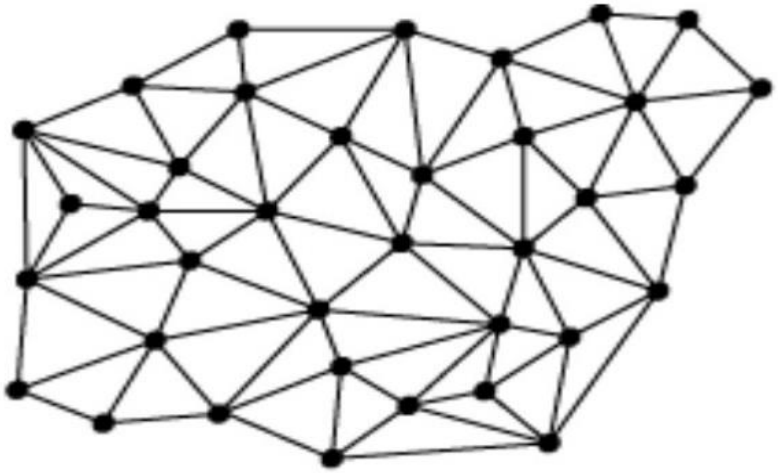
Distributed System Course

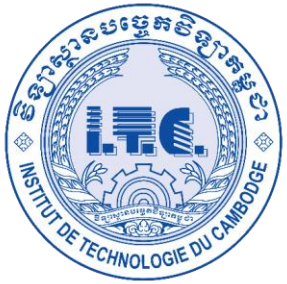
2021-22-GICI41SSD-Distributed System



Academic Year: 2021-2022 Lecturer: SOK Kimheng

Information

Course	Distributed System	48h, 12 Weeks, 4h/week (3 Groups = 96h)
	Week 1	Information, Self-Study Skill, Introduction
General Distributed System	Week 2	Distributed Communication (TCP/IP, Socket, RPC, REST, gRPC, OMQ)
	Week 3	Clock, Timestamp
	Week 4	Fault Tolerance (Two general problem, Byzantine General Problem)
	Week 5	Consensus Algorithm (Paxos, ZooKeeper, Raft)
	Week 6	**Quiz**
Blockchain	Week 7	Basic Cryptography
	Week 8	Blockchain and Bitcoin (Proof of Work)
	Week 9	Ethereum and Smart Contract (Proof of Stake)
	Week 10	Hyperledger and Self-Sovereign Identity
	Week 11	Security
	Week 12	**Final Exam**



Distributed System Course

2021-22-GICI41SSD-Distributed System

Week8:

Blockchain and Bitcoin

Academic Year: 2021-2022 Lecturer: SOK Kimheng

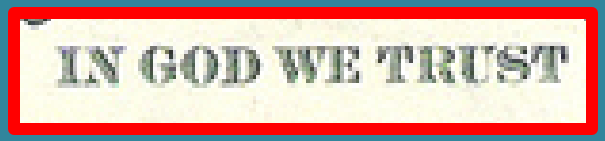
Agenda

1. Blockchain and Bitcoin
2. Blockchain beyond cryptocurrency
3. Blockchain consensus algorithms

Blockchain and Bitcoin

Money Evolution

Who do you Trust?



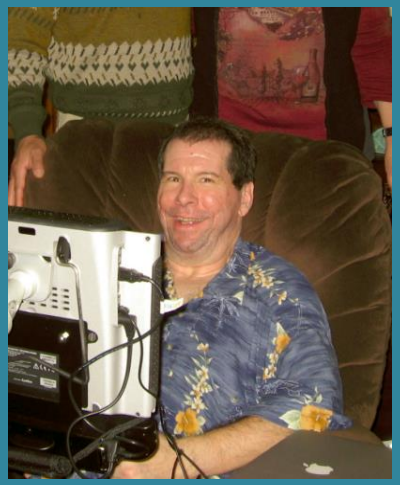
" It's very attractive to the libertarian viewpoint
If we can explain it properly.
I'm better with ***code*** *than with words though."*

