INTERACTING WITH BITCOIN

WALLETS, MINING, & MORE

AVA PAYMAN
NATHAN ZHANG

LECTURE OVERVIEW

01 Types of Users

02 Wallets

03 Wallet Mechanics

04 Mining

05 Real World Mining

INTRODUCING YOUR LECTURERS

Sehyun Chung

Education

Diego Uribe

Consulting

BLOCKCHAIN
AT BERKELEY

Types of Users

Full Nodes

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

Not every client has the entire blockchain (280+ GB)
What if I just want to send bitcoins with my phone?

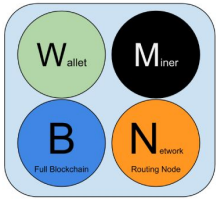
Not every client is directly connected to the network
What if I don’t need to make regular transactions?

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

Light Nodes (SPV Nodes)

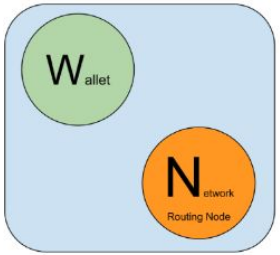
Simple Payment Verification (SPV) is method for verifying if particular transactions are included in a block without downloading the entire block

- 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

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

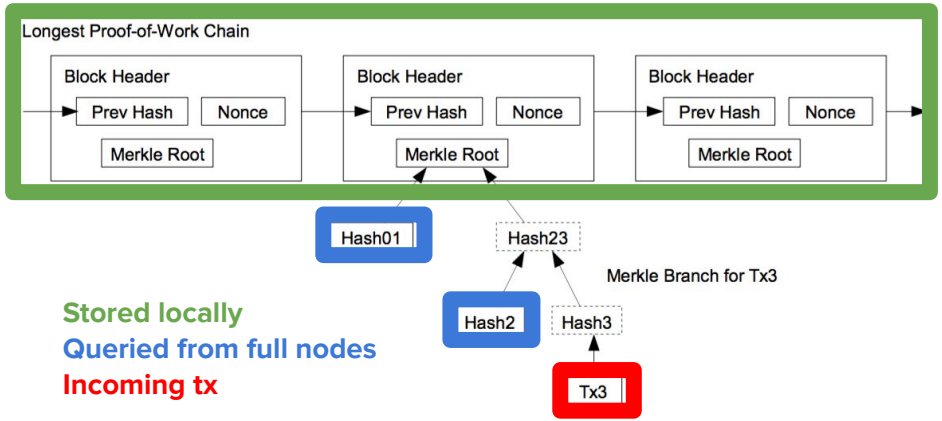


Image source: Mastering Bitcoin

QUESTIONS?

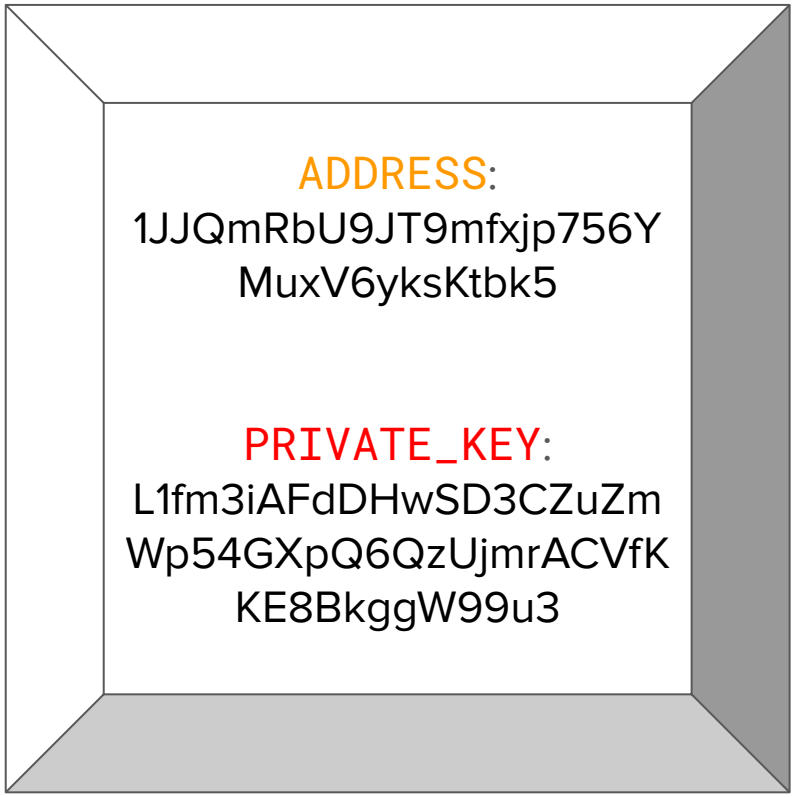
BLOCKCHAIN AT BERKELEY

What are Wallets?

Bitcoin Wallets

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

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



AUTHOR: NADIR AKHTAR

Bitcoin Wallets

What do wallets do?

- Provides a user interface to the blockchain
- Keep track of your private key
- Store, send, receive, and list transactions
- Maybe some other fancy functionalities

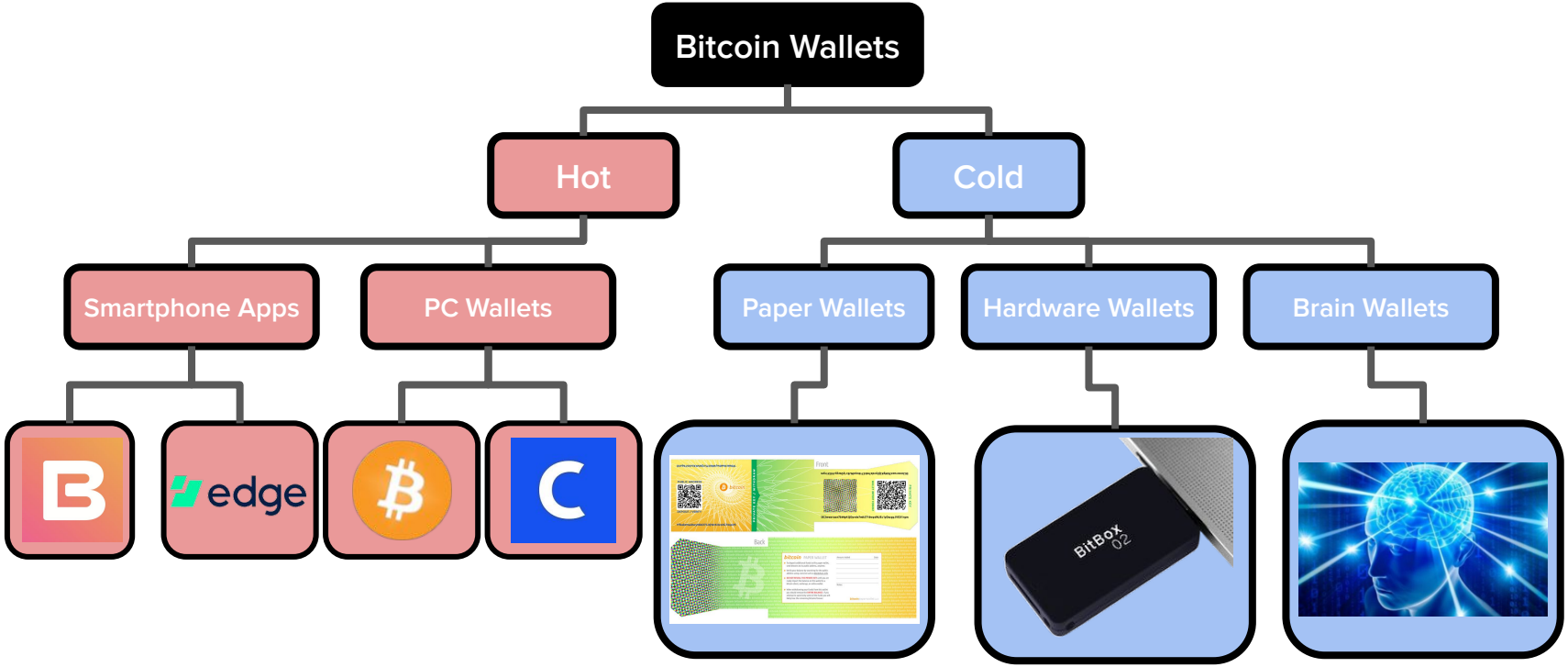
AUTHOR: SUNNY AGGARWAL & RUSTIE LIN
UPDATED: JUSTIN YU

