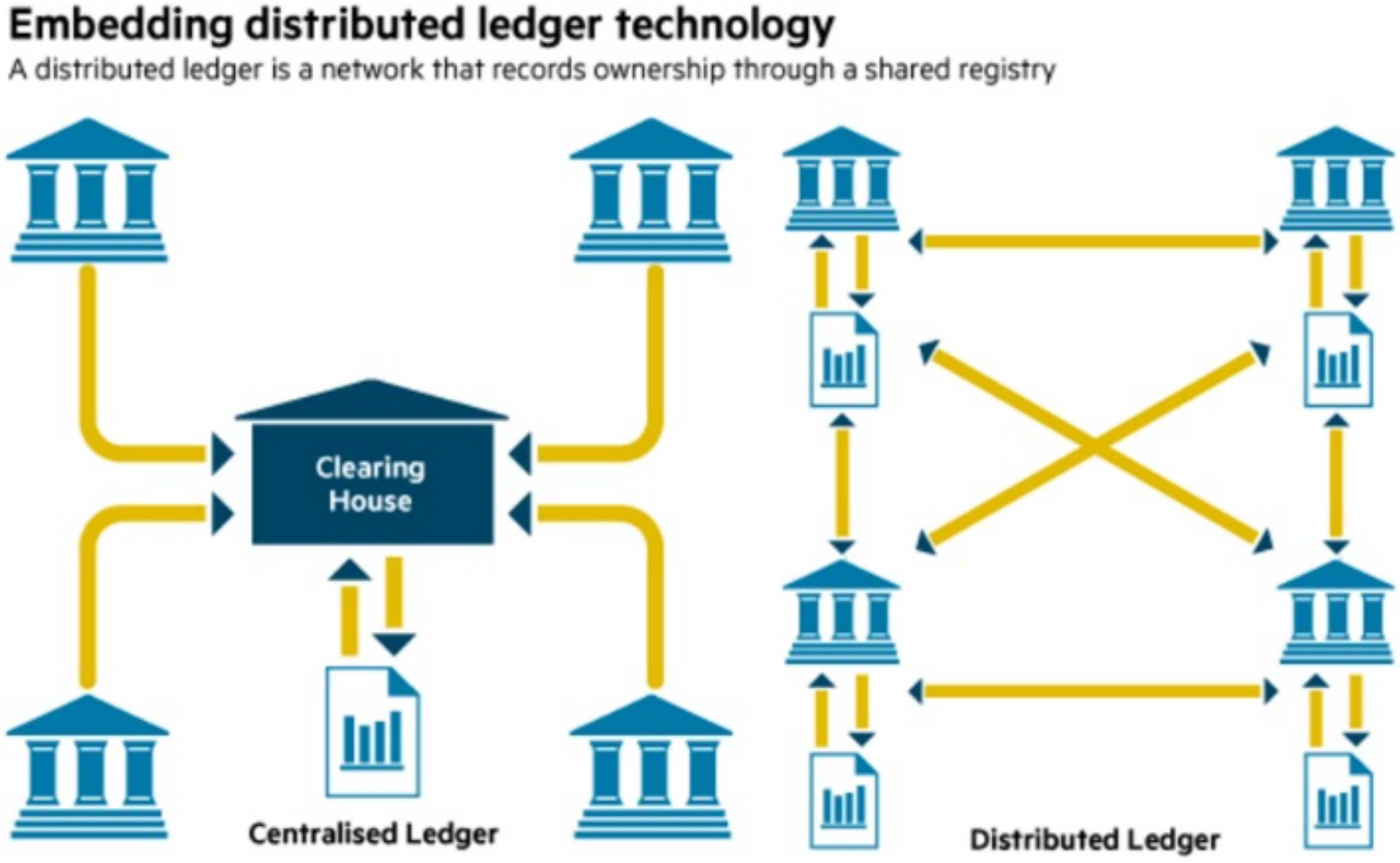
# Introduction to Blockchain

Yongdae Kim

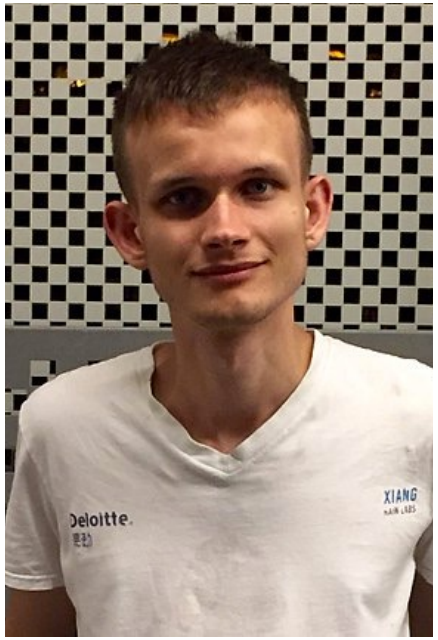
# Centralization vs. Decentralization


Embedding distributed ledger technology
A distributed ledger is a network that records ownership through a shared registry
Clearing House
Centralised Ledger
Distributed Ledger

# Bitcoin

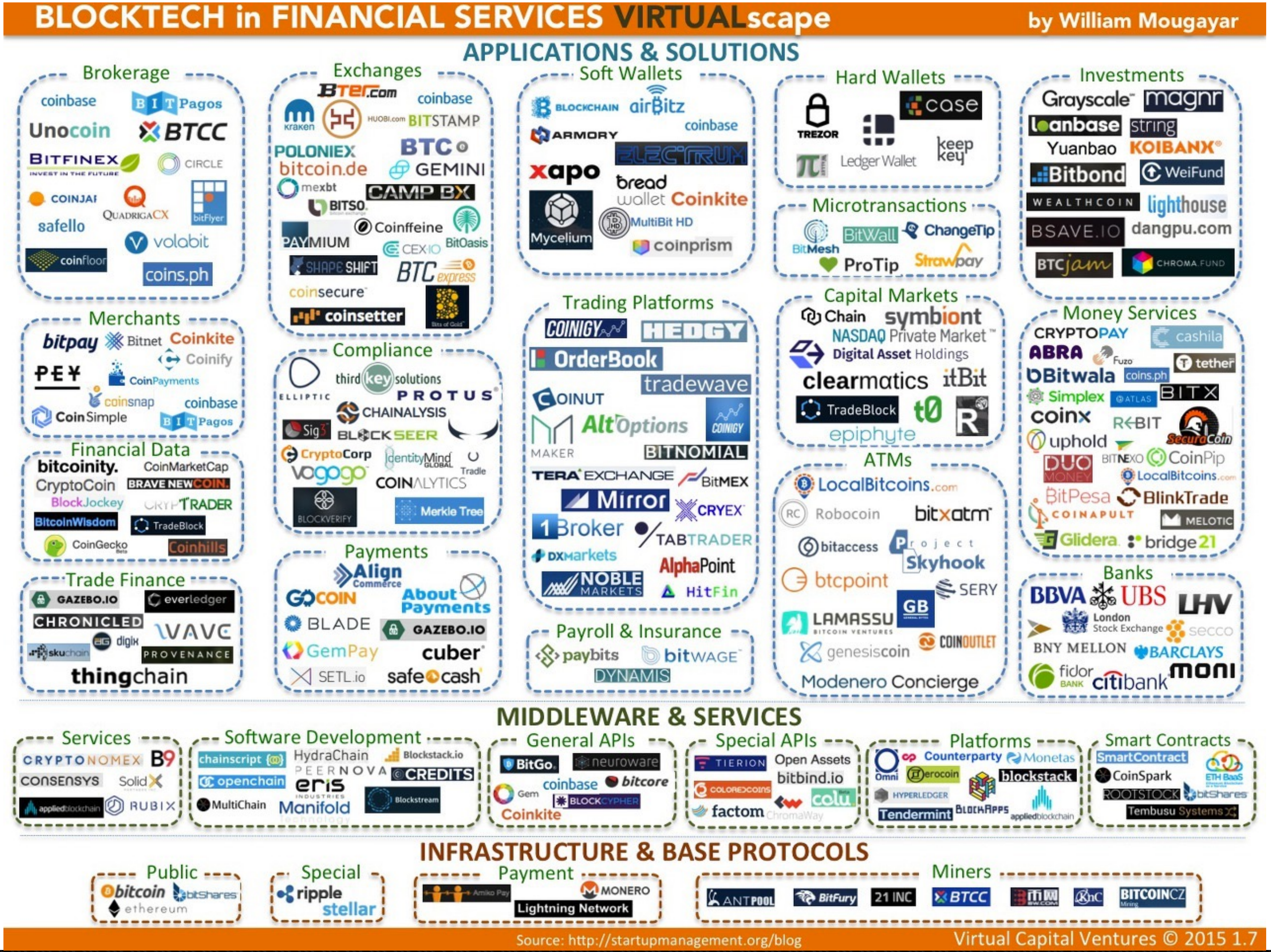
- Satoshi Nakamoto
  - “Bitcoin: A Peer-to-peer Electronic Cash System”
  - “Proof of Work”
  - Peer-to-peer Network
  - Secure
  - Decentralized Ledger technology