SATOSHI NAKAMOTO

Third Party

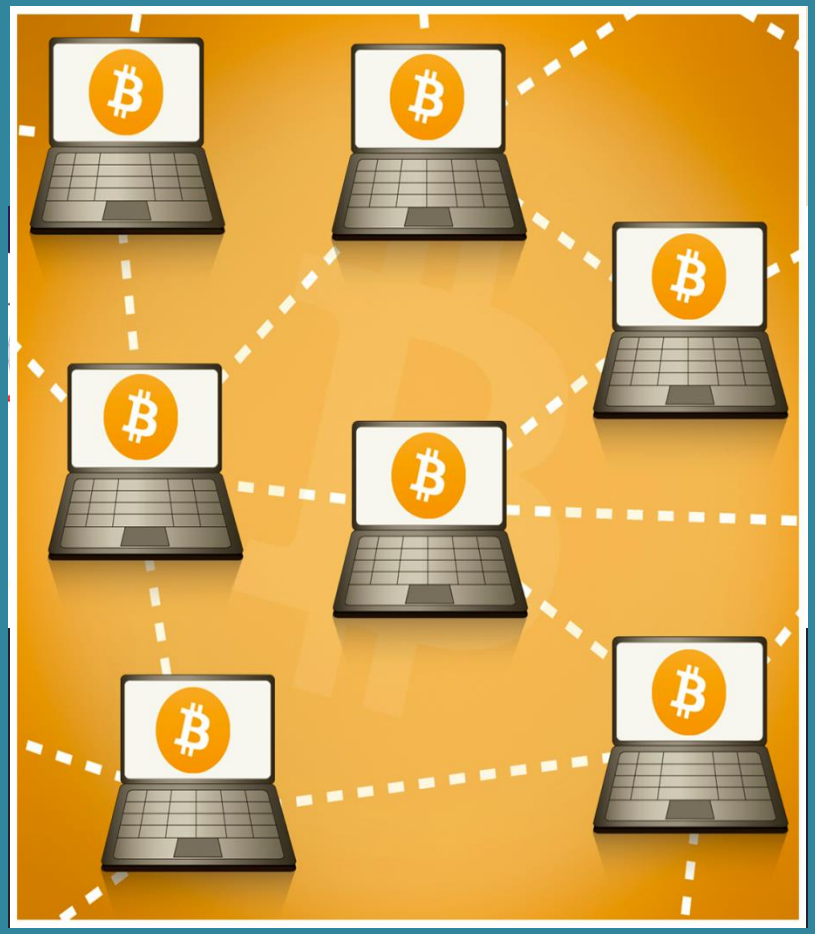
SATOSHI NAKAMOTO

HAL FINNEY

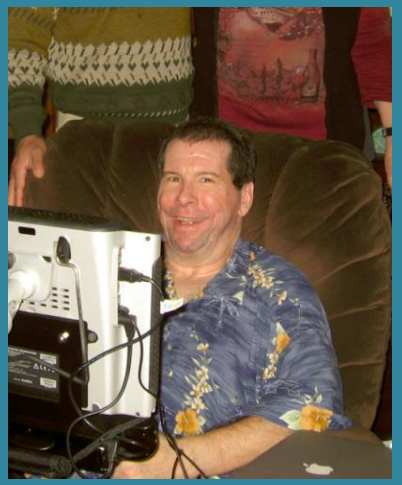


Blockchain

SATOSHI NAKAMOTO

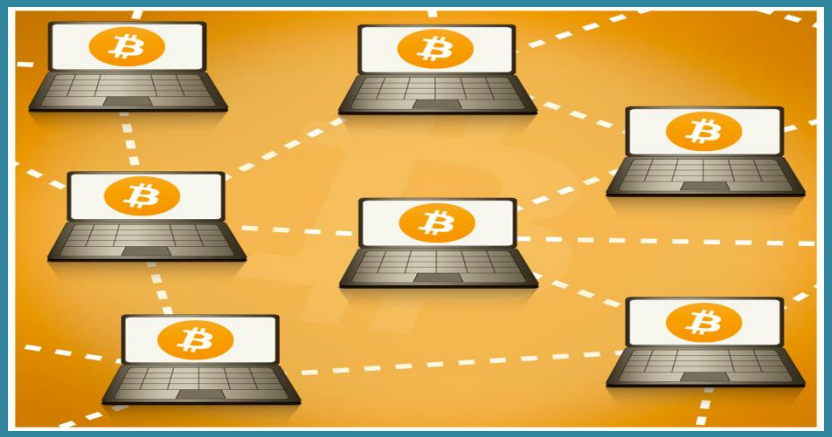


HAL FINNEY

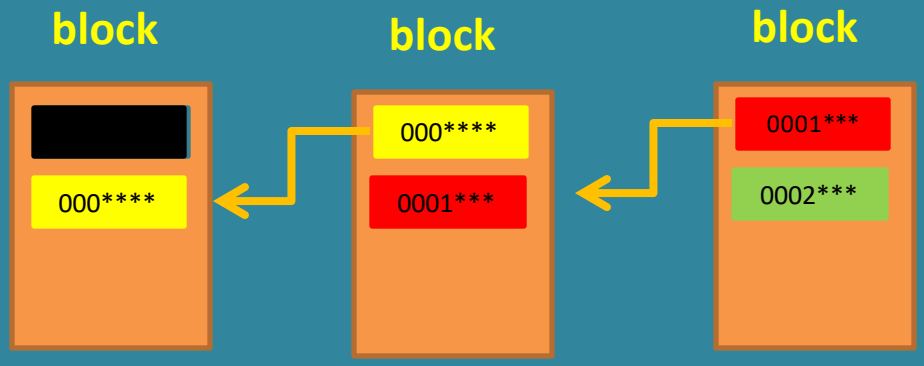


Blockchain

SATOSHI NAKAMOTO



HAL FINNEY



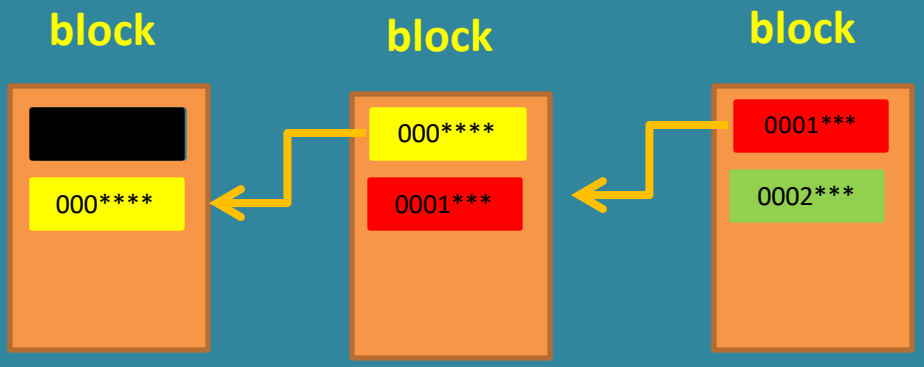
BLOCKCHAIN

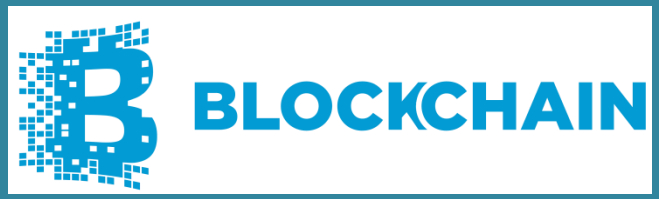
Genesis block

50 BTC

25 BTC

Blockchain





- ✓ Cryptography
- ✓ Public Distributed Ledger
- ✓ Peer-to-Peer Network

Bitcoin Wallet

Hardware Wallet

Paper Wallet

PC Wallet

Mobile Wallet

Bitcoin address

Blockchain usecase in Cambodia

ធនាគារជាតិ សហការជាមួយក្រុមហ៊ុន Soramisu ប្រើ PRIVATE BLOCKCHAIN (**Hyper Ledger**) ឈ្មោះIroha

A street view of the National Bank of Cambodia headquarters in Phnom Penh. Heng Chivoan

NBC signs blockchain agreement

Mon, 24 April 2017 Kali Kotoski

The National Bank of Cambodia (NBC) has signed an agreement with a Japanese firm to develop a blockchain-based payment system that could potentially allow for the regulated

Mining Competition

BITS Target Difficulty = 0x180130e0 (Aug 2017)

Decimal: 29201223626342991605750065618903157022235193117232857088

0x00000000000000000130e0000000000000000000000000000000000000000000

GPU FPGA ASIC

Mining Competition

12.5BTC x $9,000

$112,500

10min find correct hash for 1 Block

Kimheng Coin

BITS Target Difficulty = 0x1d00ffff (Genesis)

