EE817/IS893
Blockchain and Cryptocurrency
Bitcoin

Yongdae Kim

Cypherpunk

- 1970년대 암호는 군과 스파이 기관의 전유물
- 1980년 경부터 큰 변화
  - Data Encryption Standard (DES) by NIST
  - "New Directions in Cryptography" by Diffie-Hellman
  - David Chaum: ecash, pseudonym, reputation, …
- 1992년: Gilmore 등이 작은 그룹을 만듬
  - Cypherpunk: cipher + cyberpunk, Cypherpunk mailing list

- A Cypherpunk's Manifesto

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

  - "Privacy"는 잘못된 것을 숨기는게 아님! 커텐은 집안에 나쁜게 있어서?

주목할 만한 Cypherpunk들

- Jacob Appelbaum: Tor
- Julian Assange: WikiLeaks
- Adam Back: Hashcash
- Bram Cohen: BitTorrent
- Hal Finney: PGP 2.0, Reusable PoW
- Tim Hudson: SSLeay, the precursor to OpenSSL
- Paul Kocher: SSL 3.0
- Moxie Marlinspike: Signal
- Zooko Wilcox-O'Hearn: DigiCash, Zcash
- Philip Zimmermann: PGP 1.0
- Matt Blaze: Clipper chip, crypto export control

Cypherpunk와 블록체인

- David Chaum (1980s)
  - "Security without Identification: Transaction Systems to Make Big Brother Obsolete"
  - Anonymous Digital Cash, Pseudonymous Reputation System
- Adam Back (1997)
  - Hash cash: Anti-spam mechanism requiring cost to send email
- Wei Dai (1998)
  - B-money: Enforcing contractual agreement between two anons
  - 1. Every participant maintain separate DB: Bitcoin
  - 2. deposit some money as potential fines or rewards: PoS
- Hal Finney (2004)
  - Reusable PoW: Double spending detection was centralized
- Nick Szabo (2005)
  - "Bit Gold": Values based on amount of computational work
  - Concept of "Smart Contract"

What is Bitcoin?

- Satoshi Nakamoto, who published the invention in 2008 and released it as open-source software in 2009.
  - "Bitcoin: A Peer-to-peer Electronic Cash System"
- Bitcoin is a first cryptocurrency based on a peer-to-peer network.
- Bitcoin as a form of payment for products and services has grown, and users are increasing.

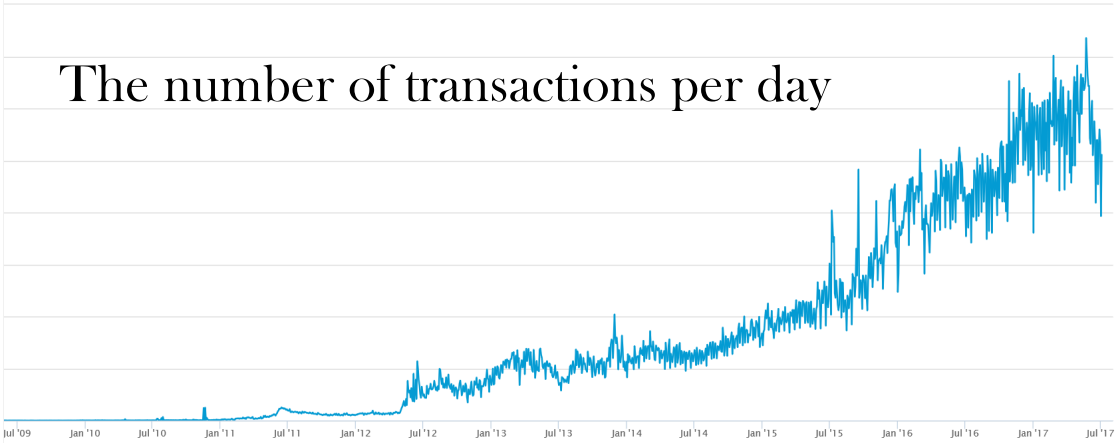
Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