Wallet Types

https://bitcoin.org/en/choose-your-wallet

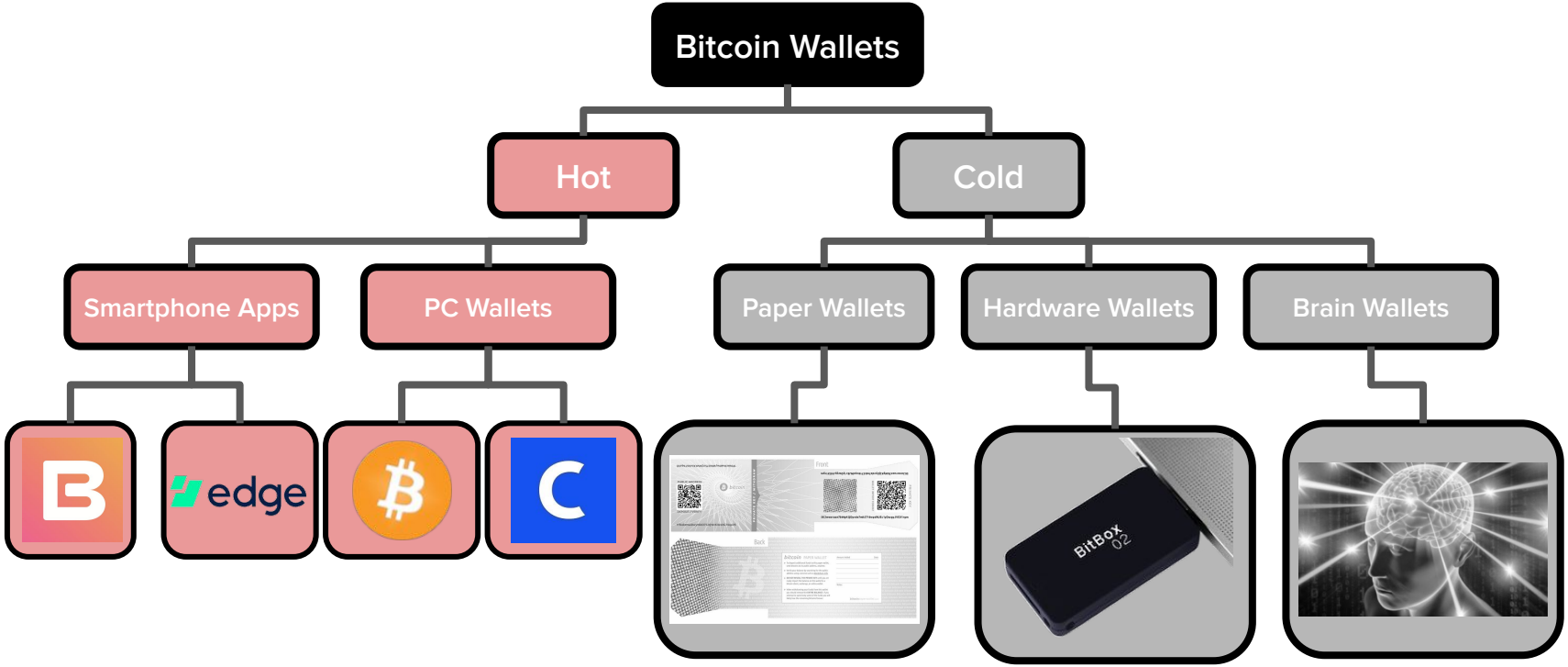
AUTHOR: SUNNY AGGARWAL & RUSTIE LIN
UPDATED: JUSTIN YU

