



암호화폐와 블록체인

김용대
카이스트
시스템보안연구실

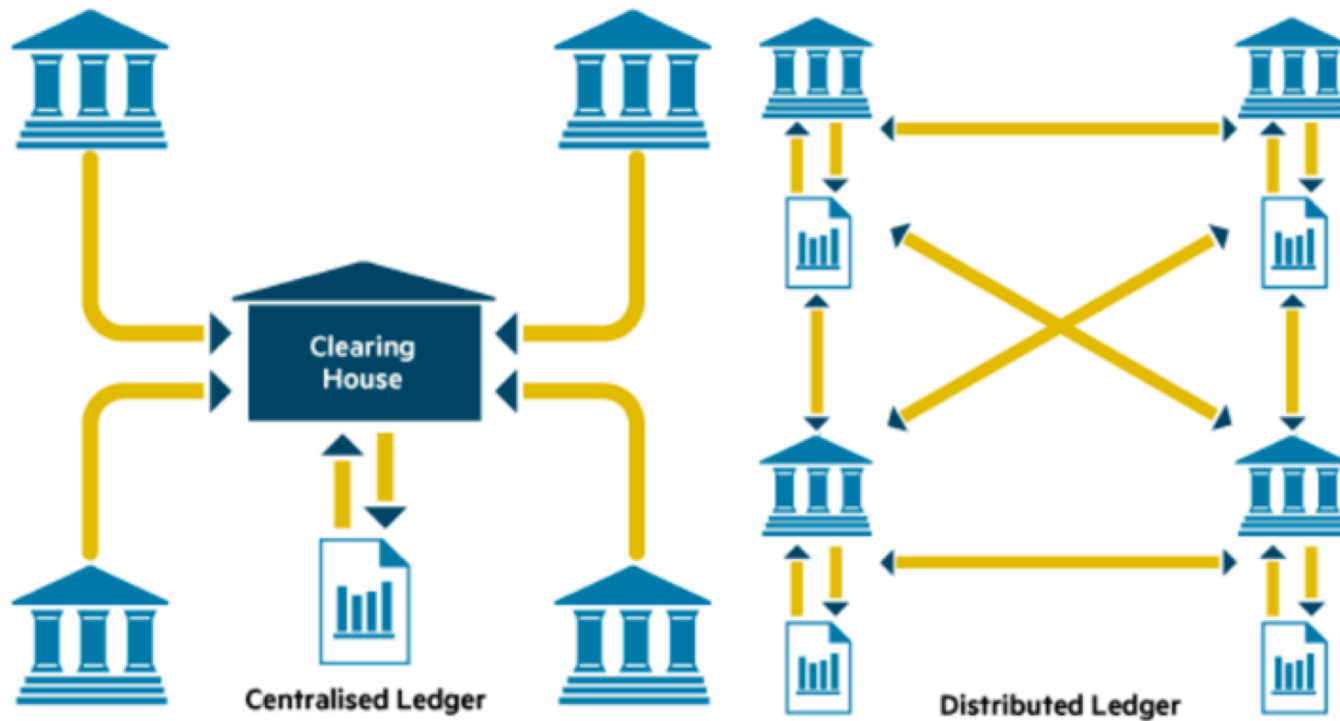
Some slides are courtesy of Vitalic Buterin and Loi Luu



중앙화 대 탈중앙화

Embedding distributed ledger technology

A distributed ledger is a network that records ownership through a shared registry



Bitcoin

❖ Satoshi Nakamoto

- “Bitcoin: A Peer-to-peer Electronic Cash System”
- “Proof of Work”
- Peer-to-peer Network
- 안전한
- 분산화된 원장 관리



Bitcoin

❖ Satoshi Nakamoto

- “Bitcoin: A Peer-to-peer Electronic Cash System”
- “Proof of Work”
- Peer-to-peer Network
- 안전한
- 분산화된 원장 관리

❖ Adam Back: 암호학자, 해커

- Hashcash – A Denial of Service countermeasure, 2002



Ethereum

- ❖ 2세대 블록체인
- ❖ 19세의 천재 Vitalek Buterin
- ❖ Turing Complete Language
- ❖ 원장에 프로그램을 저장, 실행
- ❖ 스마트 컨트랙트
- ❖ 이더리움 위에 다른 블록체인의 구현이 가능



BLOCKTECH in FINANCIAL SERVICES VIRTUALscape

by William Mougayar

APPLICATIONS & SOLUTIONS



MIDDLEWARE & SERVICES



INFRASTRUCTURE & BASE PROTOCOLS

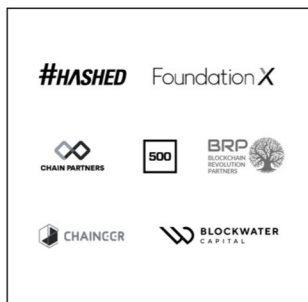


Source: <http://startupmanagement.org/blog>

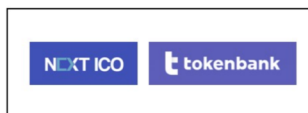
Virtual Capital Ventures © 2015 1.7

KOREA BLOCKCHAIN BUSINESS LANDSCAPE

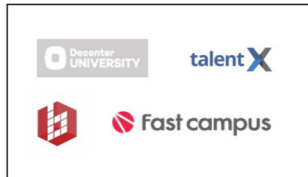
ACCELERATOR / INVESTMENT



ICO PLATFORMS



LEARNING PLATFORM



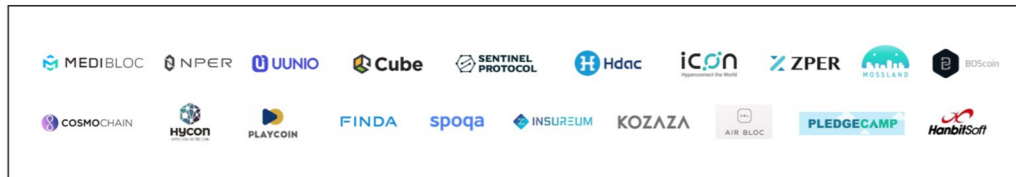
EXCHANGE



MEDIA / COMMUNITY



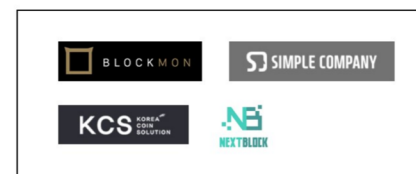
COINS



DEVELOPMENT



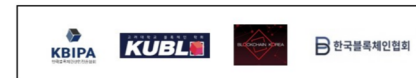
AGENCY / MARKETING



UTILITY / WALLET / SERVICE



ASSOCIATION / ACADEMY



LAW FIRMS



FoundationX
contact@foundationx.io

오늘의 주제

- ❖ 철학: Cypherpunk!
- ❖ Bitcoin 이해하기
- ❖ Ethereum의 Smart Contract 이해 하기
- ❖ 전체 블록체인 Taxonomy 이해하기
- ❖ 블록체인의 한계와 기회
- ❖ 암호화폐, 블록체인, 거래소 보안

Disclaimer: 첫번째 일반인을 대상으로 한 전반적인 블록체인 강의!

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 만듦
 - 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.

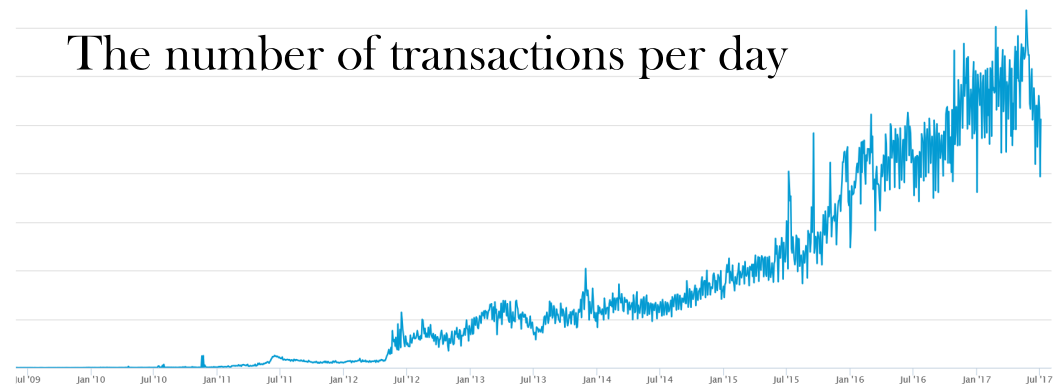
No mint or other trusted parties.

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.

