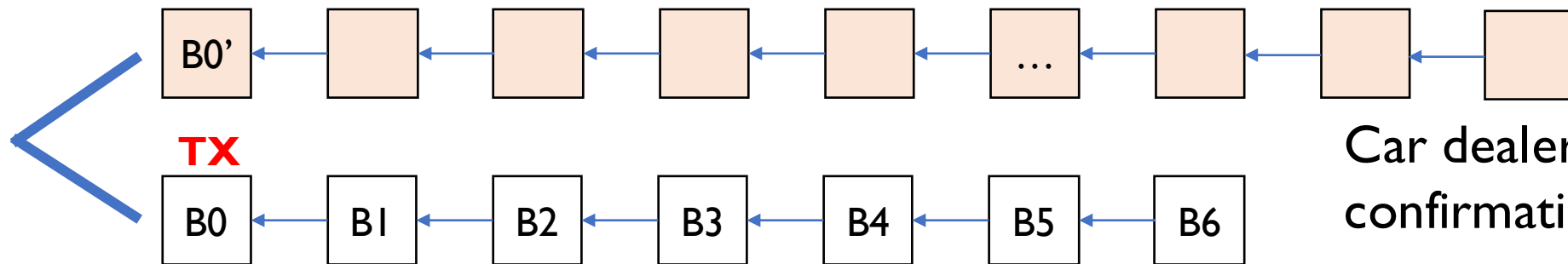


This fork will be ignored due to longest chain rule.

# Malicious forks (e.g., “private fork attack”)

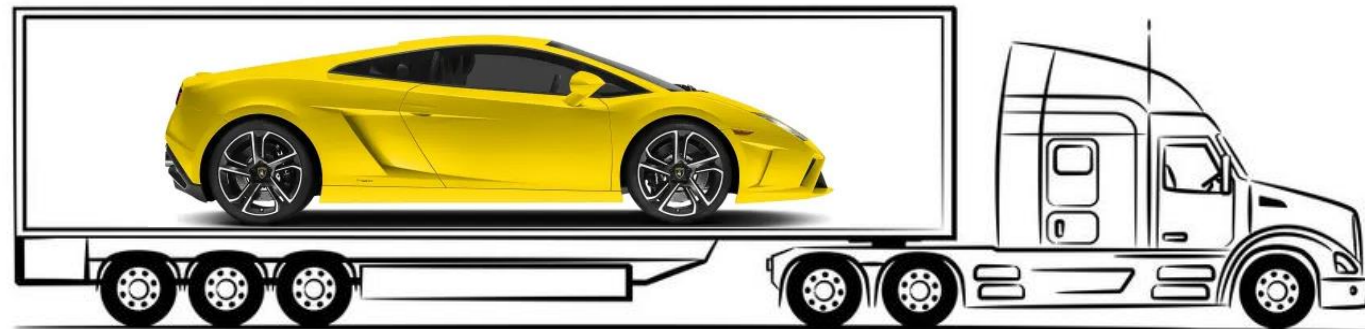
- How can an attacker get Lambo for free?

B0' is a block without **TX**.



Car dealer should wait for 6 confirmations

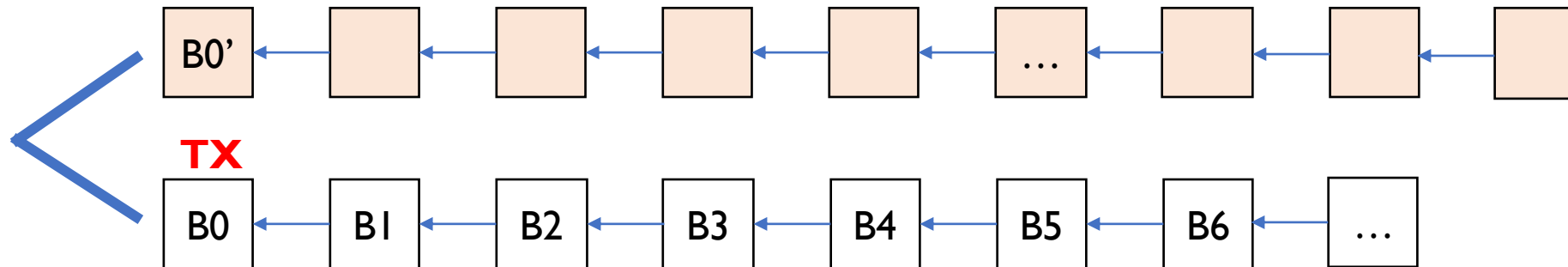
**TX** = payment for a Lambo



# Malicious forks

- An attacker who mines faster than honest miners **will certainly win**
  - Analogy: if you flip an unfair coin with  $\frac{1}{2} + \epsilon$  chance for head, you will eventually get more heads than tails.
- Translating to Bitcoin mining: If attacker has **more than 50%** hash power, it eventually can revert confirmed transactions (no matter how large K is).
- Is Bitcoin secure if attacker has **less than 50%** hash power?

