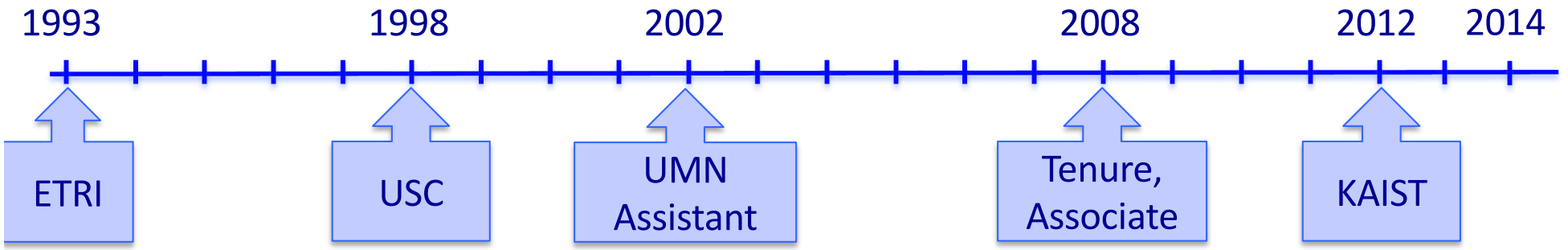
Blockchain
- Opportunities and Challenges -

Yongdae Kim

KAIST

System Security Lab

SysSec
System Security Lab



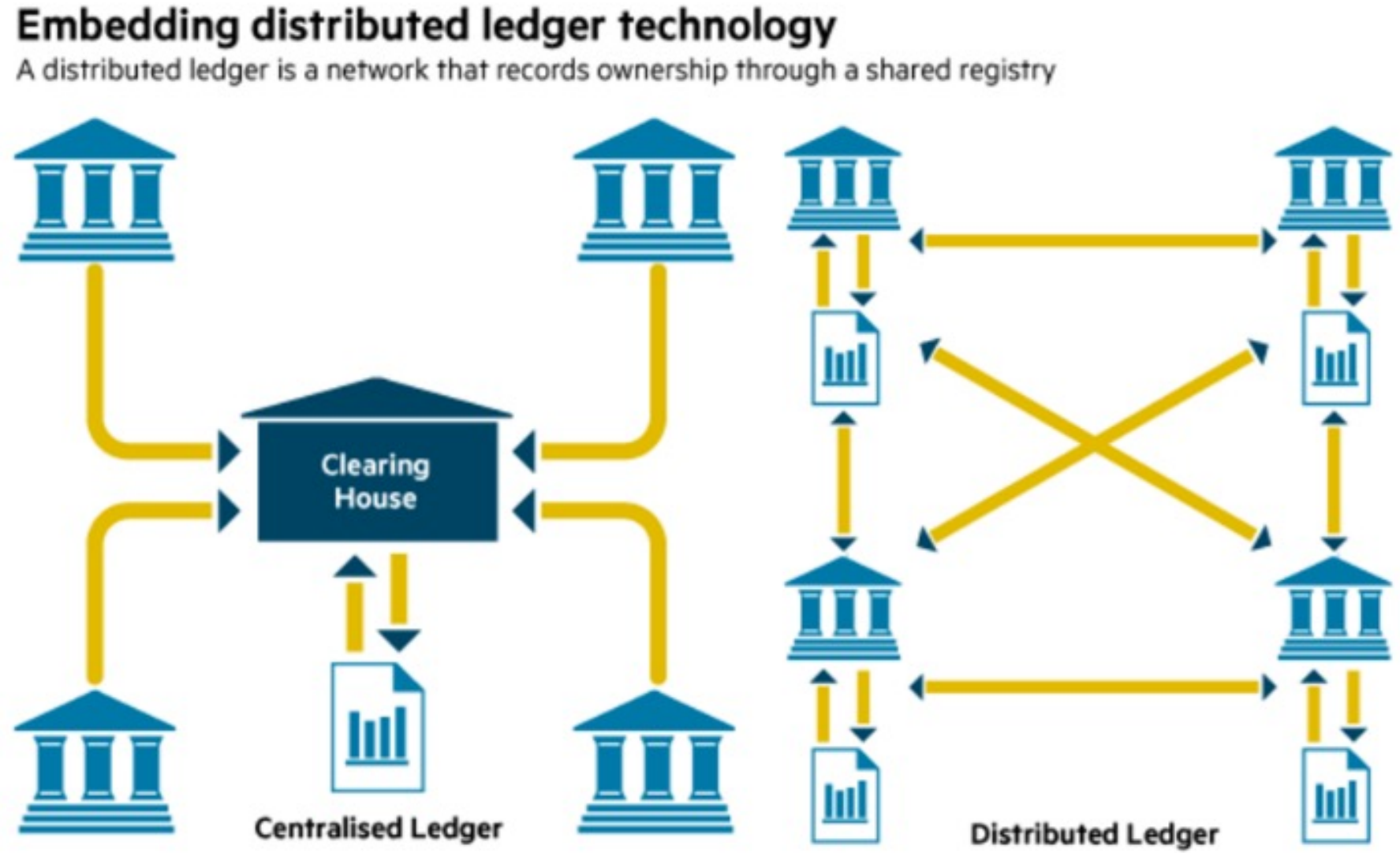
- Research: Security of Emerging Technologies such as
  - Self-driving cars/drones, 4G/5G Cellular, Blockchain, etc.
- Blockchain-Related Career
  - 2000-2004: Group Key Agreement for Peer Groups
  - 2008-2010: Attacking the Kad/Bittorrent Networks
  - 2010-2012: Social Network Analysis
  - 2011-2013: Peer-to-peer network emulation
  - 2017- : Blockchain
- Publication in Blockchain
  - Be selfish and avoid dilemmas: fork-after-withholding attacks on Bitcoin, CCS'17
  - Preventing FAW attack … in submission
  - Fickle Mining … in Submission
  - Security of Solidity Semantics …

Booming Blockchain

- Blockchain in booming all over the world
  - Cryptocurrency investment war at the end of 2018
  - 3rd Gen Blockchain after Bitcoin and Ethereum
  - Many ICOs and various Business Modem

- Today's topic
  - Blockchain Boom
  - What's going wrong?
  - What should we do?

Centralized vs. Decentralized Ledger



Bitcoin

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

Ethereum

- 2nd 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, 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, Coinffeine, PAYMIUM, CEX.IO, BitOasis, SHAPE SHIFT, BTC express, coinsecure, coinsetter, Bits of Gold

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

Hard Wallets
TREZOR, case, Ledger Wallet, keepkey

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

Microtransactions
BitMesh, BitWall, ChangeTip, ProTip, Strawpay

Merchants
bitpay, Bitnet, Coinkite, Coinify, PEX, CoinPayments, coinsnap, coinbase, CoinSimple, BitPagos

Compliance
ELLIPTIC, third key solutions, PROTUS, CHAINALYSIS, Sig3, BLOCKSEER, CryptoCorp, identityMind GLOBAL, Tradle, vogogo, COINALYTICS, BLOCKVERIFY, Merkle Tree

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

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

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

Financial Data
bitcoinity., CoinMarketCap, CryptoCoin, BRAVE NEW COIN, BlockJockey, CRYPTRADER, BitcoinWisdom, TradeBlock, CoinGecko, Coinhills

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

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

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

Payroll & Insurance
paybits, bitWAGE, DYNAMIS

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

MIDDLEWARE & SERVICES

Services
CRYPTONOMEX, B9, CONSENSYS, SolidX, applied blockchain, 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, COLOREDCOINS, factom, ChromaWay

Platforms
Counterparty, Monetas, Omni, Mercoin, blockstack, HYPERLEDGER, Tendermint, BLOCKAPPS, applied blockchain

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, BITCOINCZ

Source: http://startupmanagement.org/blog

Blockchain Psychology: Cypherpunk

- 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.