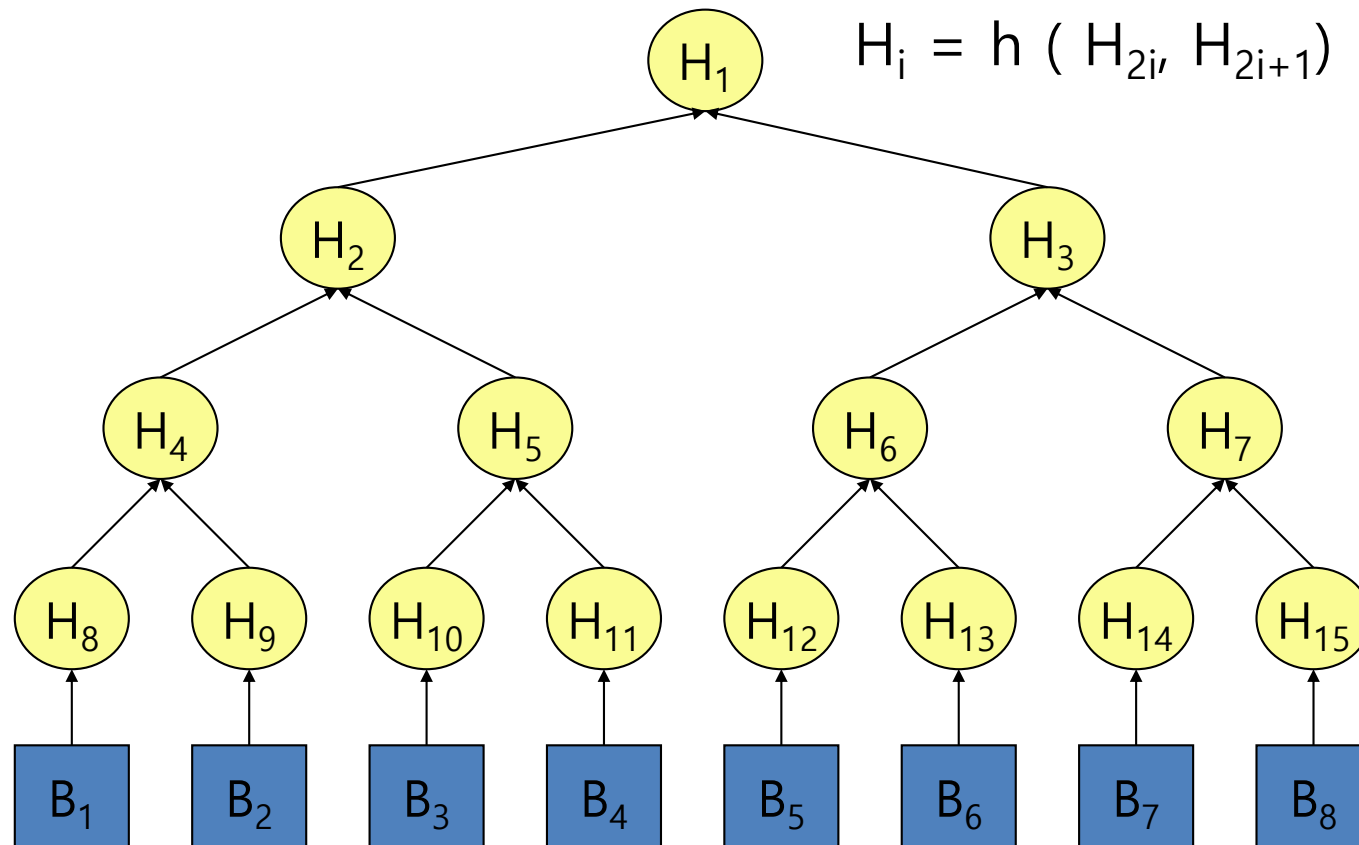
The number of transactions per day



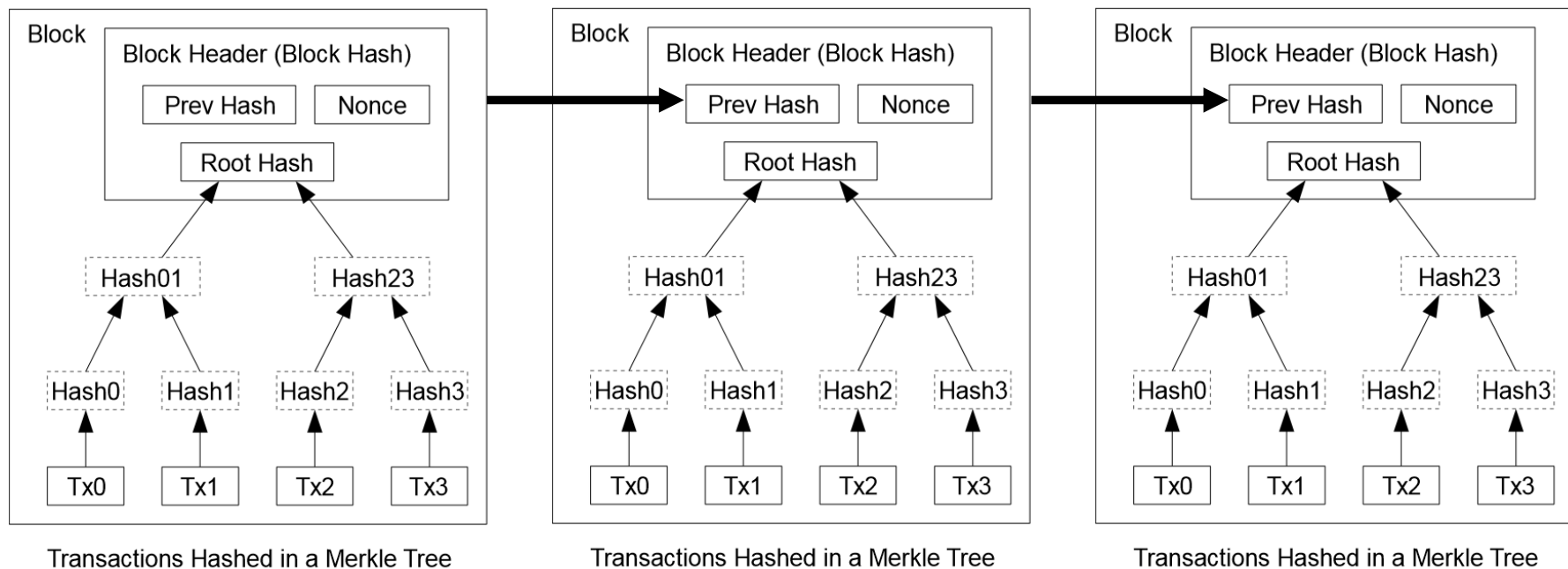
Hash function and Digital Signature

- ❖ 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: $S_{SK_A}(h(m)) = s^*$
 - Verification: $V_{PK_A}(h(m), s^*) = \text{True or False}$