Decimal: 26959535291011309493156476344723991336010898738574164086137773096960

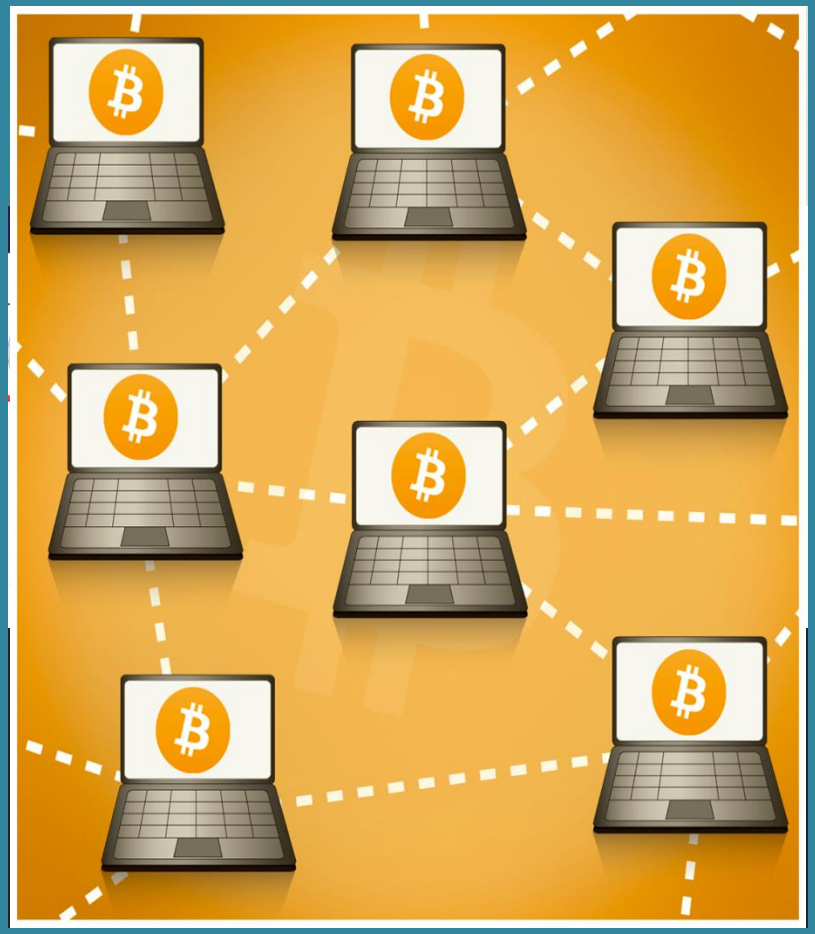
0x00000000FFFF0000000000000000000000000000000000000000000000000000