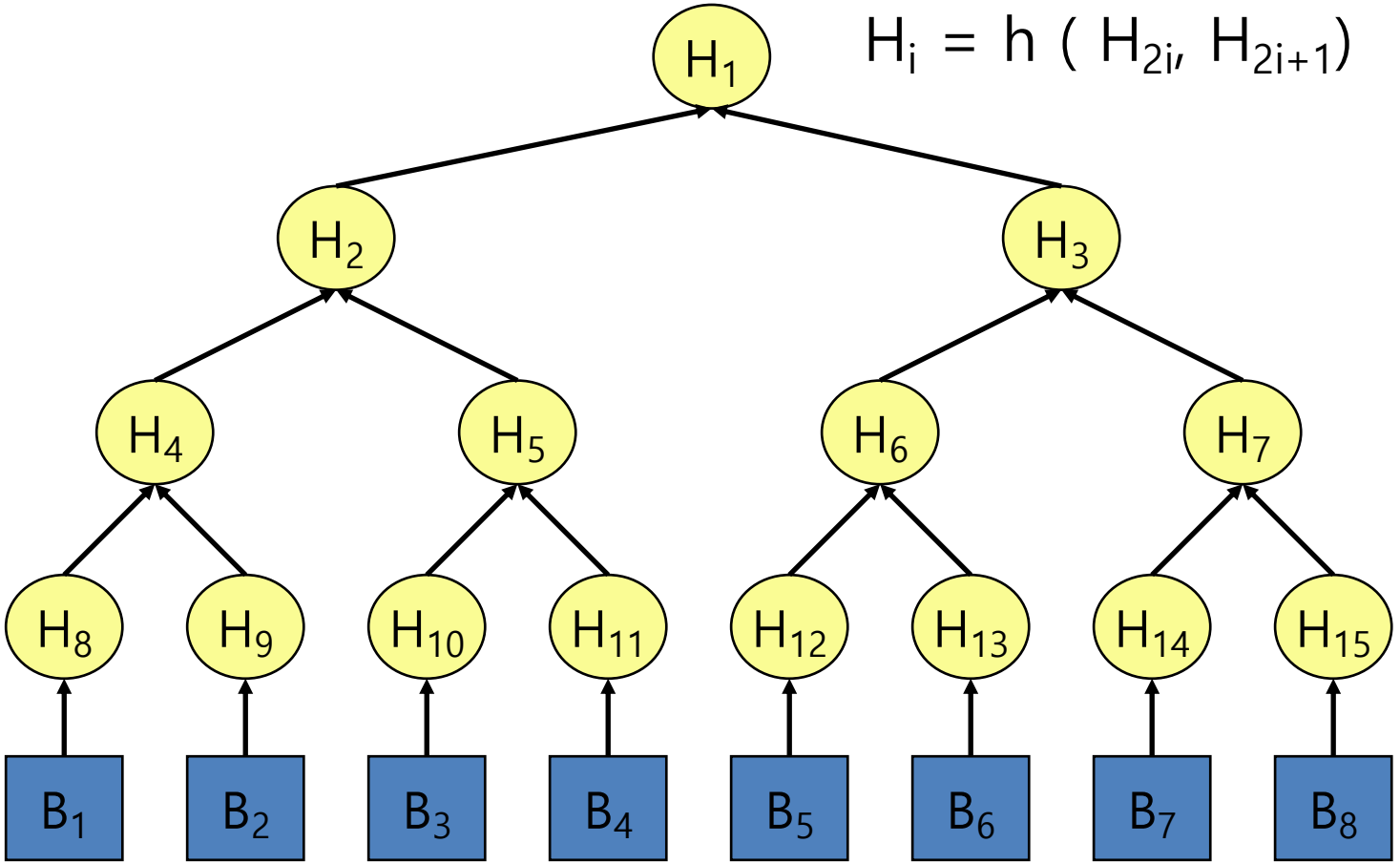


Hash function and Digital Signature

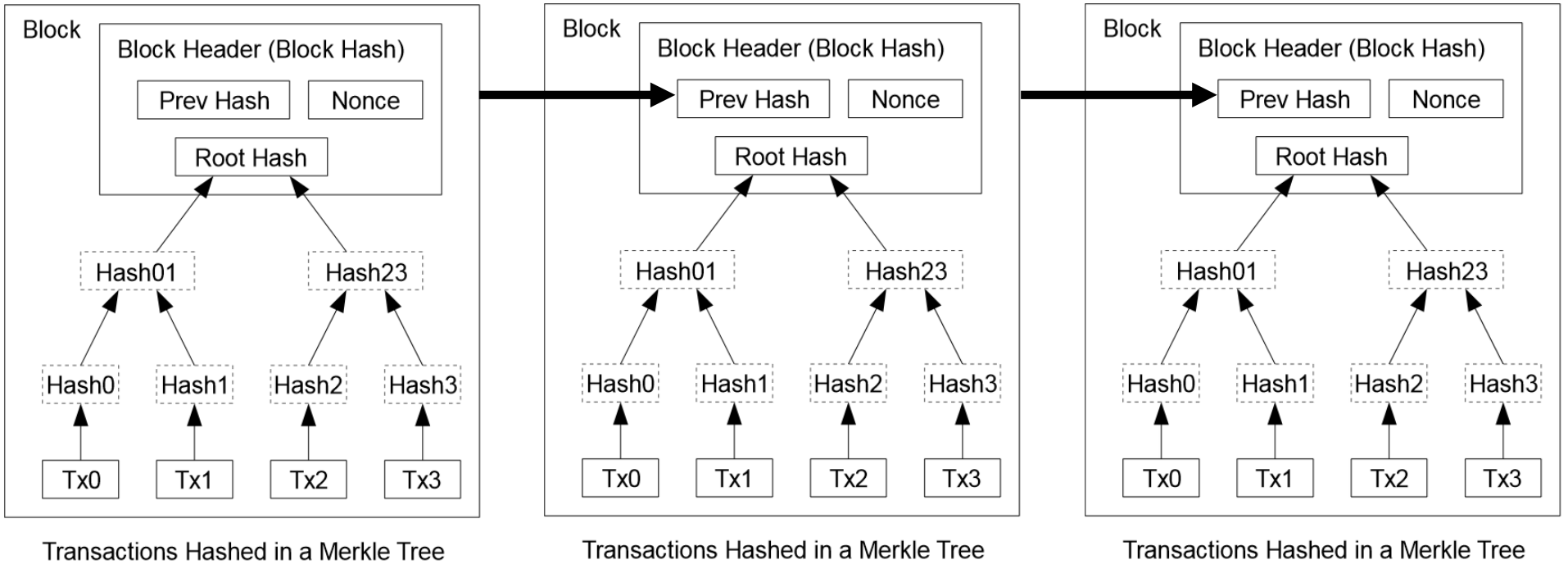
- A hash function is a function h
  - compression — h maps an input x of arbitrary finite bitlength, to an output h(x) of fixed bitlength n.
  - ease of computation — h(x) is easy to compute for given x and h
  - Properties
    - one-way: for a given y, find x' such that h(x') = y
    - collision resistance: find x and x' such that h(x) = h(x')

