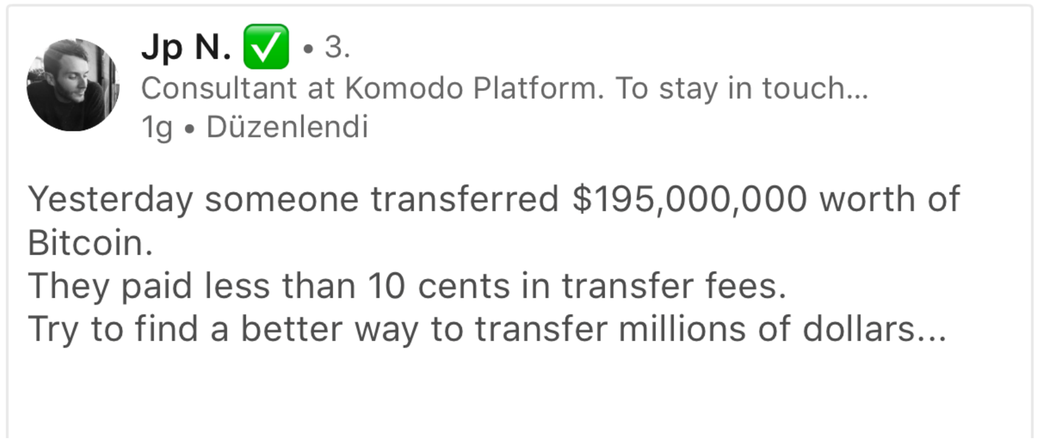
Lecture 6
BITCOIN IRL: WALLETS, MINING, & MORE

Blockchain on the news

South Korea Launches $90M Blockchain Education Course

https://ethereumworldnews.com/south-korea-90m-blockchain-education/



On Monday, the ministry's information and communication departments divulged that it had hosted its first ever lecture on distributed ledger technologies (DLT). This is reportedly the local government's first move to roll out a "blockchain technology development strategy" course that is backed by a supposed 100 billion Korean Won ($90 million USD) investment from forward-thinking regulators.

As per local media, the course has currently undertaken 42 students, who were selected via an amassment of applications and interviews to determine the best candidates for this fully-fledged course. Following the first lecture, students will need to work through six months of eight hour days that consist of tutelage, learning the ropes of the tech and more activities that are intended to put the 42 scholars through the wringer.

Image Courtesy of KiNews

LECTURE OVERVIEW

1. WALLET TYPES
2. WALLET MECHANICS
3. MINING
4. REAL WORLD MINING
5. CHANGING BITCOIN

1 WALLET TYPES

TYPES OF USERS

KEY COMPONENTS

Not every client is a miner
What if I don't have a powerful computer?

Not every client has the entire blockchain (160+ GB)
What if I just want to send bitcoins with my phone?

Not every client is directly connected to the network
What if I don't need to make regular transactions?

Not every client has a wallet
What if I have a separate wallet client?

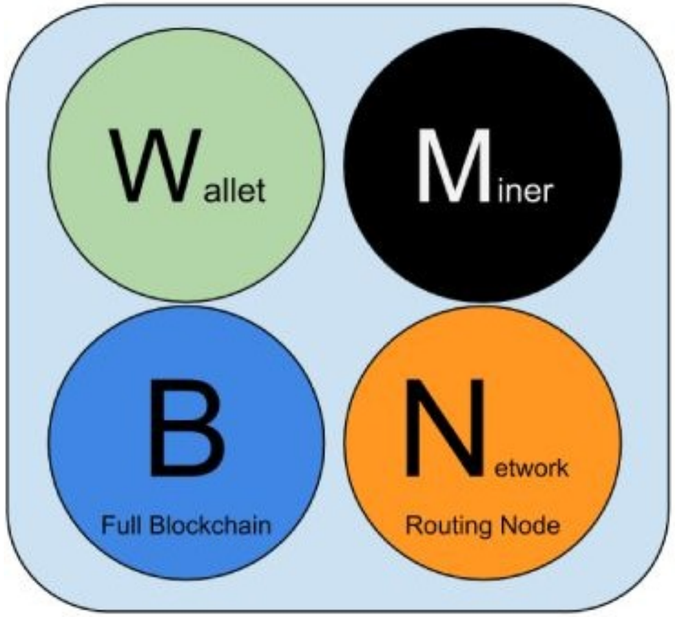


Image source: Mastering Bitcoin

TYPES OF USERS

EVERYONE

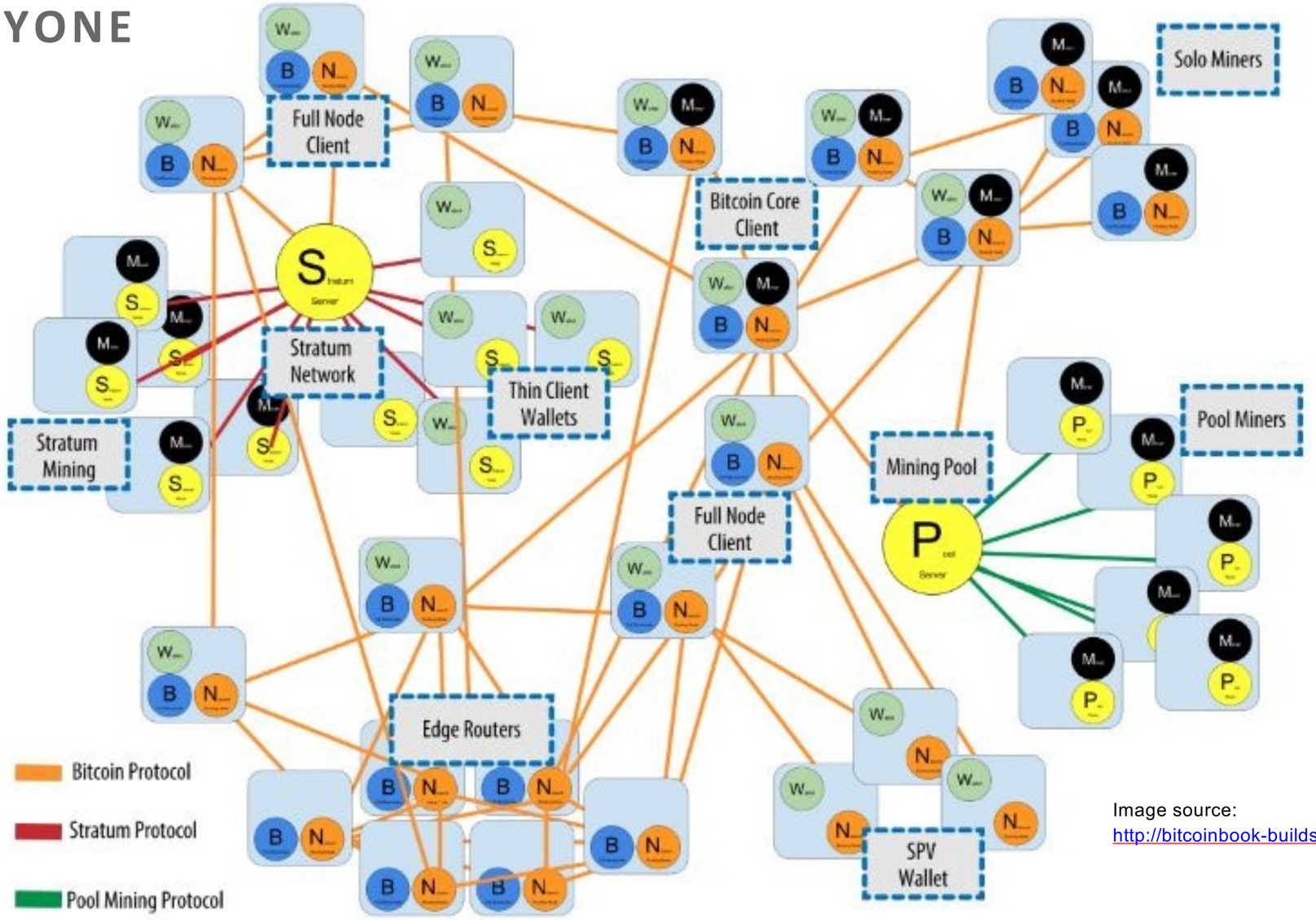


Image source:
http://bitcoinbook-builds.mkvd.net/translations/vi/chapter-6.html

BITCOIN WALLETS

KEY MANAGEMENT

To secure our **identity**, we need to secure our **private key**

How do we manage all of our keys? With wallets!

BITCOIN WALLETS

WALLET TYPES

What do wallets do?

- Keep track of your private key
- Store, send & receive, and list transactions
- Maybe some other related fancy functionality

BITCOIN WALLETS

HOT AND COLD

Wallet Forms

- Smartphone apps
  - Mycelium, AirBitz
- Online web-wallets
  - Blockchain.info, coinbase.com
- Paper Wallets
  - Bitcoinpaperwallet.com
  - Bitaddress.org
- Hardware Wallets
  - Ledger, Trezor, Case, KeepKey
- Brain Wallet

Hot Wallet

Cold Storage

BITCOIN WALLETS

HOT WALLETS

Wallet Forms

- Smartphone apps
  - Mycelium, AirBitz
- Online web-wallets
  - Blockchain.info, coinbase.com
- Paper Wallets
  - Bitcoinpaperwallet.com
  - Bitaddress.org
- Hardware Wallets
  - Ledger, Trezor, Case, KeepKey
- Brain Wallet

} Hot Wallet

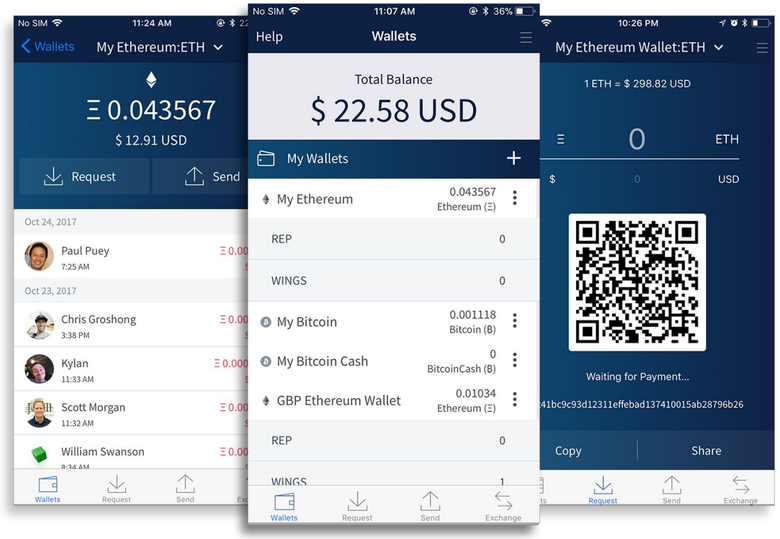
BITCOIN WALLETS

HOT WALLETS

coinbase

BLOCKCHAIN

airBitz



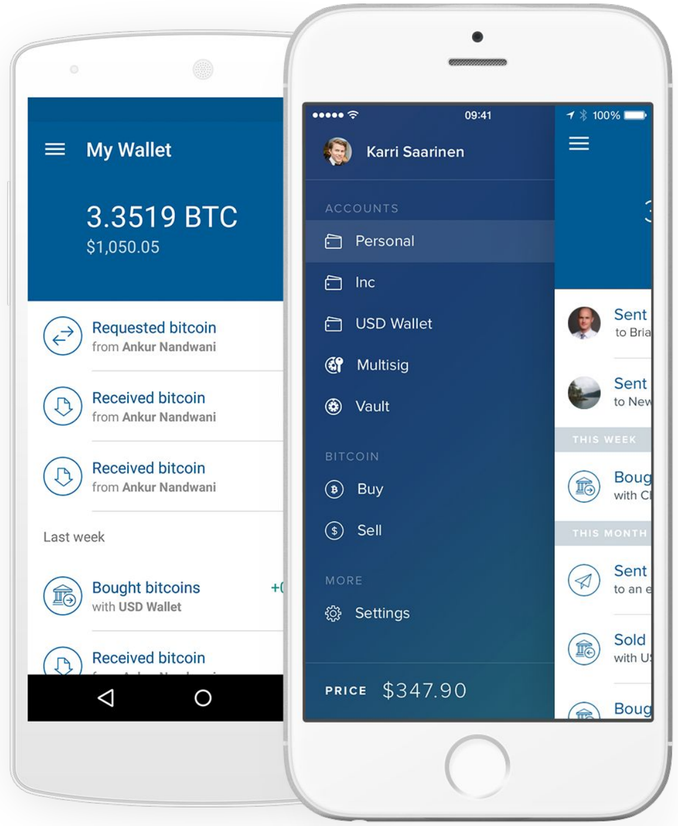


Image sources:
https://blockchain.info/
https://wallet.mycelium.com
https://airbitz.co/bitcoin-wallet/
https://www.coinbase.com/mobile

BITCOIN WALLETS

COLD STORAGE

Wallet Forms

- Smartphone apps
  - Mycelium, AirBitz
- Online web-wallets
  - Blockchain.info, coinbase.com
- Paper Wallets
  - Bitcoinpaperwallet.com
  - Bitaddress.org
- Hardware Wallets
  - Ledger, Trezor, Case, KeepKey
- Brain Wallet

} Cold Storage

BITCOIN WALLETS

PAPER WALLETS

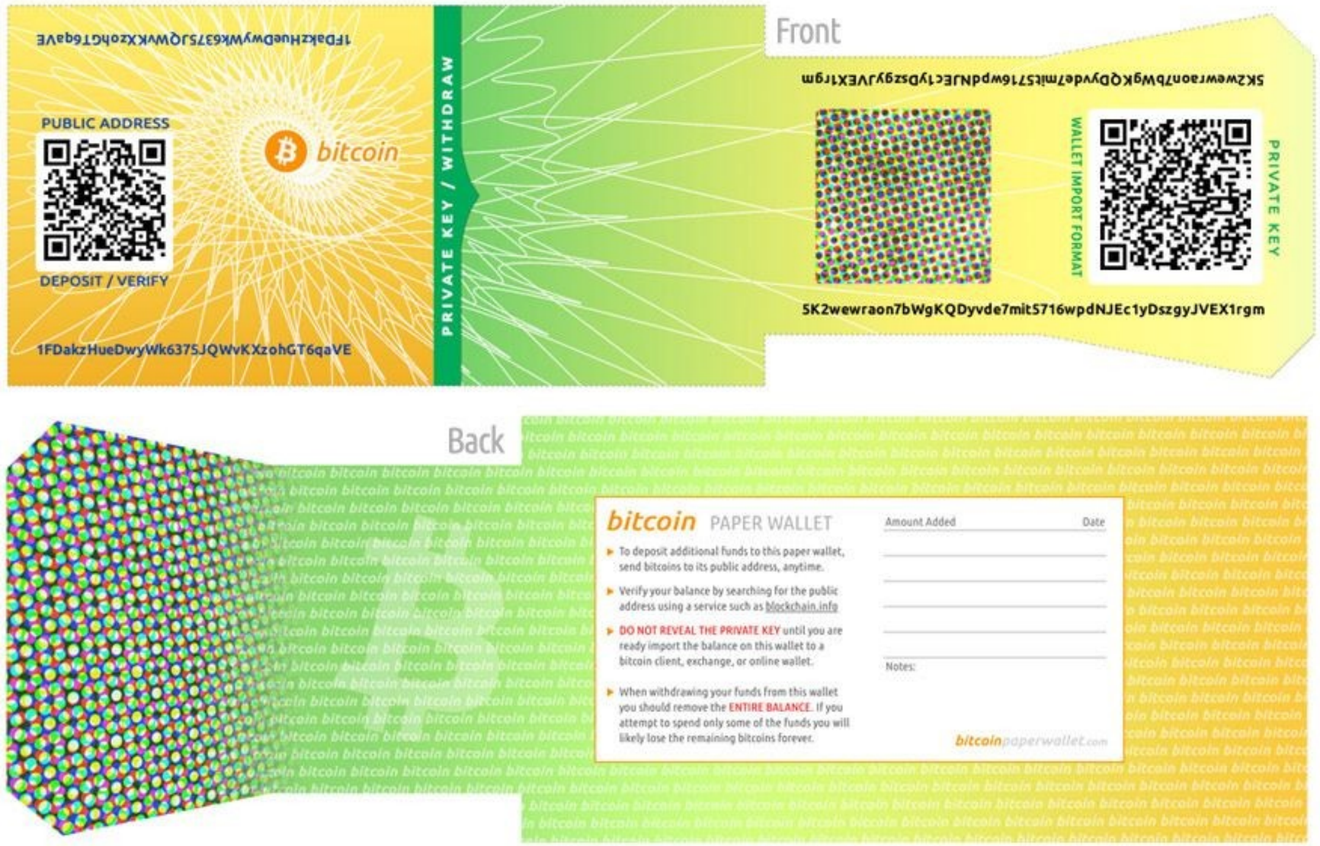


Image source: https://bitcoinpaperwallet.com/

Going Offline

ZIP

Your wallet may be vulnerable to prying eyes when you are generating the keys and printing them out. Although the wallet generator on this website is SSL-encrypted, it's still possible for someone to be snooping on you. (For example, your computer might have malware that broadcasts your screen to a remote location.) The most important safety measure is to **go offline** and run the javascript wallet generator on your own computer instead of this website.