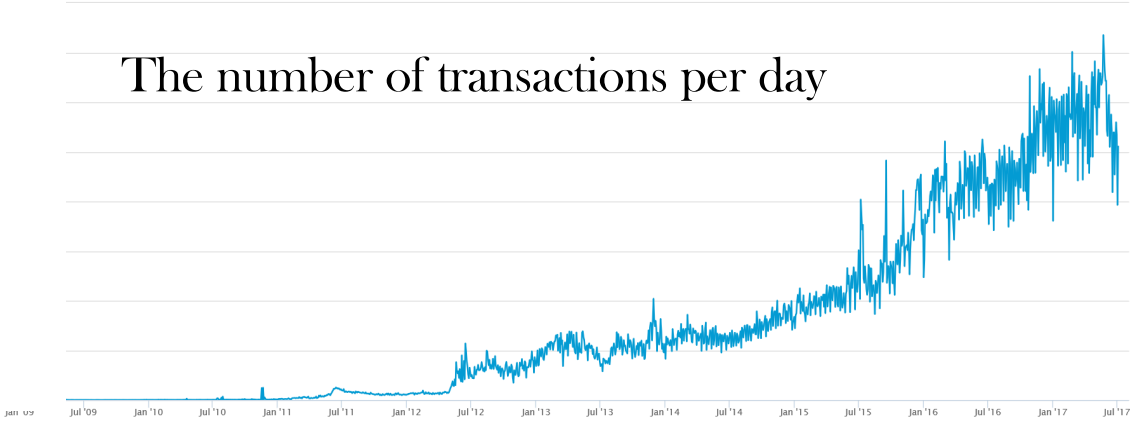
Bitcoin P2P e-cash paper

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

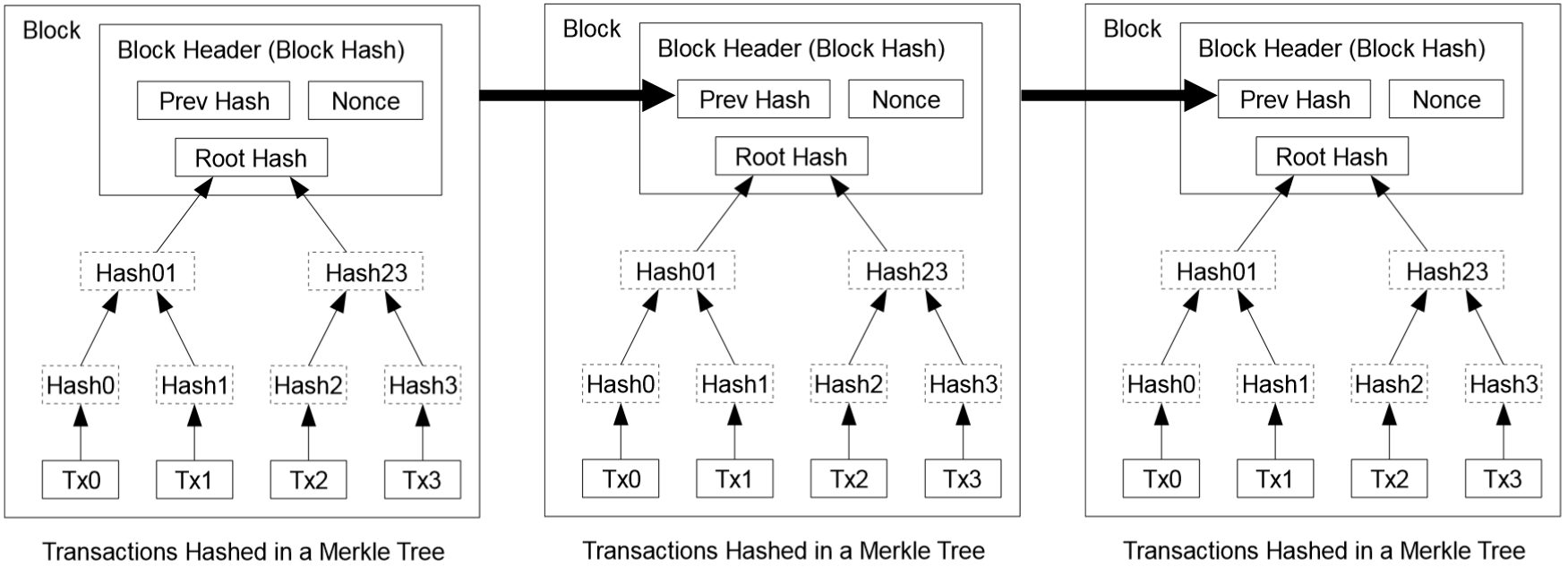
I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

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.