- Digital Signature
  - Message Integrity, Unforgeability, Public Verifiability, Non-repudiation
  - Public key: PK_A, Private key: SK_A
  - Signature: $S_{SKA}(h(m)) = s^*$
  - Verification: $V_{PKA}(h(m), s^*)$ = True or False

Merkle Hash Tree

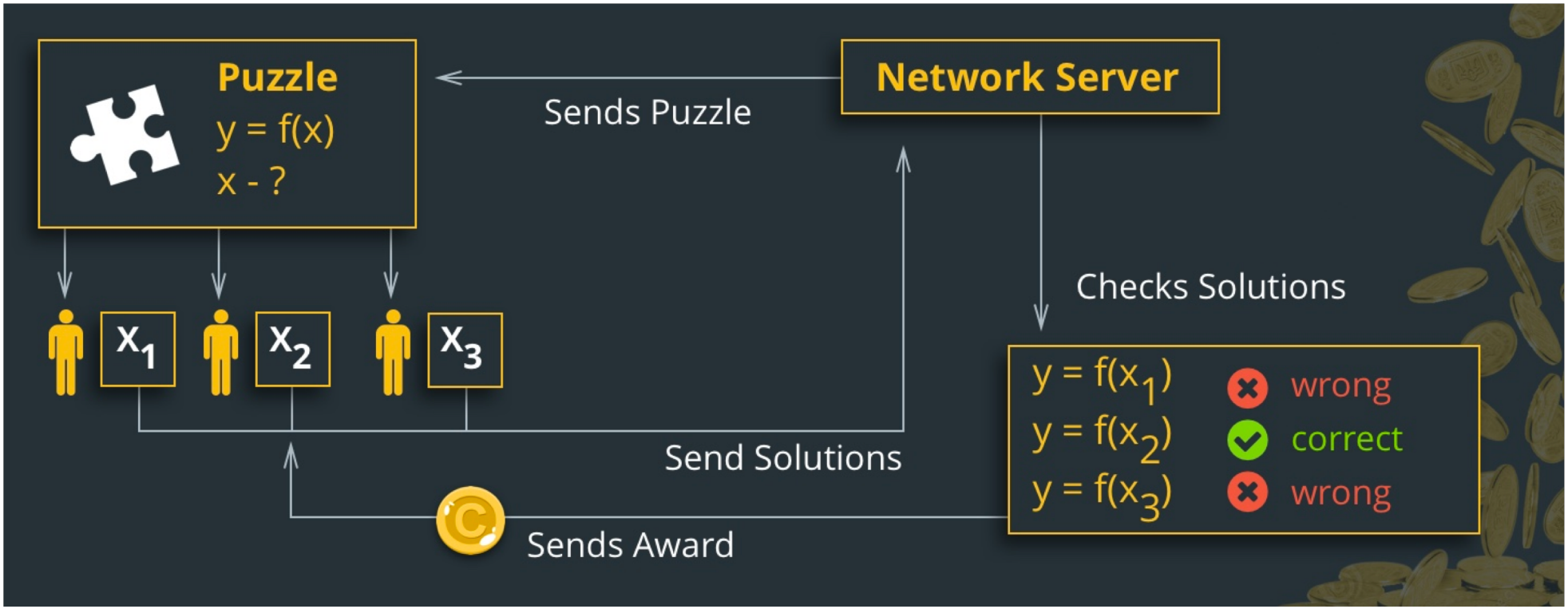


Blockchain



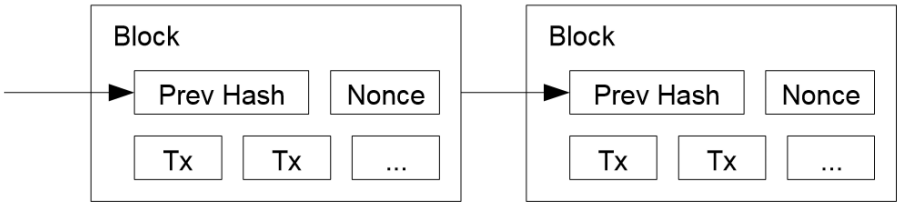
- ❖ Blocks connect as a chain.
- ❖ Each header of blocks includes the previous block's hash.

Proof-of-Work



Proof-of-Work

- Proof-of-work scheme is based on SHA-256
- Proof-of-work is to find a valid Nonce by incrementing the Nonce in the block header until the block's hash value has the required prefix zero bits.