Here's how »

TLDR: DOWNLOAD THE ZIP FILE OR GET THE UBUNTU LIVECD AND RUN THE WALLET GENERATOR WITH YOUR INTERNET CONNECTION TURNED OFF.

BITCOIN WALLETS

HARDWARE WALLETS

Image sources:
https://www.ledgerwallet.com/
https://trezor.io/
https://choosecase.com/

BITCOIN WALLETS

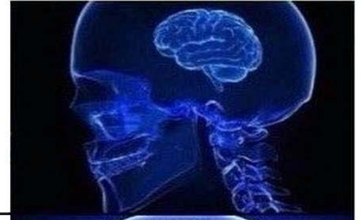
BRAIN WALLETS

- Simply memorize your private key

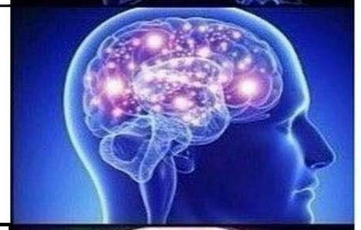
L2Skyj3pJK3nc7wgr9afokGL89dP

WV3iHQJvZiy2zEwvXDQReAgg

using a recommended bitcoin wallet

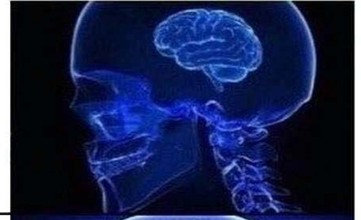


storing crypto on a hardware wallet

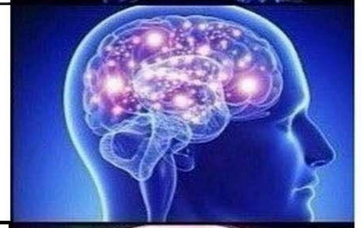


writing private keys on a post it and putting it on your computer

using a recommended bitcoin wallet



storing crypto on a hardware wallet

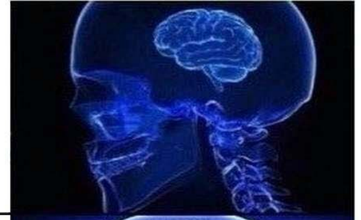


writing private keys on a post it and putting it on your computer

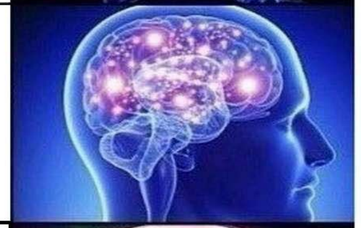
memorizing **L2Skyj3pJK3nc7wgr9afokGL89dPWV3iHQJvZiy2zEwvXDQReAgg** and forgetting it after a day

memorizing

using a recommended bitcoin wallet



storing crypto on a hardware wallet



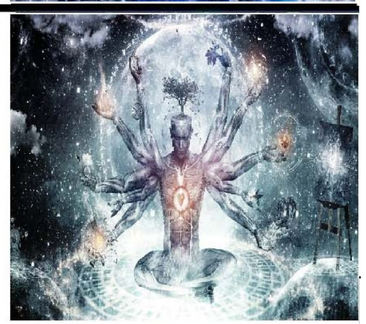
writing private keys on a post it and putting it on your computer

memorizing **L2Skyj3pJK3nc7wgr9afokGL89dPWV3iHQJvZiy2zEwvXDQReAgg** and forgetting it after a day

memorizing

storing your crypto on

coinbase

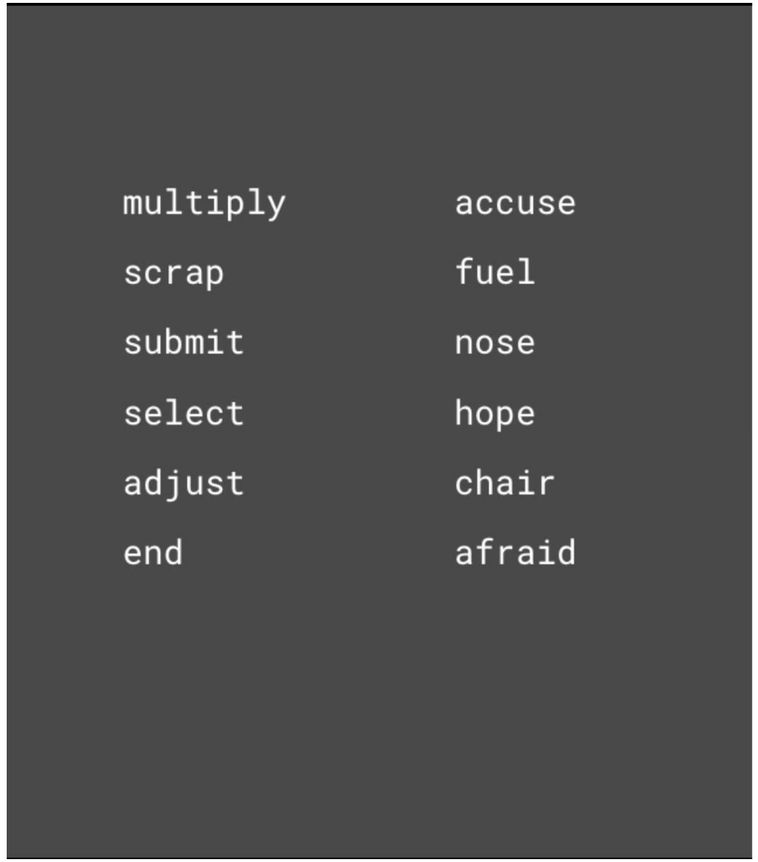


BITCOIN WALLETS

BRAIN WALLETS

Brain wallets are a mnemonic, or collection of words/phrases

- Convenient way to memorize your private key
- Easier to have something that you can turn into your private key
- Not very secure, as humans aren’t as random as we think we are



BITCOIN WALLETS

KEY STRETCHING

multiply scrap
submit select
adjust end accuse
fuel nose hope
chair afraid

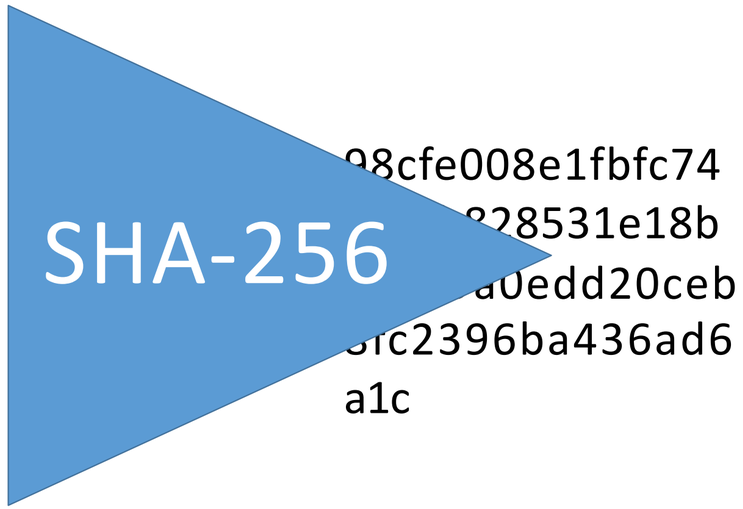
BITCOIN WALLETS

KEY STRETCHING

multi
subm
adjus
fuel r
chain

BITCOIN WALLETS

KEY STRETCHING



BITCOIN WALLETS

KEY STRETCHING

98cfe008e1fbfc74
770fb828531e18b
a4c19a0edd20ceb
8fc2396ba436ad6
a1c

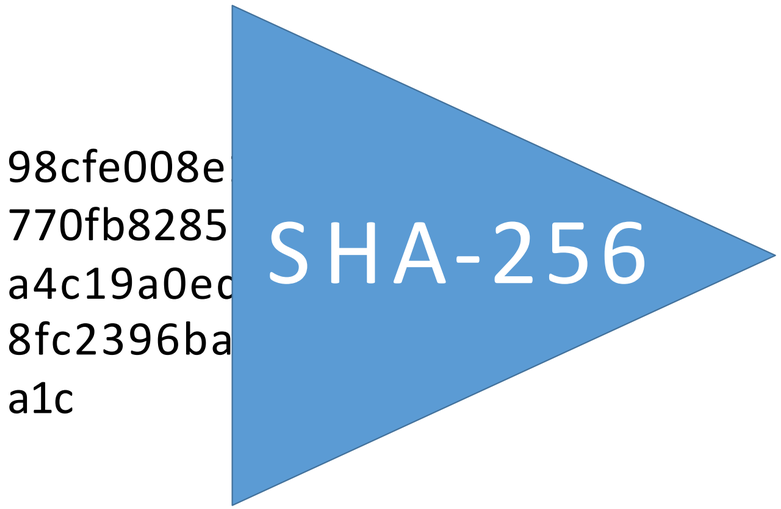
BITCOIN WALLETS

KEY STRETCHING

98cfe008e1fbfc74
770fb828531e18b
a4c19a0edd20ceb
8fc2396ba436ad6
a1c

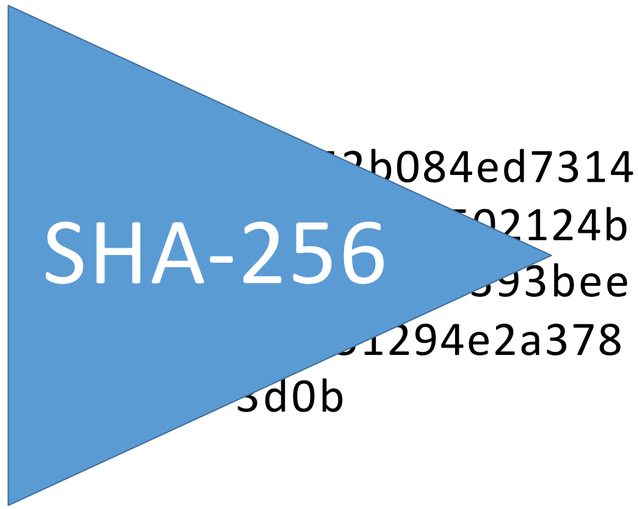
BITCOIN WALLETS

KEY STRETCHING



BITCOIN WALLETS

KEY STRETCHING



BITCOIN WALLETS

KEY STRETCHING

a4552b084ed7314
415b9367502124b
f84be086a393bee
b0fb51294e2a378
3d0b

BITCOIN WALLETS

CHOOSING A WALLET

Bitcoin.org/en/choose-your-wallet

Features

Multisignature
- 2/3 access control

Privacy
- TOR support
- New addresses for each transaction

Security

Network connection
- Full node
- 3rd party

Who holds the private keys?
- You: mycelium, airbitz, blockchain.info
- Developer: coinbase.com

Image source: https://bitcoin.org

HOW DO I GET BITCOIN?

BITCOIN ATMS

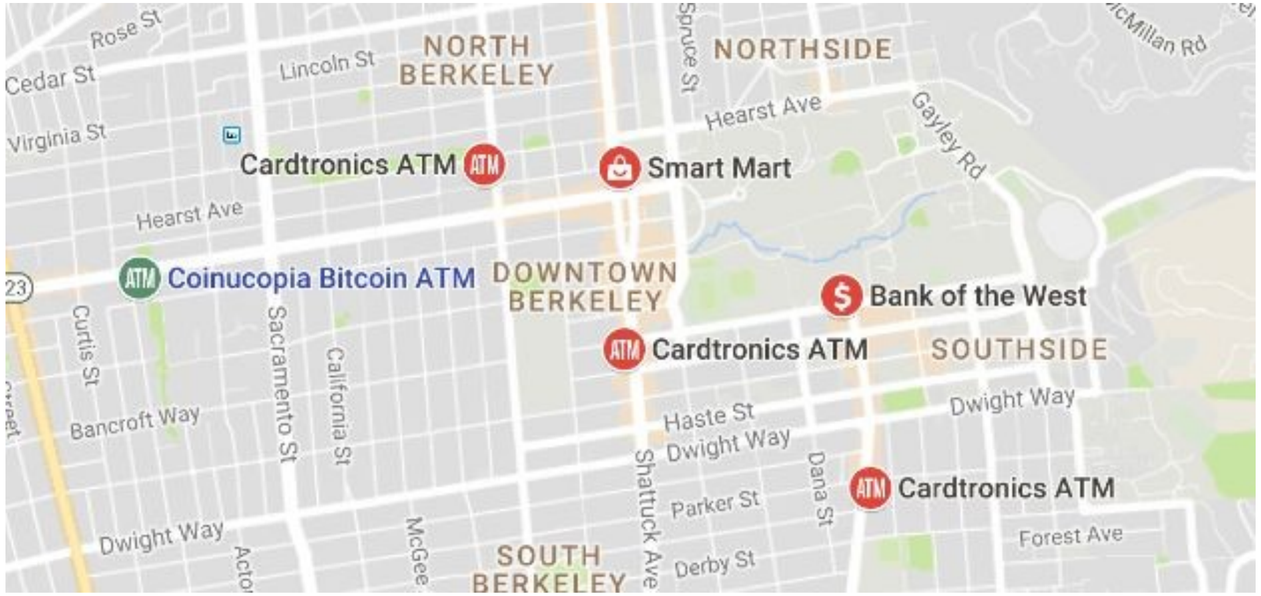


Image sources:
https://www.google.com/maps
https://coinucopia.io/

HOW DO I GET BITCOIN?

EXCHANGES

- Exchanges:
  - https://bitcoin.org/en/exchanges
- Trading between different types of currency
- Centralized and decentralized exchanges, security, easy of access, etc.