Hot vs. Cold Wallets



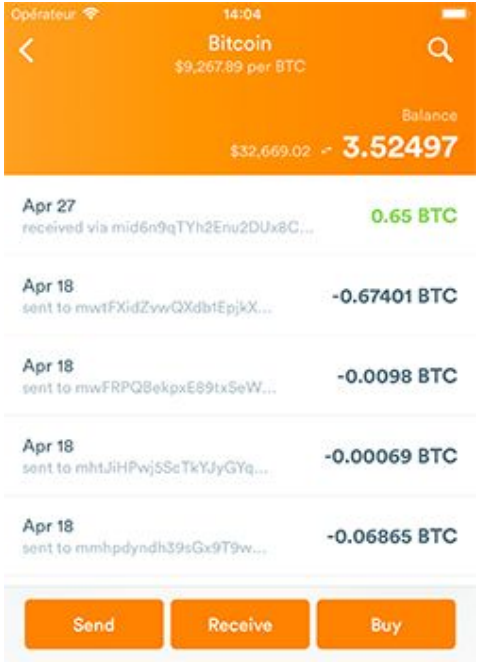
AUTHOR: SUNNY AGGARWAL & RUSTIE LIN
UPDATED: NADIR AKHTAR & HAENA LEE

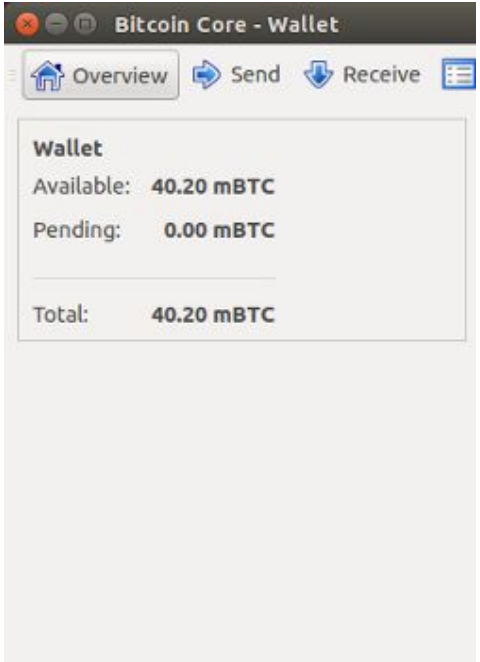
Hot Wallets



AUTHOR: SUNNY AGGARWAL & RUSTIE LIN
UPDATED: NADIR AKHTAR & HAENA LEE

Hot Wallets





AUTHOR: SEHYUN CHUNG

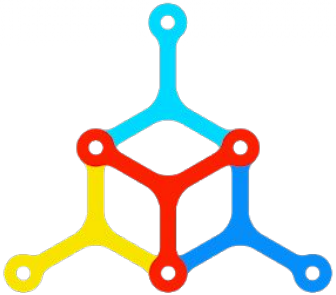
Image sources:
bitcoin.org

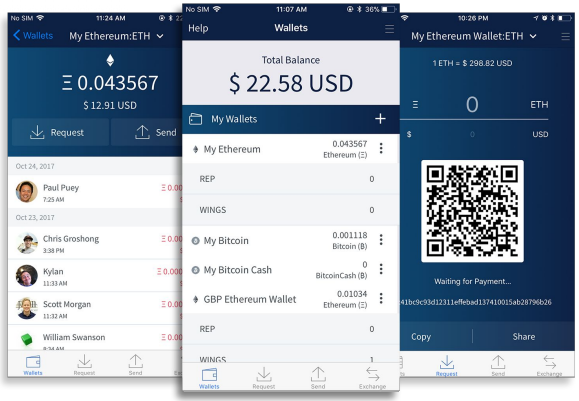
BITCOIN WALLETS

coinbase

BLOCKCHAIN

edge





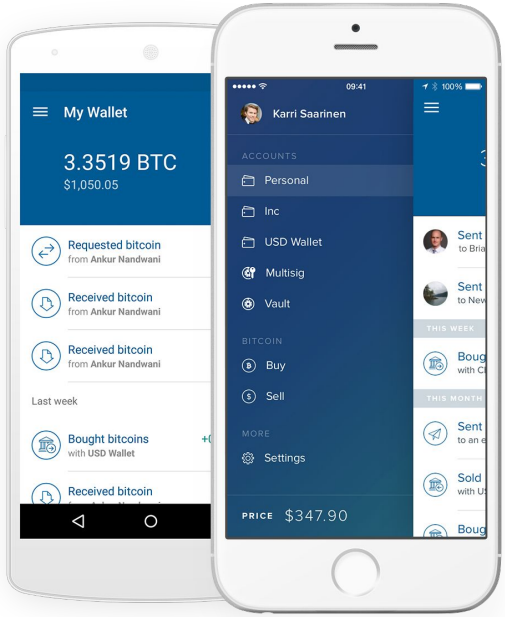
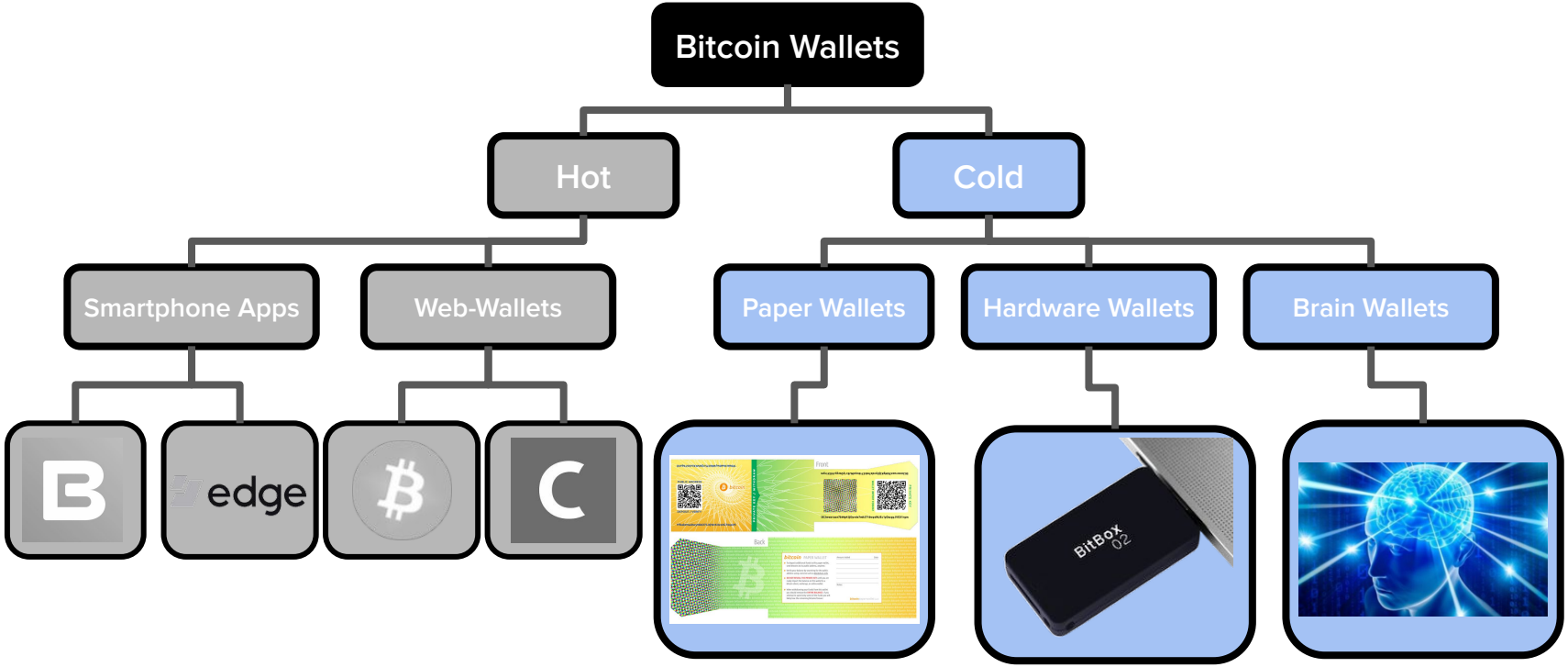


Image sources:
https://blockchain.info/
https://wallet.mycelium.com
https://airbitz.co/bitcoin-wallet/
https://www.coinbase.com/mobile

AUTHOR: RUSTIE LIN
UPDATED: HAENA LEE

Cold Wallets



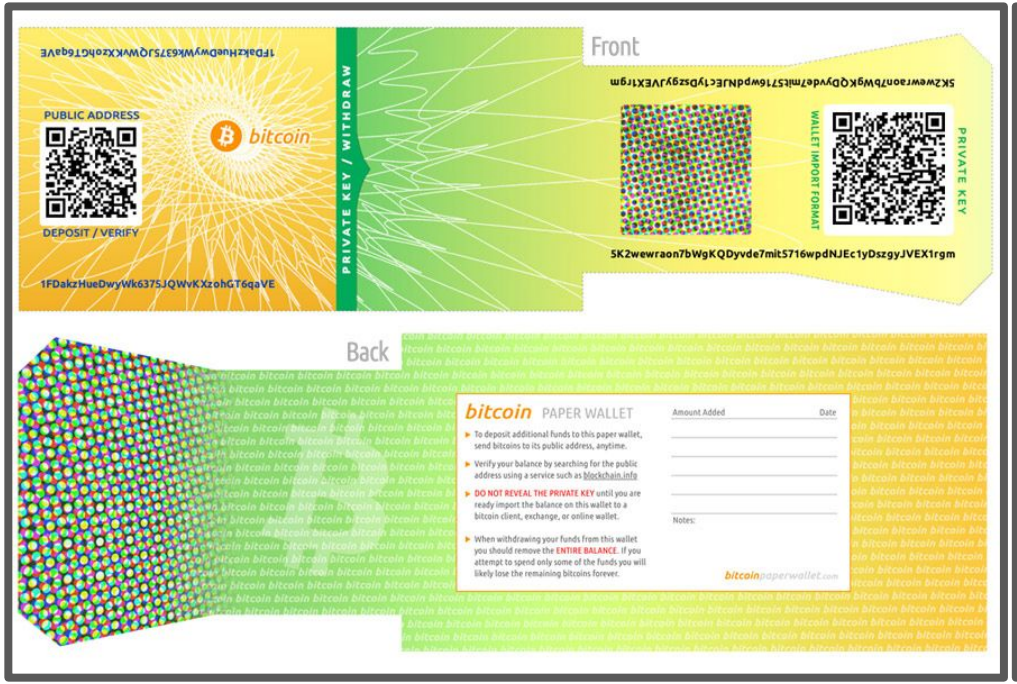
AUTHOR: SUNNY AGGARWAL & RUSTIE LIN
UPDATED: NADIR AKHTAR & HAENA LEE