B0' is a block without **TX**.



# Bitcoin's security guarantees

## Bitcoin's Security Guarantee:

Assuming malicious miners have  $< 50\%$  hash power, confirmed transactions cannot be reverted except for a small probability that decreases exponentially in  $K$ .

## Remarks:

- Very interesting and *unusual* (e.g., when compared with banks)
- Proving this is non-trivial. Need to consider all attacks, not just private attack which is just one possible attack.
  - Satoshi's original paper has an incomplete proof.

# PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

[Learn More](#)

| Name                        | Symbol | Market Cap | Algorithm | Hash Rate    | 1h Attack Cost | NiceHash-able |
|-----------------------------|--------|------------|-----------|--------------|----------------|---------------|
| <a href="#">Bitcoin</a>     | BTC    | \$1.56 T   | SHA-256   | 867,315 PH/s | \$1,934,701    | 0%            |
| <a href="#">Zcash</a>       | ZEC    | \$13.43 B  | Equihash  | 28 GH/s      | \$62,842       | 1%            |
| <a href="#">BitcoinCash</a> | BCH    | \$4.94 B   | SHA-256   | 3,821 PH/s   | \$8,525        | 0%            |
| <a href="#">Litecoin</a>    | LTC    | \$3.81 B   | Scrypt    | 3 PH/s       | \$66,887       | 7%            |

<https://www.crypto51.app/>

# Remark: Gensis block

## Bitcoin Genesis Block

### Raw Hex Version

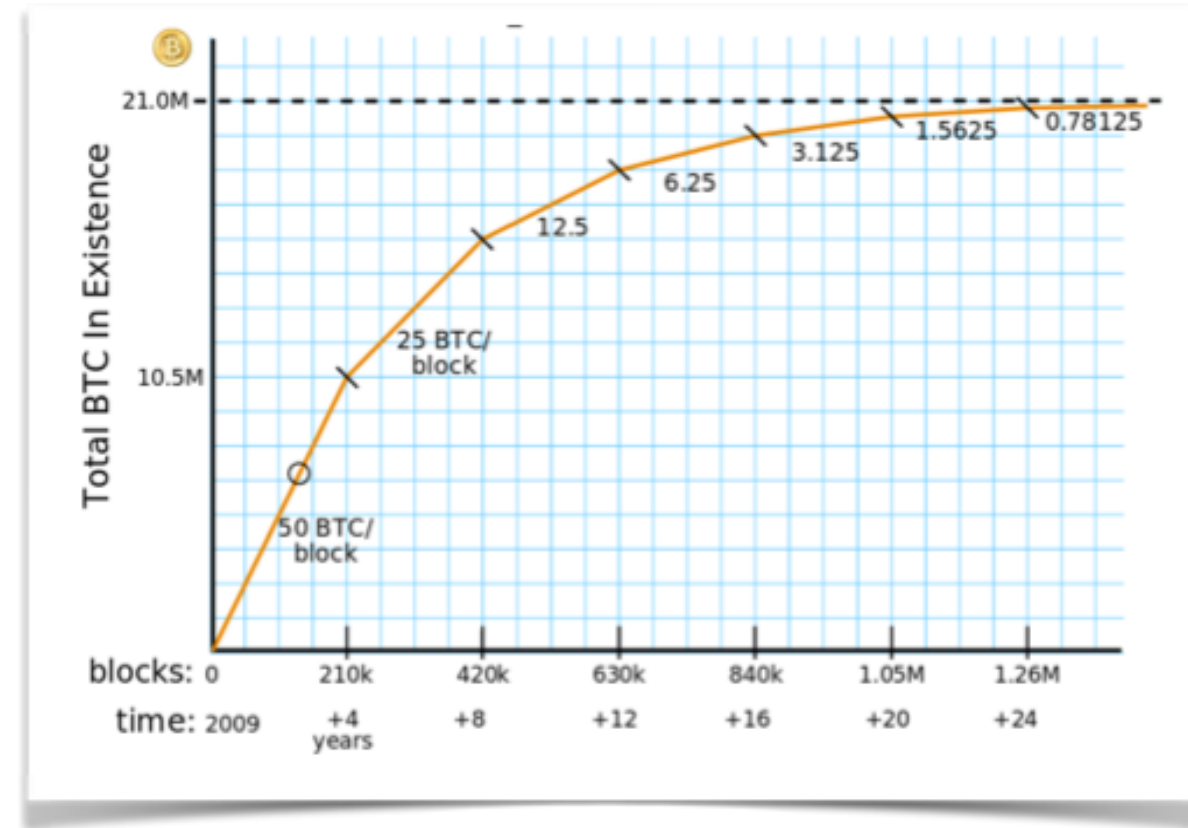
```
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;f1Yz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ã^ŠQ2:Ÿ,a
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)«_IŸŸ...¬+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....ŸŸŸŸM.ŸŸ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksŸŸŸŸ..ð.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.gŠŸ°pUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gñ|q0·.\Ö" (à9. |
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybàè.ab¶IÖ¿?Lİ8Ä
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 ÓU.â.Á.ß\8M+ø..W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 00 00 ŠLp+kñ._¬....
```