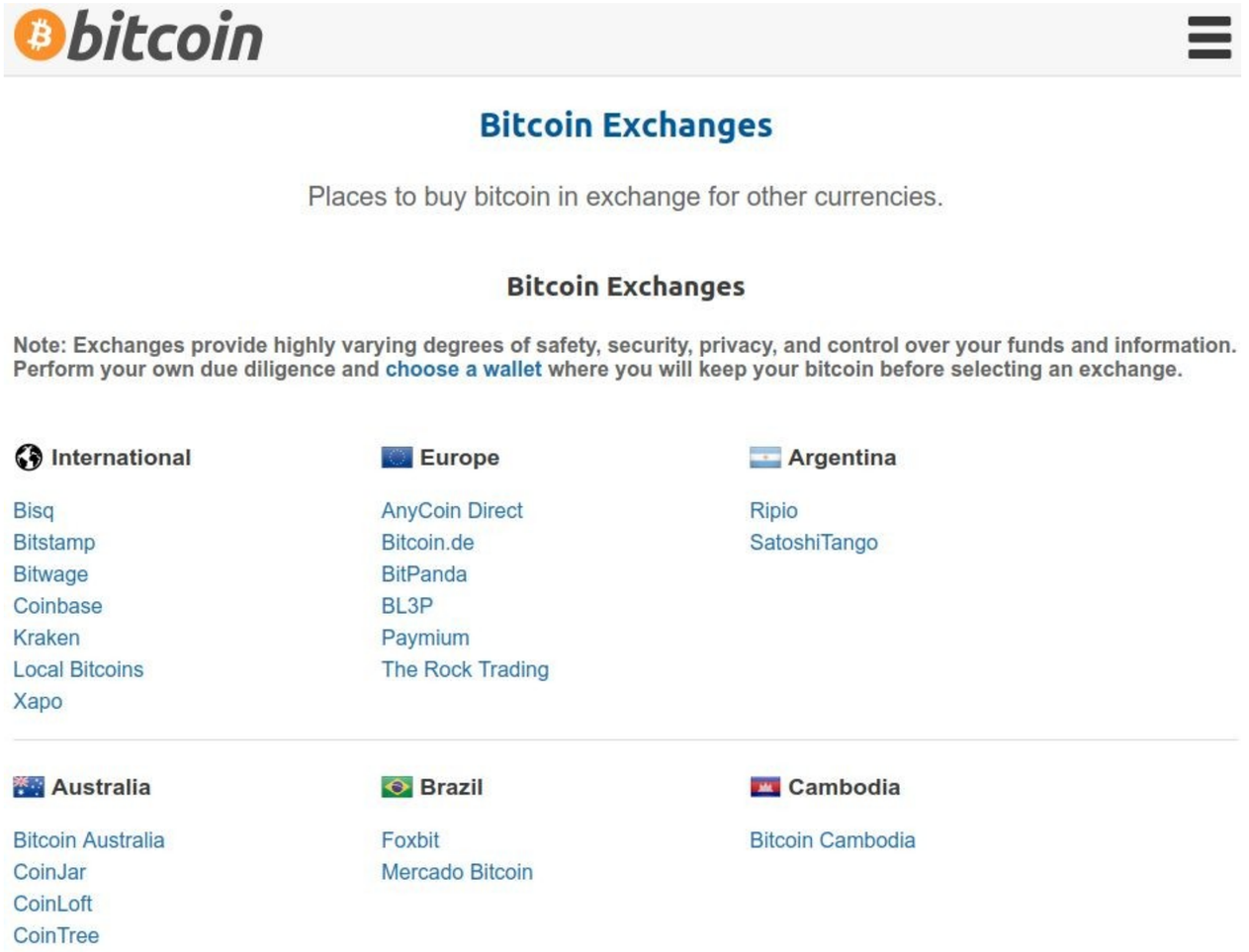


Image source: https://bitcoin.org/en/exchanges

HOW DO I GET BITCOIN?

DECENTRALIZED EXCHANGES

Decentralized exchanges don’t rely on a third party service to hold customer’s funds or private keys

- Trades are P2P
- Trustless
- Bitshares, Bisq (ex Bitsquare), Openledger, Airswap, Etherdelta, etc.

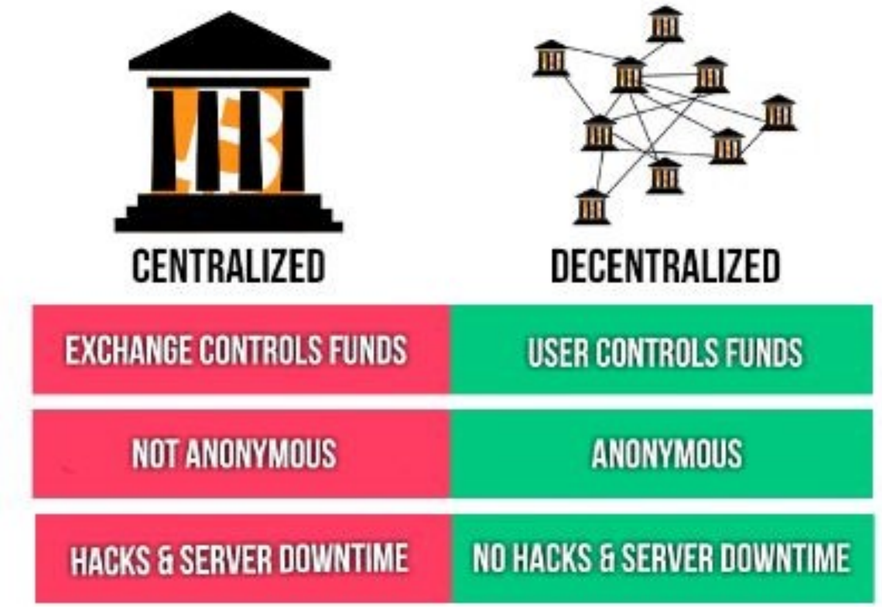


Image source:
https://www.cryptocompare.com/exchanges/guides/what-is-a-decentralized-exchange/

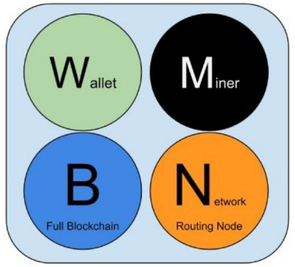
2 WALLET MECHANICS

SIMPLE PAYMENT VERIFICATION

THIN CLIENTS

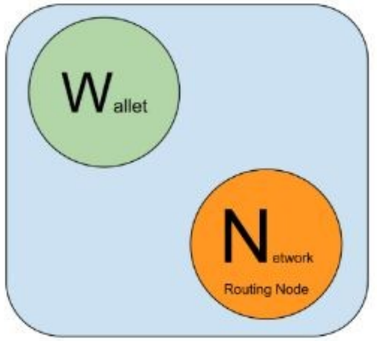
Simple Payment Verification (SPV) is method for verifying if particular transactions are included in a block without downloading the entire block

- Keep track of your transactions only
- Lightweight or thin clients



Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

Image source: http://bitcoinbook-builds.mkvd.net/translations/vi/chapter-6.html

SIMPLE PAYMENT VERIFICATION

THIN CLIENTS

Assumption: Incoming block headers are not from a false chain

- Connect to many different nodes
- Long term, chain is probably honest
- Can't really afford to put the entire blockchain on your phone, so having a thin client is a decent tradeoff

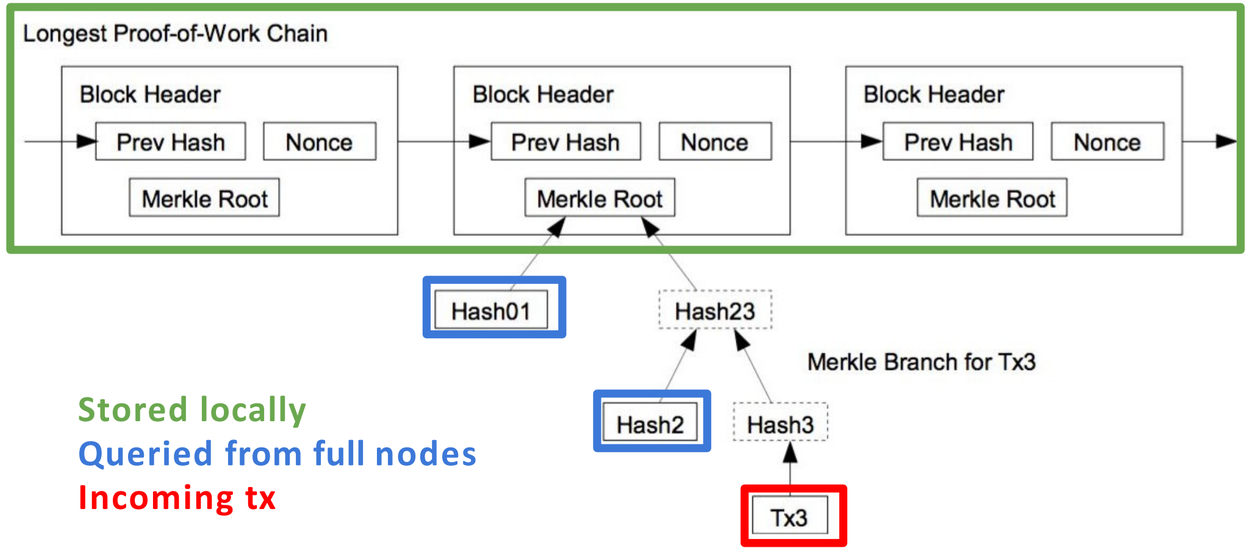


Image source: Mastering Bitcoin

MULTISIGNATURE

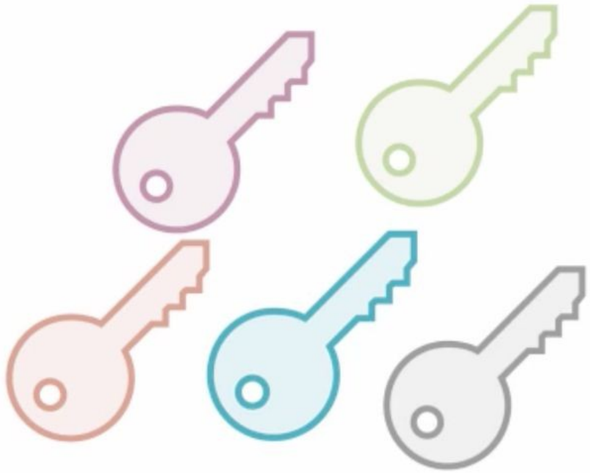
M-OF-N TRANSACTIONS

Multi-person Account Access

Regular Bitcoin Addresses

Each account has 1 key (or seed)