Contents

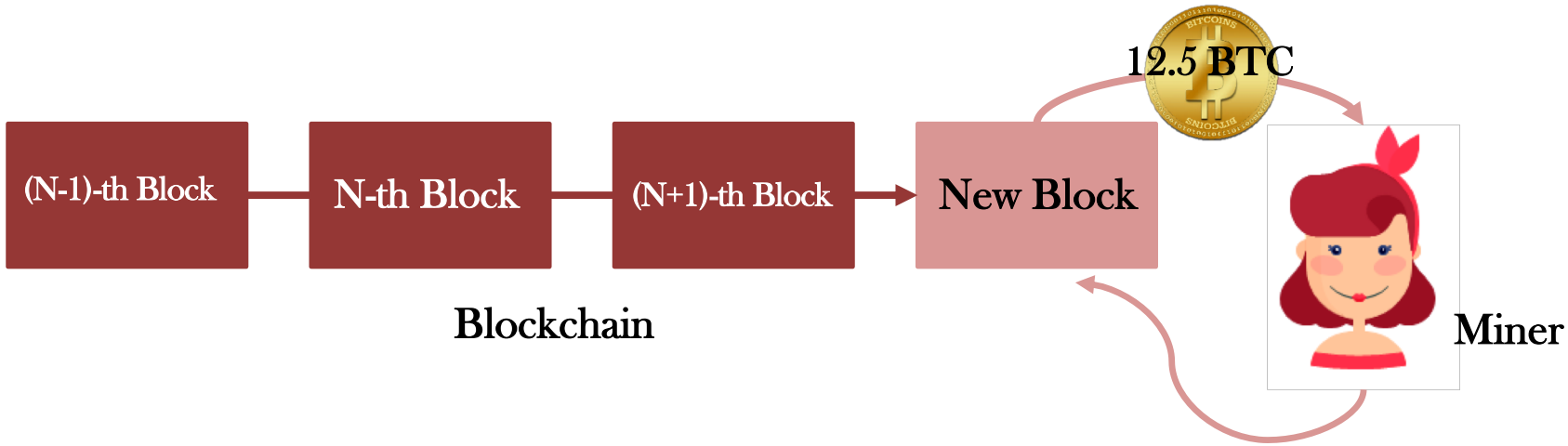
Nonce

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Valid nonce

Reward

- Performing proof-of-work is called **Mining.**
- A person who does mining is called **Miner.**
- A miner can earn 12.5 BTC (≈ $ 10k) as a reward when she succeeds to find a valid nonce.



Step (Miner)

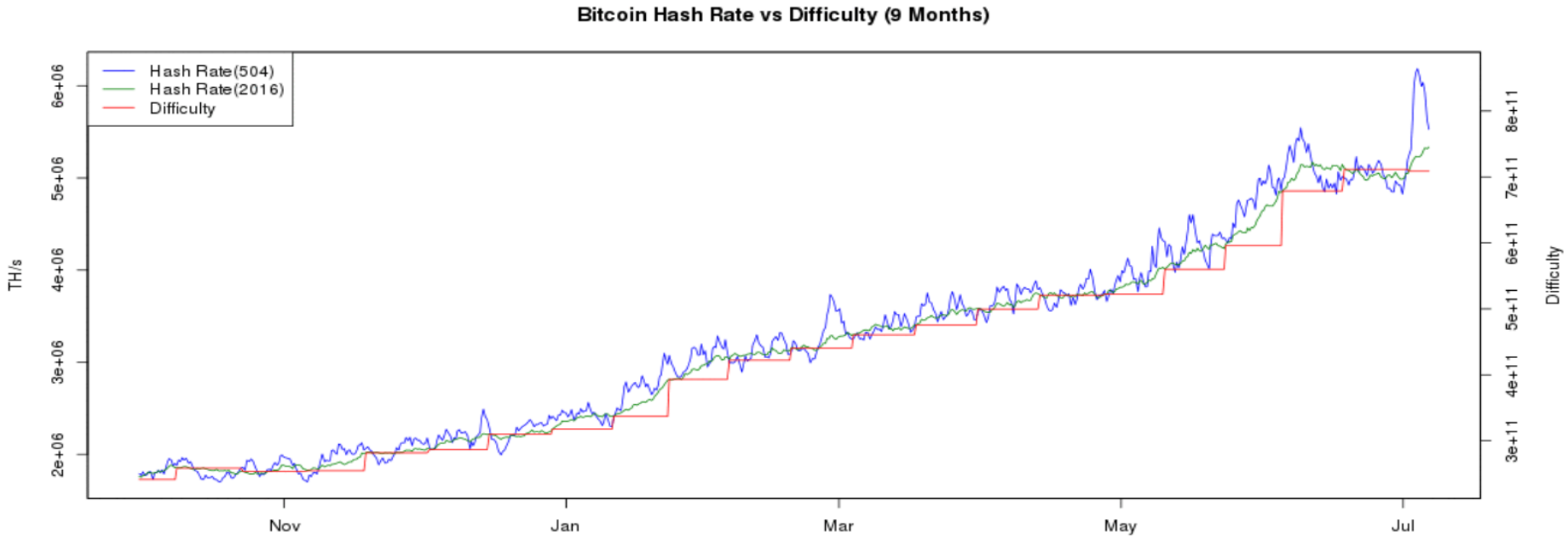
- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work for its block.
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
- Nodes express their acceptance of the block by working on creating the next chain, using the hash of the accepted block as the previous hash.

Miner's Incentive

- 12.5 BTC reward for a valid block
  - Special coin-creation transaction (first transaction in each block)
- Transaction fees (optional)
  - Offered by creator of transaction (input sum – output sum)
  - Incentive to include transaction in a block (faster processing)
- Keeping up the system
  - To preserve the value of your own bitcoin money

- Rewarded only if block is on eventual consensus branch!