Cold Storage Wallets

AUTHOR: RUSTIE LIN
UPDATED BY: SEHYUN CHUNG

Image sources:
https://www.ledgerwallet.com/
https://trezor.io/
https://bitcoin.org/

Paper Wallets



Going Offline

ZIP

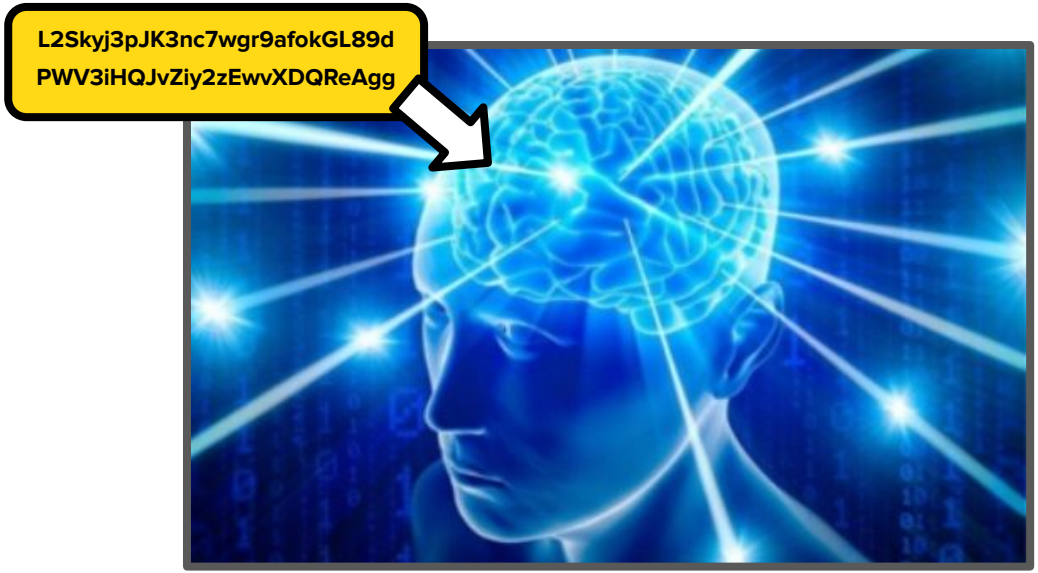
Your wallet may be vulnerable to prying eyes when you are generating the keys and printing them out. Although the wallet generator on this website is SSL-encrypted, it's still possible for someone to be snooping on you. (For example, your computer might have malware that broadcasts your screen to a remote 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.

Image source: https://bitcoinpaperwallet.com/

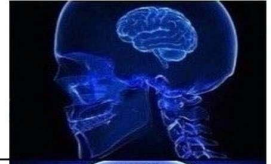
BITCOIN WALLETS



Memorize Your Private Key

AUTHOR: BRIAN HO
UPDATED: HAENA LEE

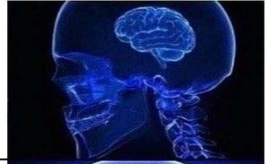
using a recommended bitcoin wallet



storing crypto on a hardware wallet

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

using a recommended bitcoin wallet



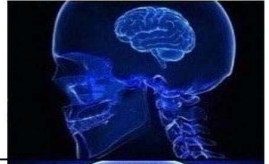
storing crypto on a hardware wallet

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

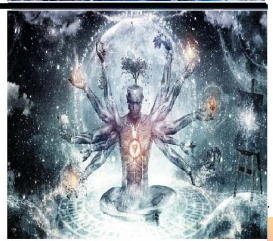
writing private keys on a post it and putting it on your computer