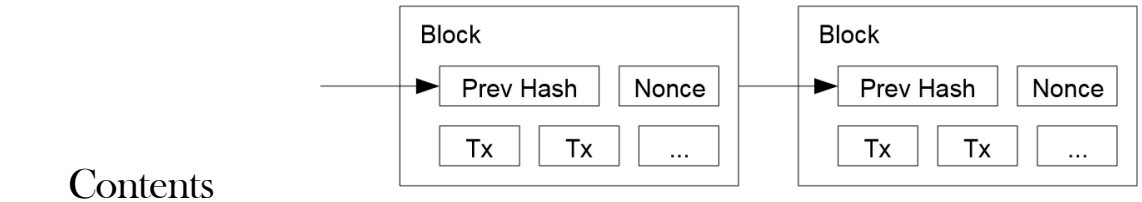
Blockchain



- 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

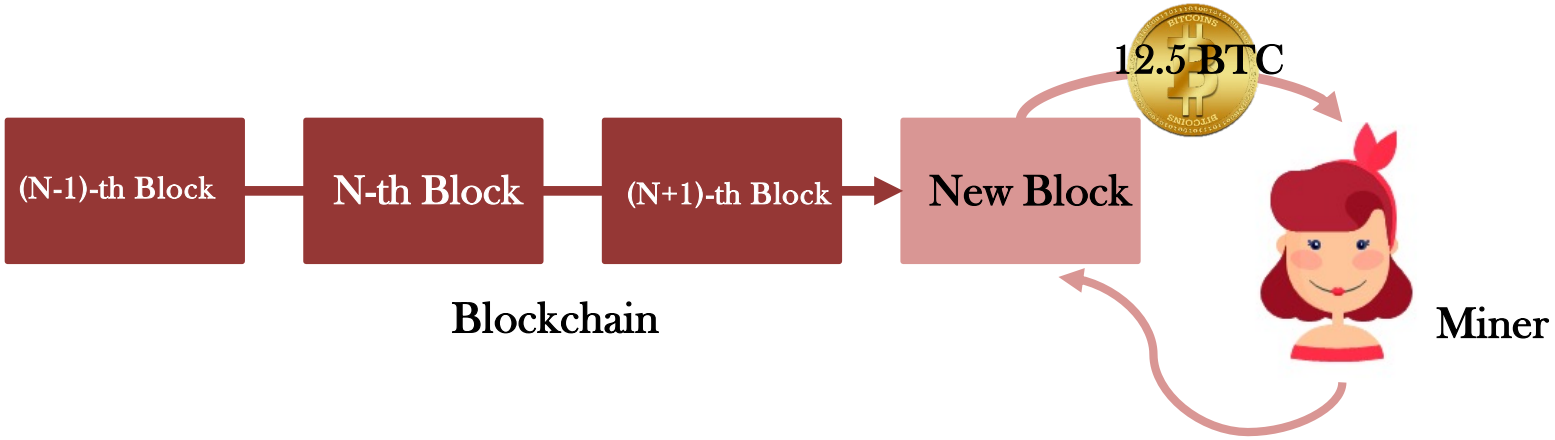
Nonce

```
"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.

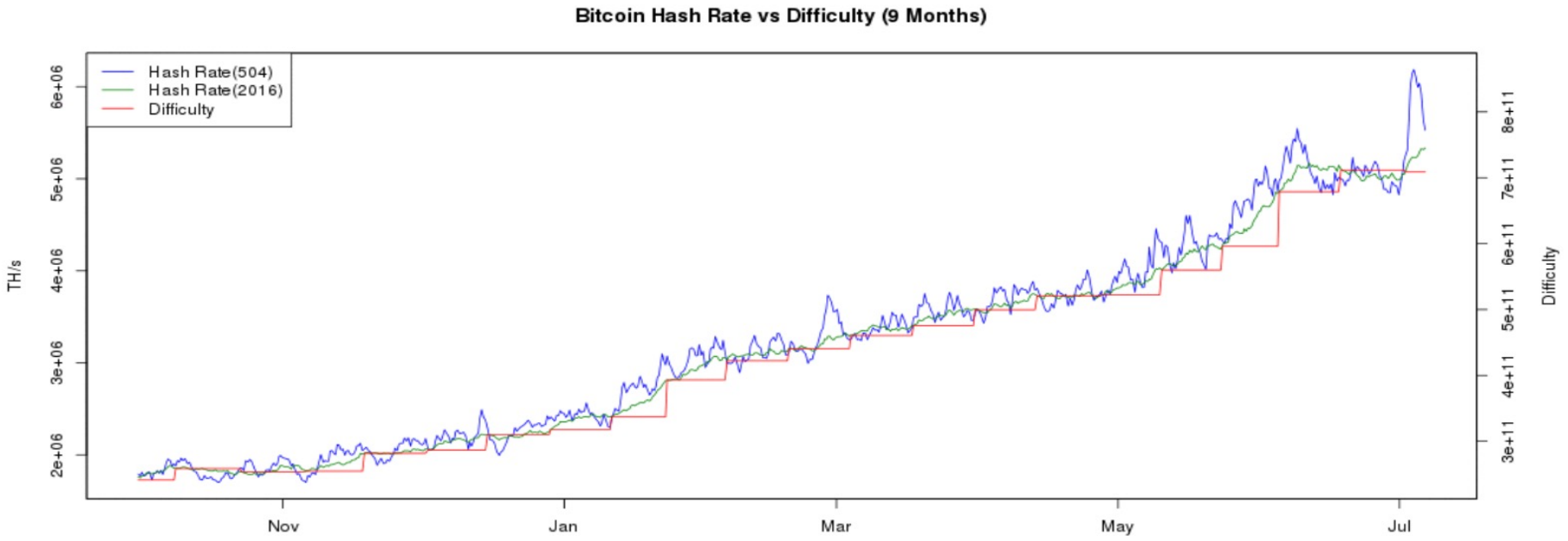


Miner's Incentive

- 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

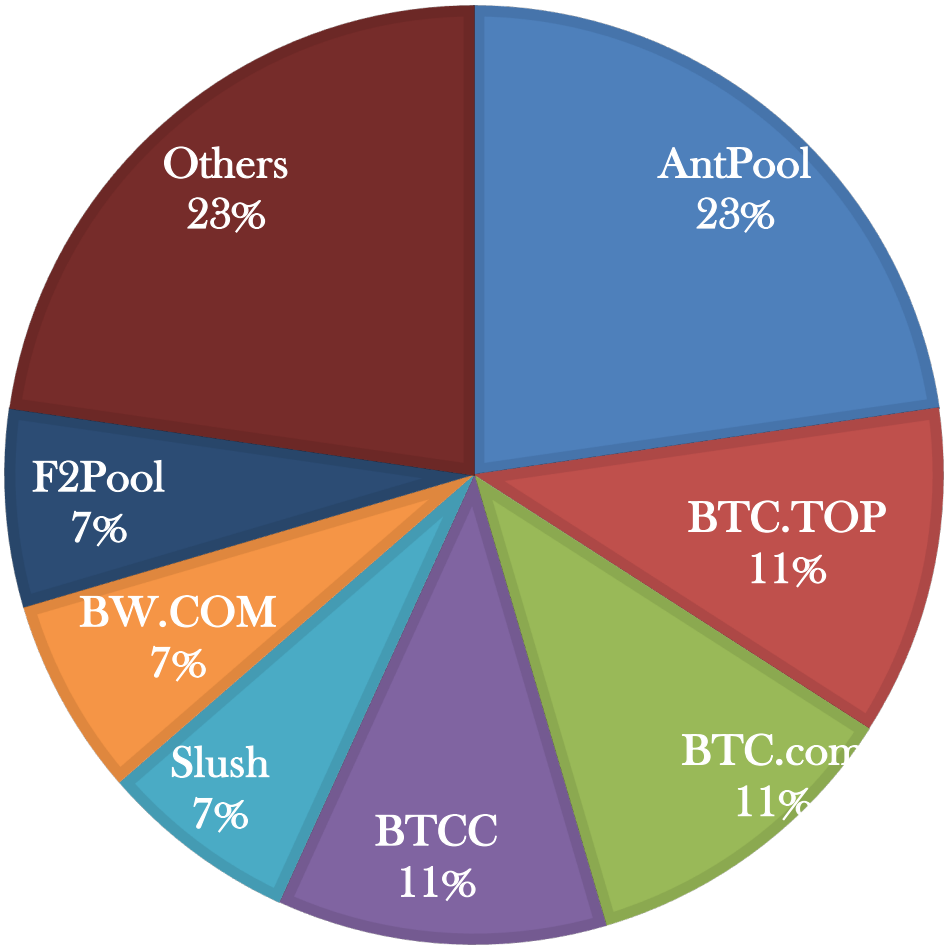
- Rewarded only if block is on eventual consensus branch!