Marco Streng
MINER

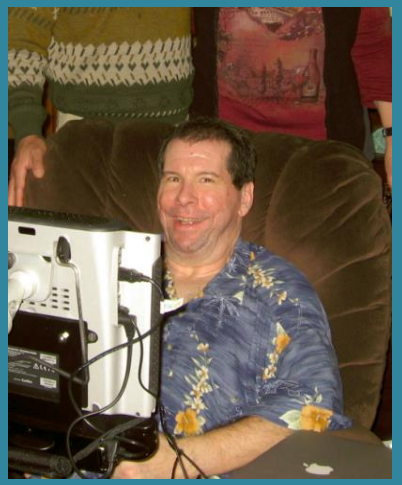
Blockchain beyond cryptocurrency

Blockchain

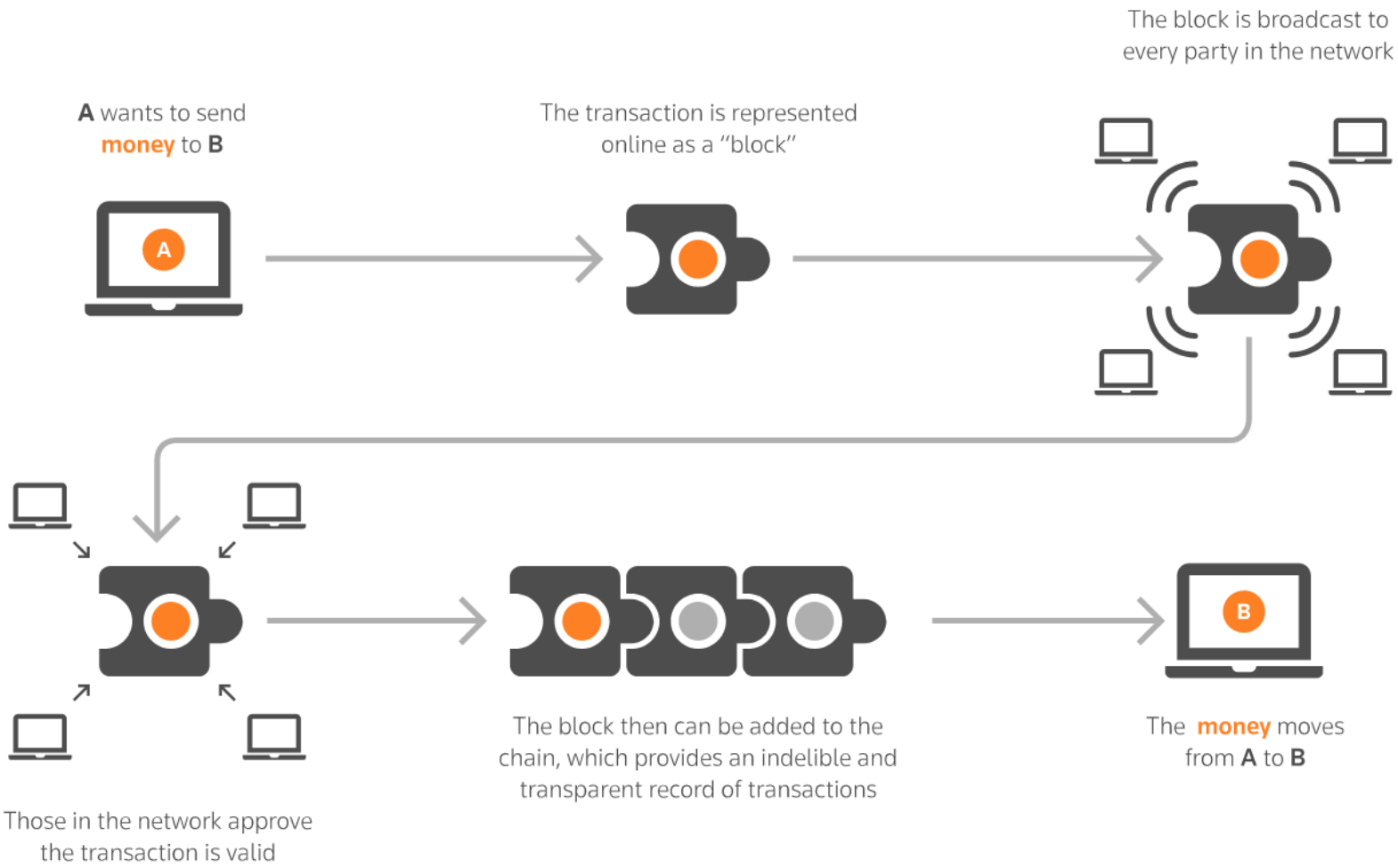
SATOSHI NAKAMOTO



HAL FINNEY



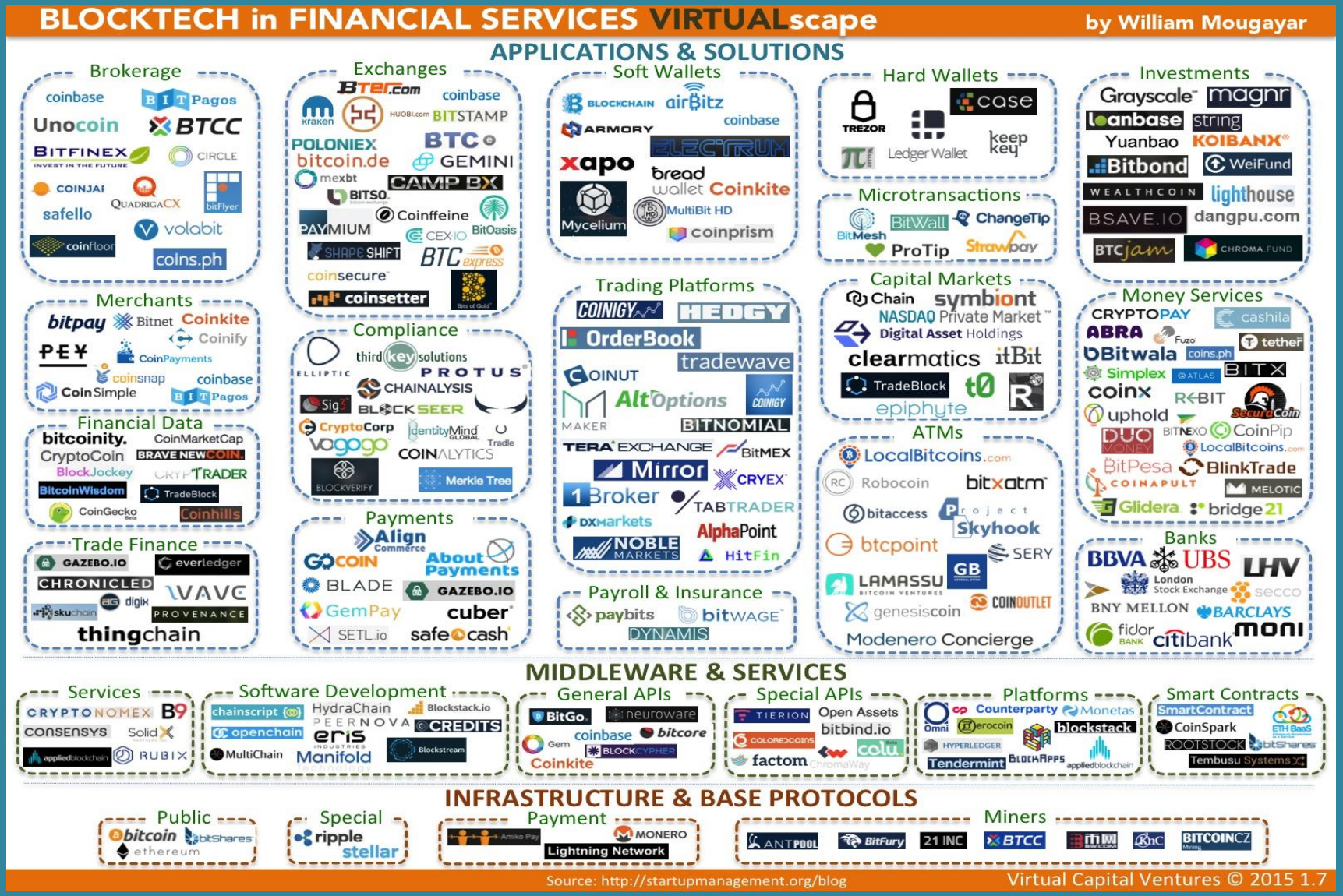
How does Blockchain works



Blockchain beyonds Crypto

- ✓ លុយអេឡិចត្រូនិច (Cryptocurrency)
- ✓ ទ្រព្យសម្បត្តិ / ឯកសារ (Assets / Files)
- ✓ កម្មសិទ្ធ (Ownership)
- ✓ ផ្លាស់ប្តូរកម្មសិទ្ធ (Change Ownership)
- ✓ កិច្ចសន្យាឆ្លាតវៃ (Smart Contract)
- ✓ ទីផ្សារឌីជីថល (Digital Market)

Blockchain Finance Ecosystem



Blockchain Usecases

Blockchain use cases list by industry

Financial
Trading
Deal origination
POs for new securities
Equities
Fixed income
Derivatives trading
Total Return Swaps (TRS)
2nd generation derivatives
The race to a zero middle office
Collateral management
Settlements
Payments
Transferring of value
Know your client (KYC)
Anti money laundering
Client and product reference data.
Crowd Funding
Peer-to-peer lending
Compliance reporting
Trade reporting & risk visualizations
Betting & prediction markets

Insurance
Claim filings
MBS/Property payments
Claims processing & admin
Fraud prediction
Telematics & ratings

Media
Digital rights mgmt
Game monetization
Art authentication
Purchase & usage monitoring
Ticket purchases
Fan tracking
Ad click fraud reduction
Resell of authentic assets
Real time auction & ad placements

Computer Science
Micronization of work (pay for algorithms, tweets, ad clicks, etc.)
Expanse of marketplace
Disbursement of work
Direct to developer payments
API platform plays
Notarization & certification
P2P storage & compute sharing
DNS

Medical
Records sharing
Prescription sharing
Compliance
Personalized medicine
DNA sequencing

Asset Titles
Diamonds
Designer brands
Car leasing & sales
Home Mortgages & payments
Land title ownership
Digital asset records

Government
Voting
Vehicle registration
WIC, Vet, SS, benefits, distribution
Licensing & identification
Copyrights