# Ethereum



- ❑ 2$^{nd}$ gen Blockchain
- ❑ Vitalek Buterin, 19 year old genius

- ❑ Turing Complete Language
- ❑ Storing and executing program on a ledger
- ❑ Smart Contract
- ❑ Implementing other blockchains on Ethereum



# BLOCKTECH in FINANCIAL SERVICES VIRTUALscape

by William Mougayar

## APPLICATIONS & SOLUTIONS

### Brokerage
coinbase, BITPagos, Unocoin, BTCC, BITFINEX INVEST IN THE FUTURE, CIRCLE, COINJAR, QuadrigaCX, bitFlyer, safello, volabit, coinfloor, coins.ph

### Exchanges
BTER.com, coinbase, kraken, HUOBI.com, BITSTAMP, POLONIEX, BTC-e, bitcoin.de, GEMINI, mexbt, CAMP BX, BITSO, PAYMIUM, Coinffeine, BitOasis, CEX.IO, SHAPESHIFT, BTC express, coinsecure, coinsetter, Bits of Gold

### Soft Wallets
BLOCKCHAIN, airBitz, coinbase, ARMORY, ELECTRUM, xapo, bread wallet, Coinkite, Mycelium, MultiBit HD, coinprism

### Hard Wallets
TREZOR, case, Ledger Wallet, keepkey

### Microtransactions
BitMesh, BitWall, ChangeTip, ProTip, Strawpay

### Investments
Grayscale, magnr, loanbase, string, Yuanbao, KOIBANX, Bitbond, WeiFund, WEALTHCOIN, lighthouse, BSAVE.IO, dangpu.com, BTCjam, CHROMA FUND

### Merchants
bitpay, Bitnet, Coinkite, Coinify, PEY, CoinPayments, coinsnap, coinbase, CoinSimple, BITPagos

### Financial Data
bitcoinity., CoinMarketCap, CryptoCoin, BRAVE NEWCOIN, BlockJockey, CRYPTRADER, BitcoinWisdom, TradeBlock, CoinGecko, Coinhills

### Trade Finance
GAZEBO.IO, everledger, CHRONICLED, digix, WAVE, skuchain, PROVENANCE, thingchain

### Compliance
ELLIPTIC, thirdkeysolutions, PROTUS, CHAINALYSIS, Sig3, BLOCKSEER, CryptoCorp, IdentityMind GLOBAL, Tradle, vogogo, COINALYTICS, BLOCKVERIFY, Merkle Tree

### Payments
Align Commerce, GoCoin, About Payments, BLADE, GAZEBO.IO, GemPay, cuber, SETL.io, safecash

### Trading Platforms
COINIGY, HEDGY, OrderBook, tradewave, COINUT, AltOptions, COINIGY, MAKER, BITNOMIAL, TERA EXCHANGE, BitMEX, Mirror, CRYEX, 1Broker, TABTRADER, DXmarkets, AlphaPoint, NOBLE MARKETS, HitFin

### Payroll & Insurance
paybits, bitWAGE, DYNAMIS

### Capital Markets
Chain, symbiont, NASDAQ Private Market, Digital Asset Holdings, clearmatics, itBit, TradeBlock, t0, R, epiphyte

### ATMs
LocalBitcoins.com, Robocoin, bitxatm, bitaccess, Project Skyhook, btcpoint, SERY, LAMASSU BITCOIN VENTURES, GB, genesiscoin, COINOUTLET, Modenero Concierge

### Money Services
CRYPTOPAY, cashila, ABRA, Fuzo, tether, Bitwala, coins.ph, Simplex, ATLAS, BITX, coinx, REBIT, SecuraCoin, uphold, DUO MONEY, BITNEXO, CoinPip, LocalBitcoins.com, BitPesa, BlinkTrade, COINAPULT, MELOTIC, Glidera, bridge21

### Banks
BBVA, UBS, LHV, London Stock Exchange, secco, BNY MELLON, BARCLAYS, fidor BANK, citibank, moni

## MIDDLEWARE & SERVICES

### Services
CRYPTONOMEX, B9, CONSENSYS, SolidX, appliedblockchain, RUBIX

### Software Development
chainscript, HydraChain, Blockstack.io, PEERNOVA, CREDITS, openchain, eris INDUSTRIES, MultiChain, Manifold Technology, Blockstream

### General APIs
BitGo, neuroware, Gem, coinbase, bitcore, BLOCKCYPHER, Coinkite

### Special APIs
TIERION, Open Assets, bitbind.io, COLORECOINS, colu, factom, ChromaWay

### Platforms
Omni, Counterparty, Monetas, Zerocoin, blockstack, HYPERLEDGER, Tendermint, BLOCKAPPS, appliedblockchain

### Smart Contracts
SmartContract, CoinSpark, ETH BaaS, ROOTSTOCK, bitShares, Tembusu Systems

## INFRASTRUCTURE & BASE PROTOCOLS

### Public
bitcoin, bitShares, ethereum

### Special
ripple, stellar

### Payment
Amiko Pay, MONERO, Lightning Network

### Miners
ANTPOOL, BitFury, 21 INC, BTCC, BW.COM, KnC, BITCOINCZ Mining

Source: http://startupmanagement.org/blog

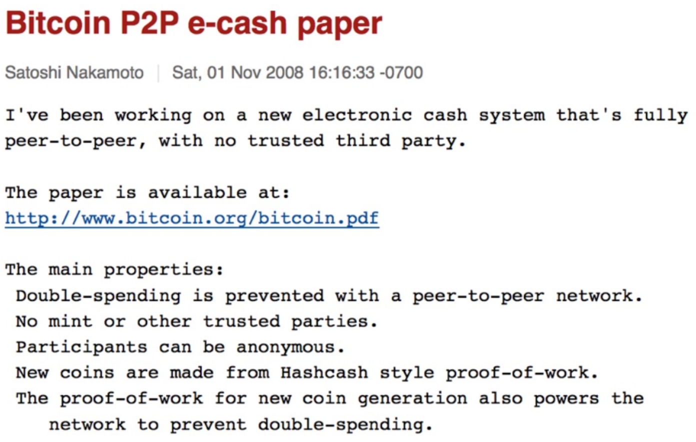
Virtual Capital Ventures © 2015 1.7

# 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
- Nick Szabo (2005)
  - “Bit Gold”: Values based on amount of computational work
  - Concept of “Smart Contract”

# What is Bitcoin?

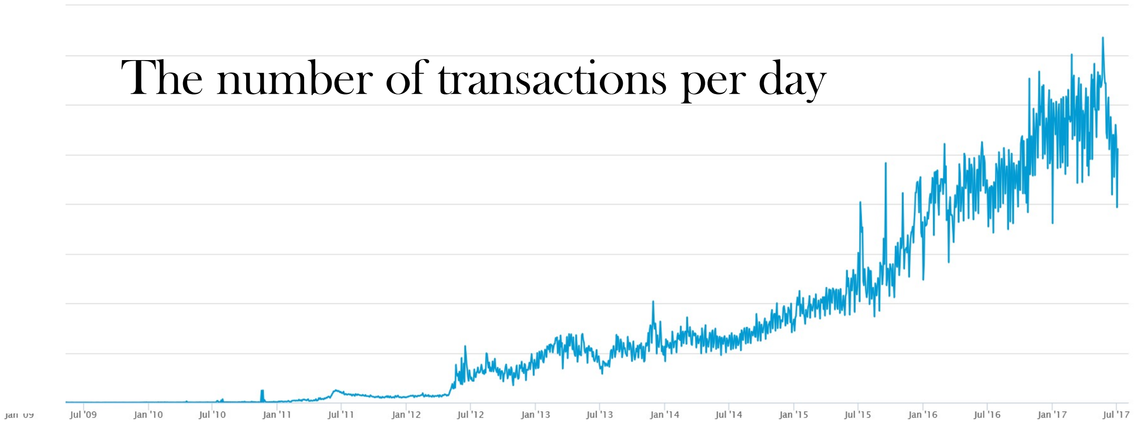
- Satoshi Nakamoto, who published the invention in 2008 and released it as open-source software in 2009.
  - "Bitcoin: A Peer-to-peer Electronic Cash System"
- Bitcoin is a first cryptocurrency based on a peer-to-peer network.
- Bitcoin as a form of payment for products and services has grown, and users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