Mining Difficulty

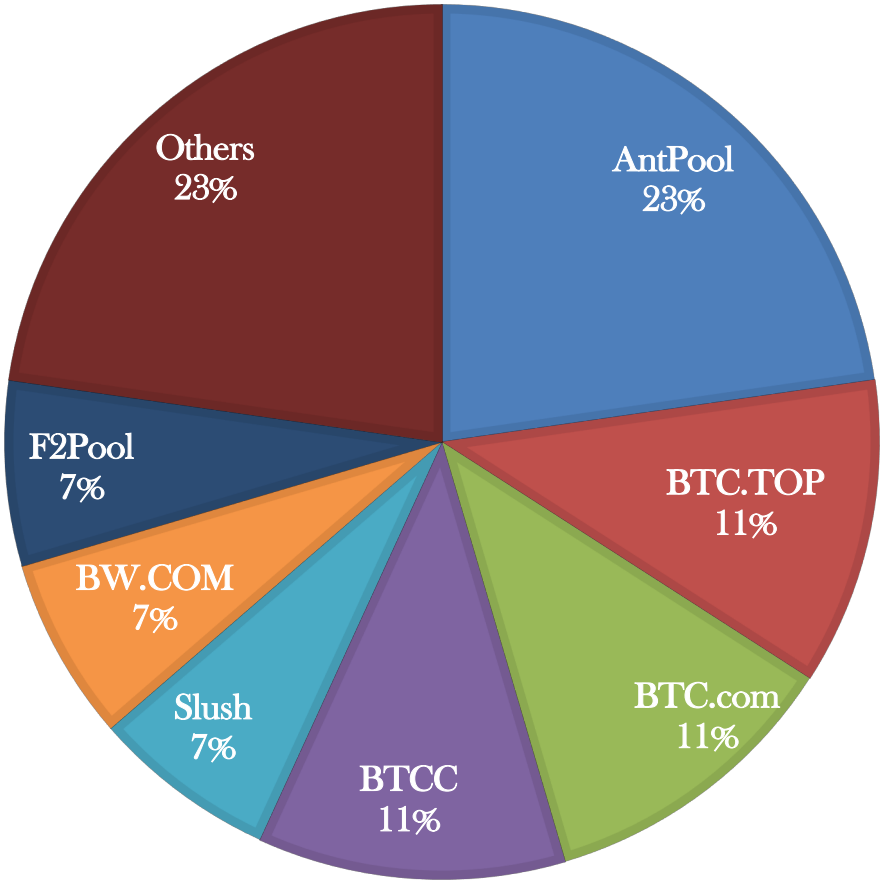


- Bitcoin adjusts automatically the mining difficulty to be an average one round period 10mins.
- The difficulty increases continuously as computing power increases.

Mining Policies

- Rate limiting on the creation of a new block
  - A block created every 10 mins (six blocks every hour)
    - How? Difficulty is adjusted every two weeks to keep the rate fixed as capa city/computing power increases
- N new bitcoins per each new block: credited to the miner ➔ incentives for miners
  - N was 50 initially. In 2013, N=25. In 2016, N=12.5.
  - Halved every 210,000 blocks (≈ every four years)
  - Thus, the total number of bitcoins will not exceed 21 million.
- Why fixed number of coins?
  - $s are minted every year.
  - To prevent de-valuation of bitcoin

Mining Pool



- Many miners started to do mining together.
- Most mining pools consist of a manager and miners.
- Currently, most computational power is possessed in mining pools.

Bitcoin Mining Hardware

Antminer S9 13 TH/S 16nm ASIC Bitcoin Miner
by AntMiner

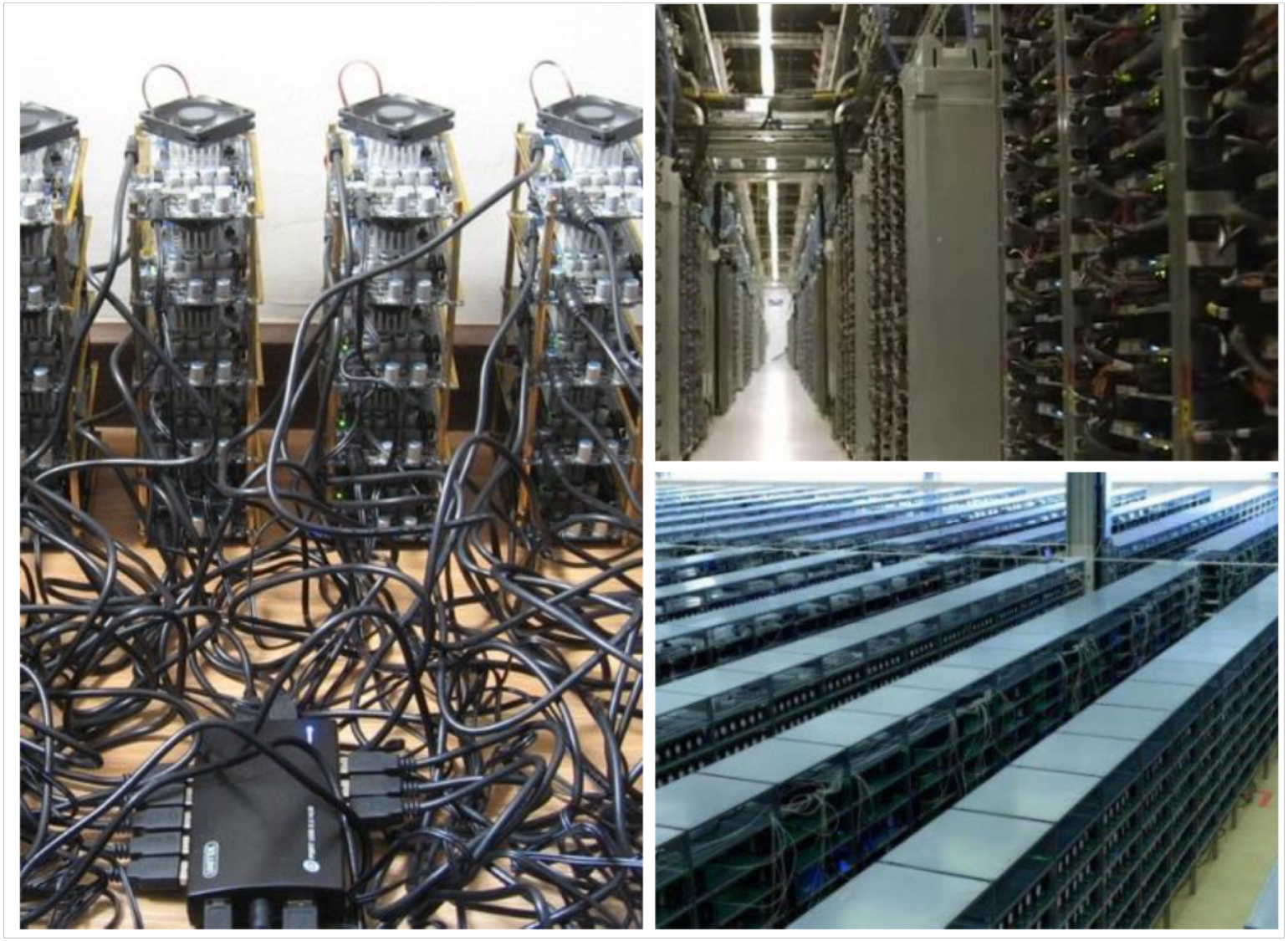
$1,887.00
FREE Shipping on eligible orders
Only 12 left in stock - order soon.