Identity
Personal
Objects
Families of objects
Digital assets
Multifactor Auth
Refugee tracking
Education & badging
Purchase & review tracking
Employer & Employee reviews

IoT
Device to Device payments
Device directories
Operations (e.g. water flow)
Grid monitoring
Smart home & office management
Cross-company maintenance markets

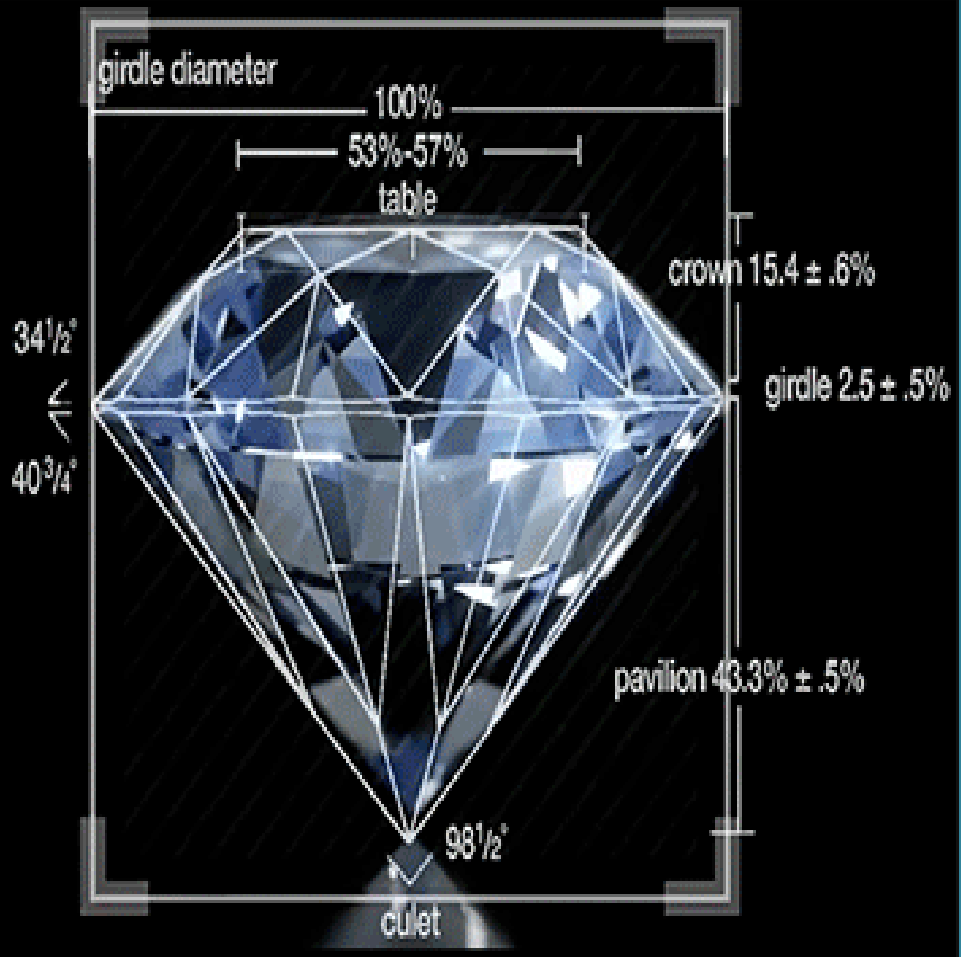
Payments
Micropayments (apps, 402)
B2B international remittance
Tax filing & collection
Rethinking wallets & banks

Consumer
Digital rewards
Uber, AirBNB, Apple Pay
P2P selling, craigslist
Cross company, brand, loyalty tracking

Supply Chain
Dynamic ag commodities pricing
Real time auction for supply delivery
Pharmaceutical tracking & purity
Agricultural food authentication
Shipping & logistics management

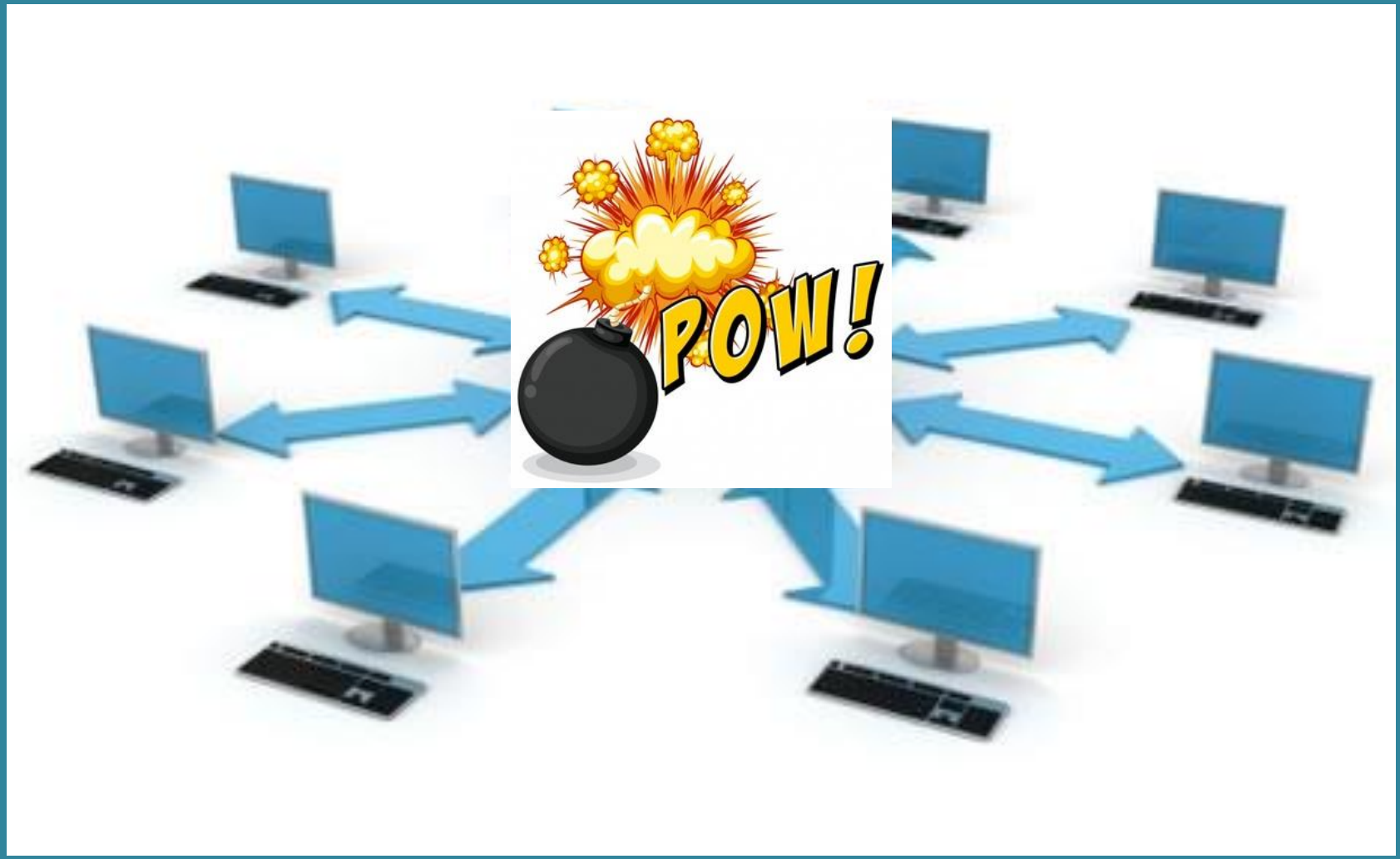
EverLedger (Diamond case)