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

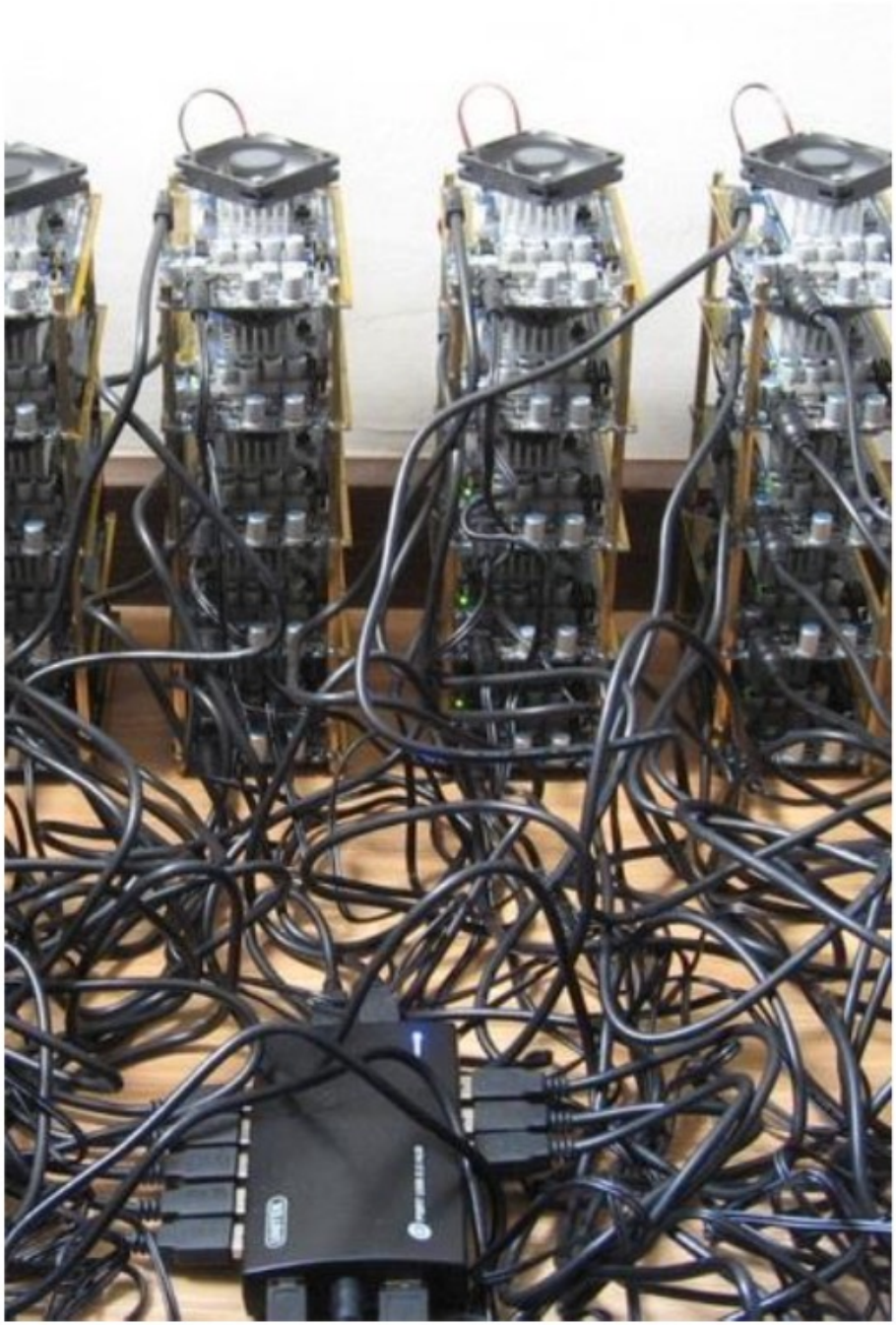
$1,887.00
FREE Shipping on eligible orders
Only 12 left in stock - order soon.

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

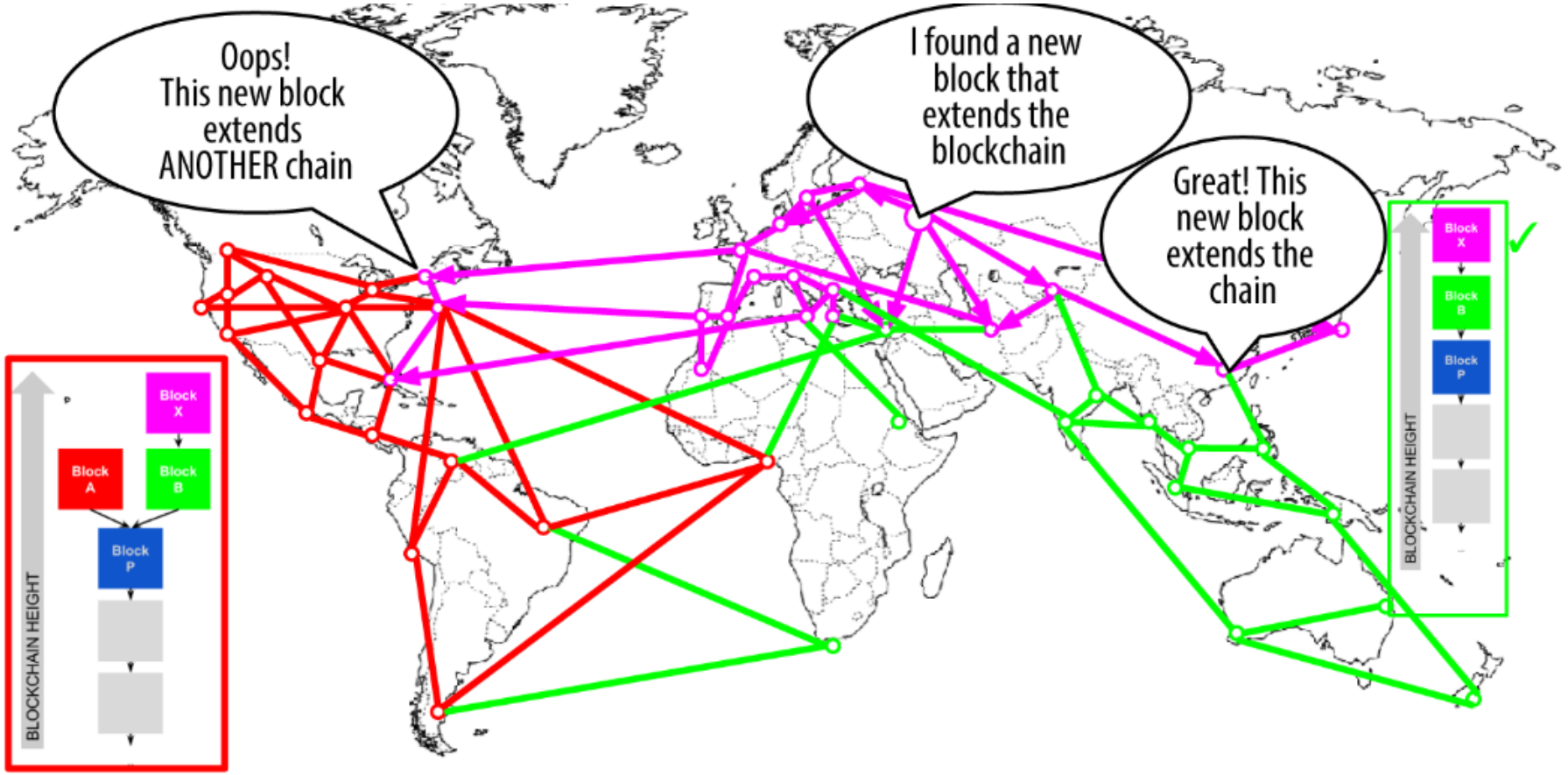
Rev 2 GekkoScience 2-Pac Compac USB Stick Bitcoin Miner 15gh/s+
by GEKKOSCIENCE

$69.97 + $4.49 shipping

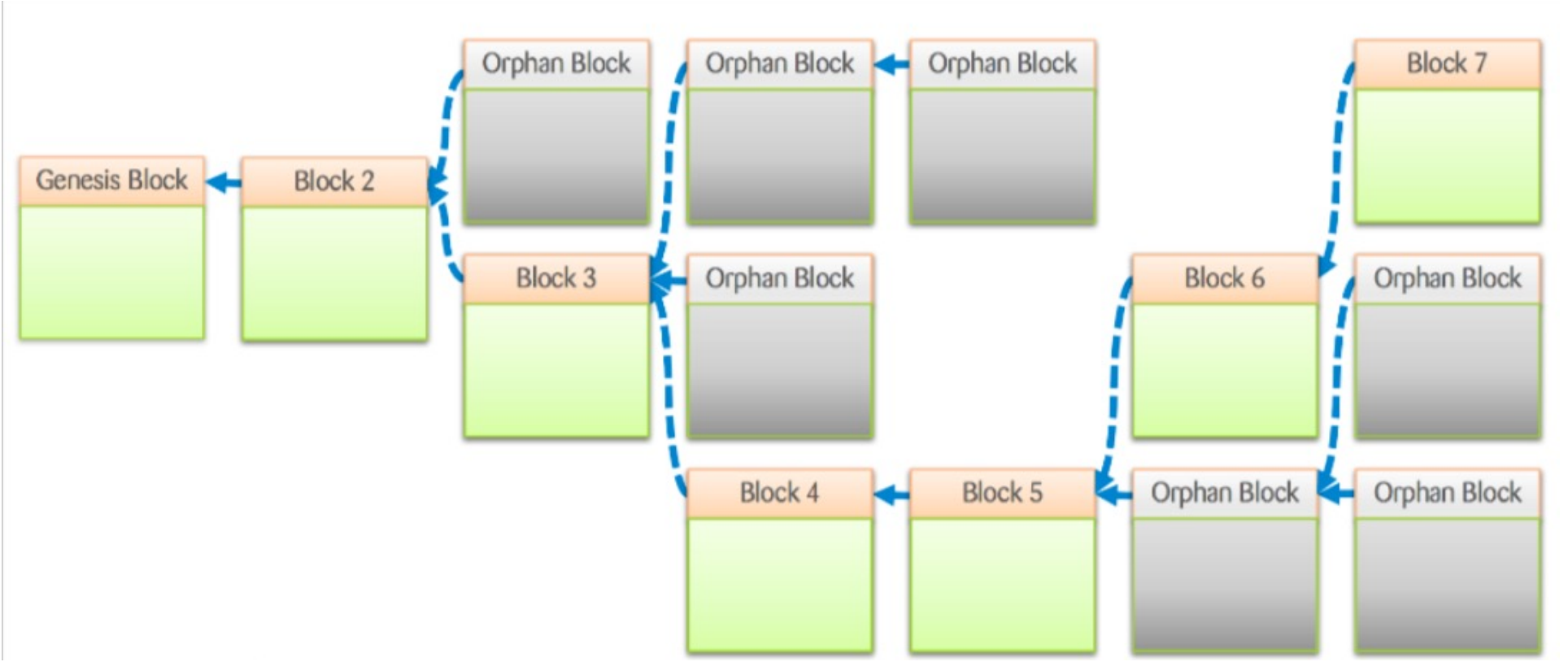
More Buying Choices
$59.97 (2 new offers)



Forks