More Buying Choices
$1,885.00 (5 used & new offers)

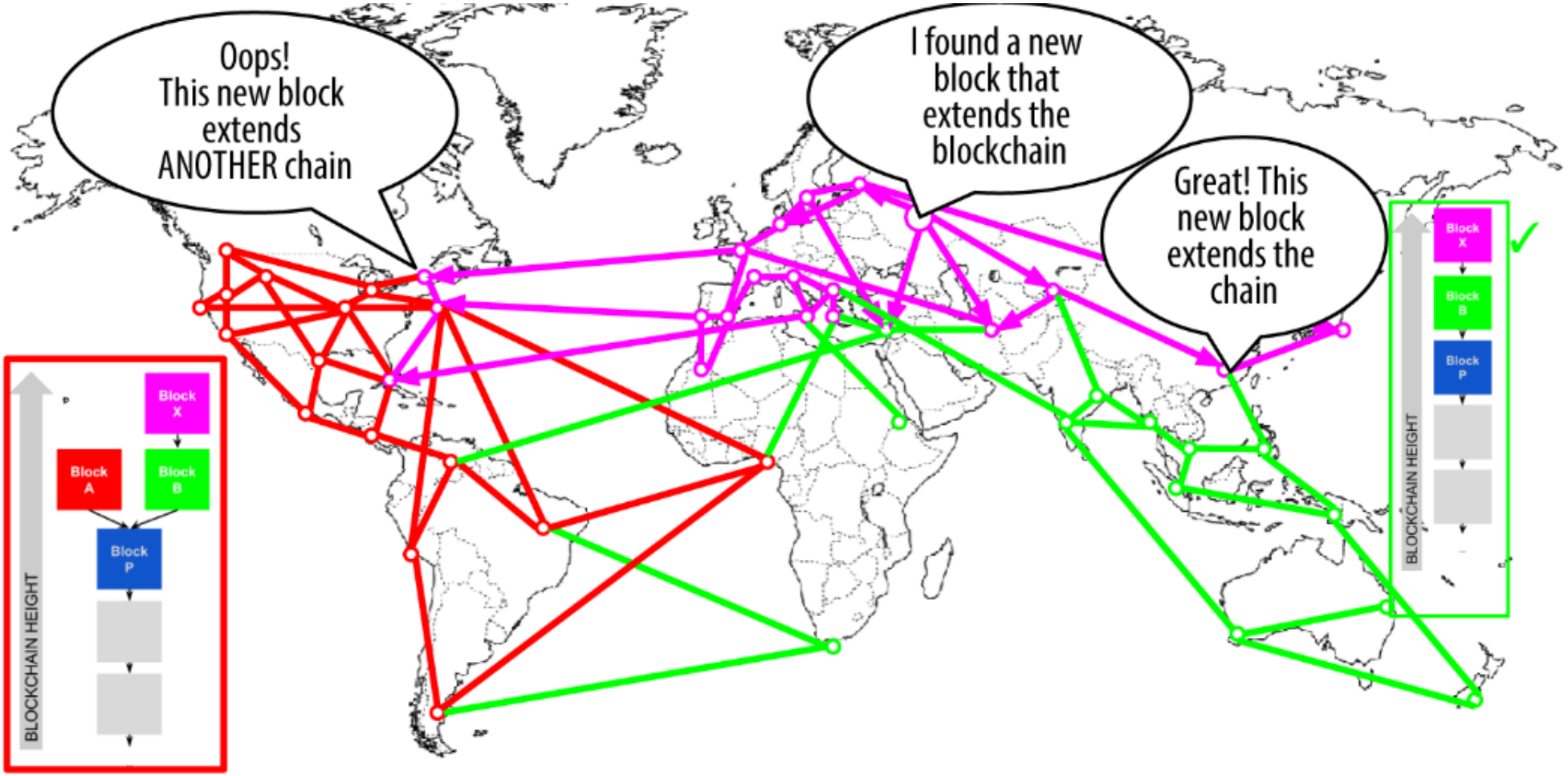
Rev 2 GekkoScience 2-Pac Compac USB Stick Bitcoin Miner 15gh/s+
by GEKKOSCIENCE