## Bitcoin P2P e-cash paper

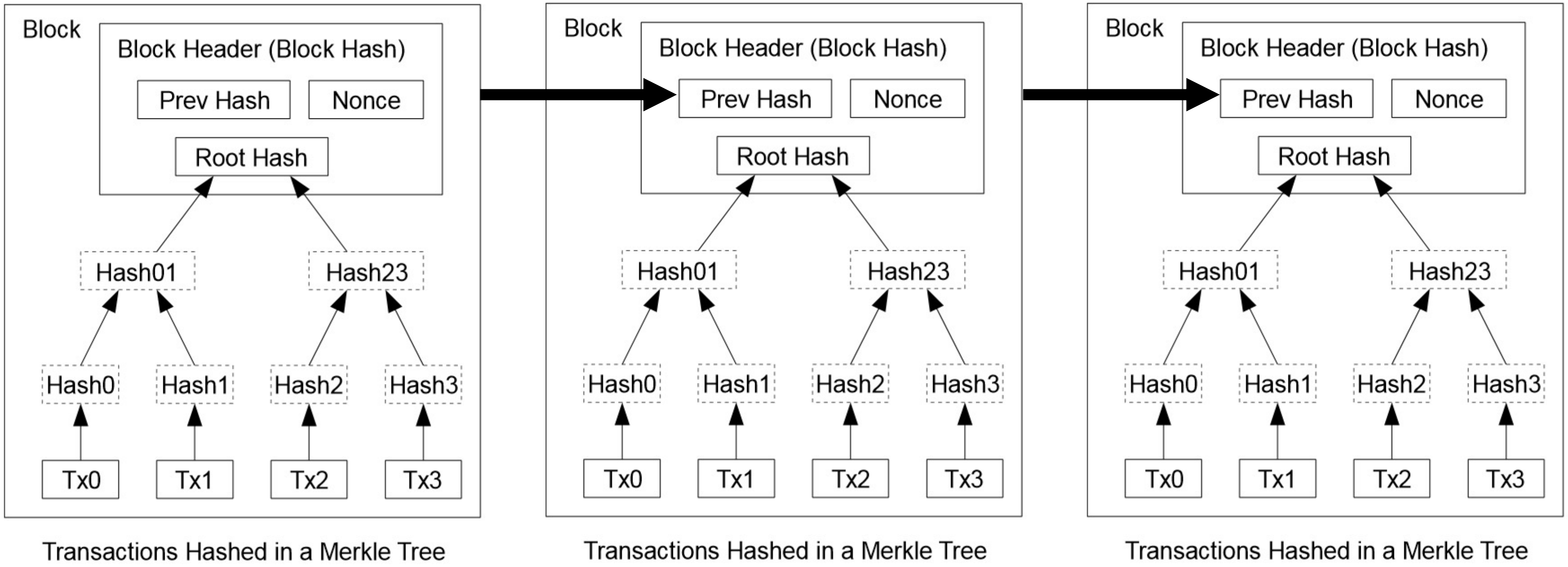
Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

```
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.
```