22 June 2015
Laser inscription registry:
GIA 18712873
Shape and cutting style:
Round Brilliant
Measurements:
5.7-5.74 x 3.58mm
Carat weight: 0.74
Color grade: G
Clarity grade: SI 1
Cut grade: Very Good

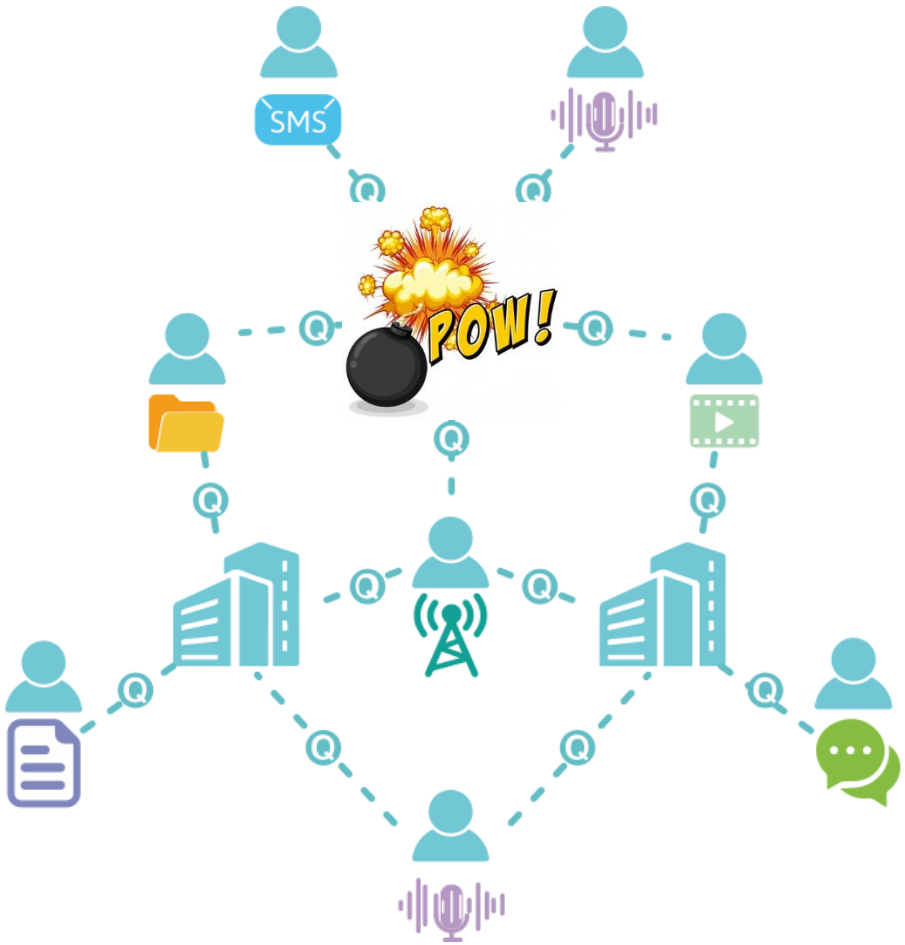


Blockchain consensus algorithms

Centralized System



Decentralized System

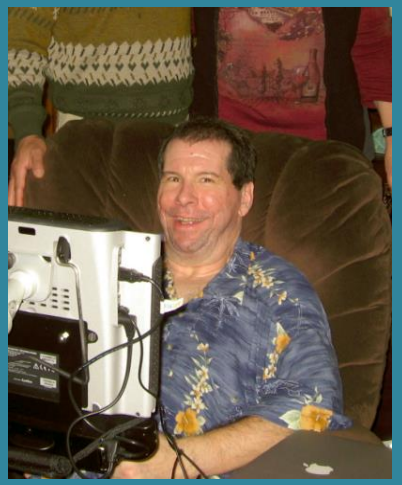


Distributed System

3rd Party (Middle Man)