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

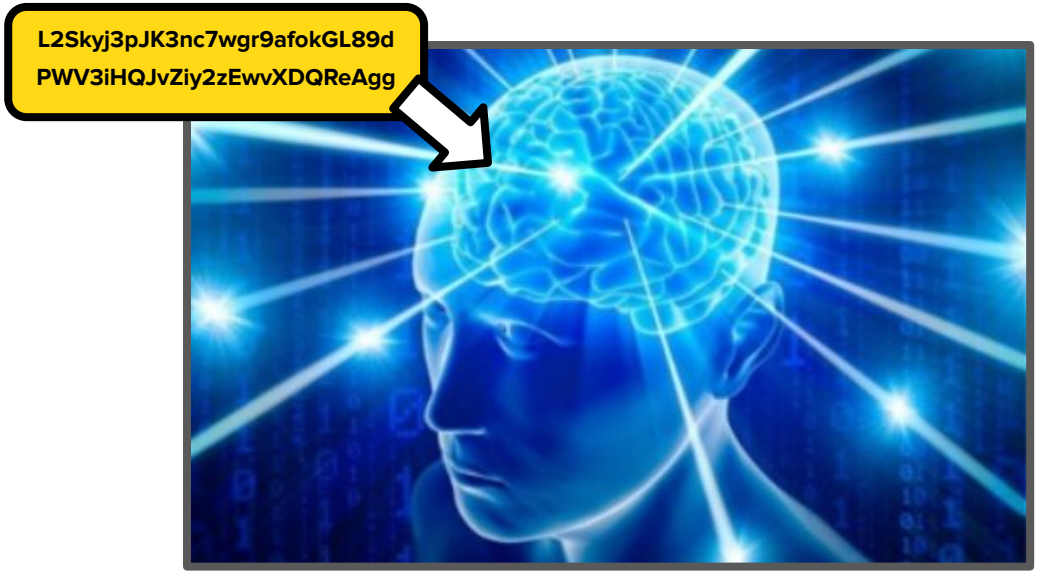
memorizing

storing your crypto on

coinbase



BITCOIN WALLETS



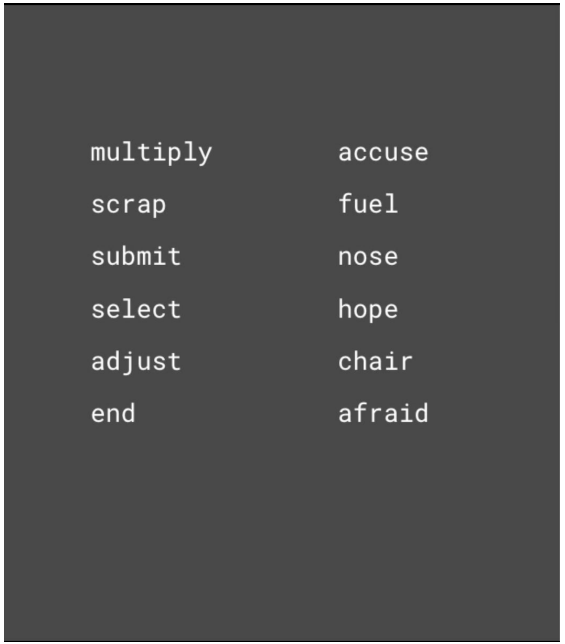
Memorize Your Private Key

AUTHOR: BRIAN HO
UPDATED: HAENA LEE

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



AUTHOR: SUNNY AGGARWAL & RUSTIE LIN
UPDATED: HAENA LEE

Brain Wallets

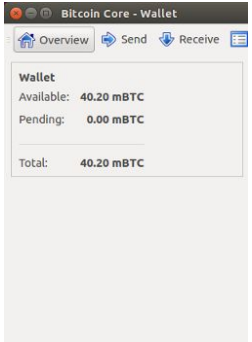
multiply accuse
scrap fuel
submit nose
select hope
adjust chair
end afraid

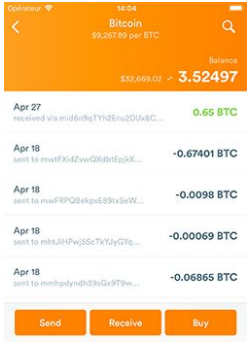
multiply accuse
scrap fuel
submit nose
select hope
adjust chair
end afraid

L2Skyj3pJK3nc7
wgr9afokGL89d
PWV3iHQJvZiy2
zEwvXDQReAgg

AUTHOR: SUNNY AGGARWAL & RUSTIE LIN
UPDATED: HAENA LEE

Different Types?



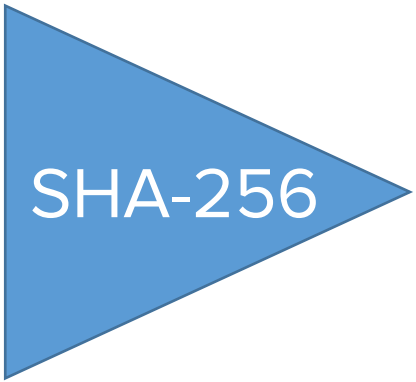


Security — Convenience

AUTHOR: SEHYUN CHUNG

BITCOIN WALLETS

- Key Stretching is a method in which we increase the unit of time it takes to get to a particular hash by repeatedly hashing something.
  - Disincentivizes Dictionary Attacks by making it take longer to perform the attack



Discussion

What are some of the tradeoffs between using an online hot wallets and an offline cold storage wallet?

Discussion

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

QUESTIONS?

BLOCKCHAIN AT BERKELEY

Acquiring Bitcoin

HOW DO I GET BITCOIN?

“But how do I get bitcoins?”

Image source: https://www.reddit.com/r/Bitcoin/

Bitcoin ATMs

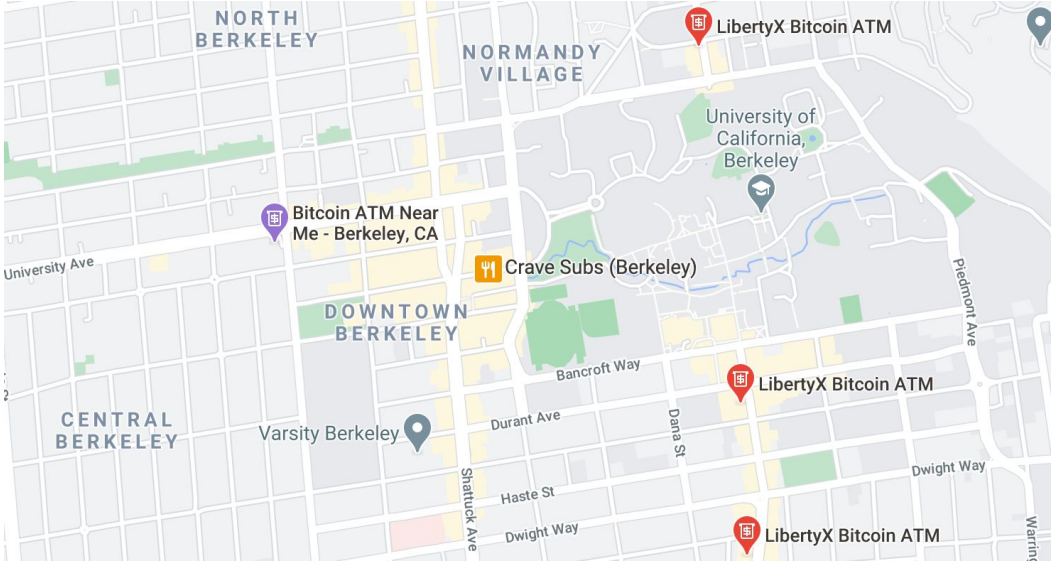


Image sources:
https://www.google.com/maps
https://coinucopia.io/

AUTHOR: RUSTIE LIN

Centralized Exchanges

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

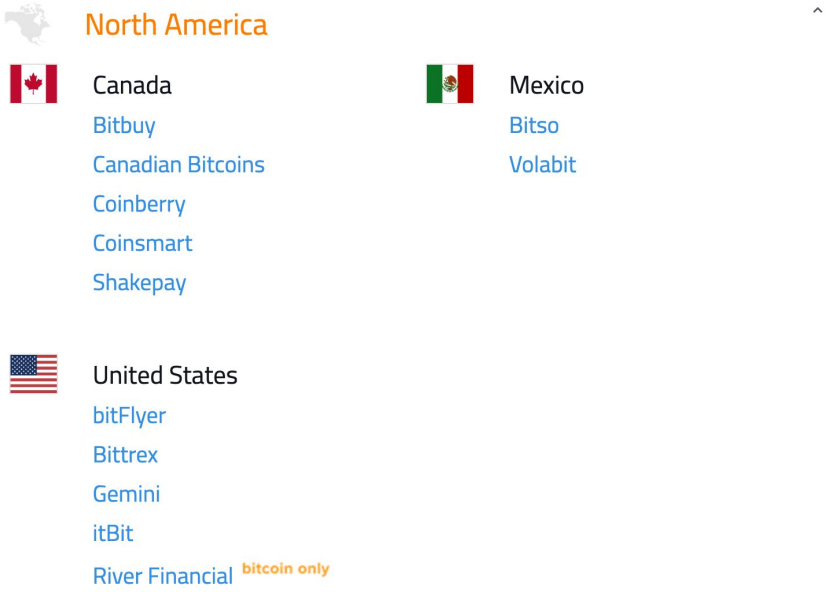


Image source: https://bitcoin.org/en/exchanges

Decentralized Exchanges (DEXs)