The number of transactions per day

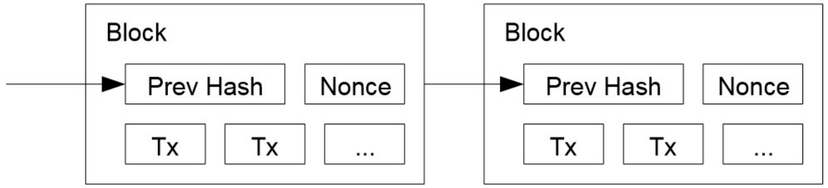
# Blockchain



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

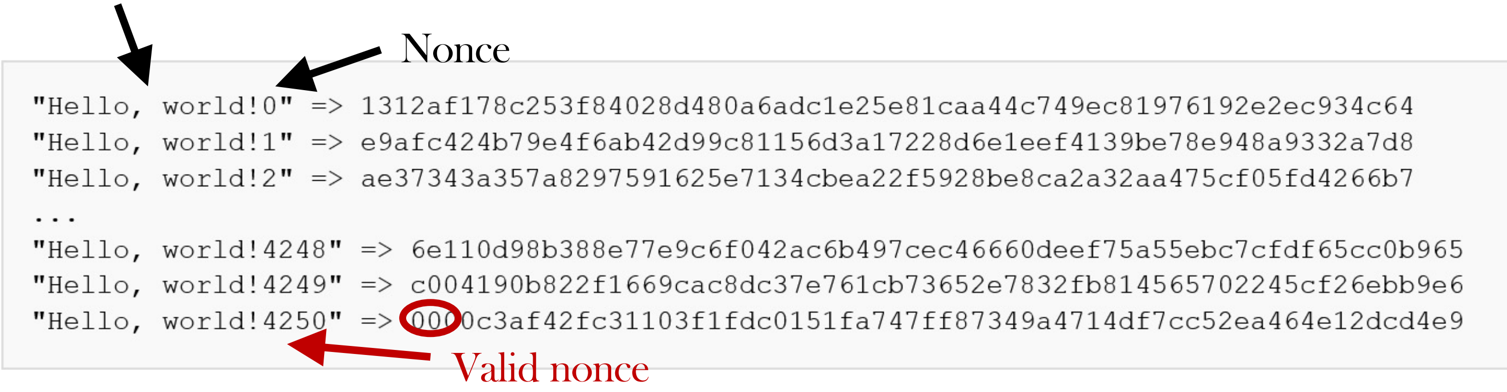
# Proof-of-Work

- 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

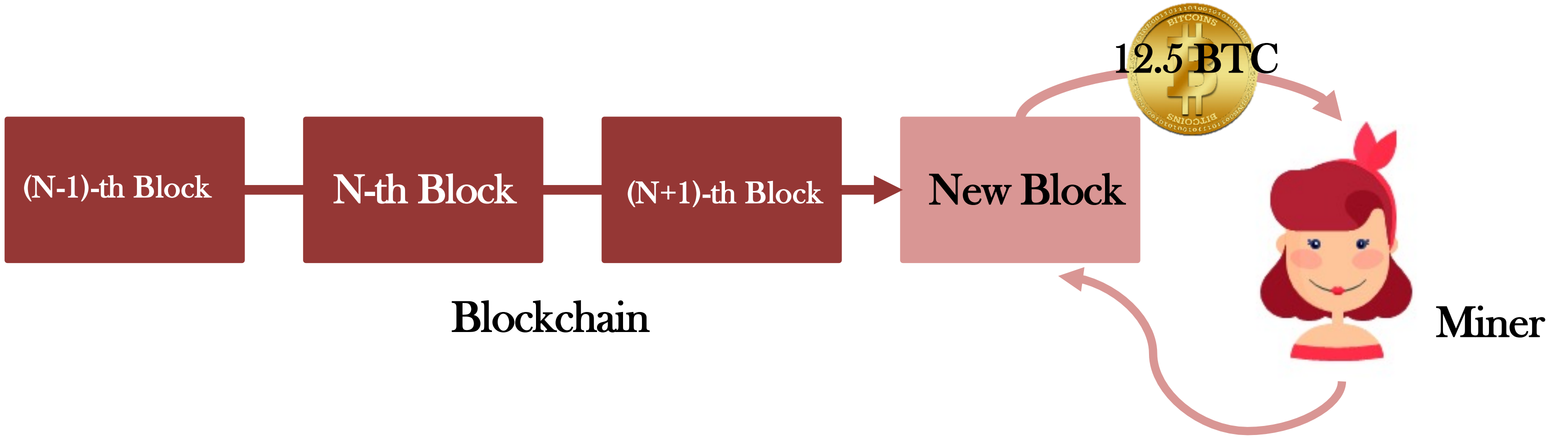


```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"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.

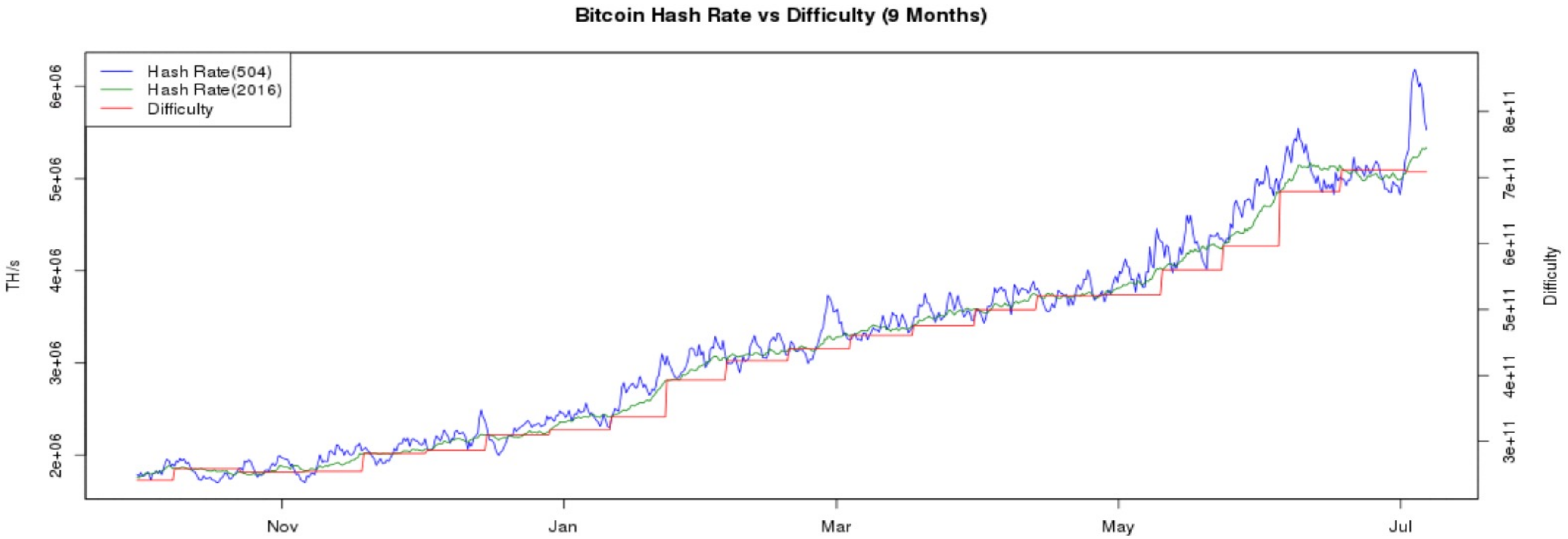


# Miner’s Incentive

- ❑ 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

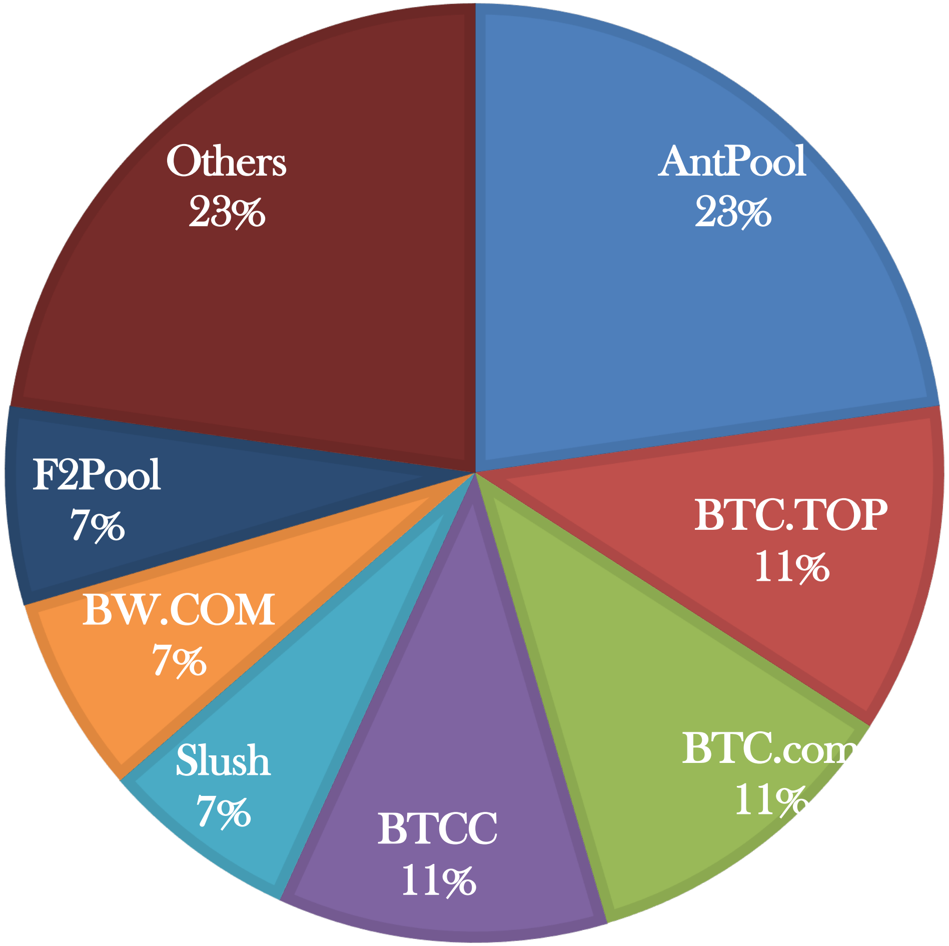
- ❑ Rewarded only if block is on eventual consensus branch!

# Mining Difficulty



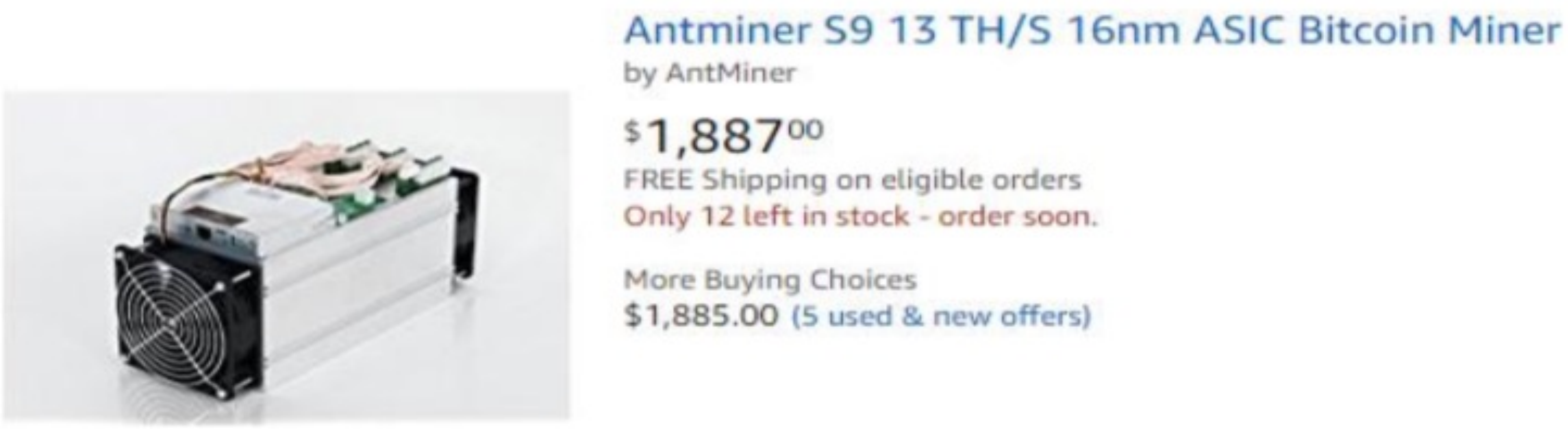