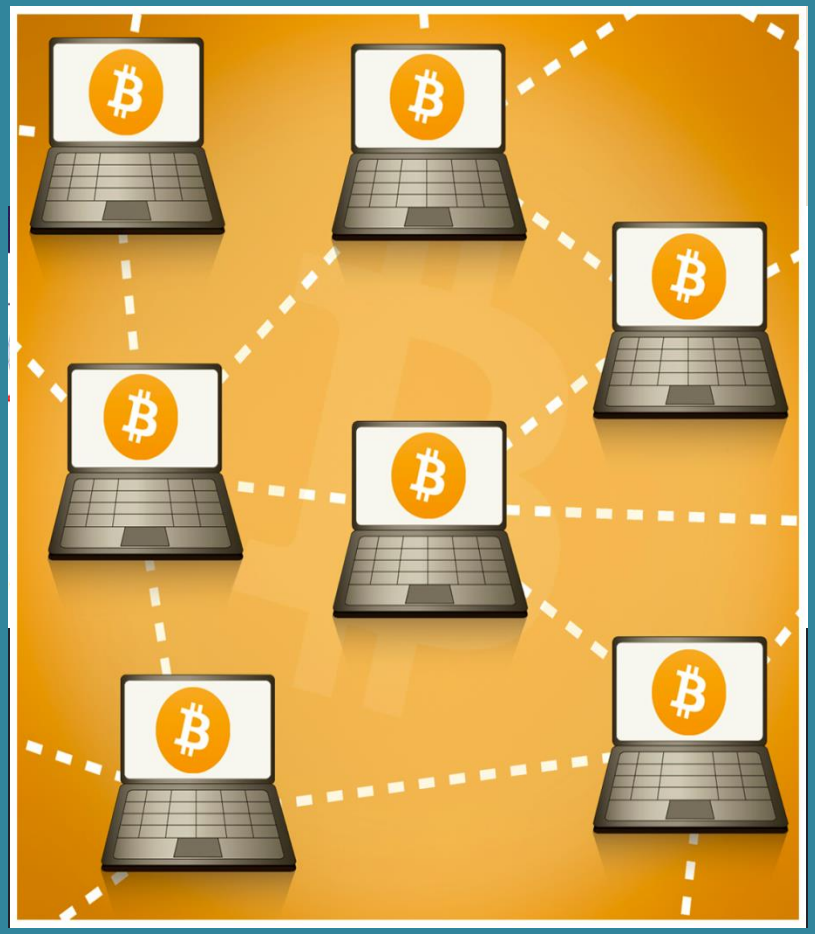
SATOSHI NAKAMOTO

HAL FINNEY

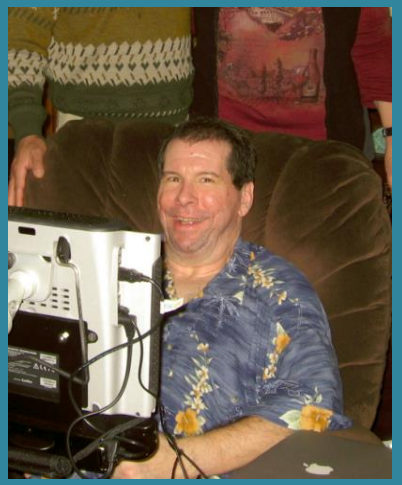


Blockchain

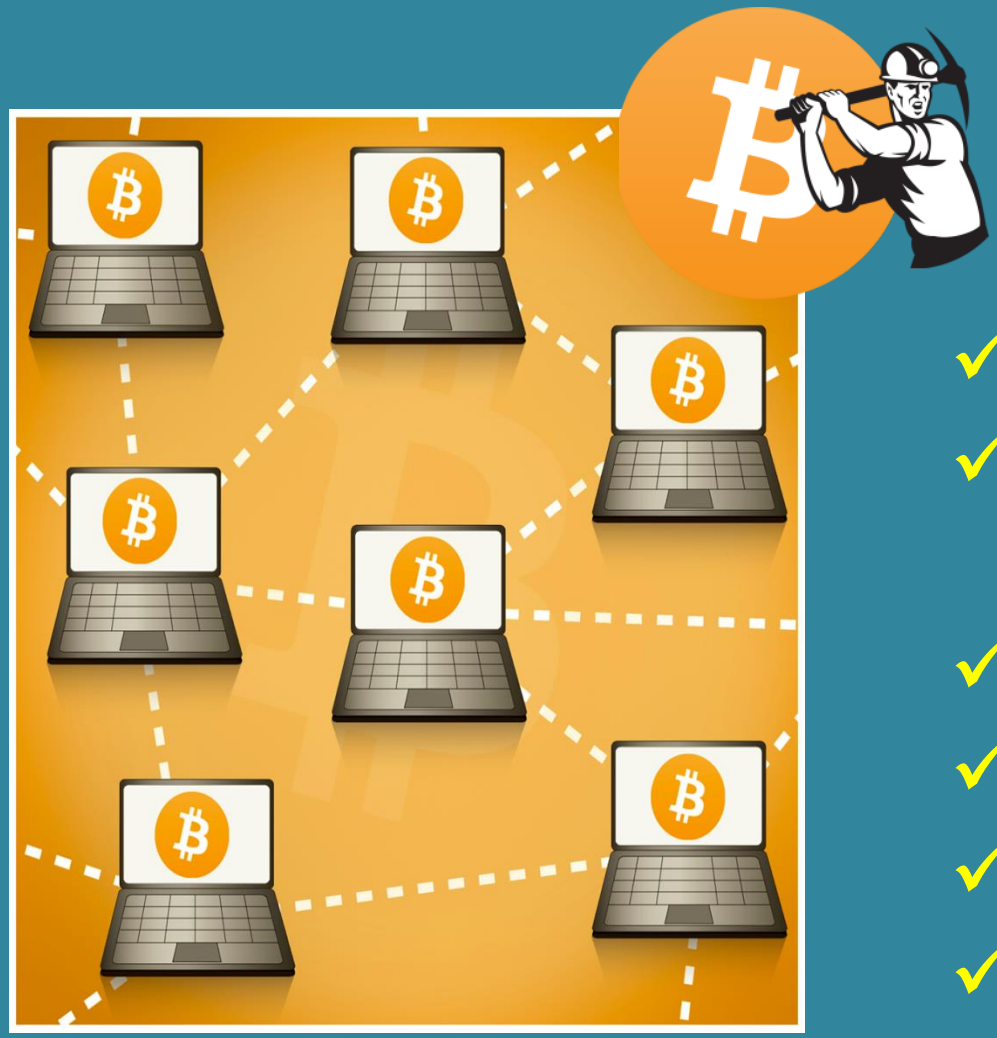
SATOSHI NAKAMOTO



HAL FINNEY



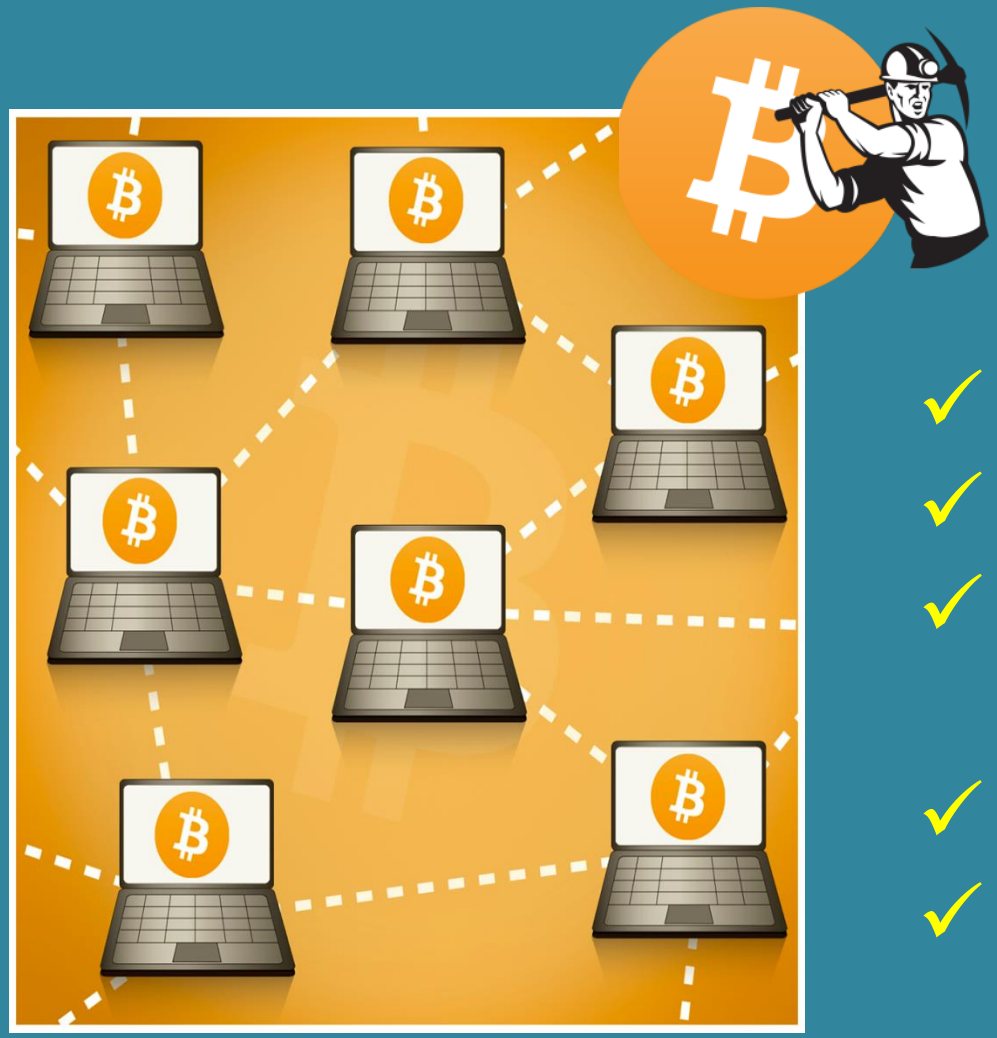
Voting Based



- ✓ Majority: 2/3
- ✓ 50+1 , 51%

- ✓ Majority by person
- ✓ Majority by cpu
- ✓ Majority by money
- ✓ Misbehave voting

Proof of Work



- ✓ **Expense CPU Power**