Merkle Hash Tree

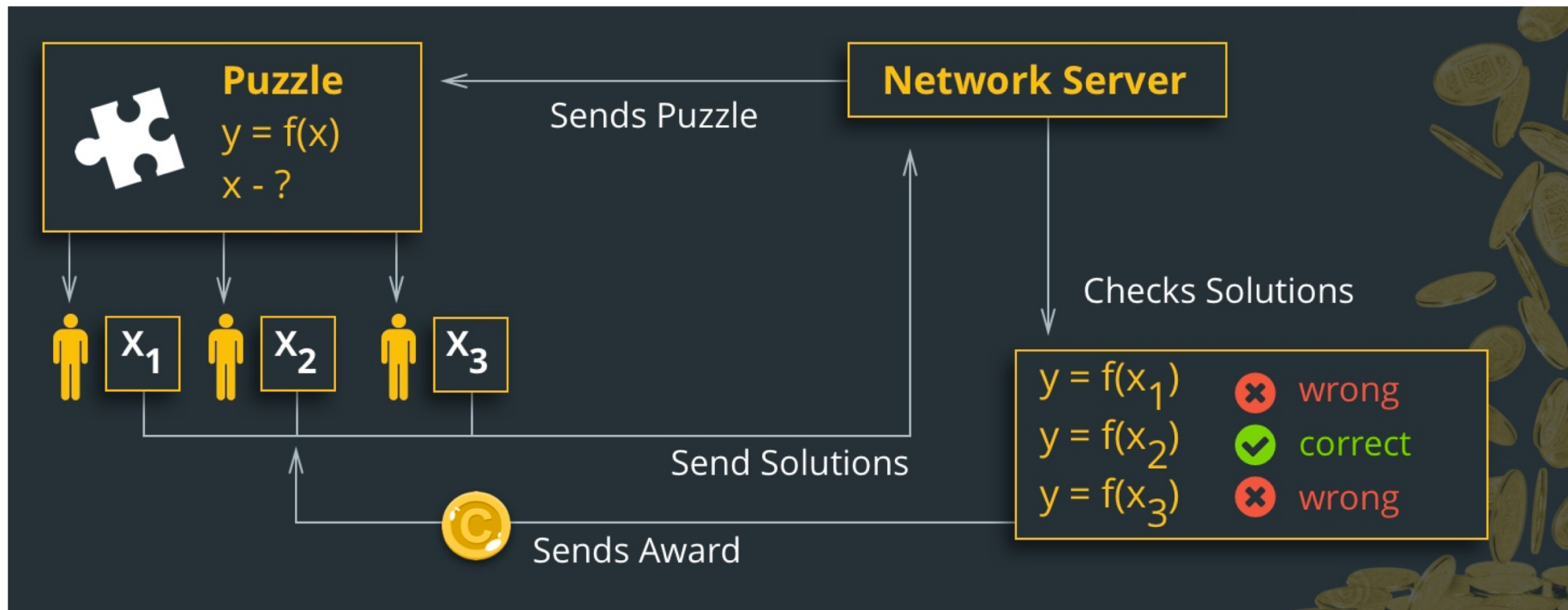


Blockchain



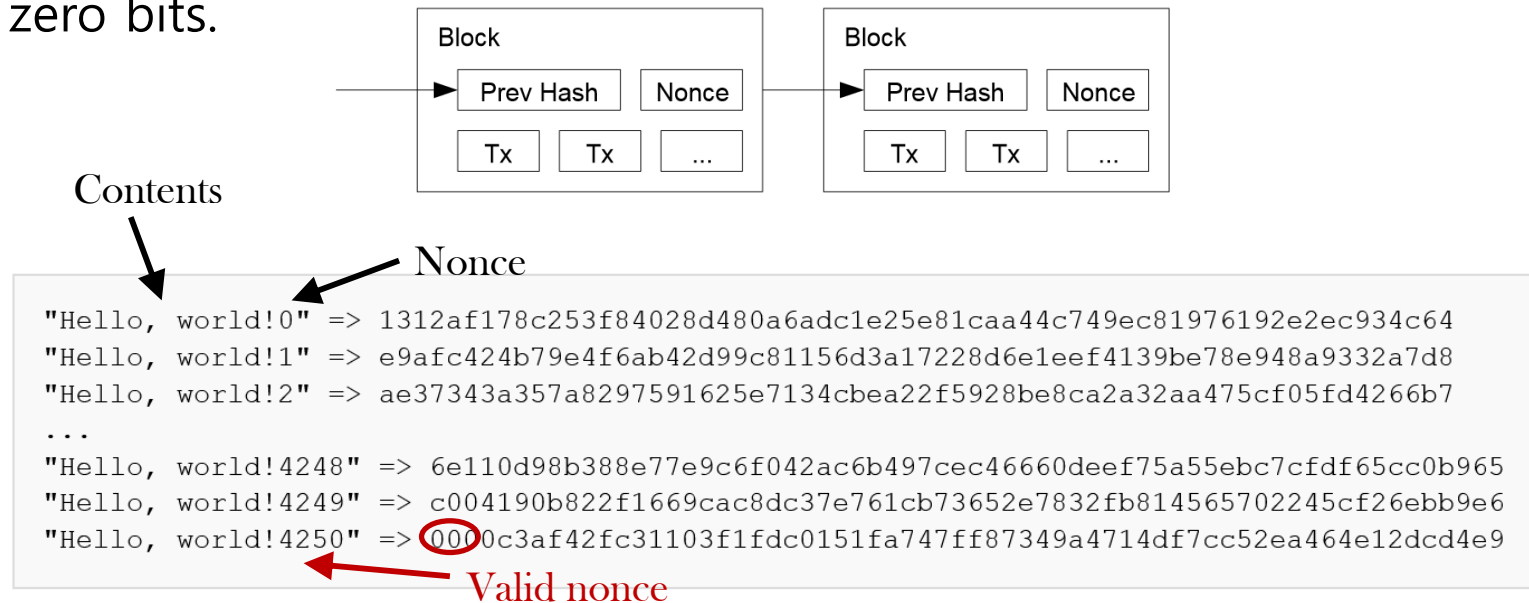
- ❖ Blocks connect as a chain.
- ❖ Each header of blocks includes the previous block's hash.

Proof-of-Work



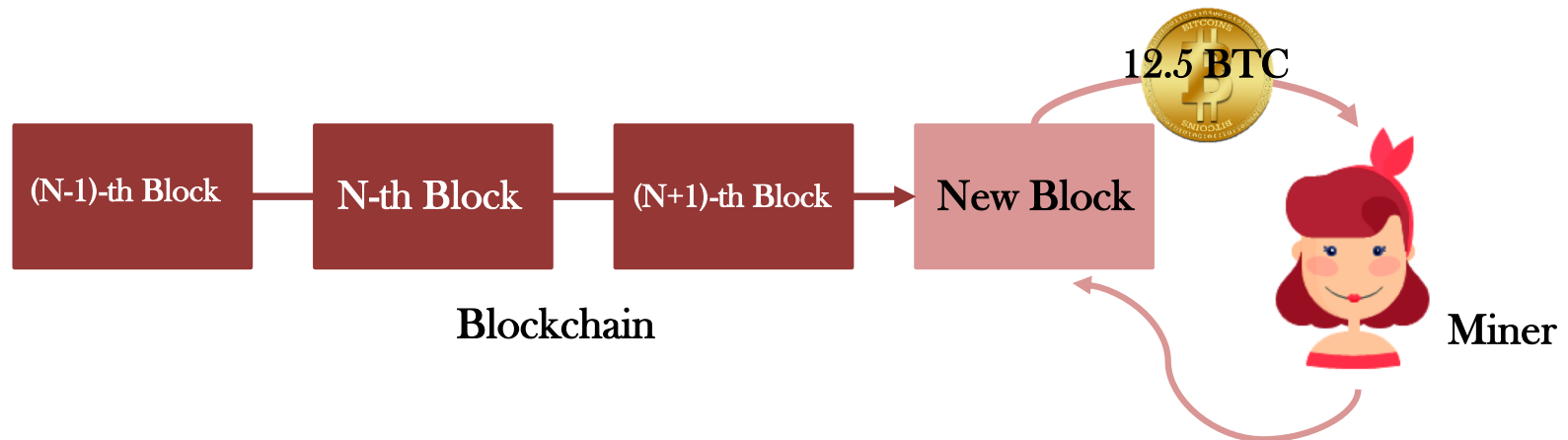
Proof-of-Work

- ❖ 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.



Reward

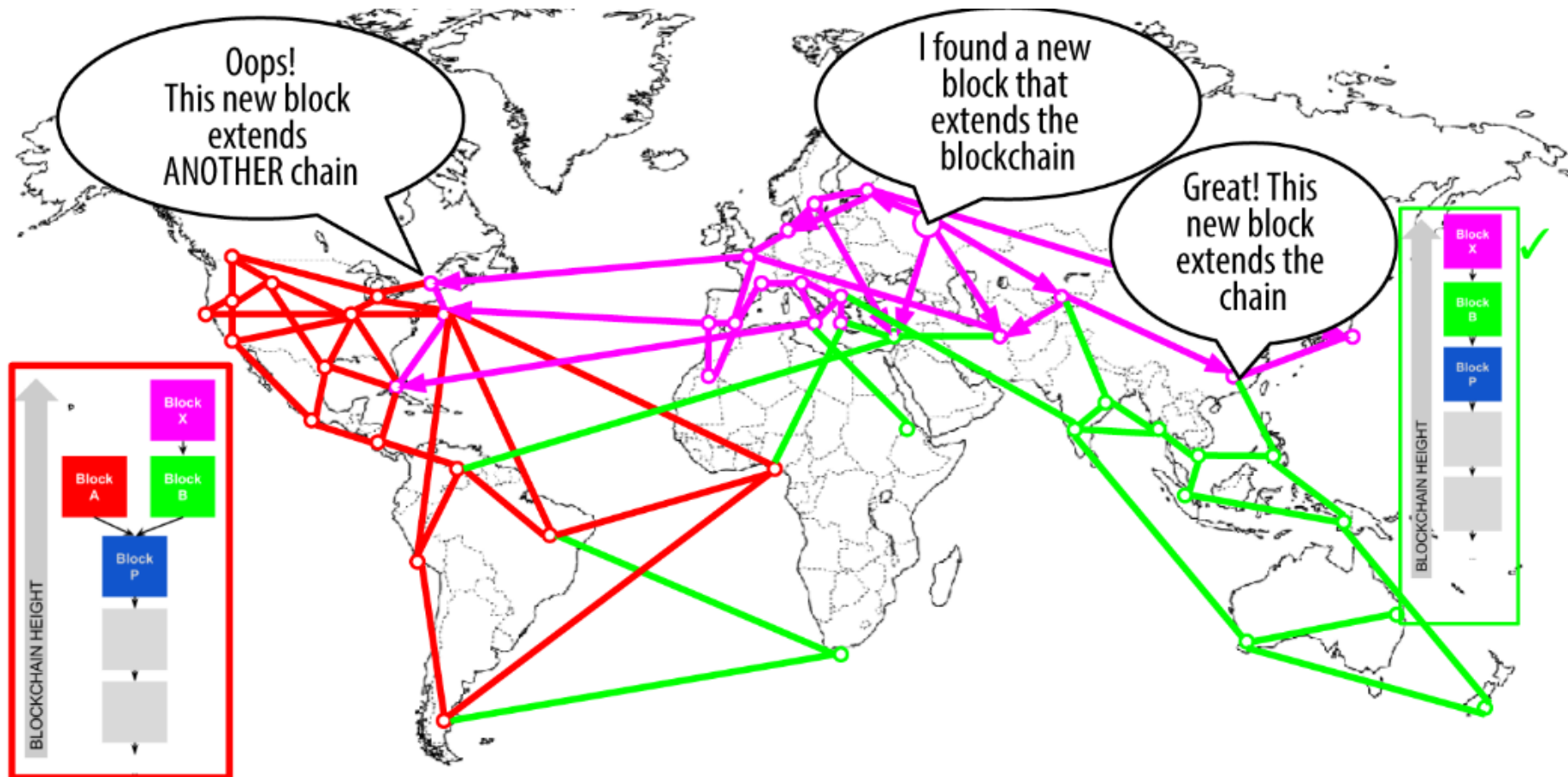
- ❖ Performing proof-of-work is called **Mining**.
- ❖ A person who does mining is called **Miner**.
- ❖ A miner can earn 12.5 BTC (\approx \$ 10k) as a reward when she succeeds to find a valid nonce.