- ❖ Bitcoin adjusts automatically the mining difficulty to be an average one round period 10mins.
- ❖ The difficulty increases continuously as computing power increases.

# Mining 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

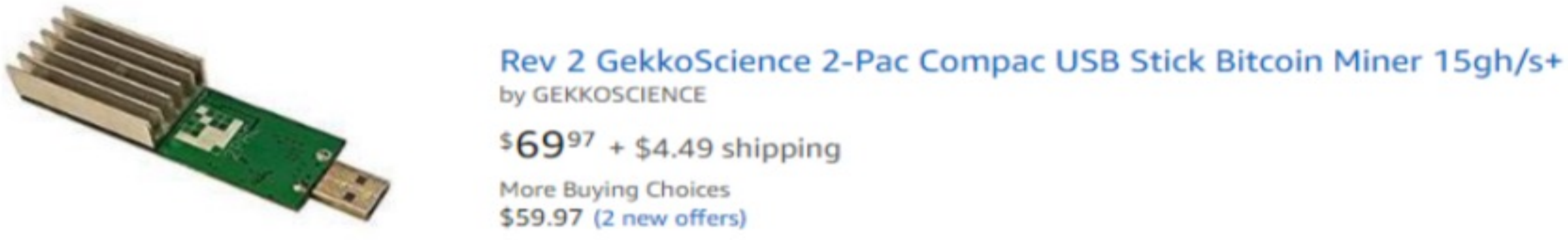
$1,887.00

FREE Shipping on eligible orders

Only 12 left in stock - order soon.

More Buying Choices

$1,885.00 (5 used & new offers)



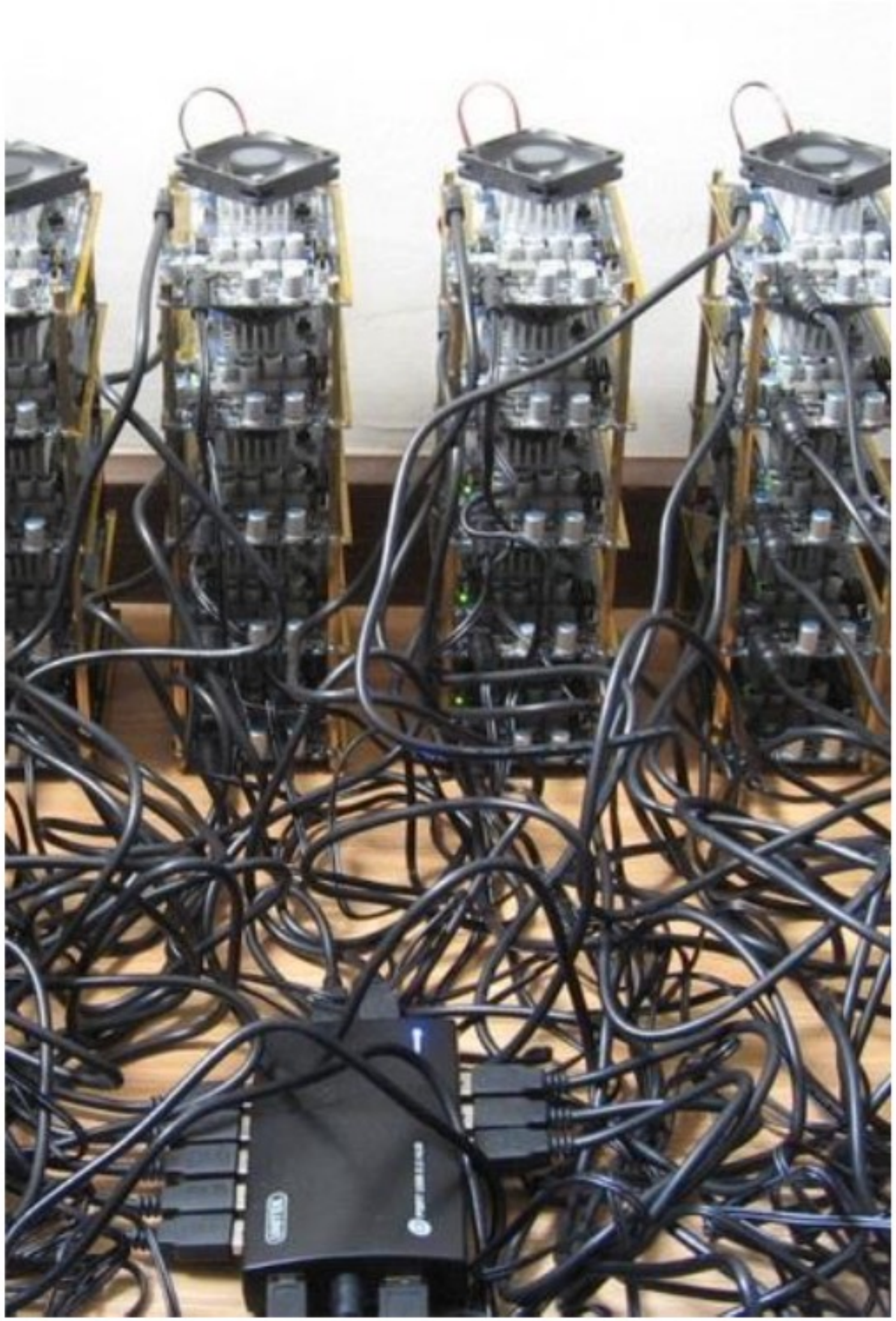
Rev 2 GekkoScience 2-Pac Compac USB Stick Bitcoin Miner 15gh/s+

by GEKKOSCIENCE

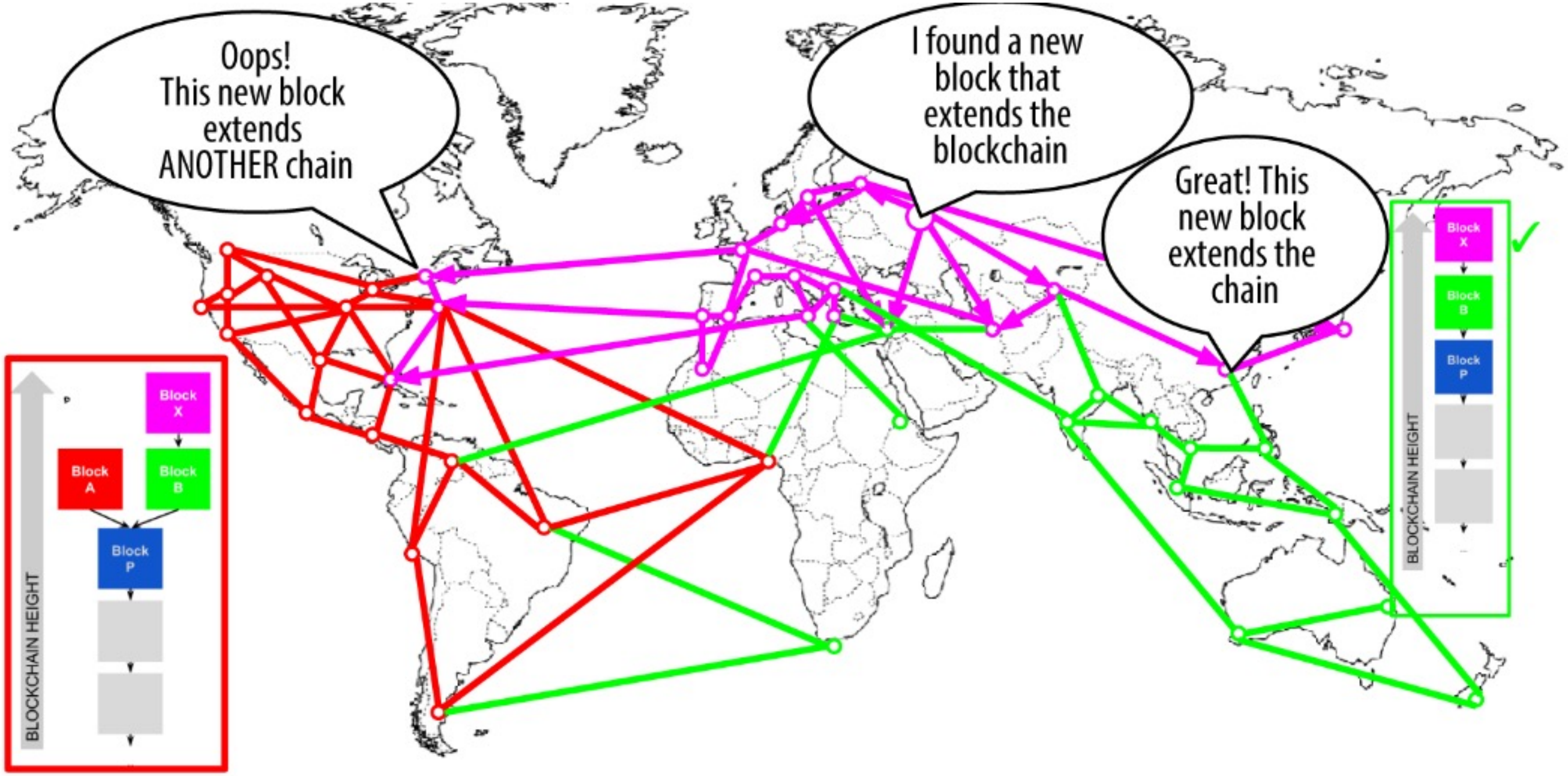
$69.97 + $4.49 shipping

More Buying Choices

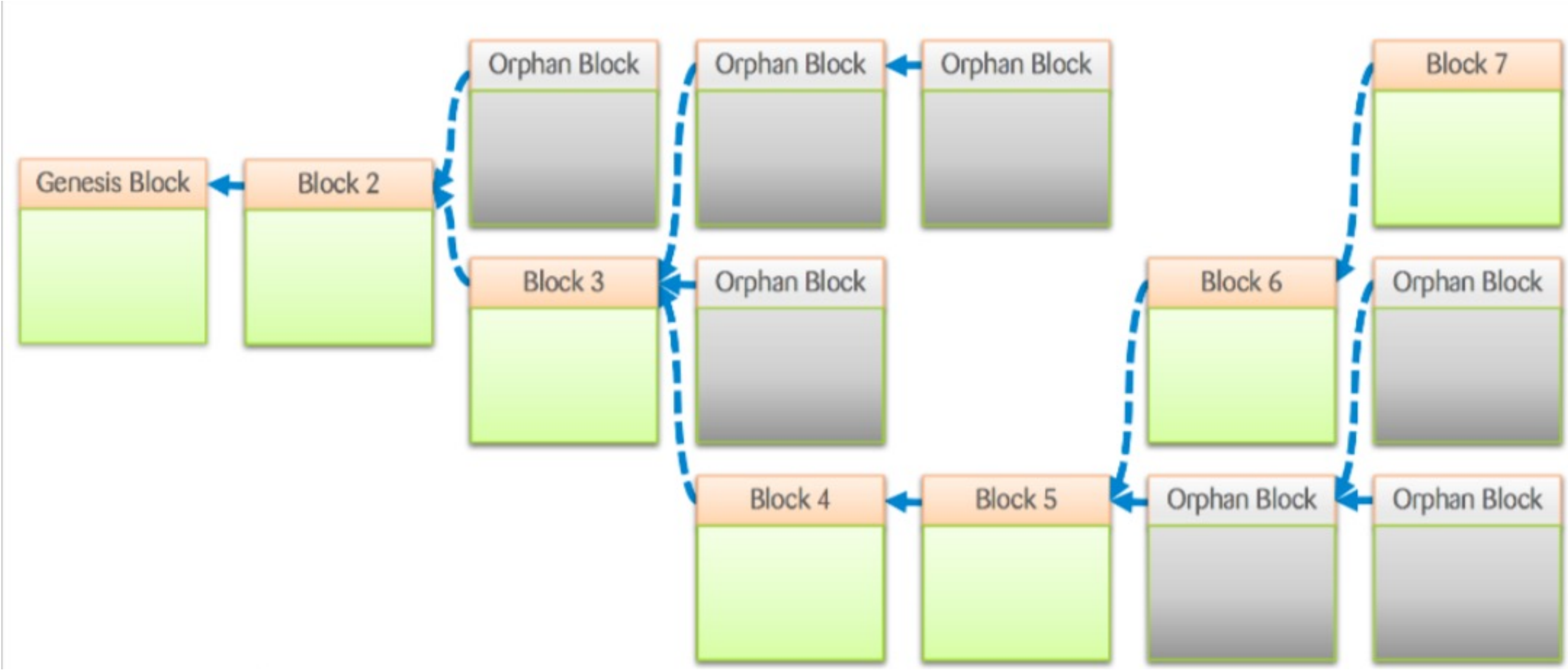