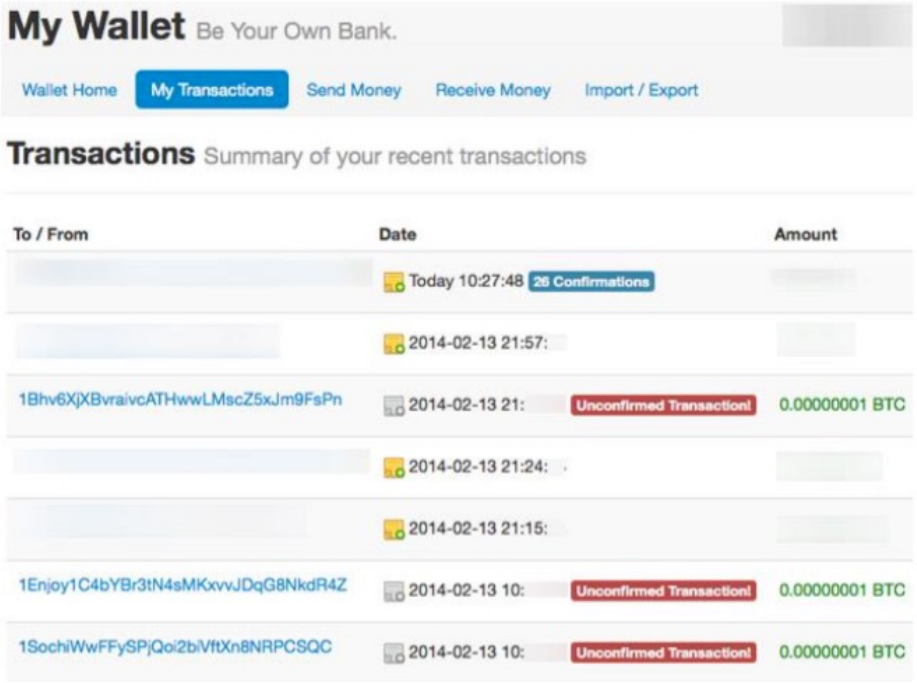

Oops!
This new block
extends
ANOTHER chain
I found a new
block that
extends the
blockchain
Great! This
new block
extends the
chain
BLOCKCHAIN HEIGHT
Block A
Block X
Block B
Block P
BLOCKCHAIN HEIGHT
Block X
Block B
Block P

Example of Blockchain Status

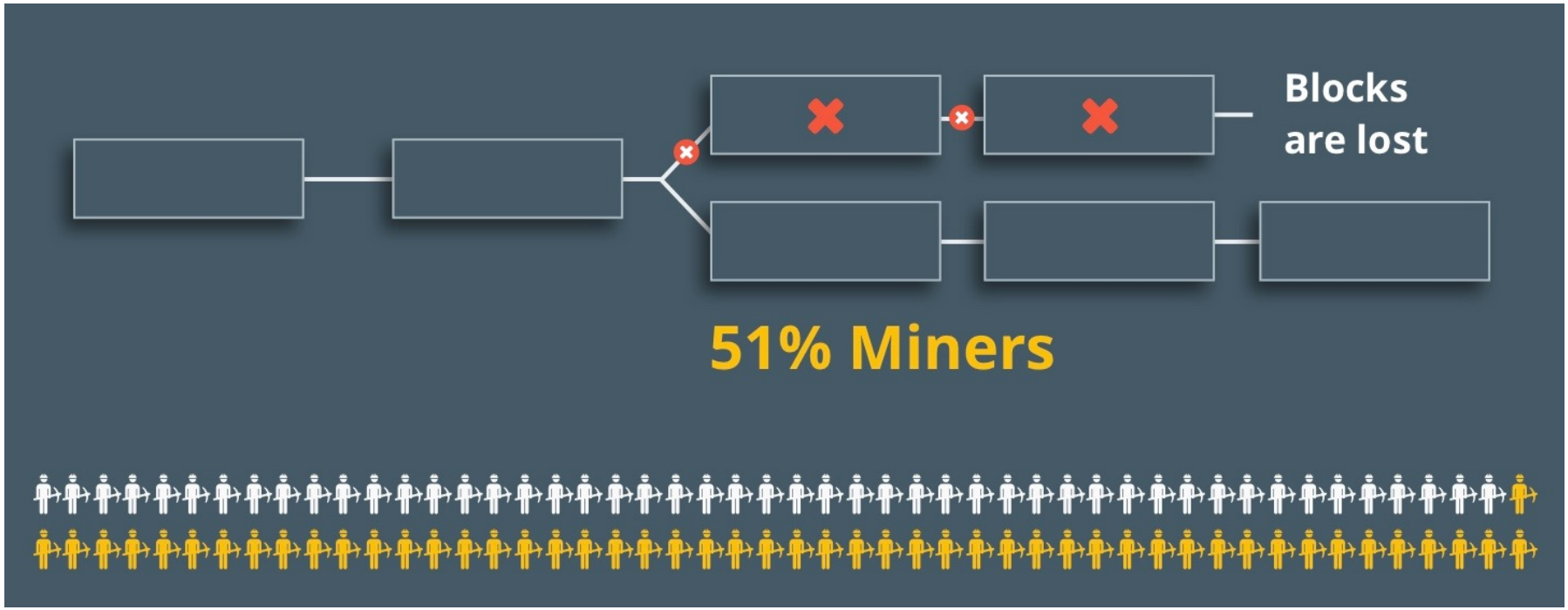


Transaction Confirmations

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



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)
```