- It's crucial that everyone starts on the same genesis
- also crucial that nobody gets a head start on mining.



# Remark: Why should miners mine?

- Each block has a **special transaction** that pays its **miner** some BTC
  - called the coinbase transaction
  - block reward is how bitcoins are created
- Today, it's 3.125 BTC (approx. \$81,000; Sep. 2026)
  - Halves every 4 years



Courtesy:  
Brian Warner

# Remark: Mining pools

- Special-purpose hardware is blazingly fast!
- => Driving hobbyist miners out of market
- => System dominated by a few big players



| FUTURES Bitcoin Miner S19j XP |                                      |       |         |
|-------------------------------|--------------------------------------|-------|---------|
| Function                      | BTC/BCH/BSV SHA256 Air-cooling Miner |       |         |
| Specifications                | 151T                                 | 3247W | 21.5J/T |
| Price/Unit                    | \$4,983                              |       |         |
| Price/T                       | \$33                                 |       |         |

151T=151,000,000,000,000 SHA-256<sup>2</sup> per sec.

CPU can do a few millions.  
One S19j XP ~ 10<sup>8</sup> laptop CPUs

See [https://en.bitcoin.it/wiki/Non-specialized\\_hardware\\_comparison](https://en.bitcoin.it/wiki/Non-specialized_hardware_comparison)

Two to three pools account for >51% mining power.  
See it live at <https://miningpoolstats.stream/bitcoin>.

# Remark: energy consumption

- Suppose  $n = 256$  bits, and difficulty  $k = 80$
- Q1: What's the probability of mining a block with one hash operation?
- Answer:  $2^{-80}$
- Q2: If we want blocks to be created 10 minutes on average, how many hash operations per sec are required?
- Answer:  $\frac{2^{80}}{10 \times 60} \approx 2 \text{ billion TH/s}$  T = trillion ( $10^{12}$ )  
 = 300,000 Joule
- Q3: Mining devices typically cost 20 Joule/TH. What's the power consumption of Bitcoin network at  $k = 80$ .
- Answer:  $2 \text{ billion TH/s} \times 20 \text{ J/TH} = 40 \text{ gigawatt (GW)}$

# Who's Building the Most Solar Energy?

Installed solar photovoltaic capacity, 2010-2022 (GW) ▶

**China** 393

**EU27** 205

**US** 113

2010 2012 2014 2016 2018 2020 2022



Source: Bruegel on EMBER and Eurostat.

**SHARE NEWS**



**BREAKING NEWS**

# 20 GW

**MELIUS SAYS THESE 6 STOCKS  
COULD GAIN FROM SPACEX'S  
MASSIVE 20 GW POWER DEMAND**



# The PoW idea appears much earlier

- The concept was first described in a 1993 paper, to compact email spams
- The term is coined by Markus Jakobsson and Ari Juels in 1999, to compact Denial of Service attacks.

## Pricing via Processing or Combatting Junk Mail

Cynthia Dwork and Moni Naor

IBM Almaden Research Center  
650 Harry Road  
San Jose, CA 95120

## PROOFS OF WORK AND BREAD PUDDING PROTOCOLS (EXTENDED ABSTRACT)

Markus Jakobsson

*Information Sciences Research Center, Bell Labs, Murray Hill, New Jersey 07974*  
[www.bell-labs.com/user/markusj](http://www.bell-labs.com/user/markusj)

Ari Juels

*RSA Laboratories, 20 Crosby Drive, Bedford, MA 01730*  
[ari@rsa.com](mailto:ari@rsa.com)