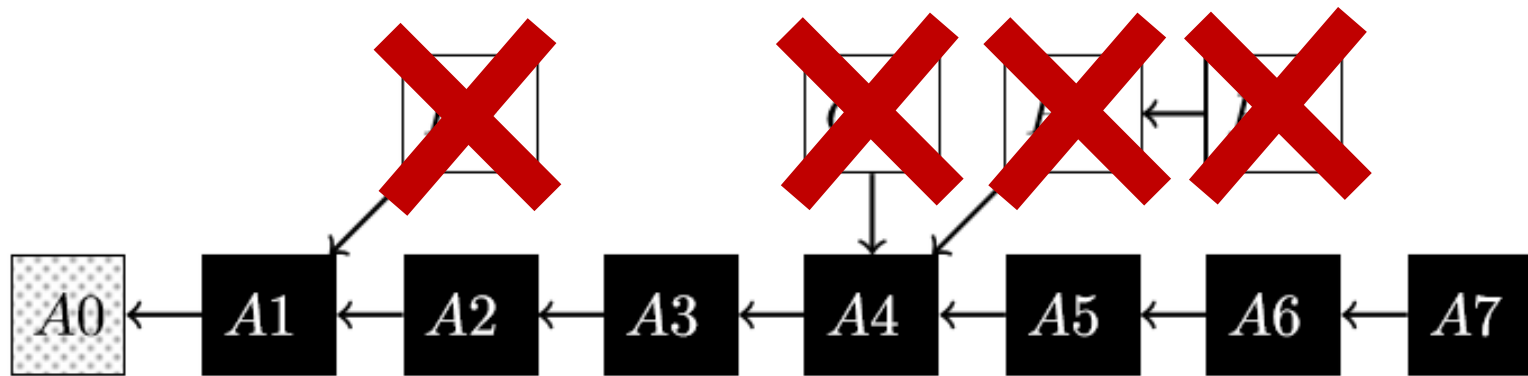
Step (Miner)

- ❖ 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.

Forks

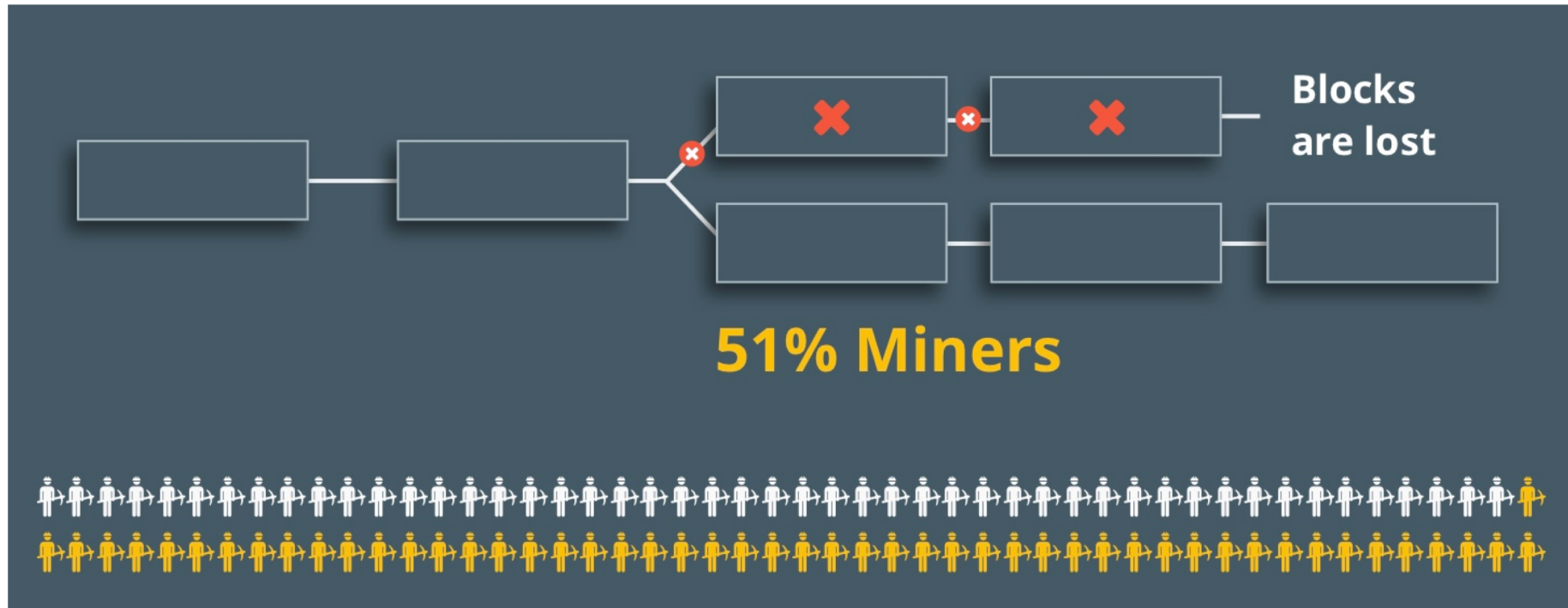


Forks



- ❖ 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.

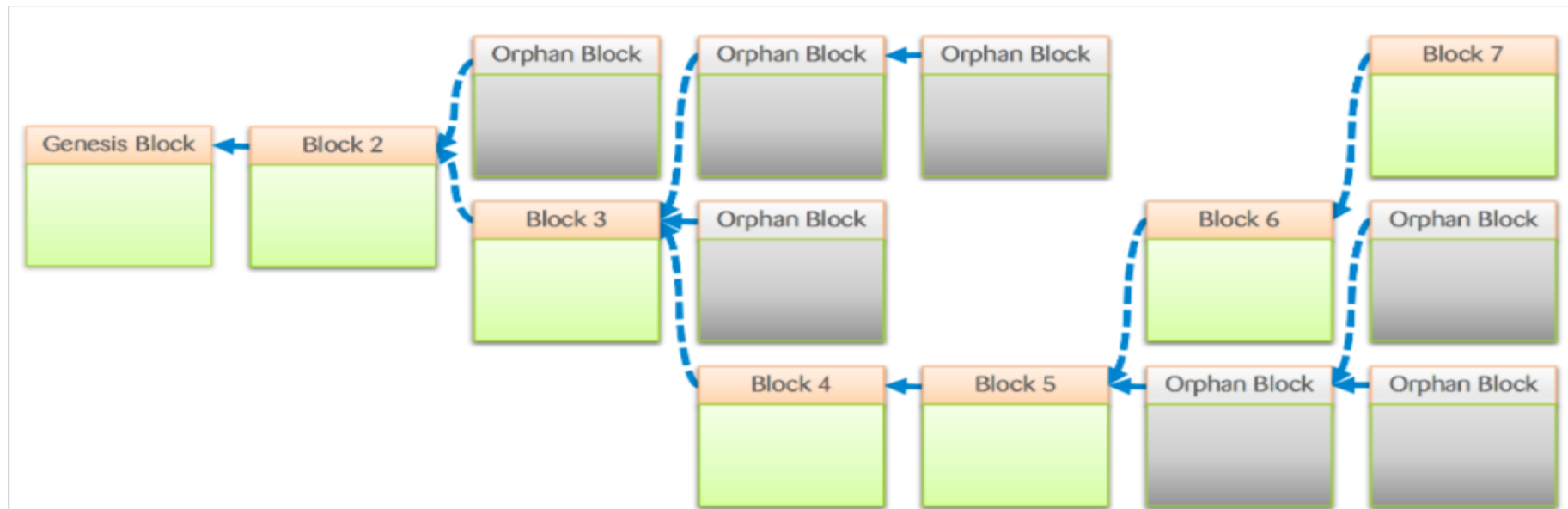
51% Attack



Mining Policies

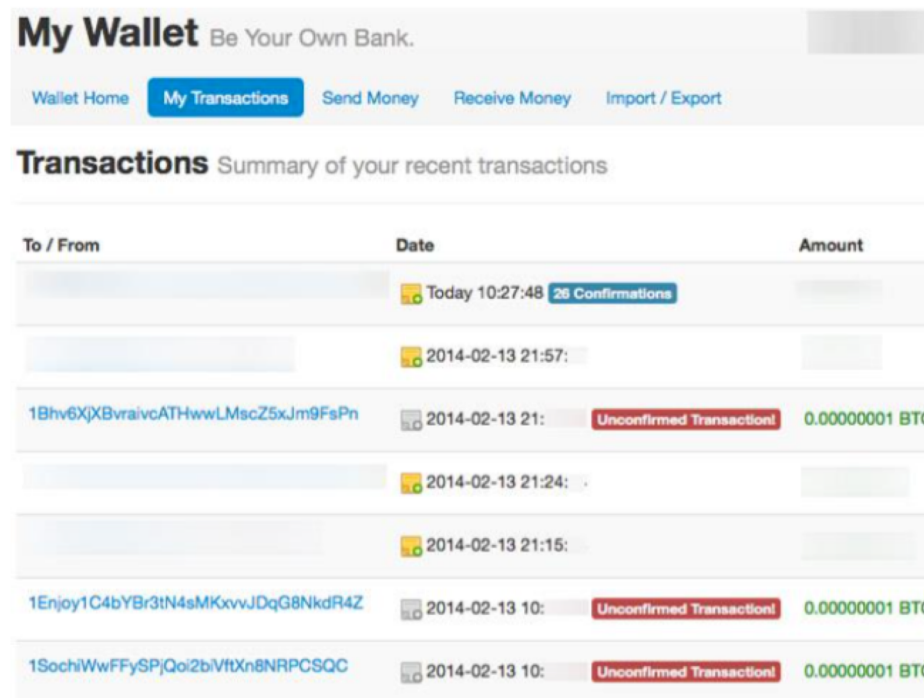
- ❖ Rate limiting on the creation of a new block
 - A block created every 10 mins (six blocks every hour)
 - How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases
- ❖ N new bitcoins per each new block: credited to the miner → incentives for miners
 - N was 50 initially. In 2013, N=25. In 2016, N=12.5.
 - Halved every 210,000 blocks (\approx 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

Example of Blockchain Status



Transaction Confirmations

- ❖ A transactions is typically considered "confirmed" once it has 6 confirmations → Probabilistic confirmation



The screenshot shows a web interface for 'My Wallet' with the tagline 'Be Your Own Bank.' The navigation bar includes 'Wallet Home', 'My Transactions' (active), 'Send Money', 'Receive Money', and 'Import / Export'. Below the navigation bar, the 'Transactions' section is titled 'Summary of your recent transactions'. It displays a table with columns 'To / From', 'Date', and 'Amount'. The table lists several transactions, including one with 26 confirmations and several unconfirmed transactions.