Digital Assets

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

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

Legal vs. Smart Contracts

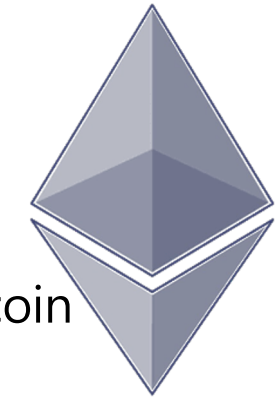
Legal: “I promise to send you $100 if my lecture is rated 1”
Smart: “I send $100 into a computer program executed in a secure environment which sends $100 to you if the rating of my lecture is 1*, otherwise it eventually sends $100 back to me”

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”)

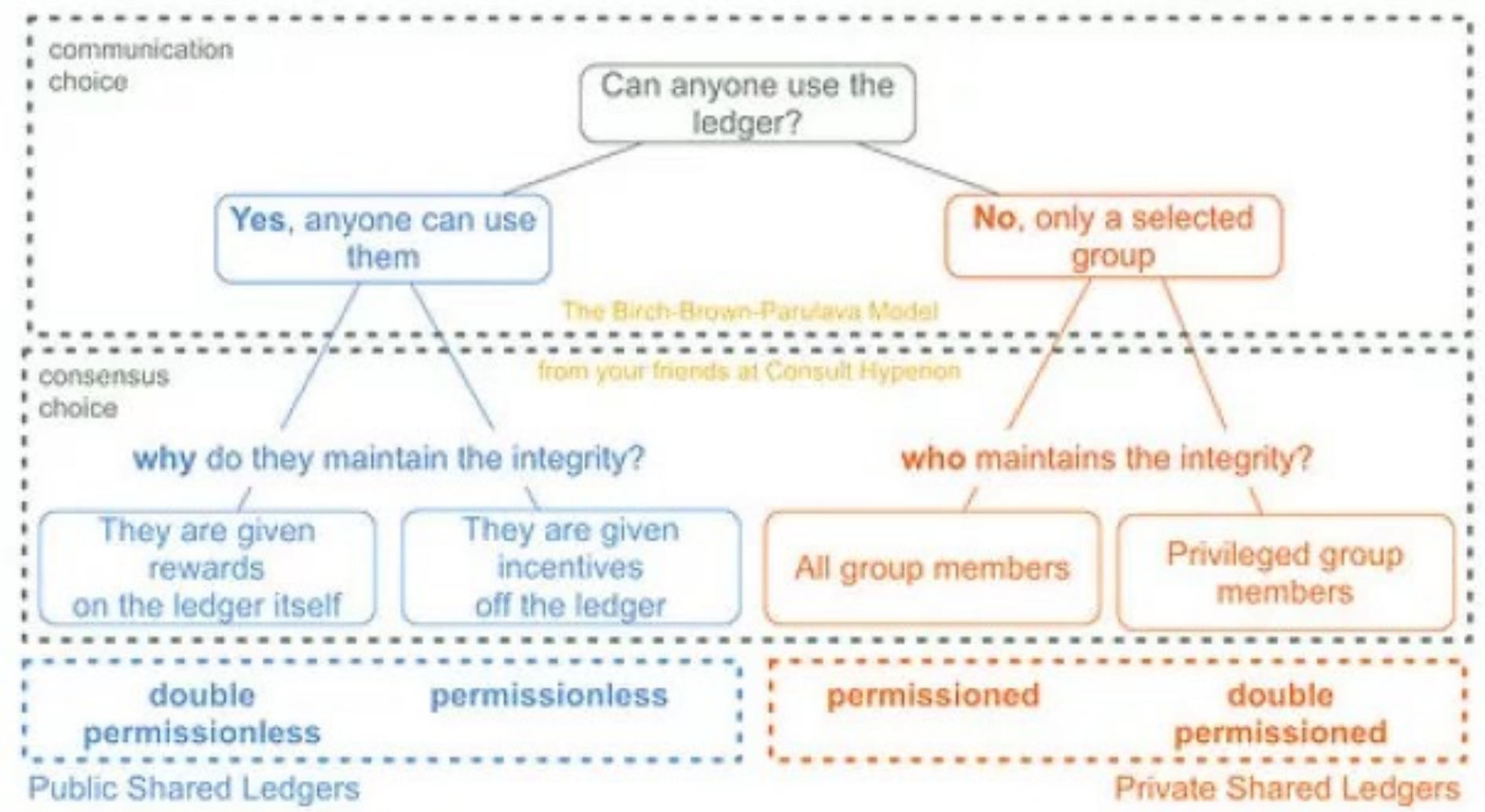
Ethereum



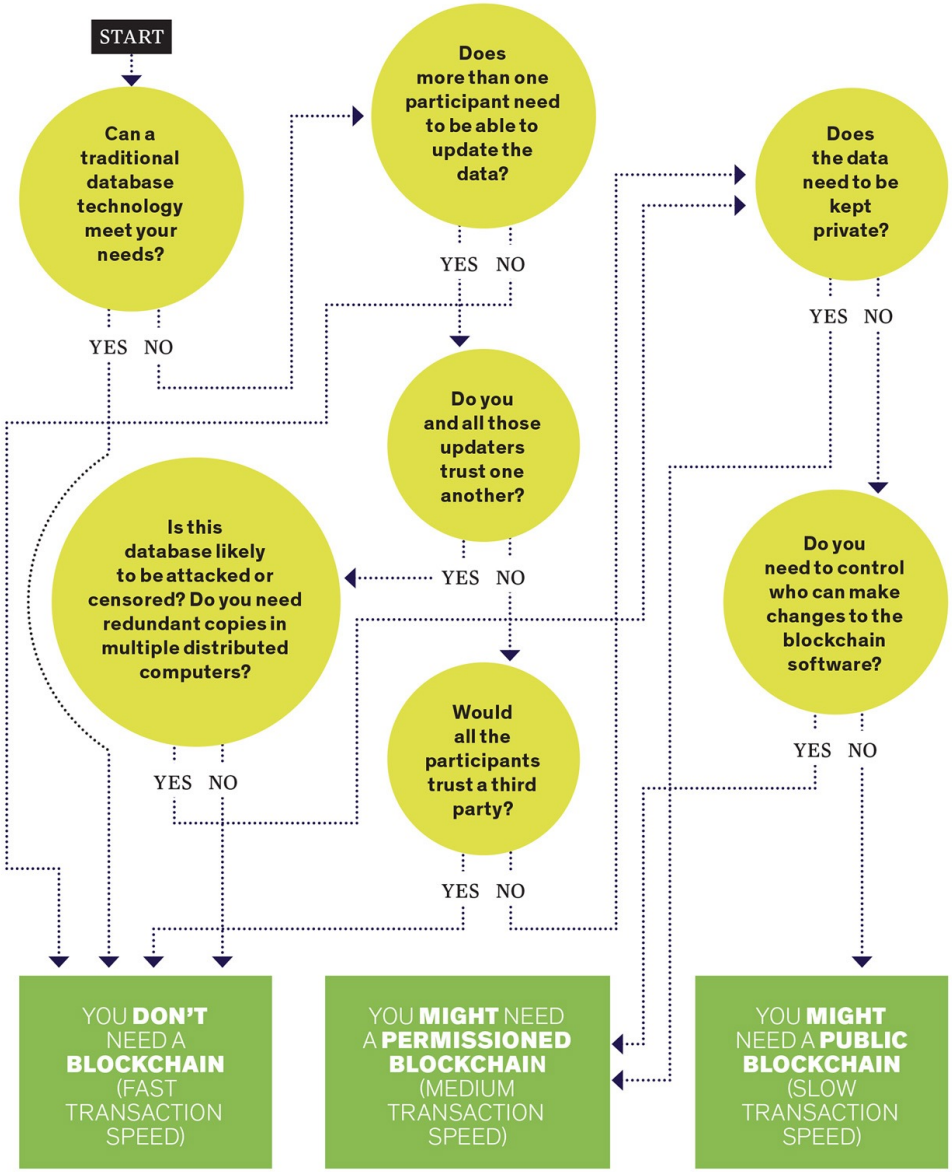
- Blockchain with expressive programming language
  - Programming language makes it ideal for smart contracts
- Why?
  - Most public blockchains are cryptocurrencies
    - » Can only transfer coins between users
  - Smart contracts enable much more applications

- 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



Blockchain Testing



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

Public Blockchain

- Pros
  - Decentralization: Preventing monopoly by nations and industries
  - Transparency: Prevention of Information Manipulation by centralized entity
  - Anti-censorship: Prevention of Information Monopoly by nations
  - Anyone can use

- Cons
  - Speed, Storage
  - Public Information
  - Governence problem in software management, overall direction
  - Difficulty in price forecasting, waste of energy

Private (Permissioned) Blockchain

- Overview
  - Consensus by small trusted entities
- Pros
  - Speed, Storage
  - Privacy
  - Governance
- Cons
  - Closedness
  - Scalability
  - Monopoly
  - Shared DB?

Current Problems?

ICO scams

Giza ICO Scammers Make Off with $2 Million

DEC 4, 2017 @ 02:46 PM 11,393

The Little Black Book of Billionaire Secrets

$15 Million ICO Halted By SEC For Being Alleged Scam

Seele ICO Investors Stung in $2 Million Telegram Group Scam

3808 Views

February 4, 2018 by Paul de Havilland — 3 Comments

TECHNOLOGY

2 Founders of $32 Million Centra Virtual Currency Project Are Arrested

By NATHANIEL POPPER APRIL 2, 2018

Misunderstandings on Blockchain

- Blockchain is fast, secure and decentralized.
- Blockchain is secure.
- VCs can evaluate Blockchain technologies.
- Platform war may end in 2-3 years.
  - Now is the time to find Business Model.

Fast, Secure and Decentralized?

- Claims taking advantages of public and private blockchain.

- Trilemma by Vitalik Buterin: Only 2/3 among below is possible.
  - Decentralized: Anyone can use. Necessary condition for robustness against censorship
  - Security: Robustness against attacks on small number of nodes
  - Scalability: Fast transaction speed

- All experts are trying to solve the Trilemma

Blockchain is Secure?

- Double-Spending, CCS2012
- Bitcoin Transaction Graph, FC2013
- Eclipse Attacks on Bitcoin, Sec2015
- Eclipse Attacks on Ethereum
- Routing Attacks on Bitcoin, SP2017
- Miner's Dilemma, SP2015
- Fork after withholding (FAW) attacks: CCS 2017 (my paper)

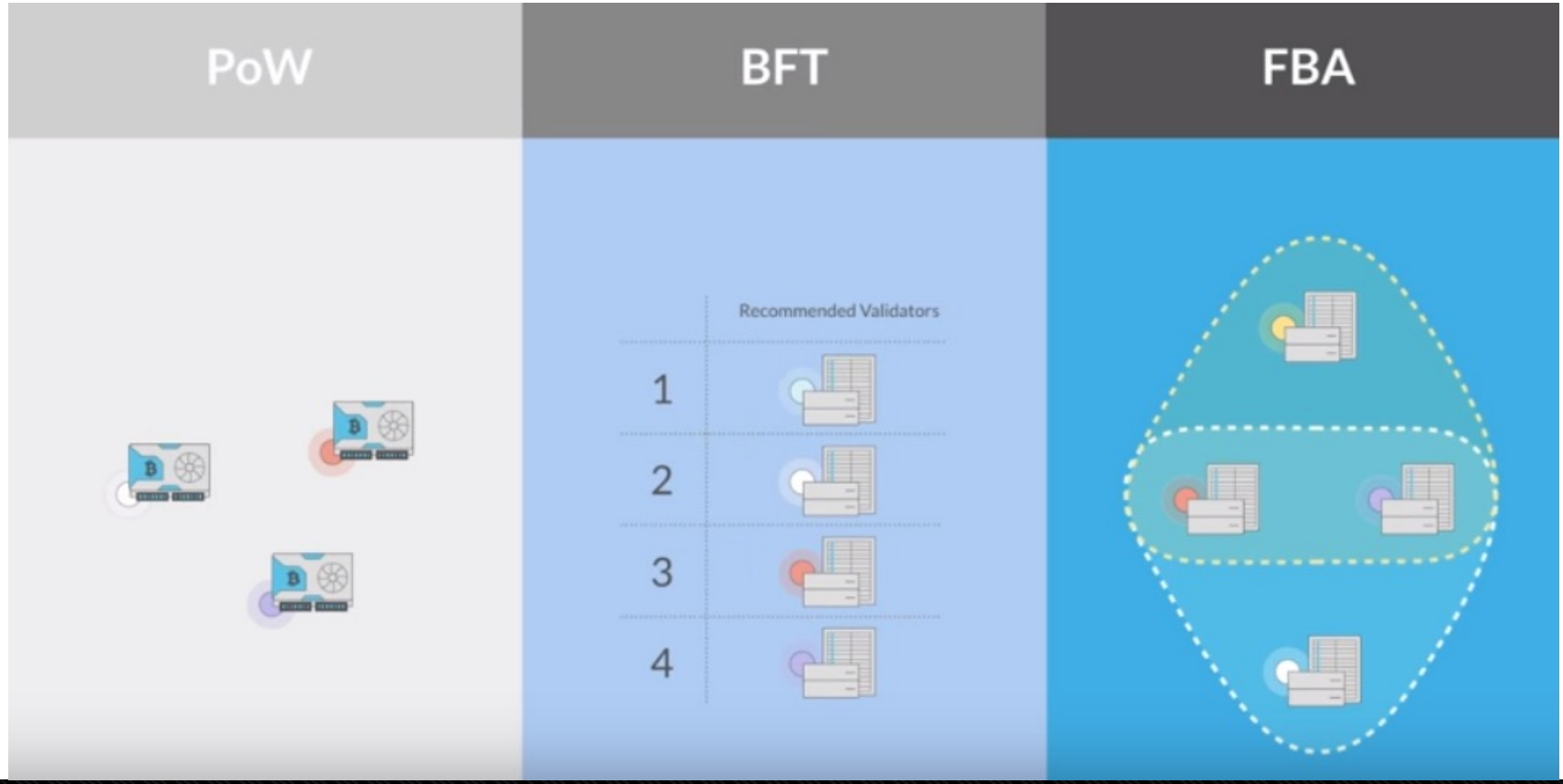
ZEUS: Analyzing Safety of Smart Contracts
NDSS 2018
Automatic detection of vulnerable smart contract
- Reentrancy - Unchecked send - Block state dependence - Transaction order dependence - Failed send - Integer overflow/underflow - Transaction state dependence
21,281 / 22,493 (94.6%) Vulnerable (1524 unique contract)