Any single person can steal funds



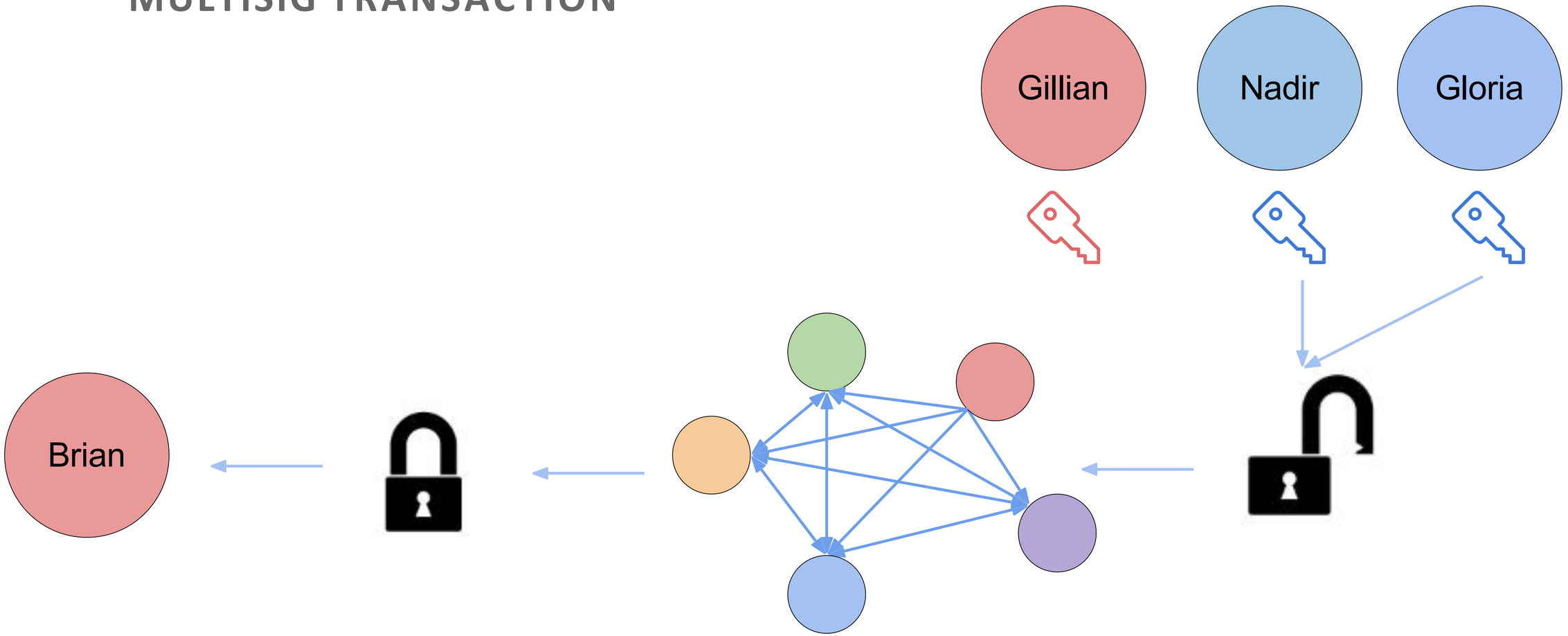
Multisignature Addresses

Multiple signatures needed

Ex: 3 of 5 signatures

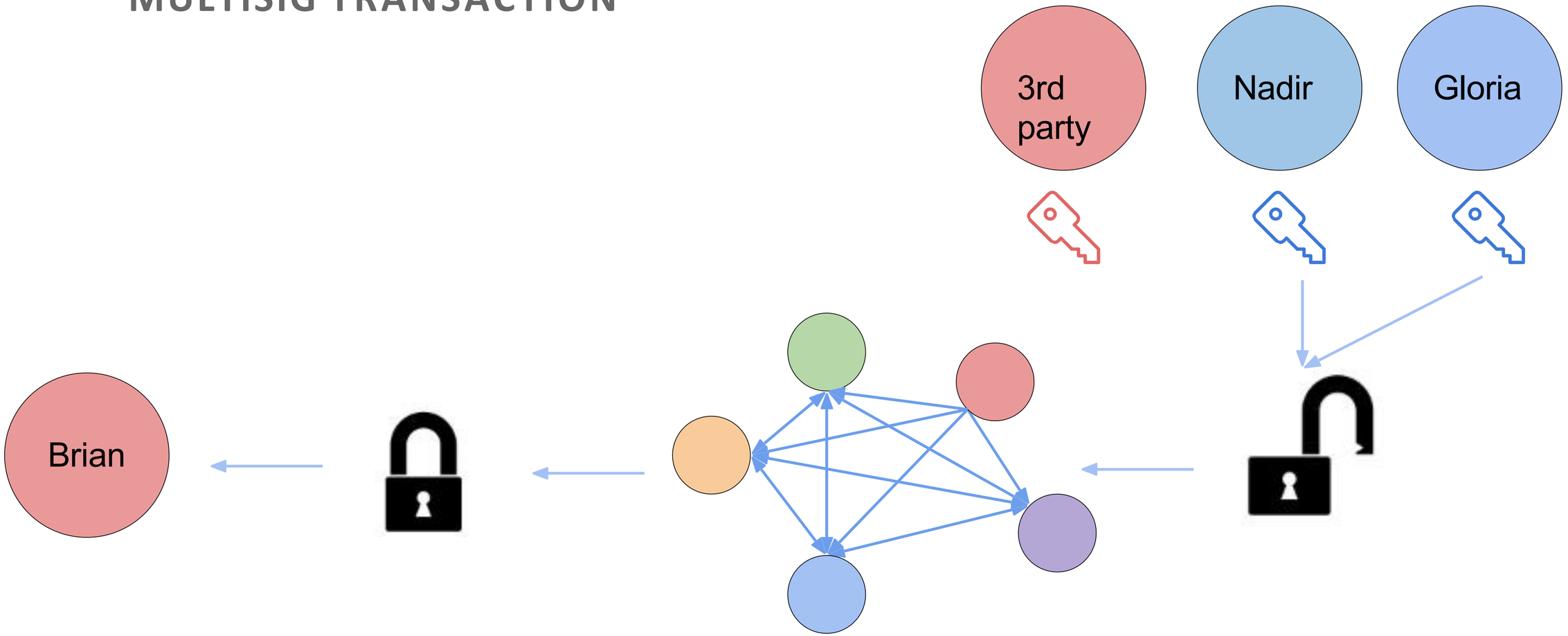
BITCOIN MECHANICS

MULTISIG TRANSACTION



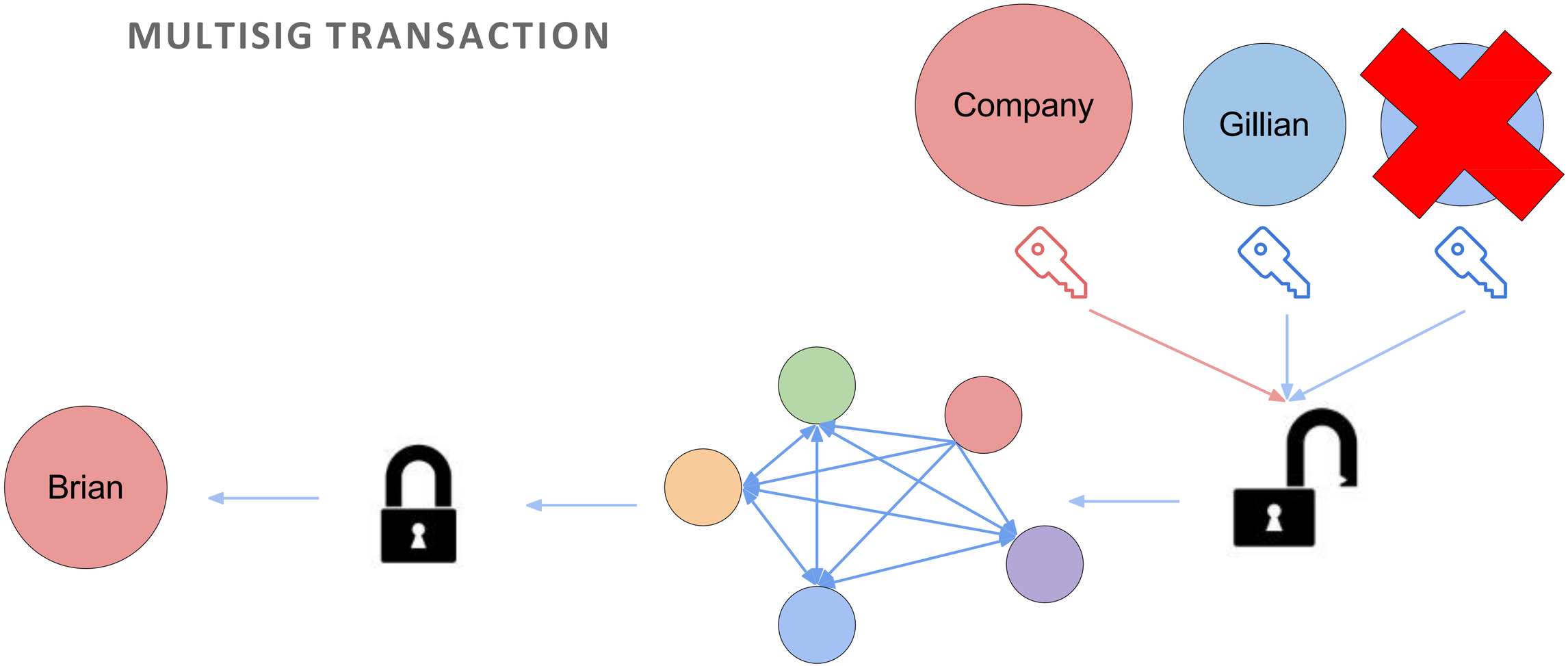
BITCOIN MECHANICS

MULTISIG TRANSACTION



BITCOIN MECHANICS

MULTISIG TRANSACTION



BITCOIN MECHANICS

KEY GENERATION PRACTICES

- Best practice is to never reuse pseudonyms

- Why?
  - Someone should not be able to determine how much bitcoin you own
  - Compromising one key is independent of the other ones
  - Keys are computationally easy to generate anyways

- Wallet software will handle this

WALLET BACKUPS

JBOK WALLETS

- **JBOK (Just a Bunch Of Keys)**
  - New backup required for every new key pair
  - Or, generate a bunch of keys when first started
  - Not too convenient because you have to store every key pair

WALLET BACKUPS

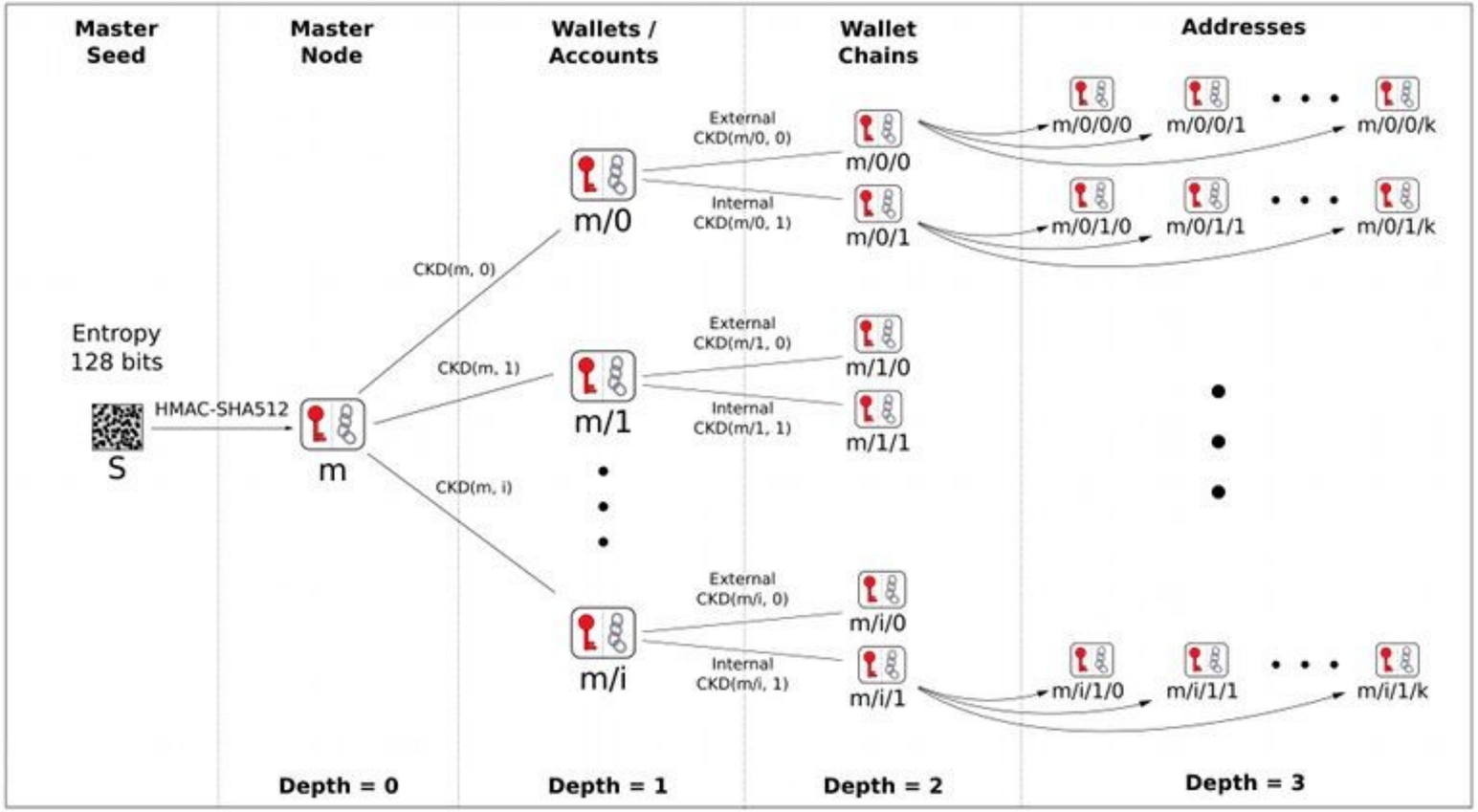
HD WALLETS

- **HD (Hierarchical Deterministic) Wallets**
  - Deterministic, and more convenient to know a seed, or master key
  - Use a one-way hash function with seed and index number
  - Exchanges use these

BITCOIN WALLETS

WALLET BACKUPS

BIP 32 - Hierarchical Deterministic Wallets



Child Key Derivation Function ~ $CKD(x,n) = HMAC\text{-}SHA512(x_{Chain}, x_{PubKey} || n)$

3

MINING

3.1 MINING REVIEW

RECIPE FOR MINING

OVERVIEW

Image source: http://www.coindesk.com/information/how-to-set-up-a-miner/

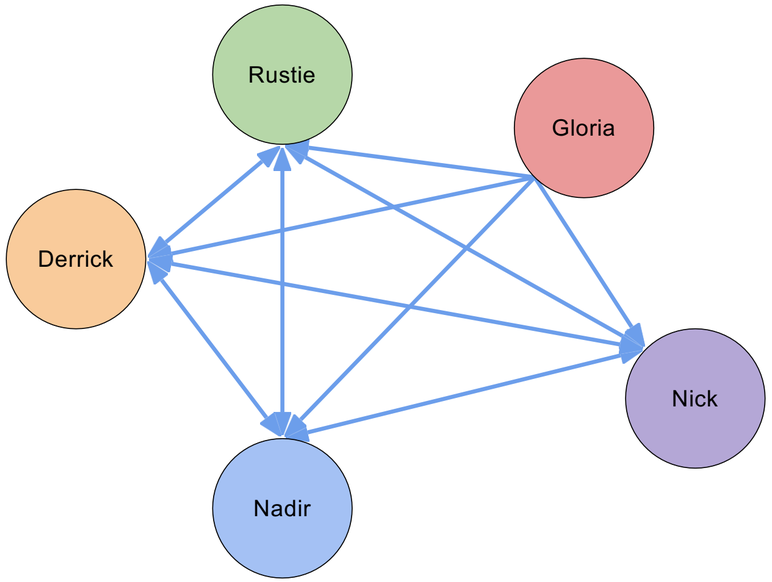
A full-fledged Bitcoin miner must:

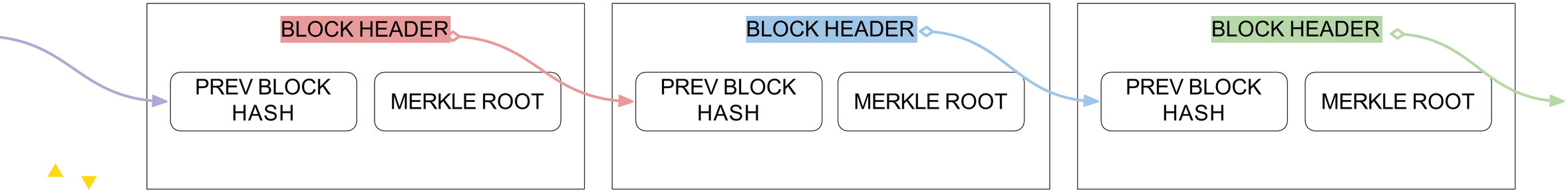
1. **Download** the entire Bitcoin blockchain
2. **Verify** incoming transactions
3. **Create** a block
4. **Find** a valid nonce
5. **Broadcast** your block
6. **Profit**!

RECIPE FOR MINING

STEP 0: DOWNLOAD THE BLOCKCHAIN

- Get blocks from your peers
- Download the entire blockchain
  - Start from the genesis block
- Stay up to date

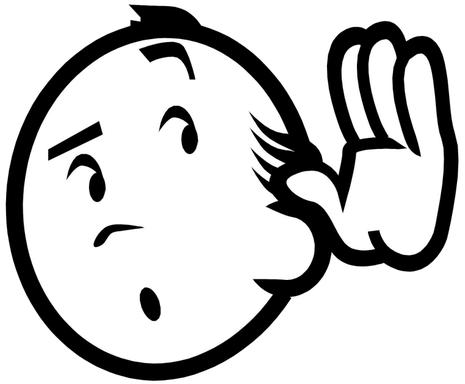




RECIPE FOR MINING

STEP 1: VERIFY TRANSACTIONS

- Listen to the Bitcoin network for transactions
- Unconfirmed (pending) transactions sit in the **mempool** for a miner to include it in a block
- Verify incoming transactions by running the unlocking script (remember P2PKH and P2SH?)



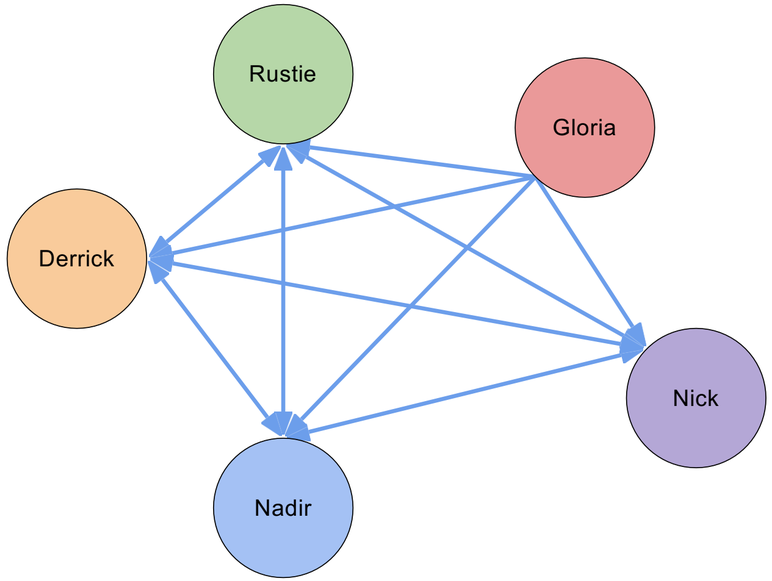
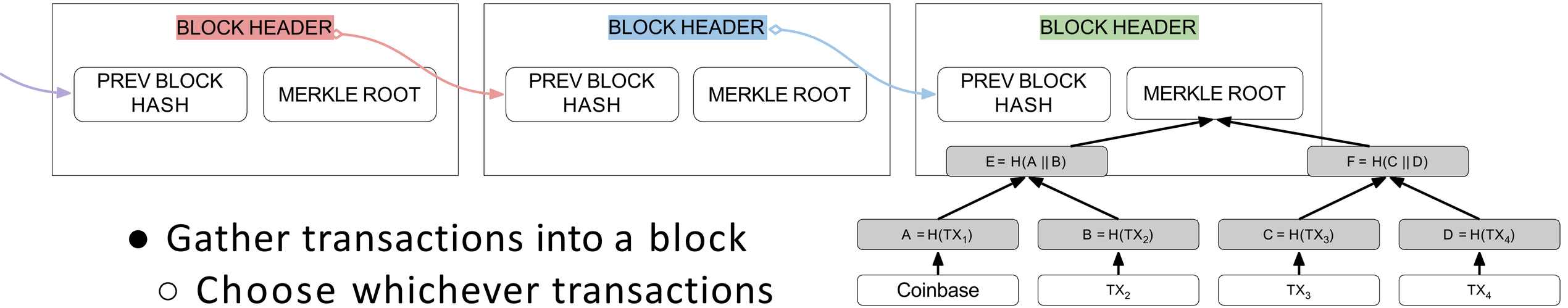


Image sources:
https://ru-clip.com/video/rVrb6rrRvNQ/what-is-a-mempool-and-how-to-speed-up-unconfirmed-transactions.html
https://englishinreims.wordpress.com/toeic-training/practice-toeic-listening-part-i/