To / From	Date	Amount
	Today 10:27:48 26 Confirmations	
	2014-02-13 21:57:	
1Bhv6XjXBvraivcATHwwLMscZ5xJm9FsPn	2014-02-13 21: Unconfirmed Transaction!	0.00000001 BTC
	2014-02-13 21:24:	
	2014-02-13 21:15:	
1Enjoy1C4bYBr3tN4sMKxvJDqG8NkdR4Z	2014-02-13 10: Unconfirmed Transaction!	0.00000001 BTC
1SochiWwFFySPjQoi2biVftXn8NRPCSQC	2014-02-13 10: Unconfirmed Transaction!	0.00000001 BTC

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!

Bitcoin Mining Hardware



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

\$1,887⁰⁰

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

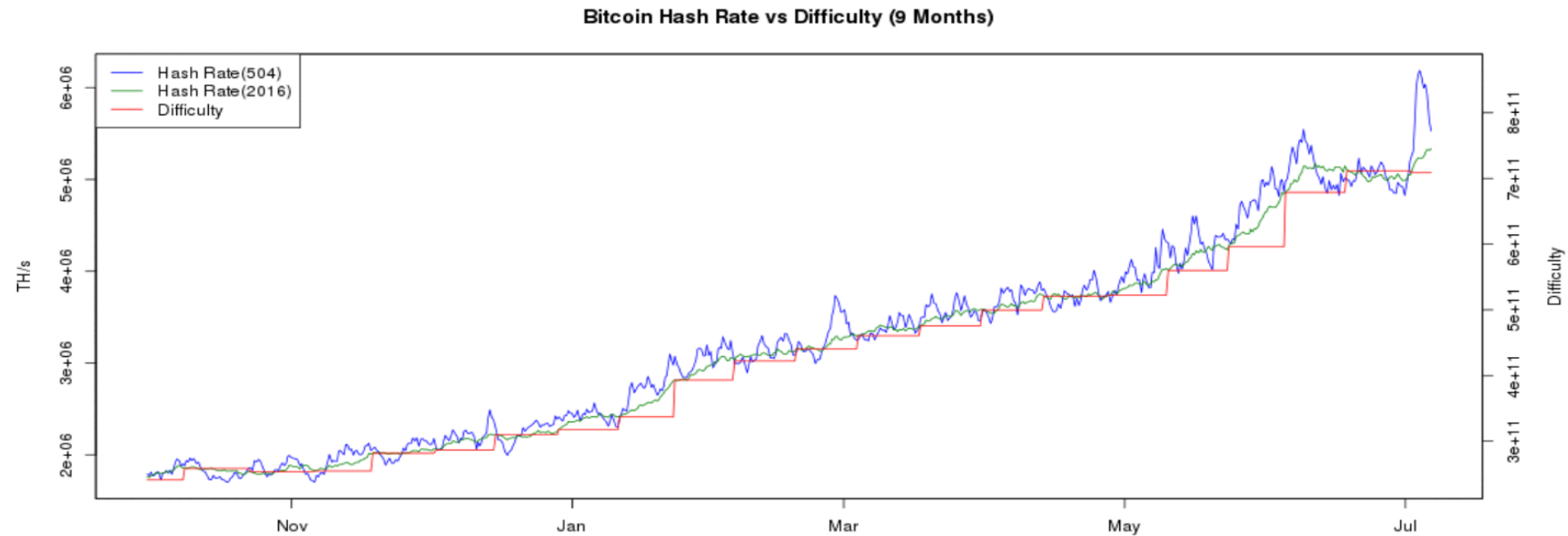
\$69⁹⁷ + \$4.49 shipping

More Buying Choices

\$59.97 (2 new offers)

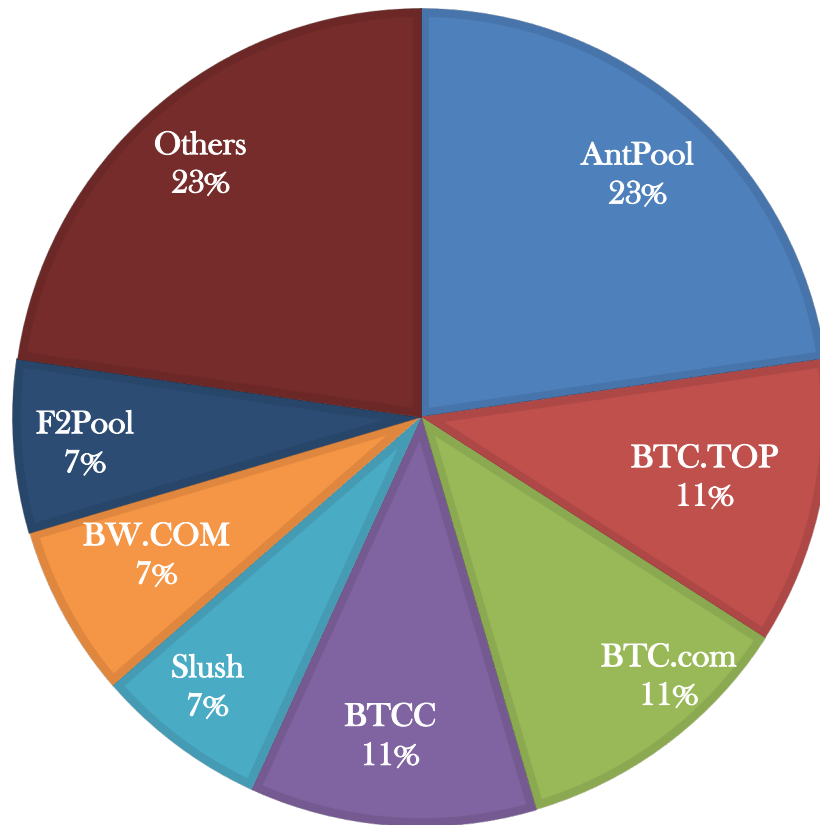


Mining Difficulty



- ❖ 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.

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

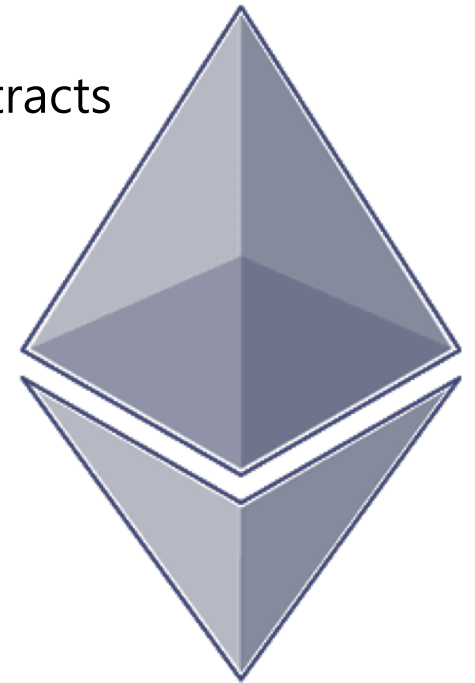
❖ Why Smart Contracts

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

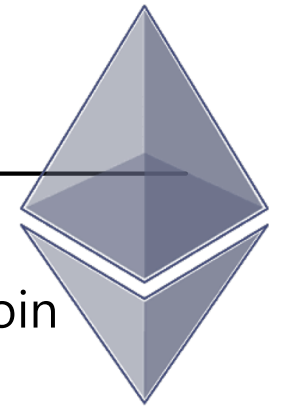
Legal contracts	Smart contracts
Good at subjective (i.e. requiring human judgement) claims	Good at objective (i.e. mathematically evaluable) claims
High cost	Low cost
May require long legal process	Fast and automated
Relies on penalties	Relies on collateral/security deposits
Jurisdiction-bound	Potentially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