Technical Evaluation of Blockchain

- Why is it possible?
  - Whitepaper, Academic Paper, … : Theoretical evaluation
  - Most are open-sourced.
  - Access to network in case of public blockchain
- But reality is …
  - Investment war ➔ Blind investment
  - The gap between the theory and the practice
  - Lacking blockchain evaluation technology

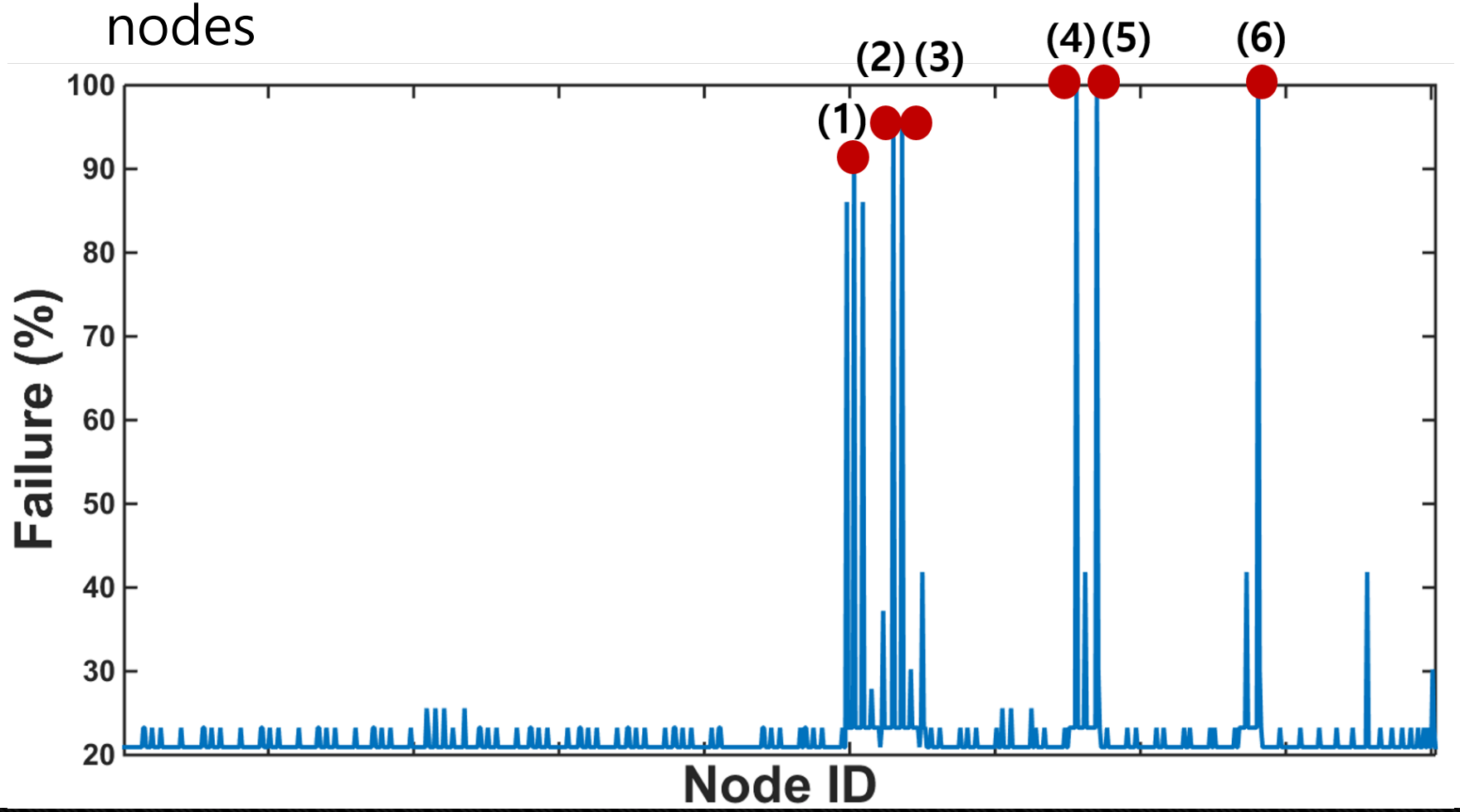
The Gap between Theory vs. Practice

- Stellar Rumens
  - Top 6 coin in Coinmarketcap
  - Designed by David Mazieres at Stanford



The Gap between Theory vs. Practice

- Cascade Failure
  - How many quorums remain after couple of broken nodes



End of Platform War?

David Mazieres
Network System, Prof @ **Stanford**
The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus

Aggelos Kiayias
Crypto, Prof @ **Edinborough**
Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol

Silvio Micali, Nikolai Zeldovich
Crypto, System, Prof @ **MIT**
Algorand: scaling Byzantine agreements for cryptocurrencies