$69.97 + $4.49 shipping

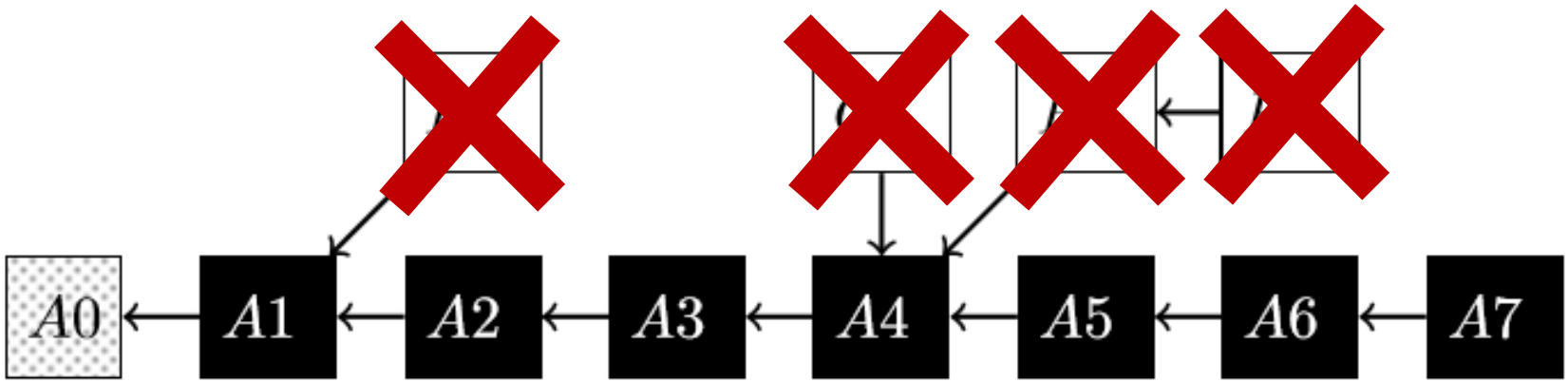
More Buying Choices
$59.97 (2 new offers)



Forks

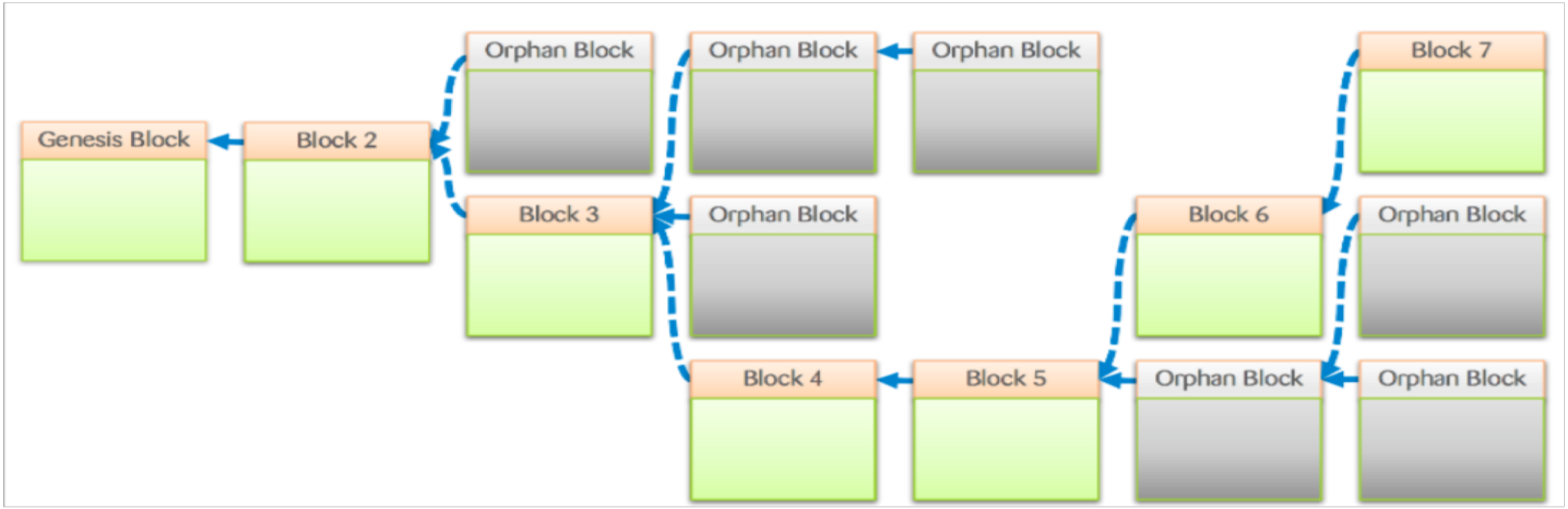

Oops!
This new block
extends
ANOTHER chain
I found a new
block that
extends the
blockchain
Great! This
new block
extends the
chain
Block
X
Block
A
Block
B
Block
P
BLOCKCHAIN HEIGHT
Block
X
Block
B
Block
P
BLOCKCHAIN HEIGHT