Ethereum

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



Ethereum



- ❖ Blockchain with expressive programming language

- Programming language makes it ideal for smart contracts

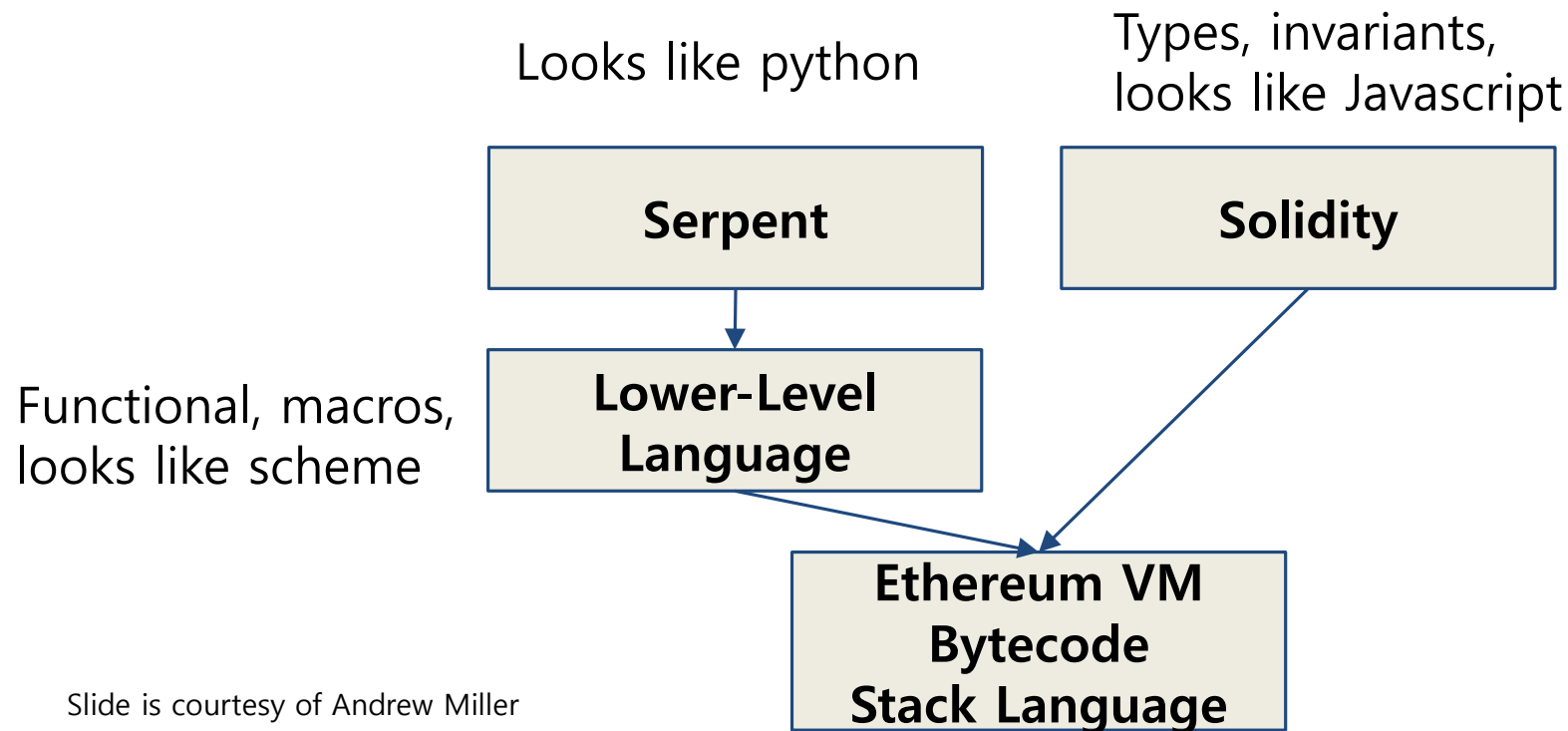
- ❖ Why?

- 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

Ethereum Languages



Slide is courtesy of Andrew Miller

Example

```
1 contract Greetings {  
2     string greeting;  
3     function Greetings (string _greeting) public {  
4         greeting = _greeting;  
5     }  
6  
7     /* main function */  
8     function greet() constant returns (string) {  
9         return greeting;  
10    }  
11 }
```

What you write



What other see
on the blockchain

6060604052604051610250380
380610250833981016040528...

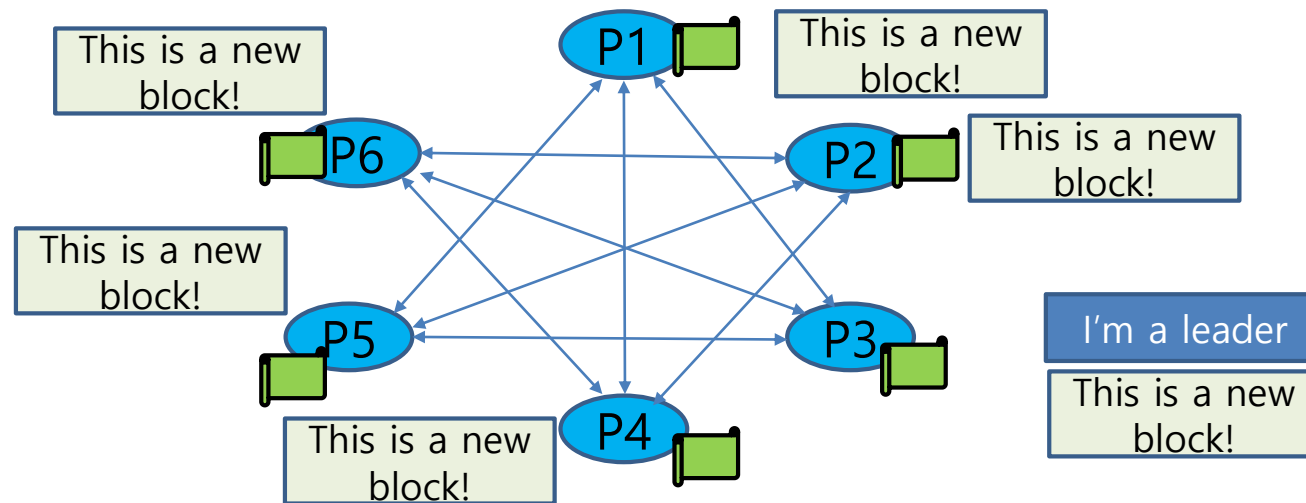


PUSH 60
PUSH 40
MSTORE
PUSH 0
CALLDATALOAD
.....

What people get from
the disassembler

Code execution

- ❖ Every (full) node on the blockchain processes every transaction and stores the entire state