- ✓ **Expense Electricity**
- ✓ **Slow (10min)**

- ✓ **Hardware Centralized**
- ✓ **Region Centralized**

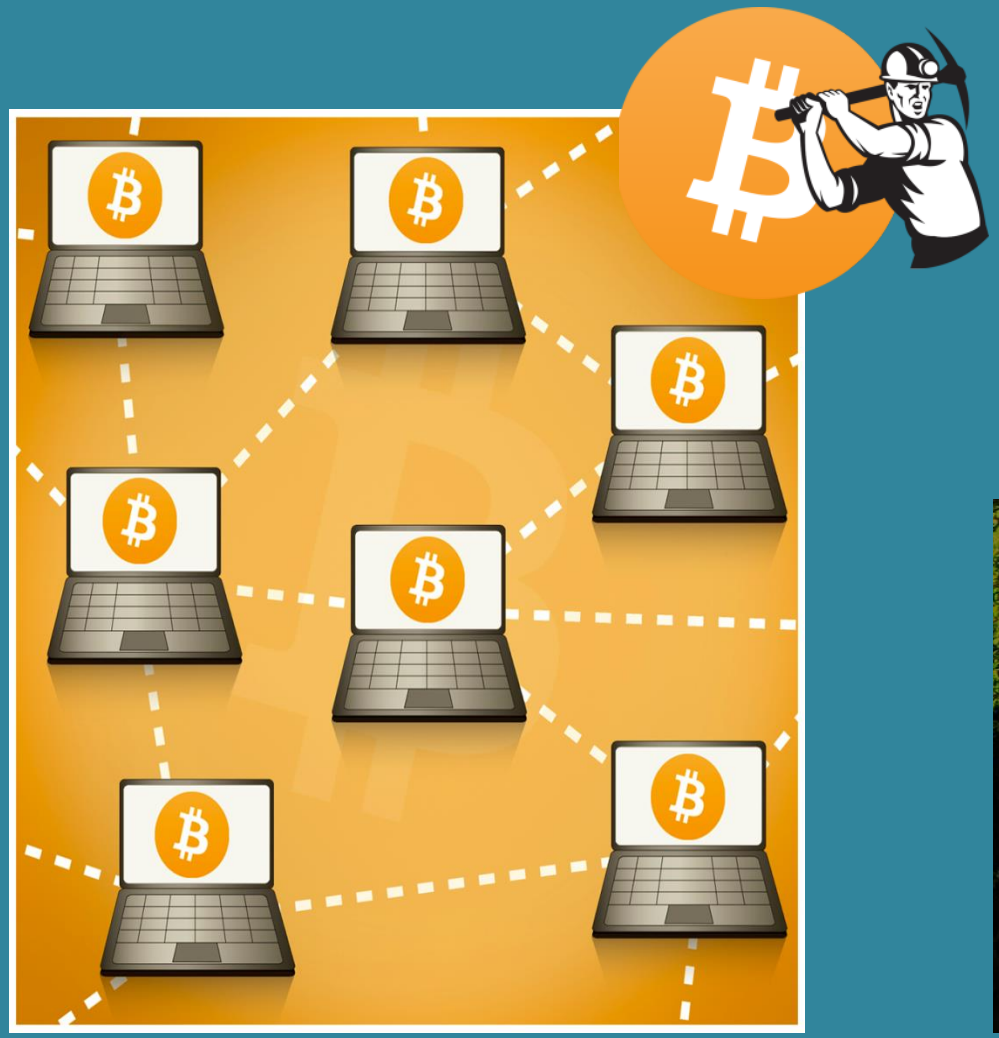
Master Node (Leader Based)

- ✓ **Attack Master Node**
- ✓ **Selection of Master**

Proof of Stake (Economy-based)

- ✓ Deposit money
- ✓ The rich get richer
- ✓ Punish when misbehave
- ✓ System might stuck

Virtual Voting Based



- ✓ Gossip protocol
- ✓ Gossip about Gossip
- ✓ Virtual voting