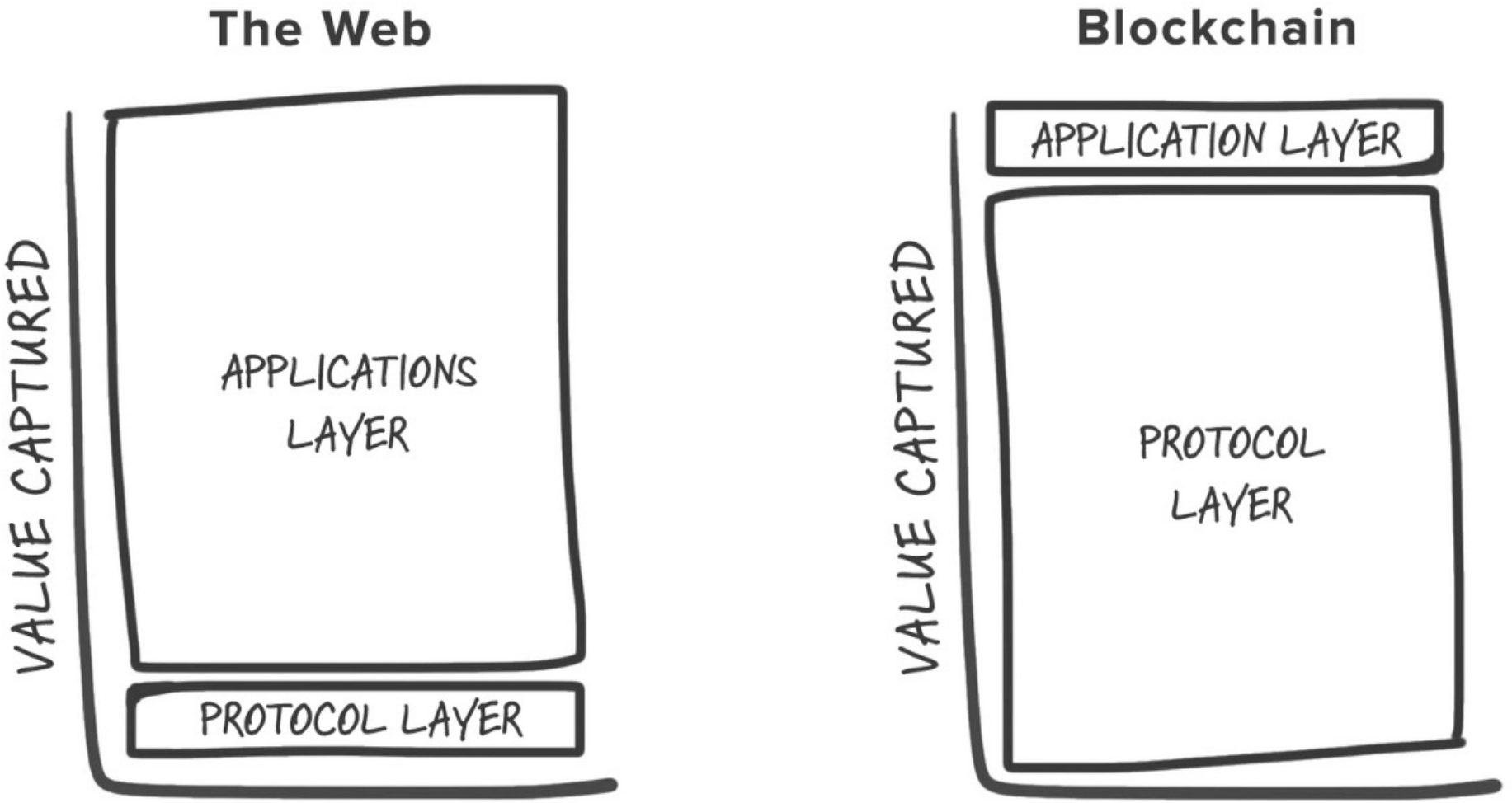
Elaine Shi, Rafael Pass
Crypto, Prof @ **Cornell**
Thunderella: Blockchains with Optimistic Instant Confirmation
Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure PoS

Emin Gun Sirer
Distributed System, Prof @ **Cornell**
Snowflake to Avalanche: A Novel Metastable Consensus Protocol Family for Cryptocurrencies

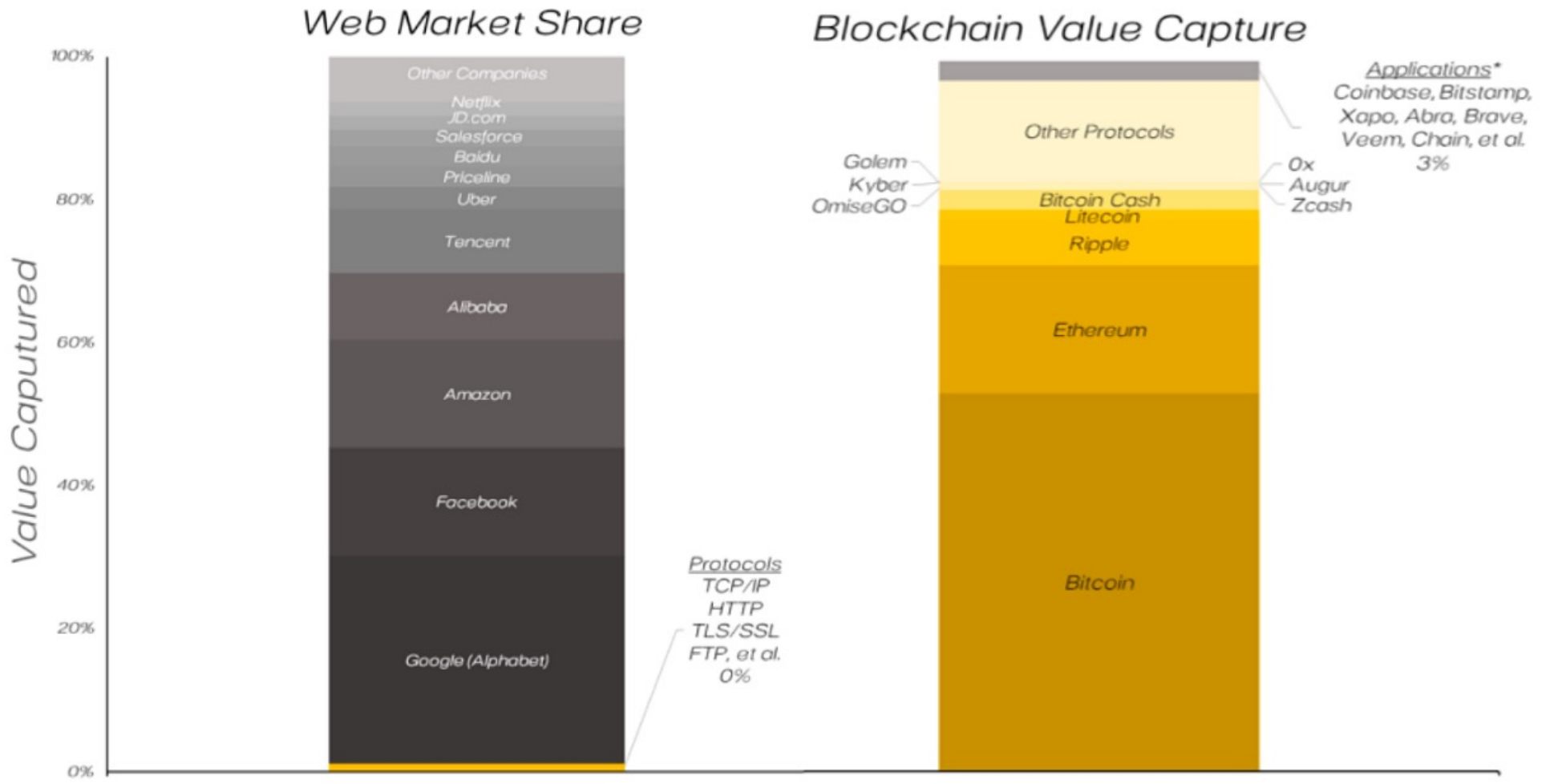
Dawn Song
Theory+Anything, Prof @ **Berkeley**
Oasis Lab

What should we do?

Platform War is not Over!



Protocol Value 97% >> Application Value 3%



* Ripple is the most valuable company in crypto space. As the vast majority of its value is a pass-through of its ownership of 62bn of the XRP protocol tokens, it is not included as an equity/application.

Source: Coinmarketcap.com, Wikipedia, Pantera data

Blockchain Evaluation Technology

- For investment or outsourcing, evaluation (trilemma) technology is necessary
  - Theoretical Evaluation
  - Evaluation of Network and Decentralized System
  - Security Evaluation
  - Evaluation of Token Economy and Incentivization

- Development of Automatic Evaluation System
  - In case of smart contract, automatic evaluation is possible because standardized development process
  - In case of consensus algorithm or blockchain on top of it, no standardized platform exists. ➔ Difficulty in automatic evaluation

R&D in Fundamental Technologies

- Fundamental vs. Application Technologies
  - What did we invest during big data boom? What do we have now?
  - Fundamental Technologies: “Design of New Blockchain”, led by Univ
    - » Education: Crypto, distributed systems, game theory, system development, probability theory, programming languages …

- Direction of Fundamental Technologies
  - Research on breaking Trilemma
    - » New Consensus algorithm!
    - » New Platform and smart contract!
  - Evaluation technology ➔ Self-regulation by private sector
    - » Implementable? Technological value? Security?
  - Fraud Detection: Money laundering, market manipulation, …

Conclusion

- Take your time! We still have time!
  - If you want to do with private blockchain, do that quick
  - For public blockchain
    - » Impossibility for solving trilemma may be proved!
    - » It will take at least 5 years, even if it is solved.
    - » Still plenty of room for technical improvement
- War on developing platform for protocol and smart contract
  - For a while, new consensus algorithms will be developed.
    - » Even new protocols require quite a long time to be stabilized.
  - Technical requirements for smart contract are still unclear.
  - Evaluation technology is still required.
- Human resource need and Research
  - Time for R&D in fundamental technologies
  - Dire need for human resources
  - Global competition, rather than local competition

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"