Forks



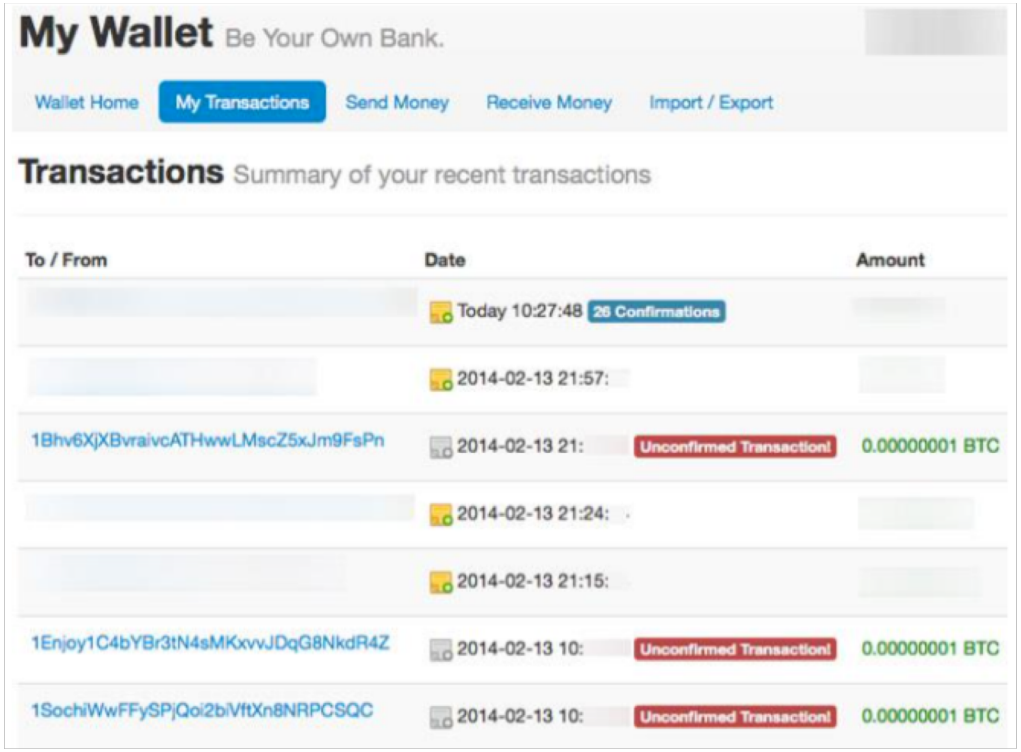
- Only one head is accepted as a valid one among heads.
- An attacker can generate forks intentionally by holding his found block for a while.

Example of Blockchain Status

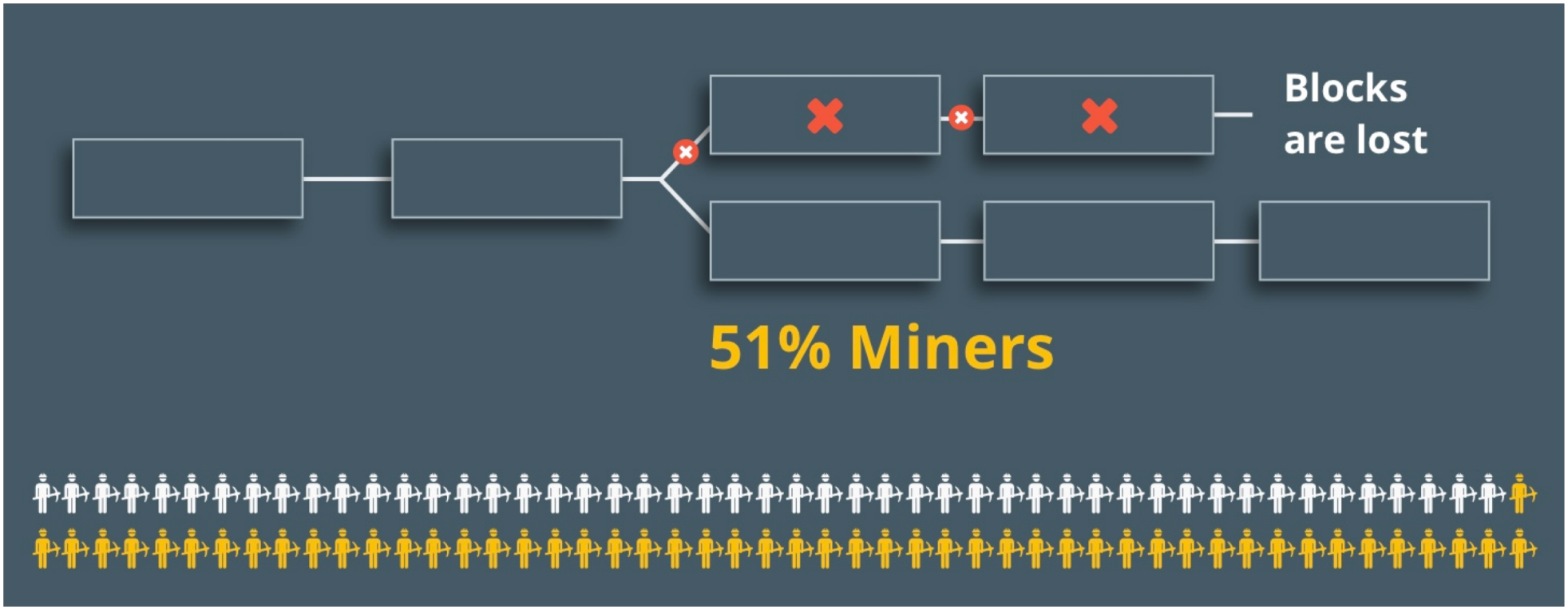


Transaction Confirmations

- A transactions is typically considered “confirmed” once it has 6 co nfirmations ➔ Probabilistic confirmation



51% Attack



Hash Rate Comparison

	Pool HashRate	Network HashRate
BTC Pool	6.103E	53.986E
BCH Pool	435.120P	3.548E
LTC Pool	40.886T	247.719T
ETH Pool	663.324G	205.490T
ETC Pool	17.589G	13.079T

	Pool HashRate	Network HashRate
ZEC Pool	107.573M	2.128G
DASH Pool	251.480T	2.558P
BTM Pool	173.546K	1.225G
XMR Pool	7.544M	399.718M