ERC-721 표준

토큰

이더리움 블록체인 네트워크에서 발행되는 디지털 자산

ERC: Ethereum Request for Comment

이더리움 블록체인 네트워크에서 발행되는 토큰의 표준

ERC-20

암호화폐를 발행하기 위한 토큰 표준



E O S

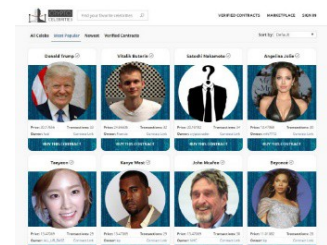


ERC-721

수집품을 발행하기 위한 토큰 표준



CryptoKitties

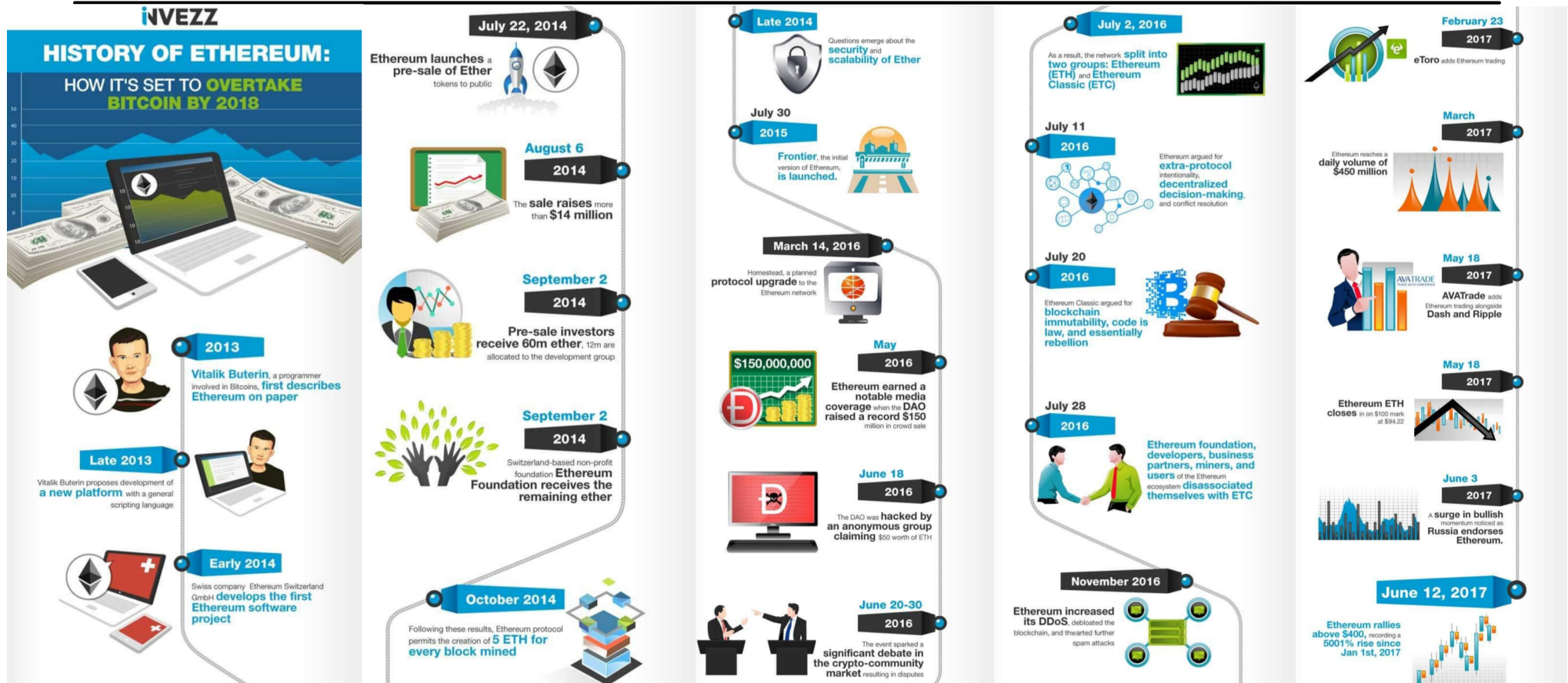


CryptoCelebrities

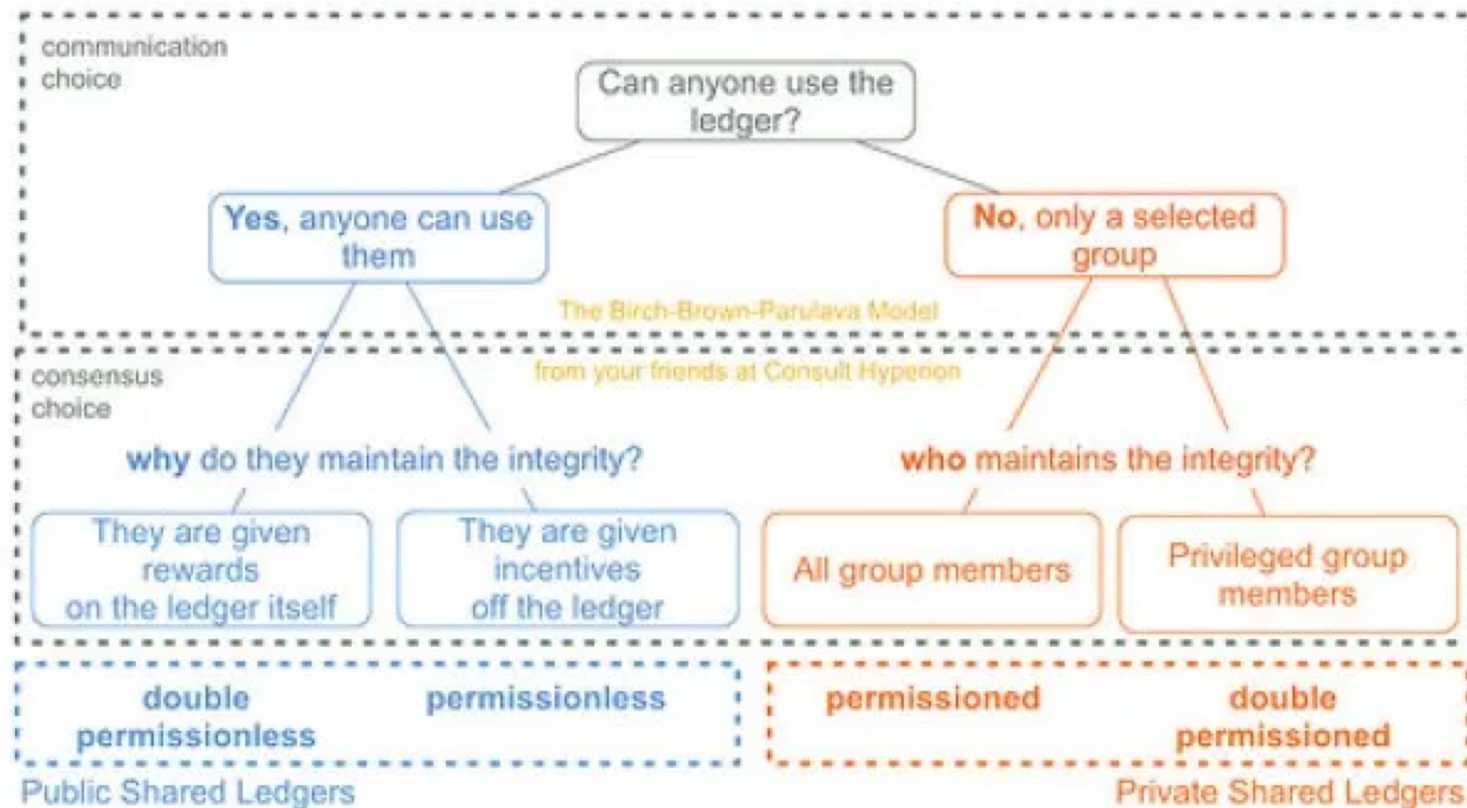


Fishbank

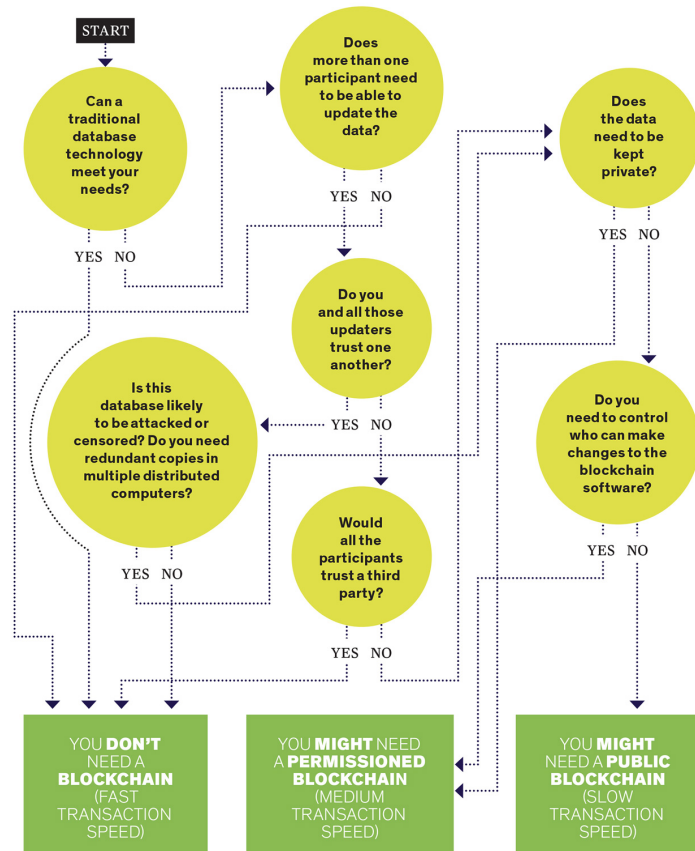
Ethereum의 역사



Taxonomy of Blockchain



Taxonomy of Blockchain



❖ Public Blockchain

- If you worry about censorship and universal access
- price volatility, low throughput, poor privacy, no governance
- Voting
 - Election officials still takes the role of creating ballots and authenticating voters. And if you trust them to do that, no reason why they shouldn't also record votes.

❖ Permissioned Blockchain

- Solves cost, speed, privacy, and predictability
- Removing miners improves the speed and storage capacity
 - Bitcoin 7 txs/s, Ethereum 20 txs/s, Multichain 1,000 txs/s
- More privacy because it restricts who can access data
- Governance: Ones who update the blockchain are the same people who update the code