RECIPE FOR MINING

STEP 2: CREATE A BLOCK

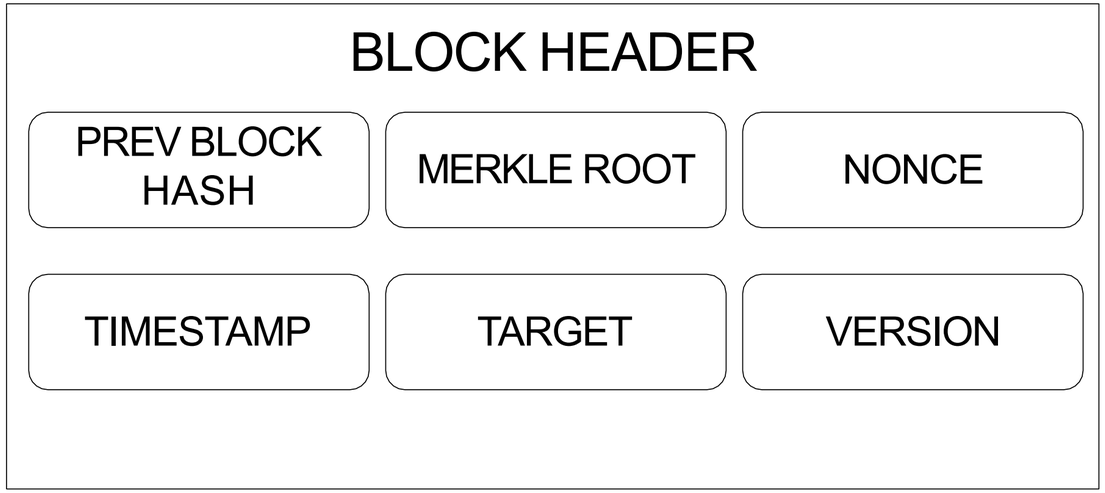


- Gather transactions into a block
  - Choose whichever transactions you want (most transaction fees)
- Get previous block hash and other necessary metadata

RECIPE FOR MINING

STEP 3: FIND A VALID NONCE

- Find the proof-of-work
- Expend computational power
- Incrementing header nonce first, then coinbase nonce as necessary to change puzzle




```
TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while (1) {
      header = makeBlockHeader(transactions, coinbase_nonce);
      for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++){
            if (SHA256(SHA256(makeBlock(header, header_nonce))) <
      TARGET)
                  break; //block found!
      }
      coinbase_nonce++;
}
```

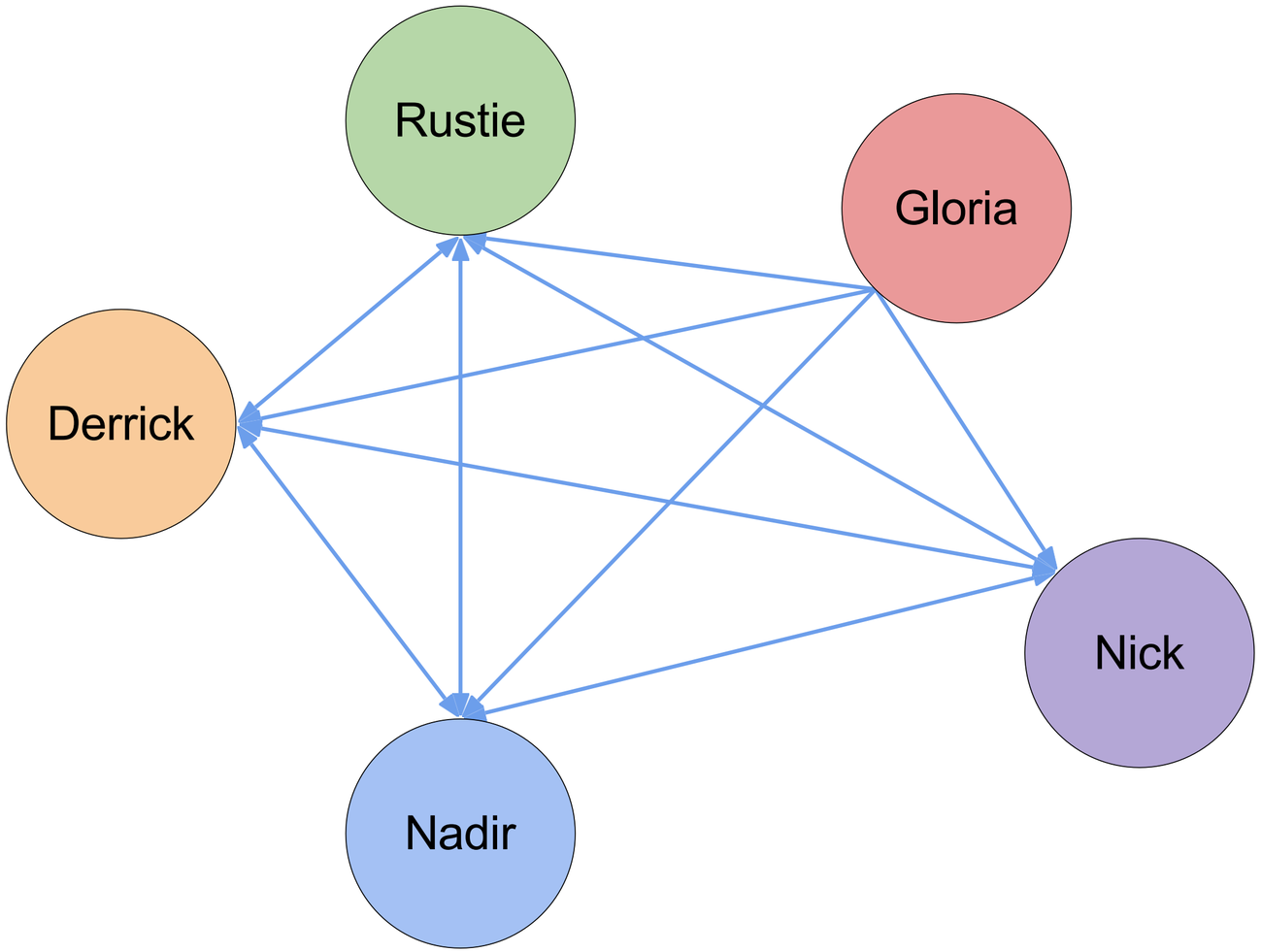
Figure 5.6 : CPU mining pseudocode.

Image source: Mastering Bitcoin

RECIPE FOR MINING

STEP 4: BROADCAST

- Broadcast to the rest of the network
- Others check transactions in the proposed block
  - Accept if it's the first valid block they see
- Propagate to everyone



RECIPE FOR MINING

STEP 5: PROFIT

Remember: Mining is a competition

- Block included in longest chain
  - Profit from block reward (coinbase transaction) and transaction fees
  - All transactions added to canon transaction history
- Not included in longest chain
  - Your block may not have been the first valid block seen by others
  - Start mining next block

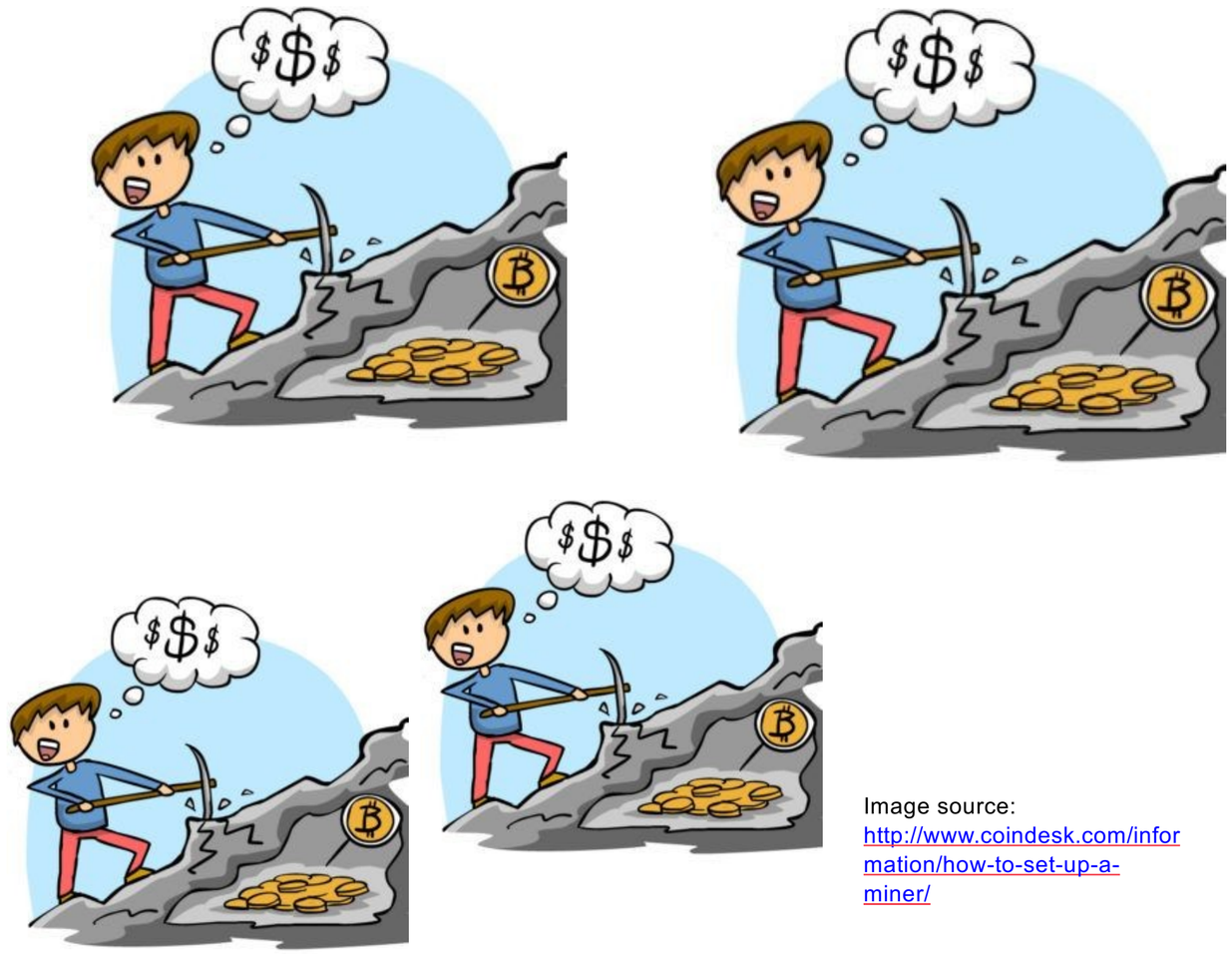


Image source: http://www.coindesk.com/information/how-to-set-up-a-miner/

3.2 MINING INCENTIVES

MINING INCENTIVES

WHY DO WE DO THINGS?

PROFIT

MINING INCENTIVES

WHY DO WE DO THINGS?

MINING INCENTIVES

WHAT IS PROFIT?

```
if revenue > cost:
 return “$$$$”
```

PROFIT = REVENUE - COST

MINING INCENTIVES

HOW TO PROFIT FROM MINING

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

if MINING_REVENUE > MINING_COST:
 miner.get_profit()
```

MINING INCENTIVES

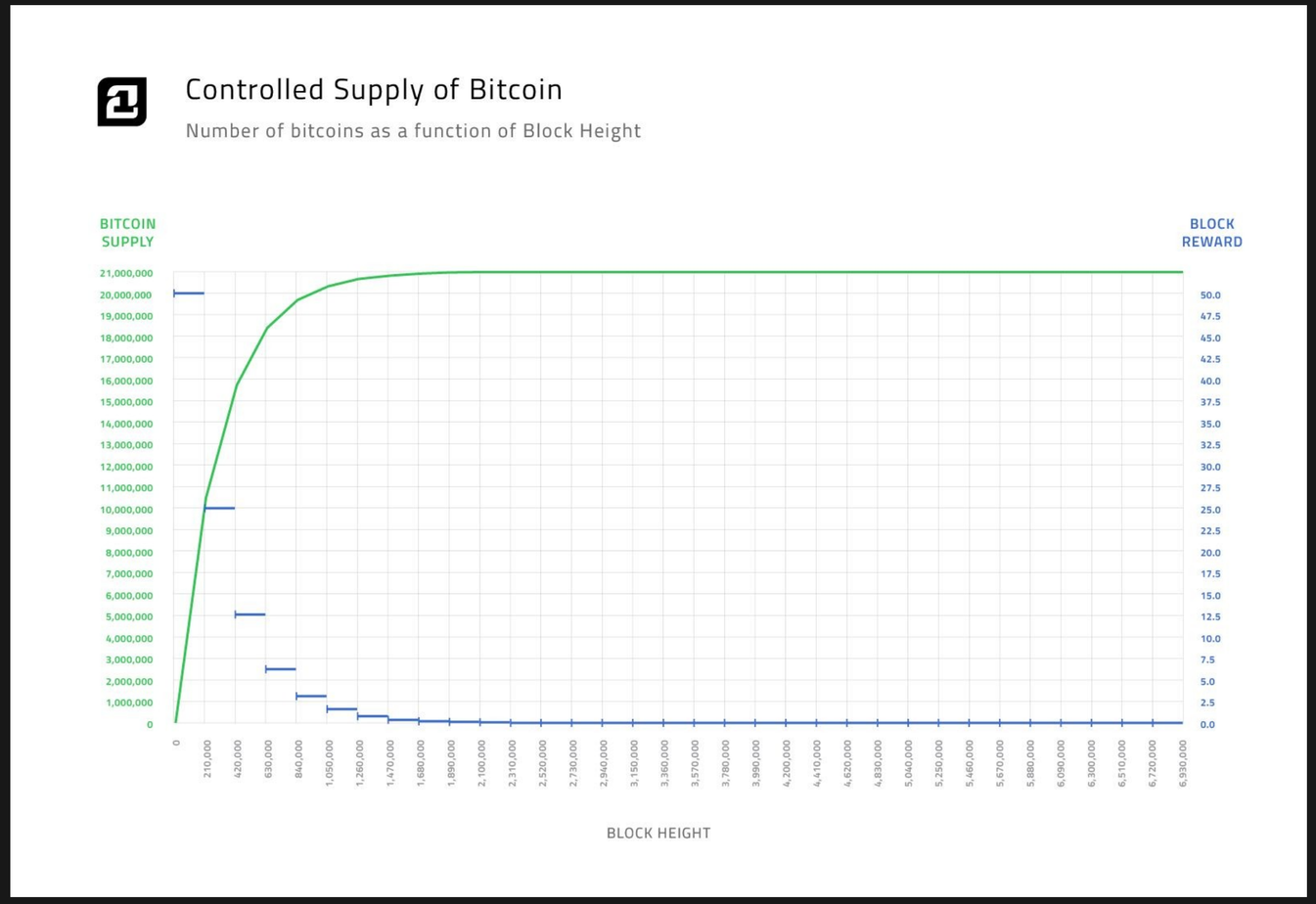
HOW TO PROFIT FROM MINING

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

if MINING_REVENUE > MINING_COST:
 miner.get_profit()
```

Image source: https://profitbitcoin.com/

MINING INCENTIVES

BLOCK REWARD



- Miner receives BTC for every confirmed block
  - Currently 12.5 per block
- Miner includes special transaction to self
  - Incentive (profit!) for honest behavior
- Halves every 210,000 blocks
  - Finite # of BTC
- BTC supply cap: 21,000,000

MINING INCENTIVES (TO DELETE?)