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

- Trades are P2P
- Trustless
- Bisq, Uniswap, BitQuick

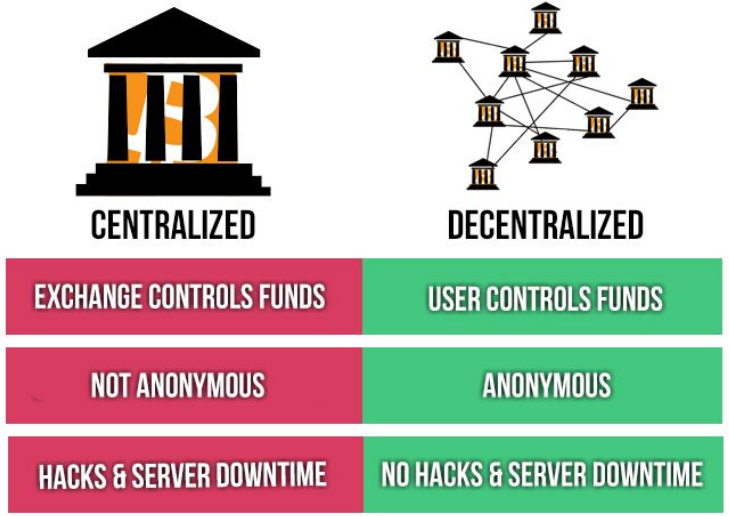


Image source: https://medium.com/@velareum/centralized-vs-decentralized-p2p-exchange-5081a095bd5c

Different Types?

Decentralized Exchanges

Centralized Exchanges

Security **Convenience**

AUTHOR: SEHYUN CHUNG

QUESTIONS?

Discussion

1. What are the pros and cons for centralized exchanges and decentralized exchanges?
2. Which wallets are suited for which kinds of users?

AUTHOR: RUSTIE LIN

BLOCKCHAIN
AT BERKELEY

CREATE A WALLET!

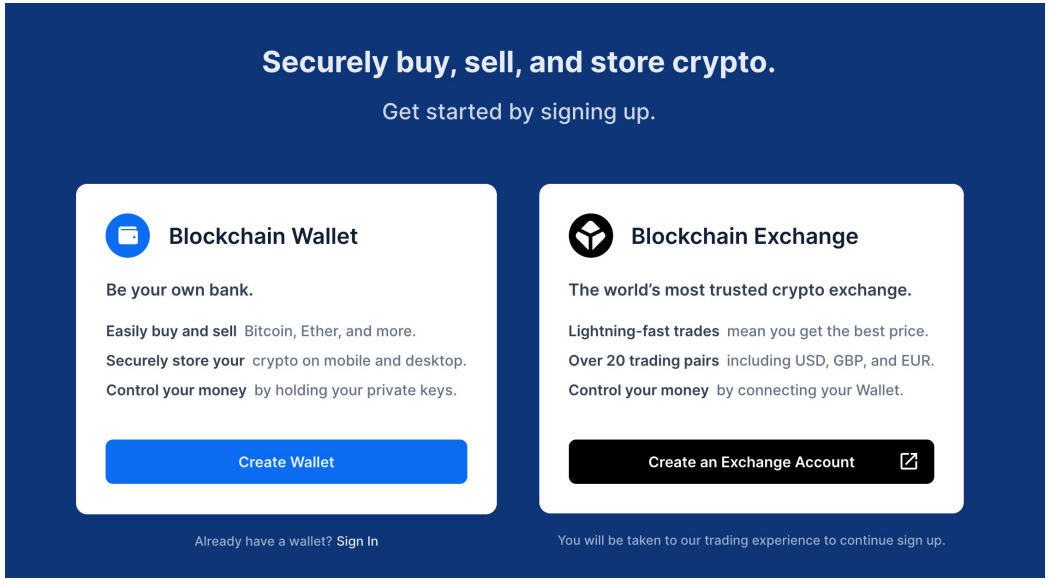
Create a paper/hardware wallet:

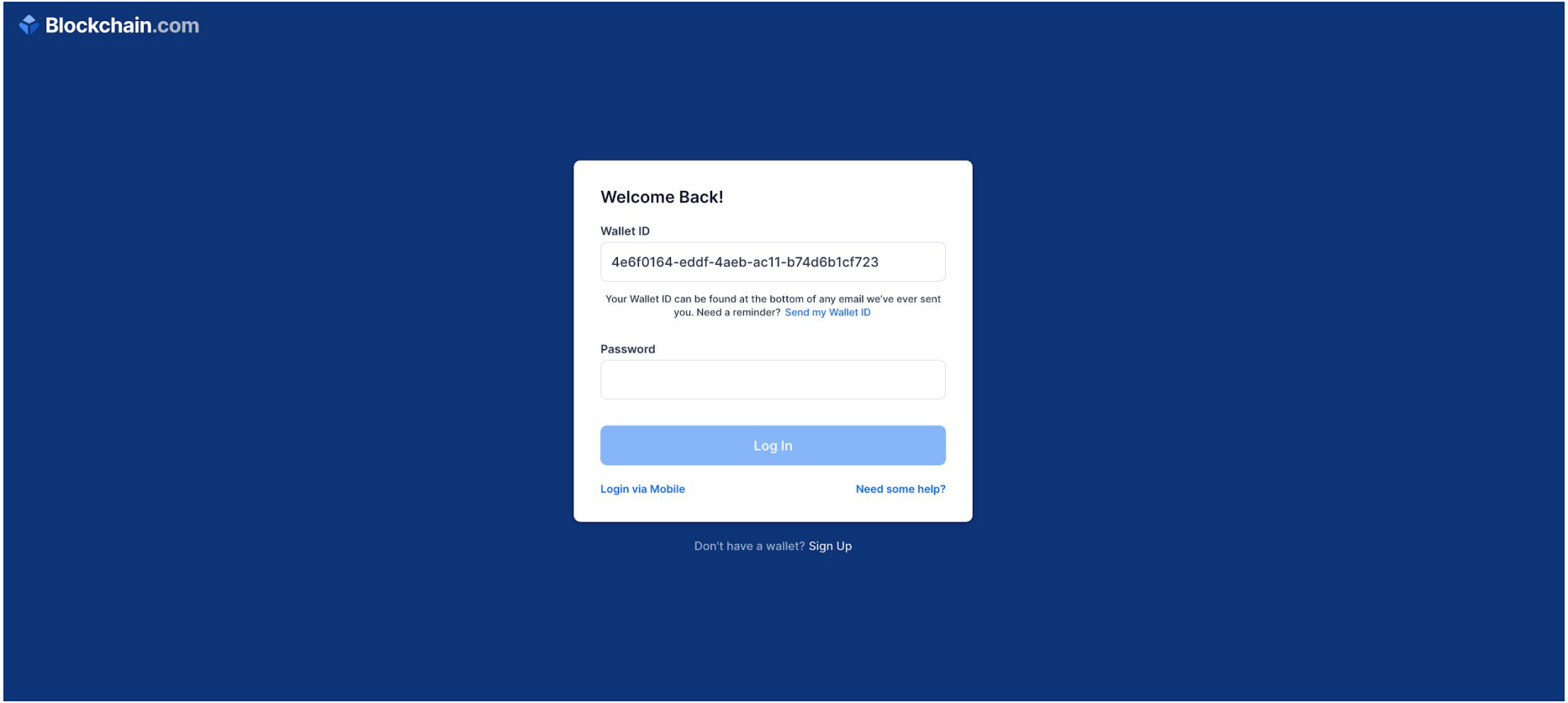
https://walletgenerator.net/

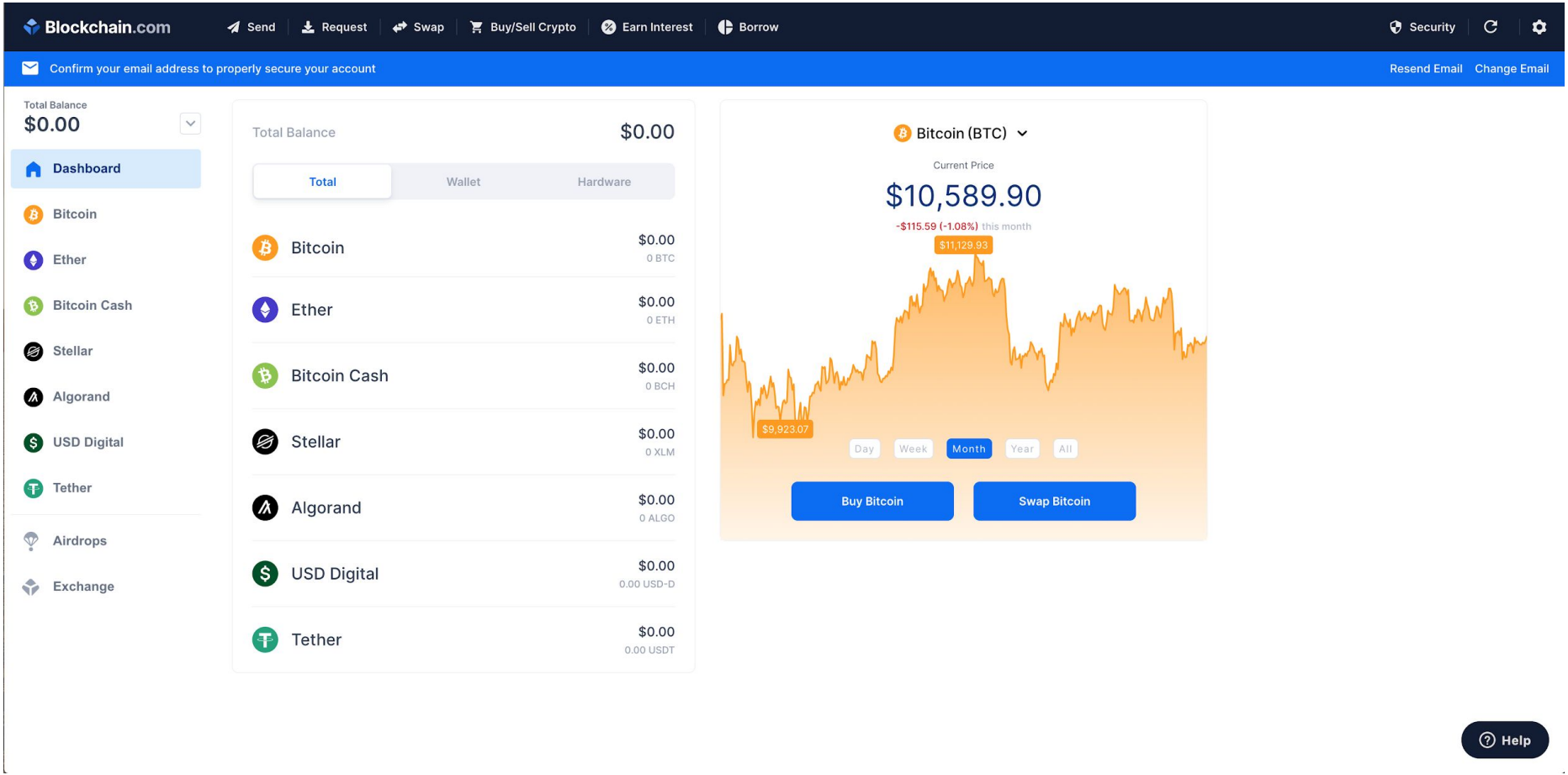
Create a digital wallet:

https://login.blockchain.com/#/signup

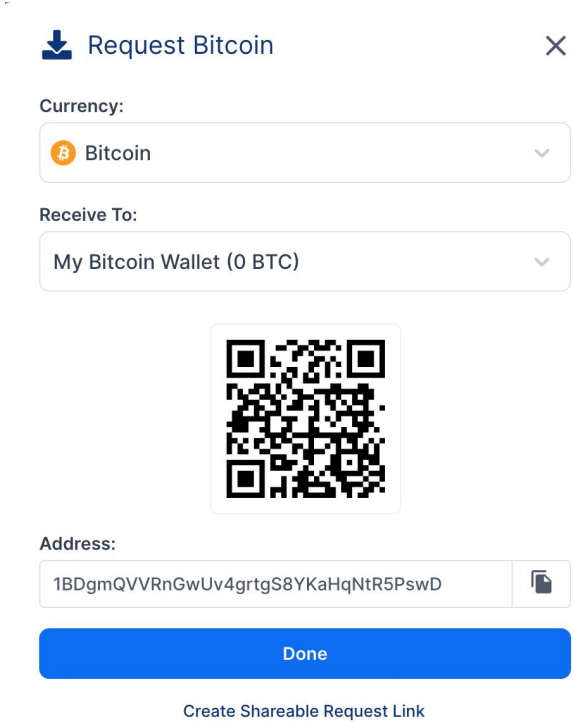
Or search for one online (make sure you can trust it! This is one of the downsides of an online wallet.)

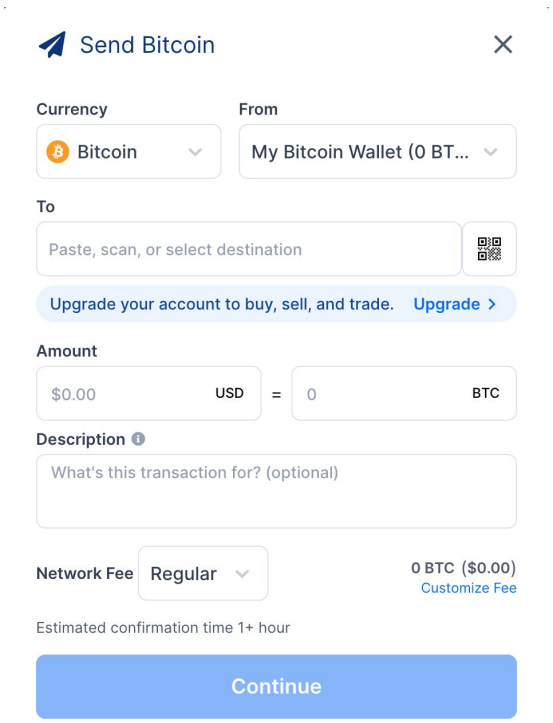



Blockchain.com
Welcome Back!
Wallet ID
4e6f0164-eddf-4aeb-ac11-b74d6b1cf723
Your Wallet ID can be found at the bottom of any email we've ever sent you. Need a reminder? Send my Wallet ID
Password
Log In
Login via Mobile
Need some help?
Don't have a wallet? Sign Up