IPO, Crowd Funding, ICO

IPO

- 전통적인 자금 투자 방식
- 엔젤투자/ 벤처캐피탈/ 기업 공개

Crowd Funding

- 온라인에 제품이나 서비스에 대한 비전 공개
- Kickstarter, Indiegogo, 와디즈 등

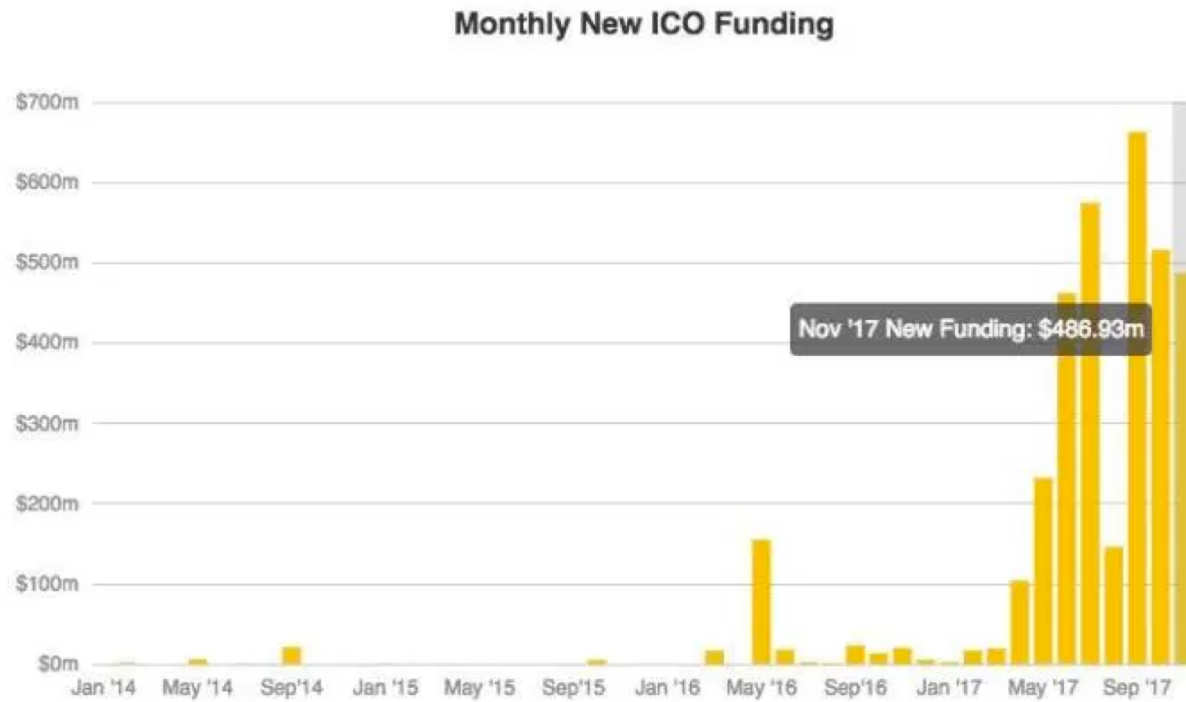
ICO

- 중간 플랫폼이 필요 없음
- 암호화폐를 받아 기업 운용에 필요한 자금을 조달

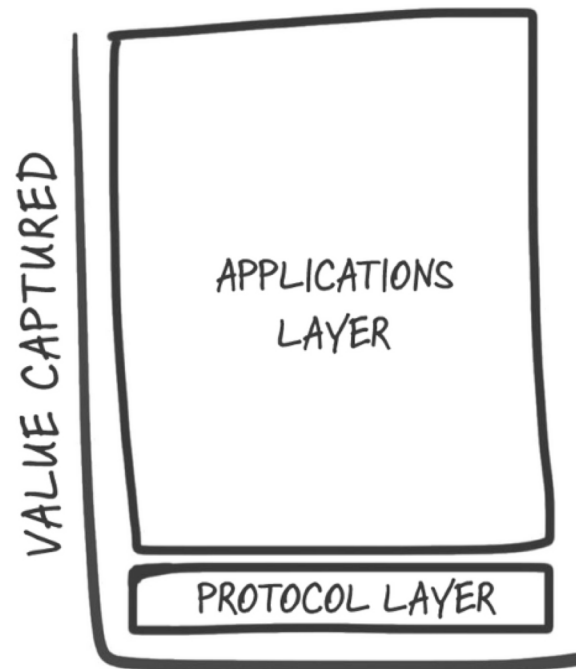
IPO: Initial Public Offer

ICO: Initial Coin Offering

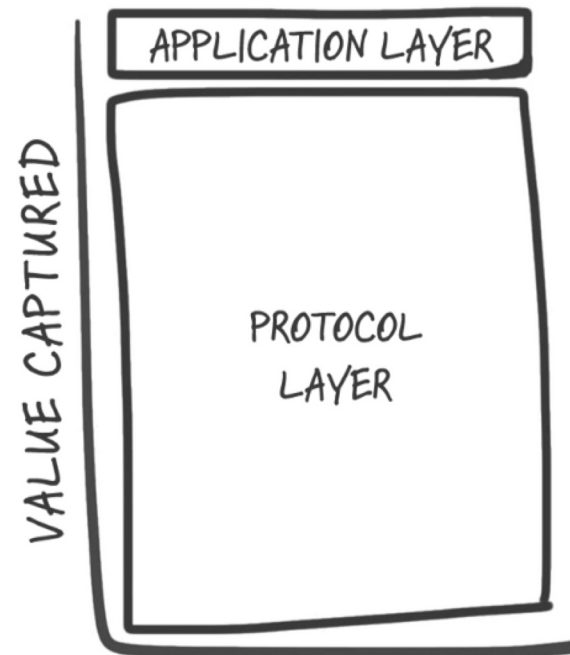
새로운 ICO Funding



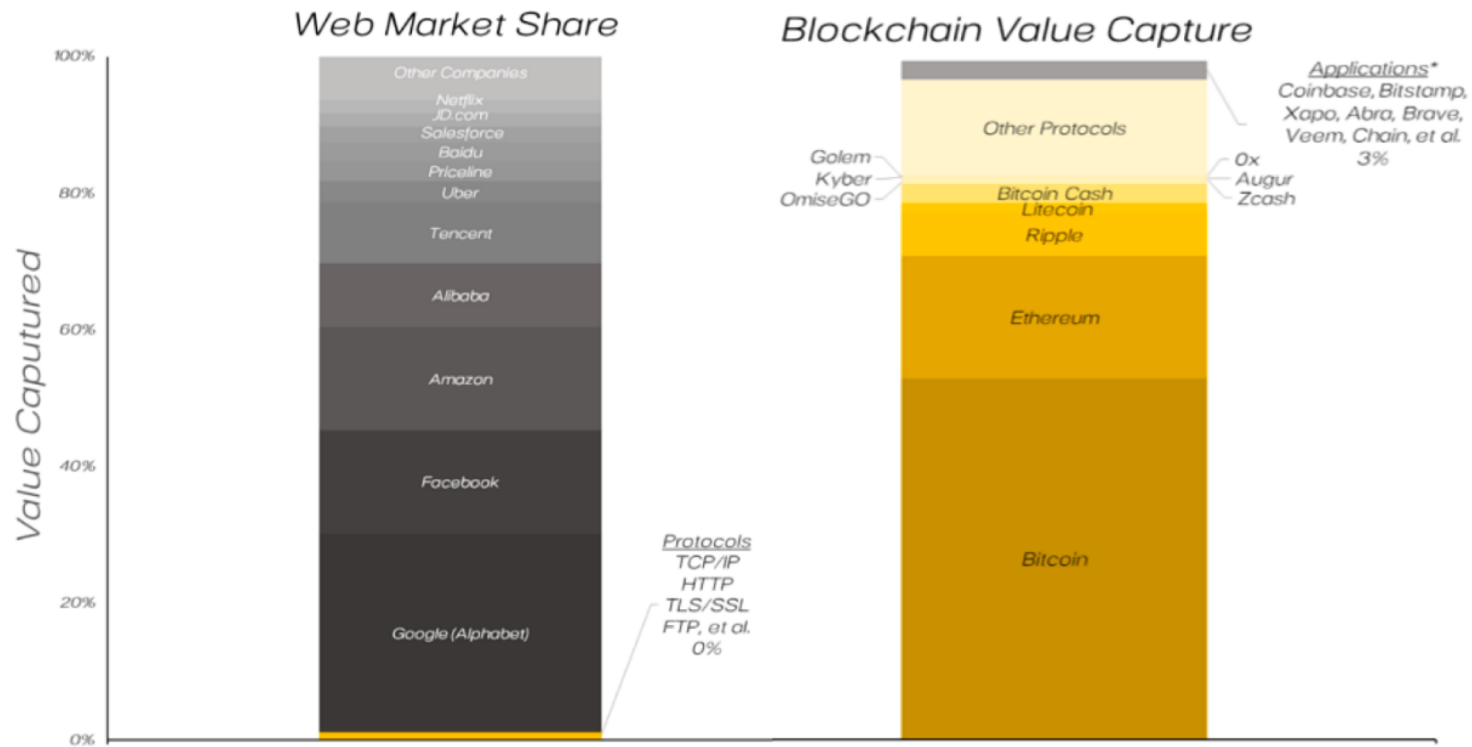
The Web



Blockchain



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

Satoshi, Vitalik, 다음은 누구?

어떤 기술/교육이 필요한가?

최근 ICO와 연구



Loi Luu
NUS 박사과정
Kyber Network CEO
SmartPool Cofounder

SMART POOL : Practical Decentralized Pooled Mining
A Secure Sharding Protocol For Open Blockchains



Silvio
Micali
암호학자
MIT 교수

Algorand: scaling Byzantine agreements for cryptocurrencies



Nikolai
Zeldovich
시스템
MIT 교수



David Mazieres
시스템
스탠포드 교수

The Stellar Consensus Protocol: A Federated Model for
Internet-level Consensus



Aggelos Kiayias
암호학
에딘버러대 교수

Ouroboros: A Provably Secure Proof-of-Stake
Blockchain Protocol

블록체인 보안 연구

- ❖ 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 (KAIST 논문)

ZEUS: Analyzing Safety of Smart Contracts

NDSS 2018

자동화 도구를 이용하여 이더리움의 취약한 스마트
컨트랙트 탐지

- Reentrancy
- Unchecked send
- Block state dependence
- Transaction order dependence
- Failed send
- Integer overflow/underflow
- Transaction state dependence

21,281 / 22,493 (94.6%) 취약
(1524 unique contract)

ICO scam 사기

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



블록체인 기술/인재 정책 제언

❖ 원천 기술 대 응용 기술

- 빅데이터 붐 때 무엇에 투자를 했는가? 그리고 현재 우리가 가진 것은?
- 응용 기술: "블록체인을 이용한 XX", **산업체 주도**
 - 새로운 블록체인 응용 개발
 - **책임있는 ICO의 허용 → 시장 경제의 구현**
- 원천 기술: "새로운 블록체인의 설계", **대학 주도**
 - 교육: 암호학, 분산시스템, 게임이론, 개발, 확률론, 프로그래밍 언어 ...
 - 연구: **블록체인 원천기술 연구센터!**

❖ 원천 기술 발전 방향성

- 트릴레마(확장성, 보안, 분산화) 해결 연구
 - 새로운 합의 알고리즘!
 - 새로운 플랫폼과 스마트 컨트랙트!
- 기술 평가 기술 연구 → 민간 주도의 자율 심사 유도
 - 구현 가능성, 가치, 안전성에 대한 기술적 평가 플랫폼 개발
- 이상 거래 탐지 연구: 작전 파악, 돈 세탁, ...

Thank You!

<https://syssec.kaist.ac.kr>