BLOCK REWARD: RATIONALE

- Given:
  - Profit is primary motivator
  - Higher incentive for honesty ⇒ more secure network
  - Pseudonymous users ⇒ no way to effectively track (or punish) dishonest behavior
- Conclusion:
  - Reward the honest nodes!
  - Proof-of-Work ensures that miners are dedicated to the network (aka willing to pay money for electricity and hardware just to earn BTC)

MINING INCENTIVES

HOW TO PROFIT FROM MINING

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

if MINING_REVENUE > MINING_COST:
 miner.get_profit()
```

MINING INCENTIVES

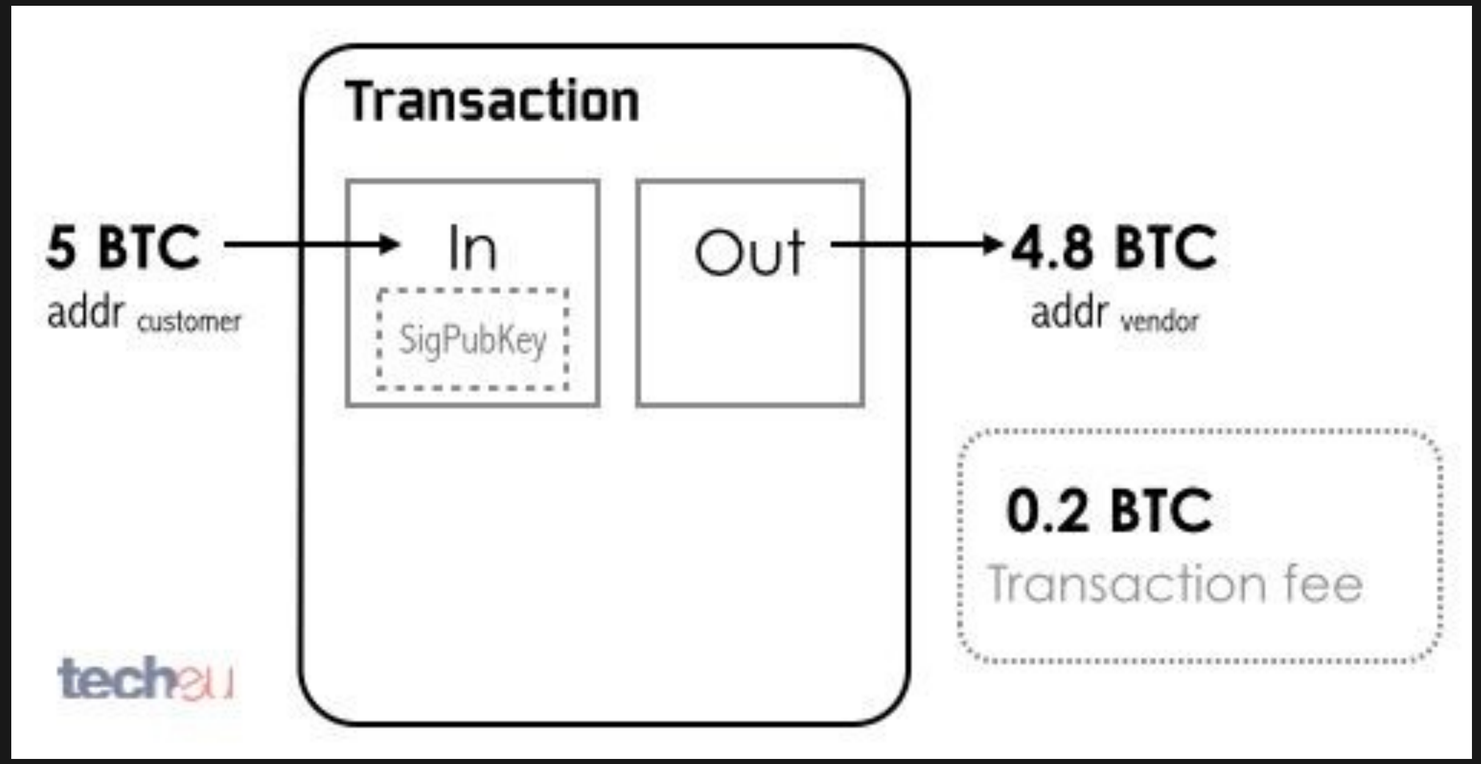
HOW TO PROFIT FROM MINING

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

if MINING_REVENUE > MINING_COST:
 miner.get_profit()
```

Image source: https://profitbitcoin.com/

MINING INCENTIVES

TRANSACTION FEES



- Tx creator sets tx fee
  - Voluntary, but practically necessary...
- Extra income for miners on top of block reward (esp. as reward diminishes)
  - Higher transaction fee ⇒ faster confirmation time
- `TX_FEE = INPUT - OUTPUT`
- **When block reward becomes 0, TX fees will become primary source of revenue for miners**

MINING INCENTIVES

HOW TO PROFIT FROM MINING

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

if MINING_REVENUE > MINING_COST:
 miner.get_profit()
```

Image source: https://profitbitcoin.com/

MINING INCENTIVES

HOW TO PROFIT FROM MINING

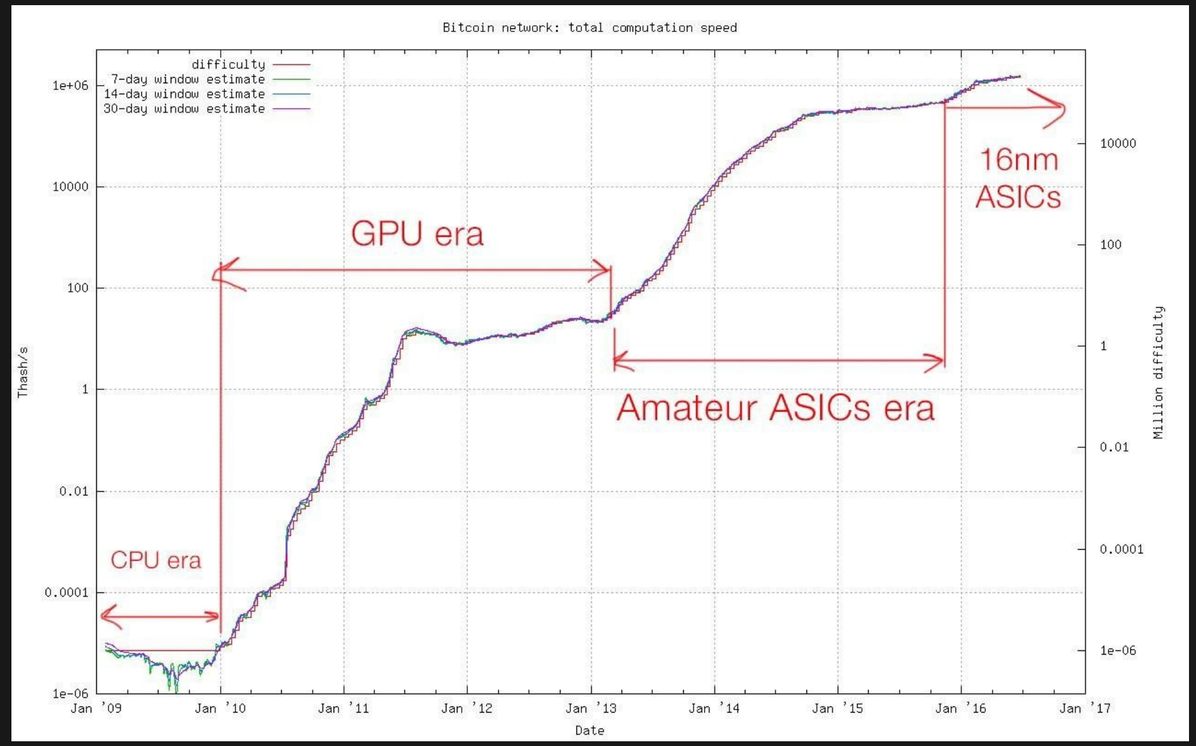
```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

if MINING_REVENUE > MINING_COST:
 miner.get_profit()
```

Image source: https://profitbitcoin.com/

MINING INCENTIVES

FIXED COST: HARDWARE COSTS

	hashes / second	time to block (years)
CPU	20 million	7,620,101
GPU	200 million	762,010
FPGA	1billion	152,357
ASIC	14 trillion	10.88



MINING INCENTIVES

FIXED COST: CPU MINING

	hashes / second	time to block (years)
CPU	20 million	7,620,101
GPU	200 million	762,010
FPGA	1billion	152,357
ASIC	14 trillion	10.88

```
TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while (1) {
      header = makeBlockHeader(transactions, coinbase_nonce);
      for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++){
            if (SHA256(SHA256(makeBlock(header, header_nonce))) <
      TARGET)
                  break; //block found!
      }
      coinbase_nonce++;
}
```

Figure 5.6 : CPU mining pseudocode.

(from Princeton Textbook, 5.2)

- Keep in mind that hardware costs are fixed, unlike everything else

MINING INCENTIVES

FIXED COST: GPU MINING

	hashes / second	time to block (years)
CPU	20 million	7,620,101
GPU	200 million	762,010
FPGA	1billion	152,357
ASIC	14 trillion	10.88

- Order of magnitude faster than CPUs
  - Larger consumption of energy and higher production of heat
- Most common in 2012
- Disadvantages:
  - Many components (floating point units) not applicable to mining
  - Not meant to be run in “farms” side by side

MINING INCENTIVES

FIXED COST: FPGA MINING

	hashes / second	time to block (years)
CPU	20 million	7,620,101
GPU	200 million	762,010
FPGA	1 billion	152,357
ASIC	14 trillion	10.88

- **F**ield **P**rogrammable **G**ate **A**rrays
  - Developing Bitcoin-specific hardware without losing all customizability
- Trade-off between dedicated SHA-256 and general purpose hardware
  - If Bitcoin fails, SHA-256 specific hardware is worthless
  - But if Bitcoin thrives, specialized hardware generates higher **PROFIT**!

MINING INCENTIVES

FIXED COST: ASIC MINING

	hashes / second	time to block (years)
CPU	20 million	7,620,101
GPU	200 million	762,010
FPGA	1billion	152,357
ASIC	14 trillion	10.88

- **A**pplication-**S**pecific **I**ntegrated **C**ircuit
  - Does nothing but SHA-256 -- but does it better than anything else
- Huge variety with various tradeoffs
  - Lower base cost vs lower electricity usage
  - Compact device vs higher hashrate
- Manufacturing ASICs takes large upfront capital, inducing production centralization
- Antminer S9 (14TH/s): $3000

MINING INCENTIVES

HOW TO PROFIT FROM MINING

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

if MINING_REVENUE > MINING_COST:
 miner.get_profit()
```

Image source: https://profitbitcoin.com/

MINING INCENTIVES

HOW TO PROFIT FROM MINING

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

if MINING_REVENUE > MINING_COST:
 miner.get_profit()
```

Image source: https://profitbitcoin.com/

MINING INCENTIVES

OPERATING COSTS

- Energy consumed in mining:
  - **Embodied energy,** to produce your hardware
  - **Electricity**, to power your hardware
  - **Cooling**, to maintain your hardware
- Infrastructure
  - Warehouses
  - Personnel
- All energy converted to heat -- is this not wasteful?
  - The “data furnace” approach: using mining equipment to generate heat
    - Unless a high percentage of the network stops mining during the heat, leading to miners dropping out for days on end, or even a whole summer!

MINING INCENTIVES

HOW TO PROFIT FROM MINING

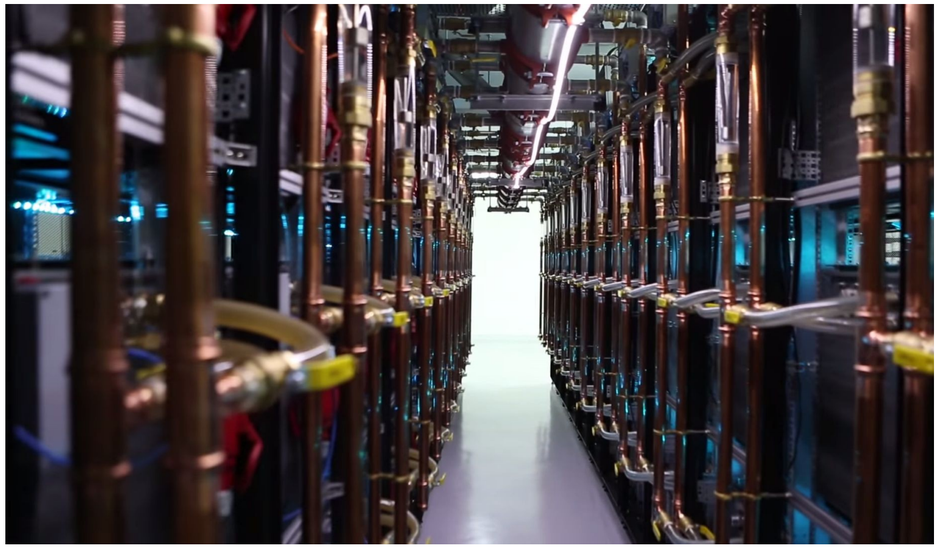
```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