$59.97 (2 new offers)



# Forks

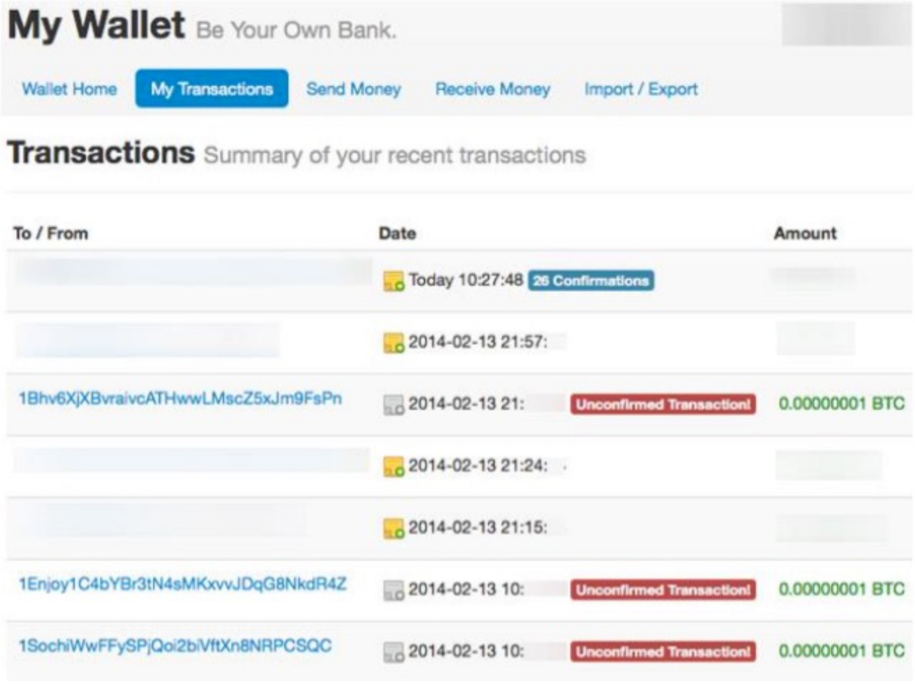

Oops!
This new block extends ANOTHER chain
I found a new block that extends the blockchain
Great! This new block extends the chain
BLOCKCHAIN HEIGHT
Block X
Block A
Block B
Block P
BLOCKCHAIN HEIGHT
Block X
Block B
Block P
✓

# Example of Blockchain Status



# Transaction Confirmations

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

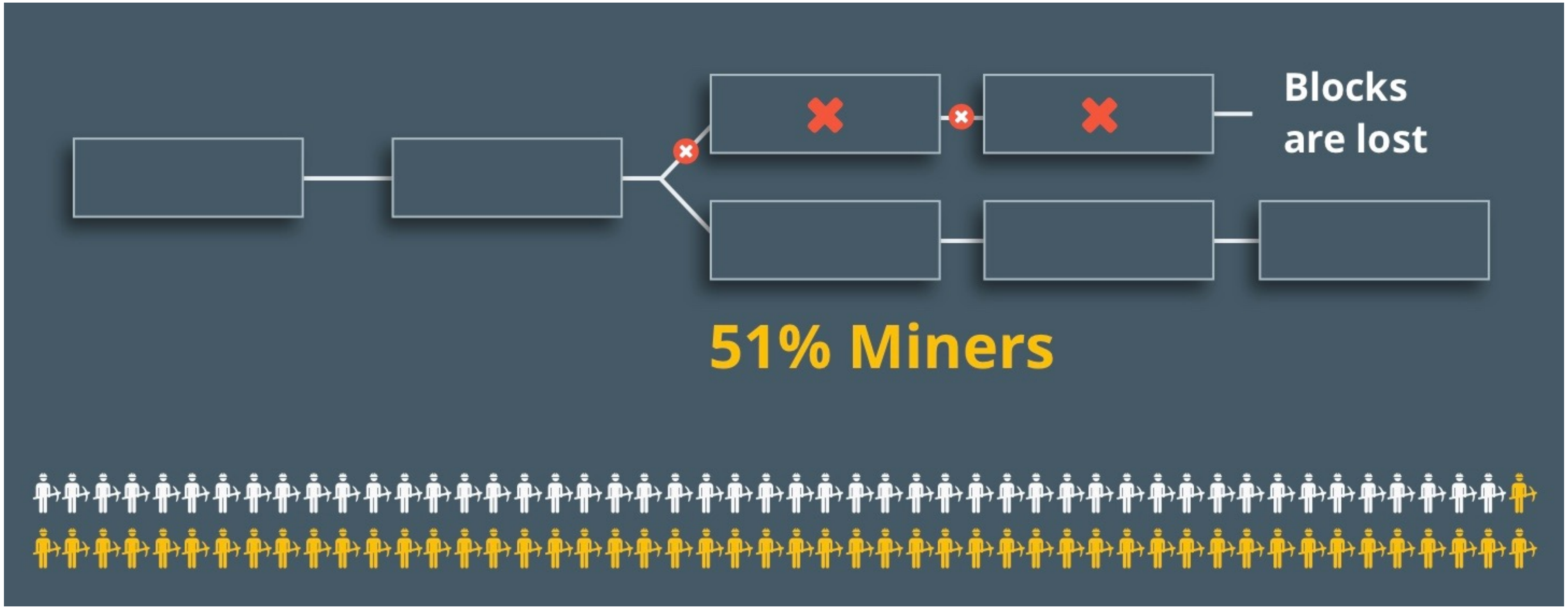


**My Wallet** Be Your Own Bank.

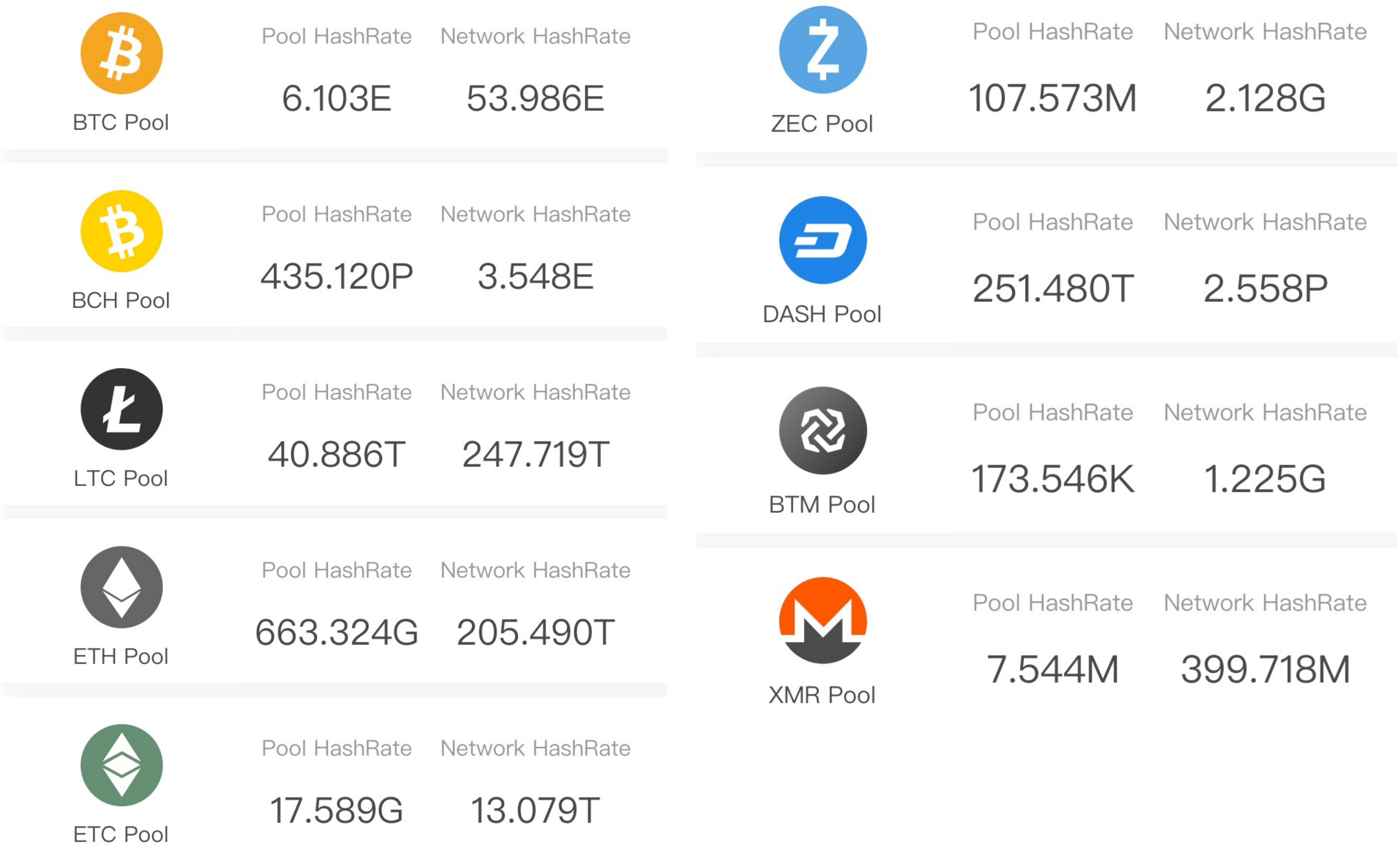
**Transactions** Summary of your recent transactions

| To / From | Date | | Amount |
|---|---|---|---|
| [redacted] | Today 10:27:48 | 26 Confirmations | [redacted] |
| [redacted] | 2014-02-13 21:57: | | [redacted] |
| 1Bhv6XjXBvraivcATHwwLMscZ5xJm9FsPn | 2014-02-13 21: | Unconfirmed Transaction! | 0.00000001 BTC |
| [redacted] | 2014-02-13 21:24: | | [redacted] |
| [redacted] | 2014-02-13 21:15: | | [redacted] |
| 1Enjoy1C4bYBr3tN4sMKxvvJDqG8NkdR4Z | 2014-02-13 10: | Unconfirmed Transaction! | 0.00000001 BTC |
| 1SochiWwFFySPjQoi2biVftXn8NRPCSQC | 2014-02-13 10: | Unconfirmed Transaction! | 0.00000001 BTC |

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

# Smart Contract

- Definition: A smart contract is a computer program executed in a secure environment that directly controls digital assets

### Computer Program