if MINING_REVENUE > MINING_COST:
 miner.get_profit()
```

Image source: https://profitbitcoin.com/

4 REAL WORLD MINING

REAL WORLD MINING

CHINESE ASIC MINING FARM



Source: https://www.theregister.co.uk/2014/08/12/chinese_bitcoin_farms_from_scifi_to_scuzzy/

REAL WORLD MINING

ASICS

Source: https://sc01.alicdn.com/kf/HTB18YN_JFXXXXcgXFXXq6xXFXXXw/221223714/HTB18YN_JFXXXXcgXFXXq6xXFXXXw.jpg

Source: https://mybtcpool.com/product/datacenter-hosting/

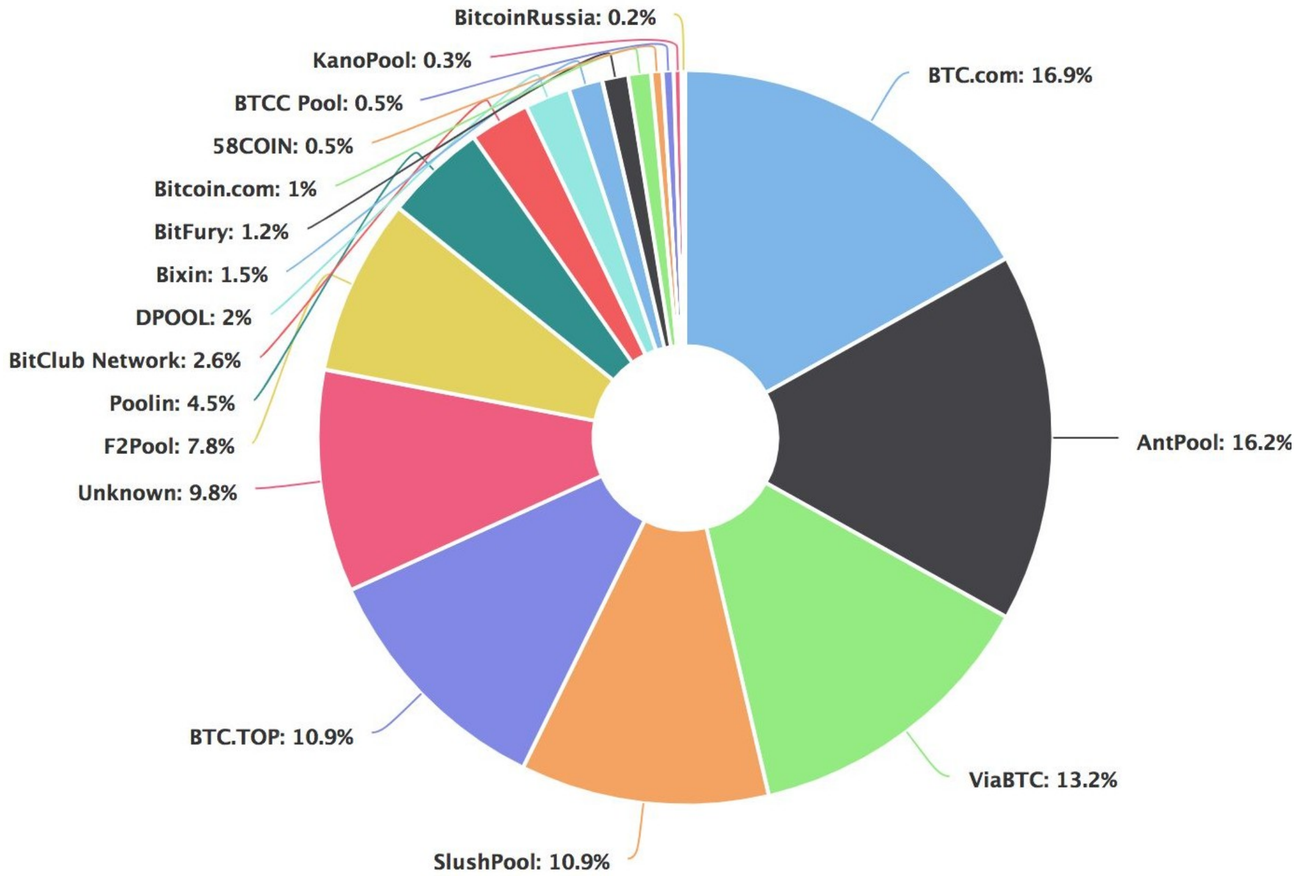
REAL WORLD MINING

MINING POOLS

Source: blockchain.info (9/26/18)

Mining pools allow individual miners to combine, or 'pool', their computational power together

- Reduces variance in mining rewards
- Run by **pool managers** or **pool operators**
- Pool manager usually takes a cut of the mining rewards



REAL WORLD MINING

MINING SHARES

Miners in a pool submit **shares** (‘near-valid’ blocks) to the pool manager

- Producing shares implies computational power being expended
- Pool operator pays for valid shares
  - Rewards distributed proportional to # of shares submitted
- Valid blocks are shares as well
  - Individual who finds valid block is not awarded any extra coins

FAQ: Why can't someone submit shares in a pool and keep the reward of the valid block for themselves?

- The valid block is based on the Merkle root given by the pool operator.
- Pool public key → Coinbase tx → Merkle Root

REAL WORLD MINING

MINING POOL SCHEMES

Pay-per-share

Pool pays out **at every share submitted.** By default will be proportional to work done by individuals

1. More beneficial for **miners**
2. Individual miners have no risk from reward variance
    a. Pool takes on the risk completely
3. Problem:???

Proportional

Pool pays out **when blocks are found,** proportional to the work individuals have submitted for this block

1. More beneficial for the **pool**
2. Individual miners still bear some risk in variance proportional to size of the pool
3. Lower risk for pool operators - only pay out when reward is found
    a. Individuals thus incentivized to submit valid blocks

Problem??

REAL WORLD MINING

MINING POOL SCHEMES

Pay-per-share

Pool pays out **at every share submitted.** By default will be proportional to work done by individuals

1. More beneficial for **miners**
2. Individual miners have no risk from reward variance
    a. Pool takes on the risk completely
3. Problem: No incentive for individuals to actually submit valid blocks
    a. Individuals are paid regardless

Proportional

Pool pays out **when blocks are found,** proportional to the work individuals have submitted for this block

1. More beneficial for the **pool**
2. Individual miners still bear some risk in variance proportional to size of the pool
3. Lower risk for pool operators - only pay out when reward is found
    a. Individuals thus incentivized to submit valid blocks

Risk for miners to never get paid

a. Not a problem if pool is sufficiently large

POOL REWARDS

OTHER REWARD SCHEMES

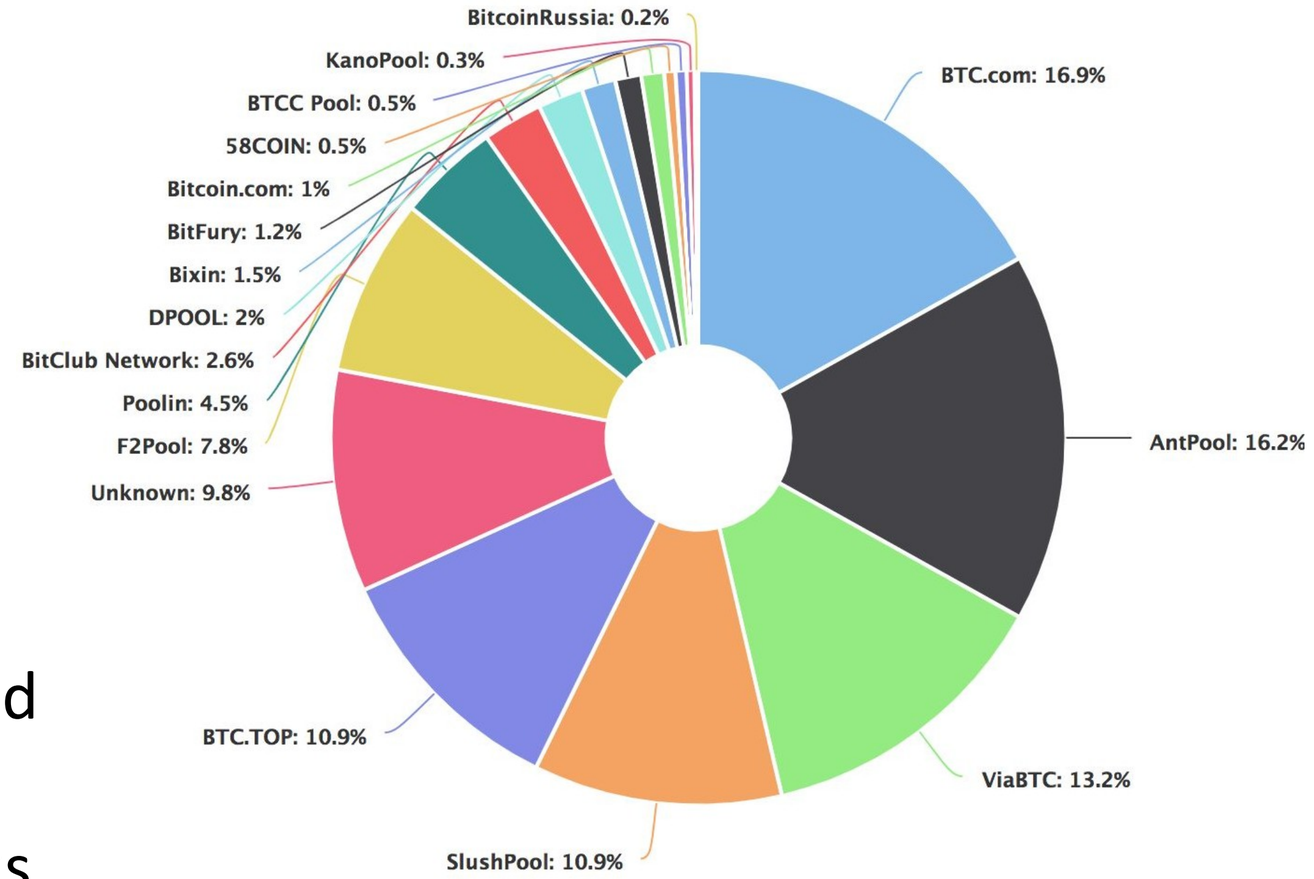
- **CPPSRB** - Capped Pay Per Share with Recent Backpay.
- **DGM** - Double Geometric Method. A hybrid between PPLNS and Geometric reward types that enables to operator to absorb some of the variance risk. Operator receives portion of payout on short rounds and returns it on longer rounds to normalize payments.
- **ESMPPS** - Equalized Shared Maximum Pay Per Share. Like SMPPS, but equalizes payments fairly among all those who are owed.
- **POT** - Pay On Target. A high variance PPS variant that pays on the difficulty of work returned to pool rather than the difficulty of work served by pool
- **PPLNS** - Pay Per Last N Shares. Similar to proportional, but instead of looking at the number of shares in the round, instead looks at the last N shares, regardless of round boundaries.
- **PPLNSG** - Pay Per Last N Groups (or shifts). Similar to PPLNS, but shares are grouped into "shifts" which are paid as a whole.
- **RSMPPS** - Recent Shared Maximum Pay Per Share. Like SMPPS, but system aims to prioritize the most recent miners first.
- **Score** - Score based system: a proportional reward, but weighed by time submitted. Each submitted share is worth more in the function of time *t* since start of current round. For each share score is updated by: score += exp(t/C). This makes later shares worth much more than earlier shares, thus the miner's score quickly diminishes when they stop mining on the pool. Rewards are calculated proportionally to scores (and not to shares). (at slush's pool C=300 seconds, and every hour scores are normalized)
- **SMPPS** - Shared Maximum Pay Per Share. Like Pay Per Share, but never pays more than the pool earns.
- **FPPS** - Full Pay Per Share. Similar to PPS, but not only divide regular block reward (12.5 BTC for now) but also some of the transaction fees. Calculate a standard transaction fee within a certain period and distribute it to miners according to their hash power contributions in the pool. It will increase the miners' earnings by sharing some of the transaction fees.

Source: https://en.bitcoin.it/wiki/Comparison_of_mining_pools

REAL WORLD MINING

MINING POOLS

Source: blockchain.info (9/26/18)



Pros

- Allows individual miners to participate
- Easy to upgrade software changes

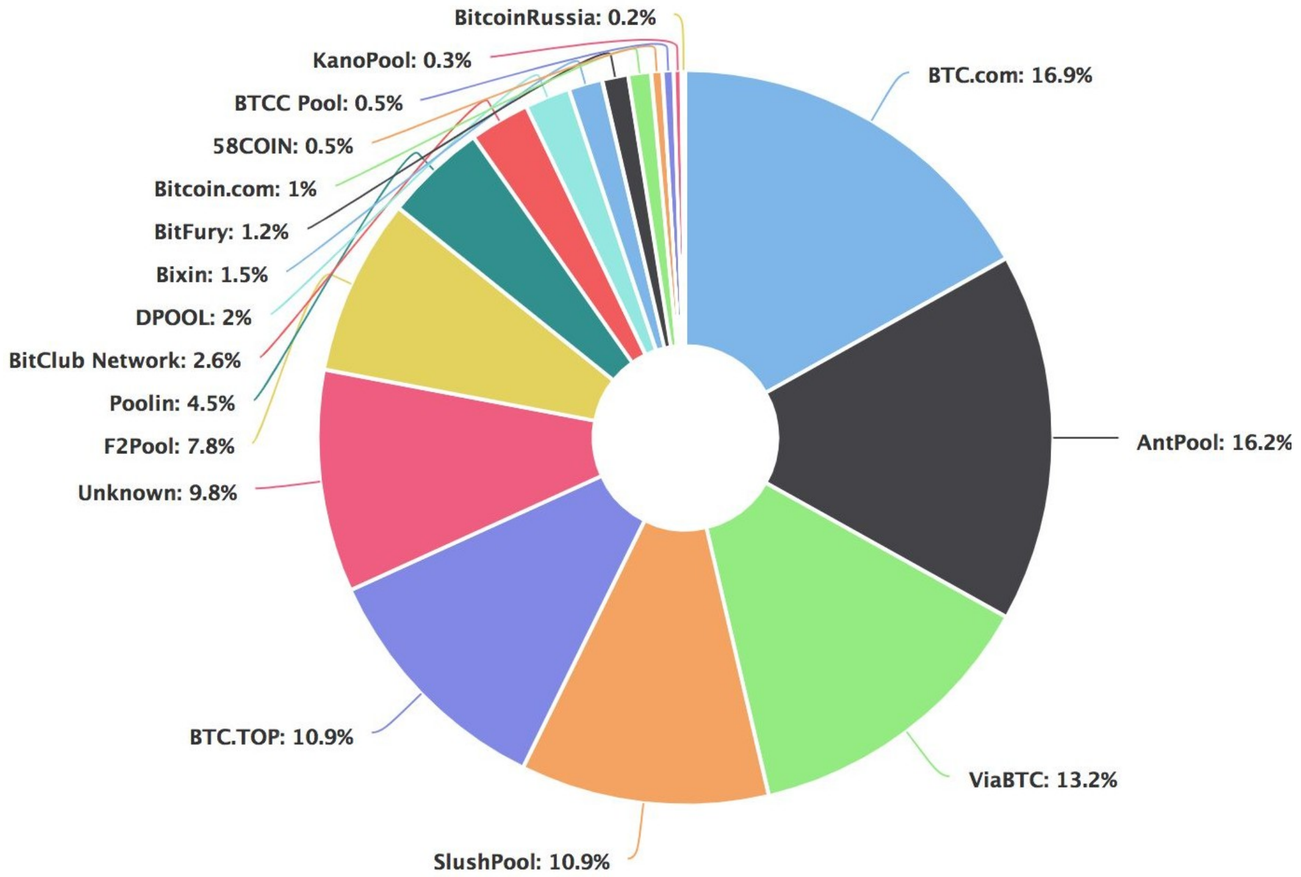
Cons

- Pool manager must be trusted
- Centralized
- Enables a multitude of attacks

REAL WORLD MINING

MINING POOLS

Source: blockchain.info (9/26/18)



Community exhibits backlash against large mining pools

- Ex: GHash.io in 2014

Single entity might be be participating in multiple pools

- Called “**Laundering hashes**”
- Actual concentration of control over mining hardware **is unknown**

REAL WORLD MINING

MINING POOLS

Quick facts

- Today's (9/24/18) network hashrate: **60,089,527 TH/s**
- Mining Reward /yr = (1yr /10 mins) *12.5 = **657k BTC /yr**
- Assume constant price of $10,000

Suppose you want to start mining today.

- Antminer S9: Costs $3000, **14 TH/s**
- **% of network hashrate** = (14 TH/s) / (60,089,527 TH/s) = **0.000000232985**

Expected Annual Reward

- 0.000000232985 *657k /yr
  ≈ 0.1530716 BTC /yr ≈ **$1530.72 / yr**

Solo mining

- 1block mined per 2,426,566 blocks
  ⇒ 12.5 BTC every 16,851 days
  ⇒ **$125,000 once every 46.2 years**

Mining with mining pool

- Assume pool has ⅙ network hashrate
  - Pool finds every 6th block ≈ 1per hr
- $1530.72 /yr /8760 hrs/yr
  ≈ **$0.17 every hour**

Paradox:

- The more secure Bitcoin gets, the greater the appeal for mining pools

5

CHANGING BITCOIN

DECENTRALIZING MINING

THE PROBLEM

- In practice, “One CPU One Vote” isn’t real
  - ASICs
  - Mining pools
  - Mining farms

Source:
https://www.theregister.co.uk/2014/08/12/chinese_bitcoin_farms_from_scifi_to_scuzzy/

Source:
https://sc01.alicdn.com/kf/HTB18YN_JFXXXXcgXFXXq6xXFXXXw/221223714/HTB18YN_JFXXXXcgXFXXq6xXFXXXw.jpg

Source:
https://www.buybitcoinworldwide.com/wp-content/themes/kepler/img/miners/21.jpg

DECENTRALIZING MINING

PUZZLE REQUIREMENTS REVIEW

- A refresher on puzzle requirements:
  - Quick to verify
  - Adjustable difficulty
  - Computationally difficult
  - Solving rate proportional to computational power
  - “Progress free”- Avalanche Effect
  - Pseudorandomly generated
- Bitcoin’s puzzle is a “partial hash-preimage puzzle”
  - Doesn’t matter what follows the prerequisite number of zeros

DECENTRALIZING MINING

ASIC-RESISTANCE

Memory-hard: requires large amount of memory instead of computational power

Memory-bound: memory bottlenecks computation time

- Memory-hard puzzles viably deter ASICs:
  - ASICs are optimized to execute a specific algorithm
    - Useless optimization if memory is the limiting agent

DECENTRALIZING MINING

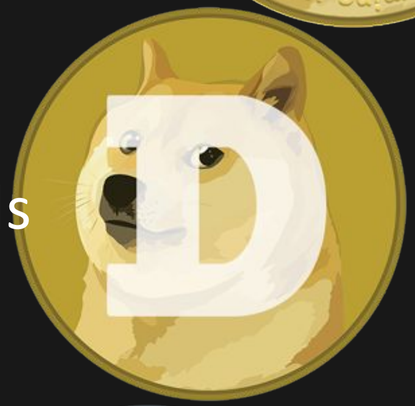
SCRYPT

Scrypt (“ess crypt”): a hash function.

The mining puzzle is the same partial hash-preimage puzzle.

Design considerations:

- Used for hashing passwords
- Hard to brute-force



Used by Litecoin and Dogecoin

DECENTRALIZING MINING

SCRYPT

Two main steps:

1. Fill buffer w/ interdependent data
2. Access data in pseudorandom way

Without using memory, `V[j]`, a previously computed value, must be computed on the fly.

Drawbacks:

1. Requires equal amount of memory to verify
2. ASIC developed; not resistant!

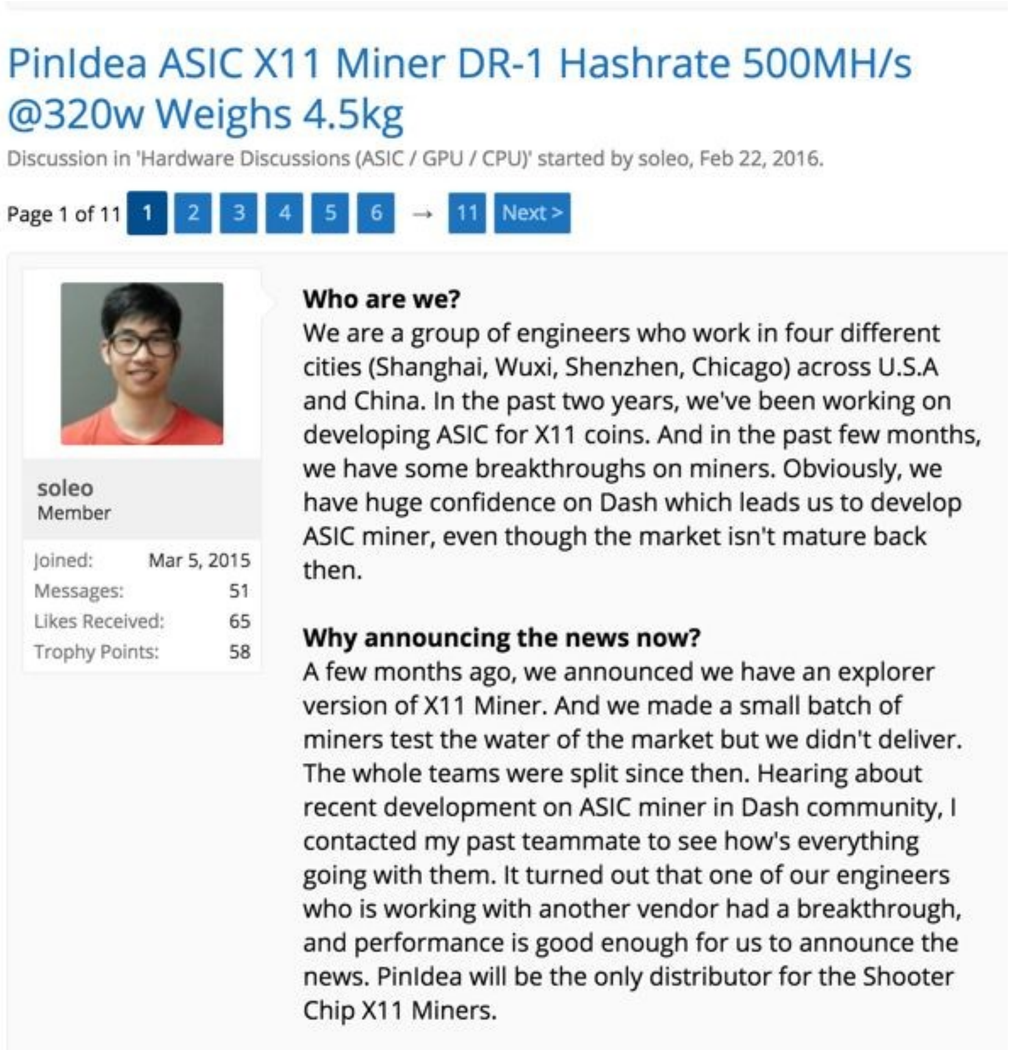
Figure 8.1: Scrypt pseudocode