```
if HAS_EVENT_X_HAPPENED() is true:
     send(party_A, 1000)
else:
     send(party_B, 1000)
```

### Properties of Secure Environments

Correctness of execution

- The execution is done correctly, is not tampered

Integrity of code and data

Optional properties

- Confidentiality of code and data
- Verifiability of execution
- Availability for the programs running inside

### Digital Assets

Domain name
Website
Money
Anything tokenisable (e.g. gold, silver, stock share etc)
Game items
Network bandwidth, computation cycles

### Legal vs. Smart Contracts

Legal: “I promise to send you $100 if my lecture is rated 1”
Smart: “I send $100 into a computer program executed in a secure environment which sends $100 to you if the rating of my lecture is 1*, otherwise it eventually sends $100 back to me”

# Smart vs. Legal Contracts

- Why Smart Contracts
  - Automated processing
  - Trust reduction
    - » Trust the secure environments, not a very large number of contract enforcement mechanisms
  - Unambiguous, terms clearly expressed in code

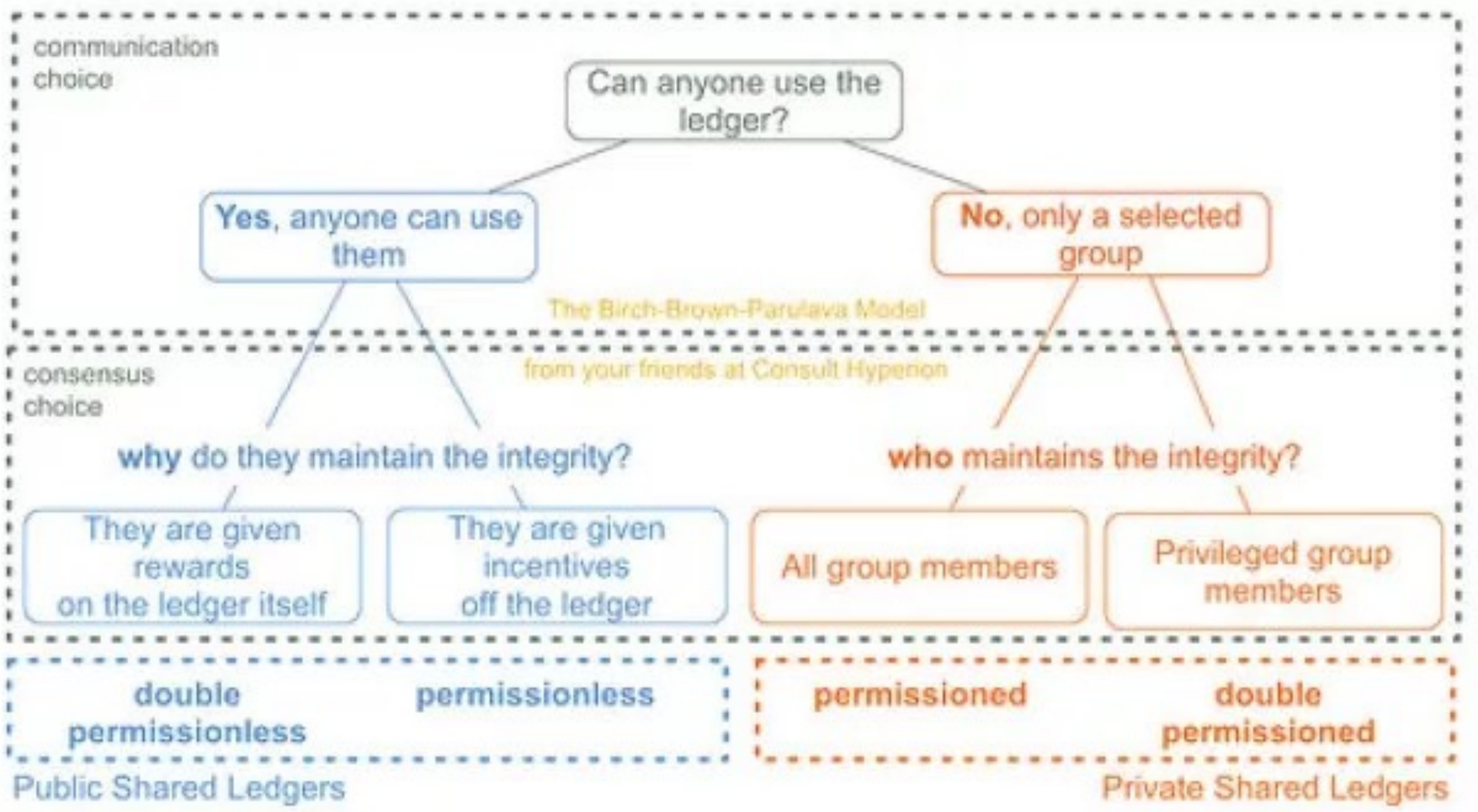
| Legal contracts | Smart contracts |
|---|---|
| Good at subjective (i.e. requiring human judgement) claims | Good at objective (i.e. mathematically evaluable) claims |
| High cost | Low cost |
| May require long legal process | Fast and automated |
| Relies on penalties | Relies on collateral/security deposits |
| Jurisdiction-bound | Potentially international ("a-legal") |

# Ethereum

- Blockchain with expressive programming language
  - Programming language makes it ideal for smart contracts
- Why?
  - Most public blockchains are cryptocurrencies
    - Can only transfer coins between users
  - Smart contracts enable much more applications

- Two types of account:
  - Normal account like in Bitcoin
    - has balance and address
  - Smart Contract account
    - like an object: containing (i) code, and (ii) private storage (key-value storage)
    - Code can
      - Send ETH to other accounts
      - Read/write storage
      - Call (ie. start execution in) other contracts

# Taxonomy of Blockchain



communication choice

Can anyone use the ledger?

**Yes**, anyone can use them

**No**, only a selected group

The Birch-Brown-Parulava Model

from your friends at Consult Hyperion

consensus choice

**why** do they maintain the integrity?

**who** maintains the integrity?

They are given rewards on the ledger itself

They are given incentives off the ledger

All group members

Privileged group members

**double permissionless**

**permissionless**

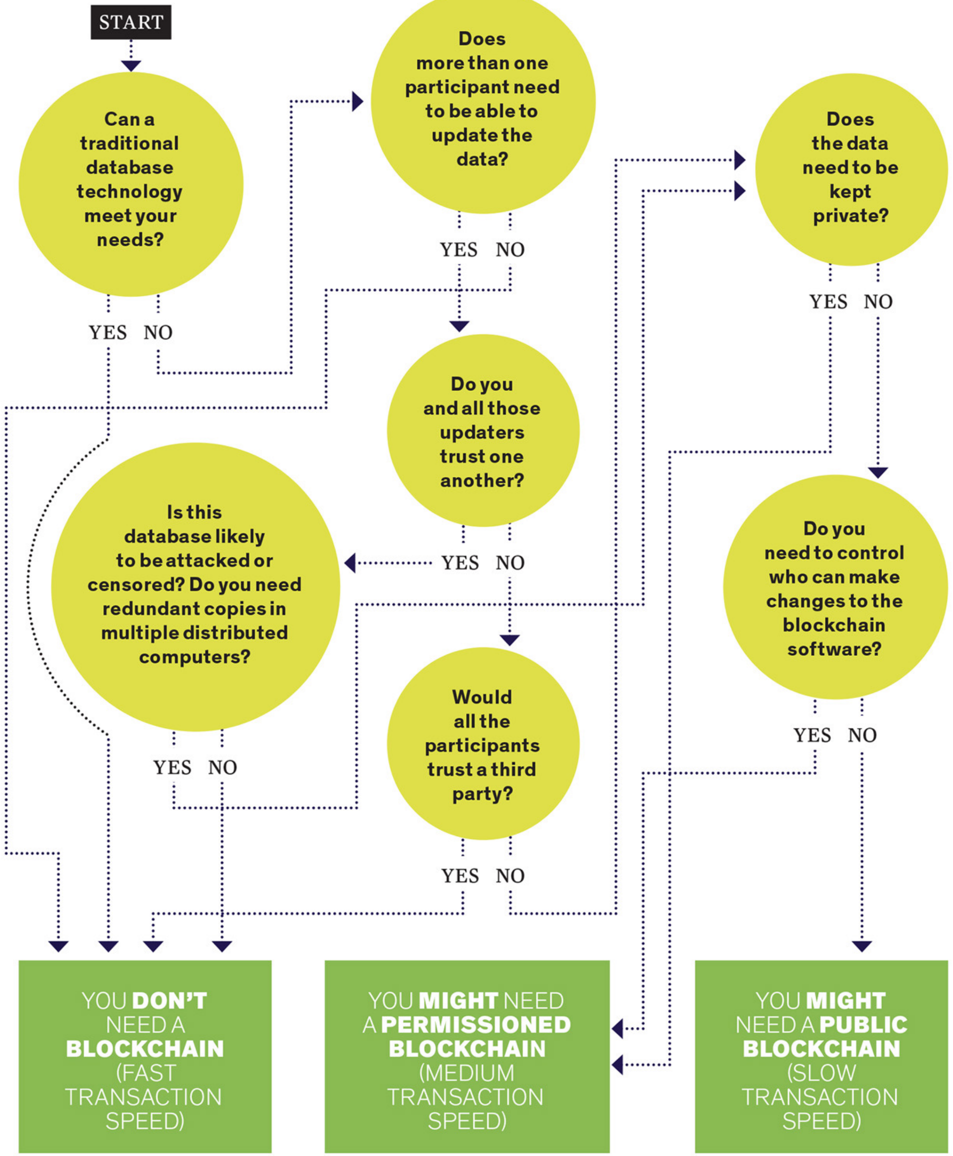
**permissioned**

**double permissioned**

Public Shared Ledgers

Private Shared Ledgers

# Blockchain Testing



START

Can a traditional database technology meet your needs?

YES NO

Does more than one participant need to be able to update the data?

YES NO

Do you and all those updaters trust one another?

YES NO

Is this database likely to be attacked or censored? Do you need redundant copies in multiple distributed computers?

YES NO

Would all the participants trust a third party?

YES NO

Does the data need to be kept private?

YES NO

Do you need to control who can make changes to the blockchain software?

YES NO

YOU **DON'T** NEED A **BLOCKCHAIN** (FAST TRANSACTION SPEED)

YOU **MIGHT** NEED A **PERMISSIONED BLOCKCHAIN** (MEDIUM TRANSACTION SPEED)

YOU **MIGHT** NEED A **PUBLIC BLOCKCHAIN** (SLOW TRANSACTION SPEED)

https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain

# Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google "Yongdae Kim"