```
def scrypt(N, seed):
   V = [0] * N  // initialize memory buffer of length N

  // Fill up memory buffer with pseudorandom data
  V[0] = seed
  for i = 1 to N:
     V[i] = SHA-256(V[i-1])

  // Access memory buffer in a pseudorandom order
  X = SHA-256(V[N-1])
  for i = 1 to N:
     j = X % N  // Choose a random index based on X
     X = SHA-256(X ^ V[j]) // Update X based on this index

  return X
```

DECENTRALIZING MINING

ASIC-RESISTANCE

- **x11** or **x13**: Chain 11 or 13 different hash functions together respectively
  - Used by DASH
  - Significantly harder to design ASIC
    - ...but not impossible, mind you
- Periodically switching mining puzzle
  - Going from SHA-1 to SHA-3 to Scrypt for 6 months each
  - Not implemented



PinIdea ASIC X11 Miner DR-1 Hashrate 500MH/s @320w Weighs 4.5kg

Discussion in 'Hardware Discussions (ASIC / GPU / CPU)' started by soleo, Feb 22, 2016.

Page 1 of 11 1 2 3 4 5 6 → 11 Next >

soleo
Member

Joined: Mar 5, 2015
Messages: 51
Likes Received: 65
Trophy Points: 58

Who are we?
We are a group of engineers who work in four different cities (Shanghai, Wuxi, Shenzhen, Chicago) across U.S.A and China. In the past two years, we've been working on developing ASIC for X11 coins. And in the past few months, we have some breakthroughs on miners. Obviously, we have huge confidence on Dash which leads us to develop ASIC miner, even though the market isn't mature back then.

Why announcing the news now?
A few months ago, we announced we have an explorer version of X11 Miner. And we made a small batch of miners test the water of the market but we didn't deliver. The whole teams were split since then. Hearing about recent development on ASIC miner in Dash community, I contacted my past teammate to see how's everything going with them. It turned out that one of our engineers who is working with another vendor had a breakthrough, and performance is good enough for us to announce the news. PinIdea will be the only distributor for the Shooter Chip X11 Miners.

Mike Hearn, Bitcoin Core developer: “There’s really no such thing as an ASIC-resistant algorithm.”

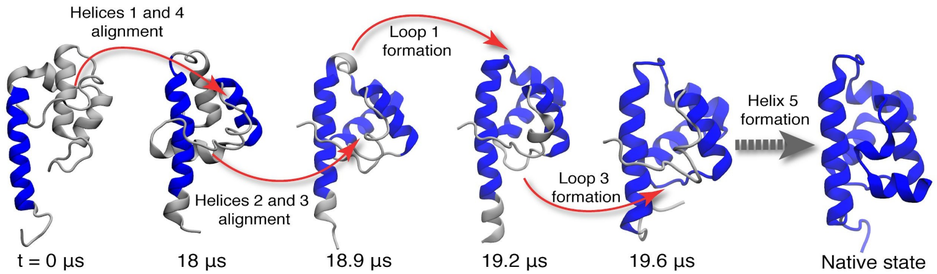
DECENTRALIZING MINING

ASIC-RESISTANCE

- Pros of ASIC-resistance:
  - ASICs dominate the network, suppressing regular people
  - Increase in democracy and decrease in centralization
- Cons:
  - ASICs can only solve the puzzle, nothing more
  - Crash in exchange rate ⇒ useless electricity-gobbling hardware

PROOF-OF-USEFUL-WORK

NOT A PUZZLING CONCEPT



- “Repurpose” computing power
- Examples:
  - Searching for large primes
  - Finding aliens
  - Simulating proteins at the atomic level
  - Generating predictive climate models

Project	Founded	Goal	Impact
Great Internet Mersenne Prime Search	1996	Finding large Mersenne primes	Found the new “largest prime number” twelve straight times, including $2^{57885161} - 1$
distributed.net	1997	Cryptographic brute-force demos	First successful public brute-force of a 64-bit cryptographic key
SETI@home	1999	Identifying signs of extraterrestrial life	Largest project to date with over 5 million participants

PROOF-OF-USEFUL-WORK

DOES IT WORK?

- Most distributed computing problems are unsuitable for proof-of-work
  - Fixed amount of data
    - Missing an inexhaustible puzzle space
  - Potential solutions not equally likely
    - Missing an equiprobable solution space
  - Cannot rely on central entity to delegate tasks
    - Missing decentralized algorithmically generated problem
- In summary, **Proof-of-Useful-Work does not work**

CONSENSUS UPDATES

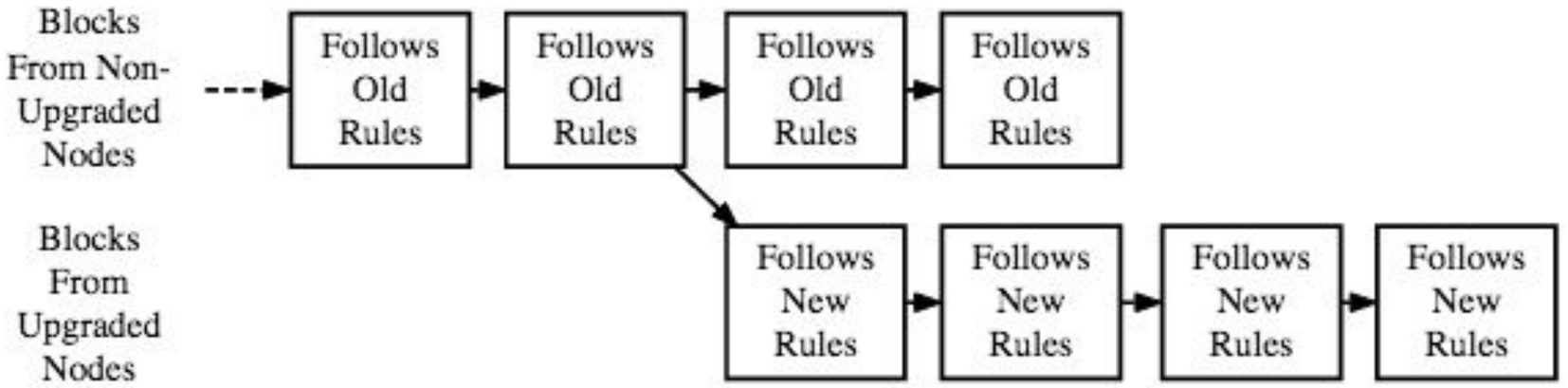
BITCOIN CORE

- **Bitcoin Core:**
  - The team of developers in charge of the Bitcoin GitHub repo
  - The software designed by these developers used by full Bitcoin nodes

CONSENSUS UPDATES

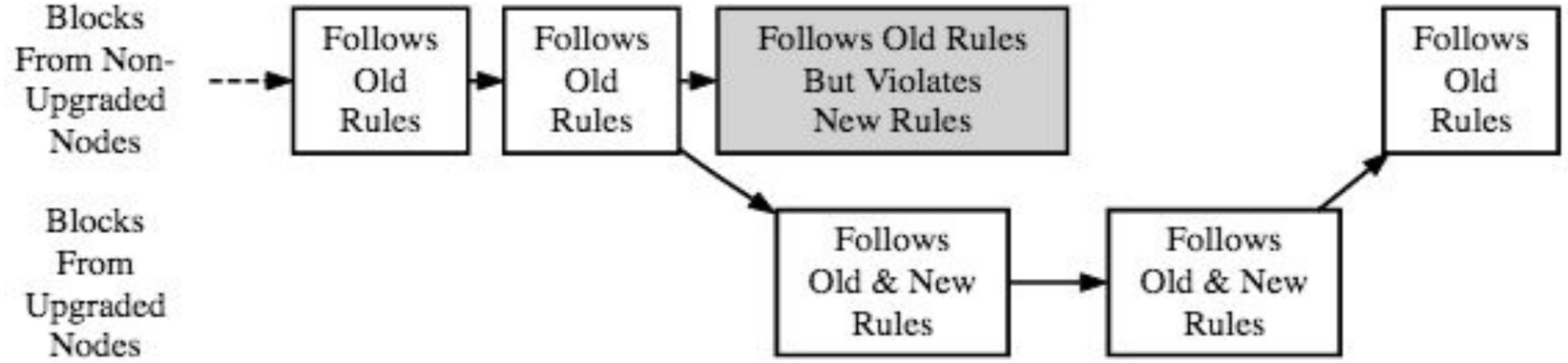
FORKS

Hard Fork



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

Soft Fork



A Soft Fork: Blocks Violating New Rules Are Made Stale By The Upgraded Mining Majority

CONSENSUS UPDATES

FORKS

Hard Fork

1.A block following the new consensus rules is accepted by upgraded nodes but rejected by non-upgraded nodes. For example, a new transaction feature is used within a block: upgraded nodes understand the feature and accept it, but non-upgraded nodes reject it because it violates the old rules. This creates permanently divergent chains.

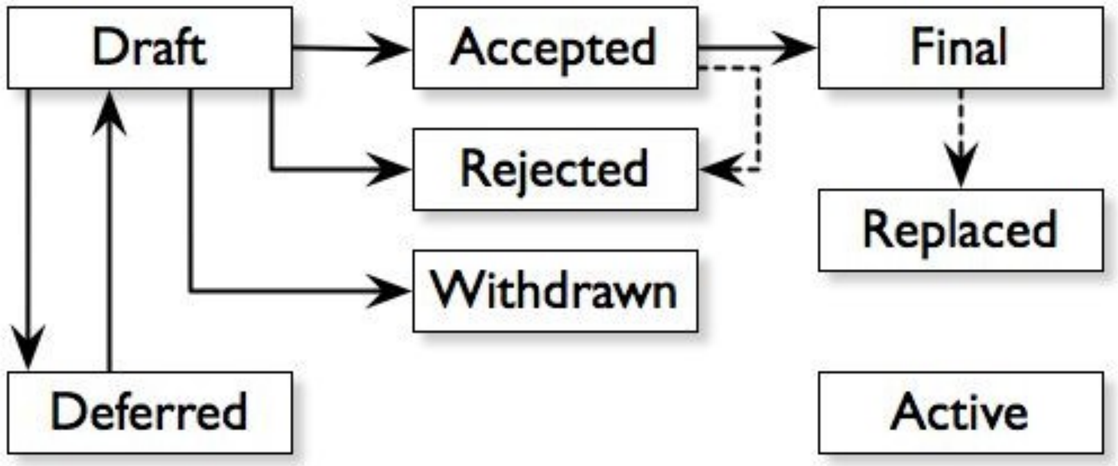
Soft Fork

2.A block violating the new consensus rules is rejected by upgraded nodes but accepted by non-upgraded nodes. For example, an abusive transaction feature is used within a block: upgraded nodes reject it because it violates the new rules, but non-upgraded nodes accept it because it follows the old rules.

CONSENSUS UPDATES

BITCOIN IMPROVEMENT PROPOSAL (BIP)

- **BIP:** Bitcoin Improvement Proposal
  - Three types:
    - Standards Track BIPs
    - Informational BIPs
    - Process BIPs
- First BIP proposed by Amir Taaki on 2011-08-19
- Signal support for a BIP by including reference in block when mining



Source: https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals

QUESTIONS?

References

Slides mainly adopted from

- Blockchain @ Berkeley : https://blockchain.berkeley.edu/
- Blockchain @ Princeton : http://bitcoinbook.cs.princeton.edu/