Blockchain.com
Send
Request
Swap
Buy/Sell Crypto
Earn Interest
Borrow
Security
Confirm your email address to properly secure your account
Resend Email
Change Email
Total Balance
$0.00
Dashboard
Bitcoin
Ether
Bitcoin Cash
Stellar
Algorand
USD Digital
Tether
Airdrops
Exchange
Total Balance
$0.00
Total
Wallet
Hardware
Bitcoin
$0.00
0 BTC
Ether
$0.00
0 ETH
Bitcoin Cash
$0.00
0 BCH
Stellar
$0.00
0 XLM
Algorand
$0.00
0 ALGO
USD Digital
$0.00
0.00 USD-D
Tether
$0.00
0.00 USDT
Bitcoin (BTC)
Current Price
$10,589.90
-$115.59 (-1.08%) this month
$11,129.93
$9,923.07
Day
Week
Month
Year
All
Buy Bitcoin
Swap Bitcoin
Help

Send and receive BTC



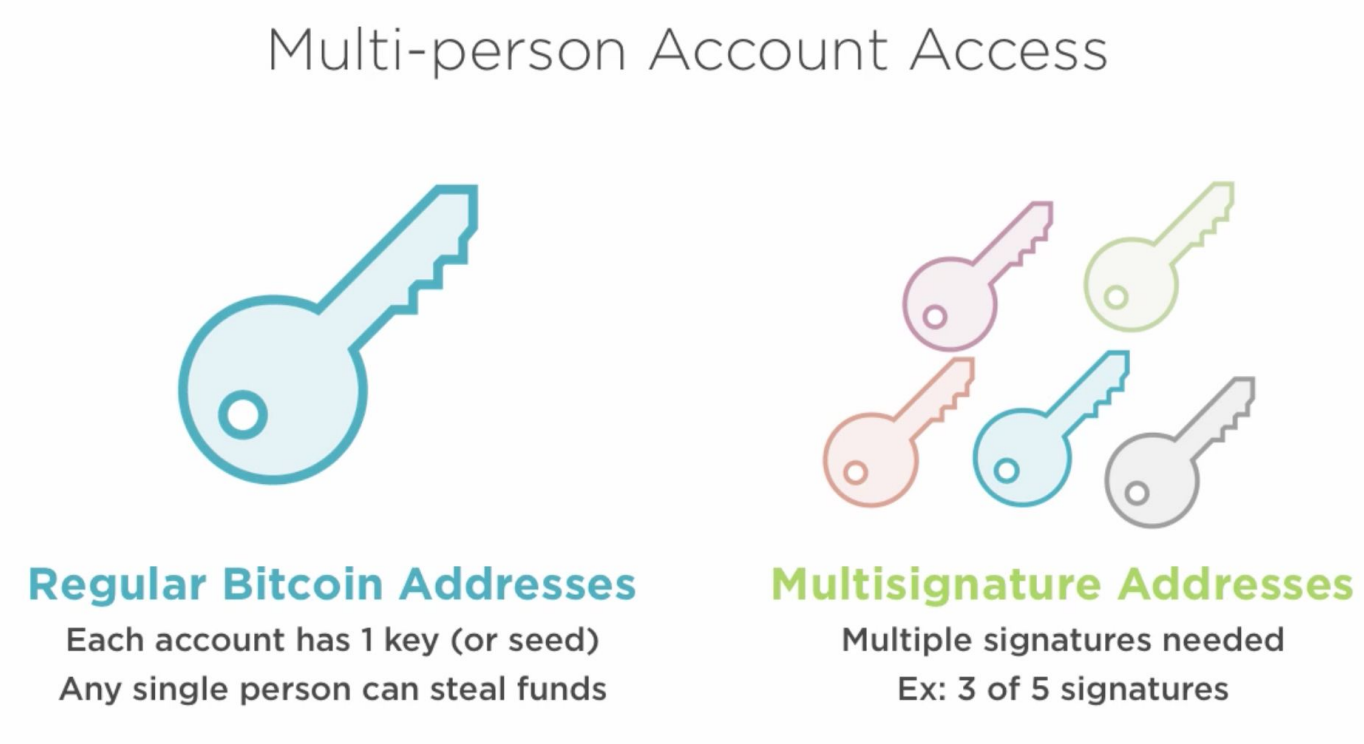


QUESTIONS?

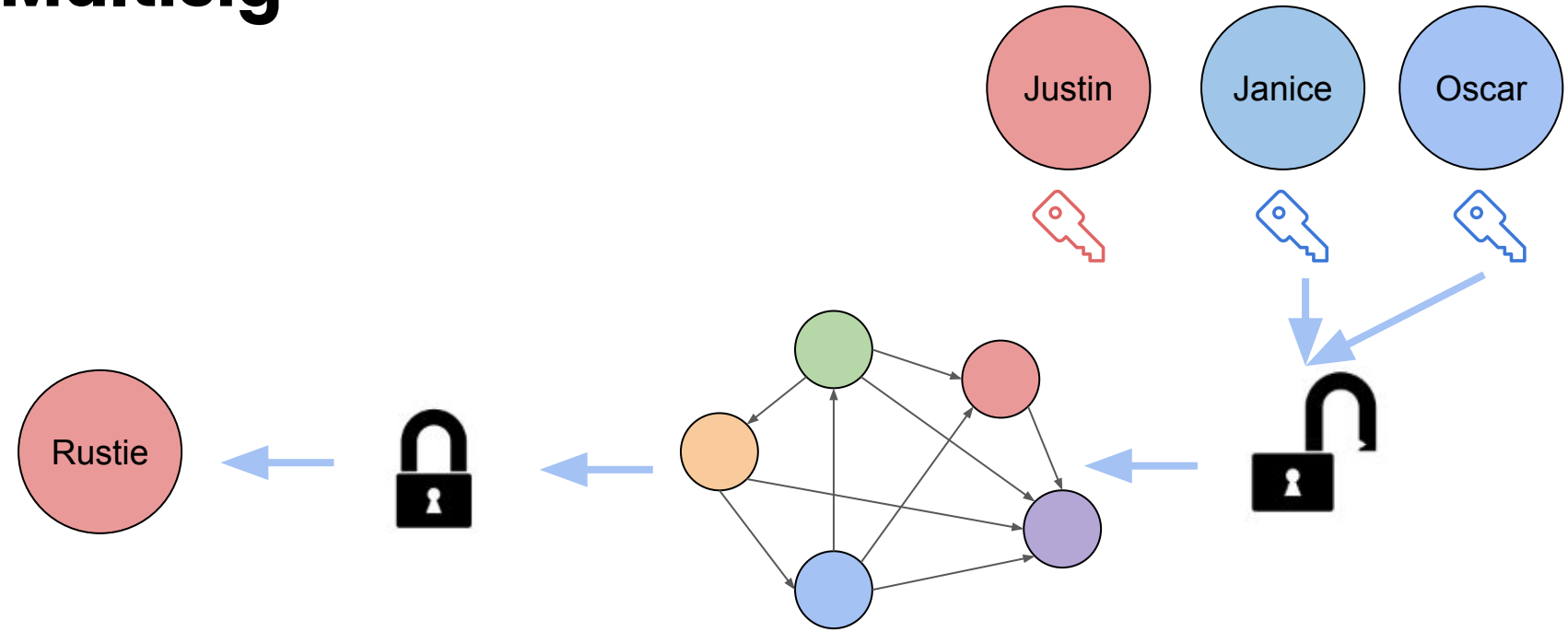
BLOCKCHAIN AT BERKELEY

Wallet Mechanics

Multisig


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

Multisig



AUTHOR: RUSTIE LIN

Best Practices

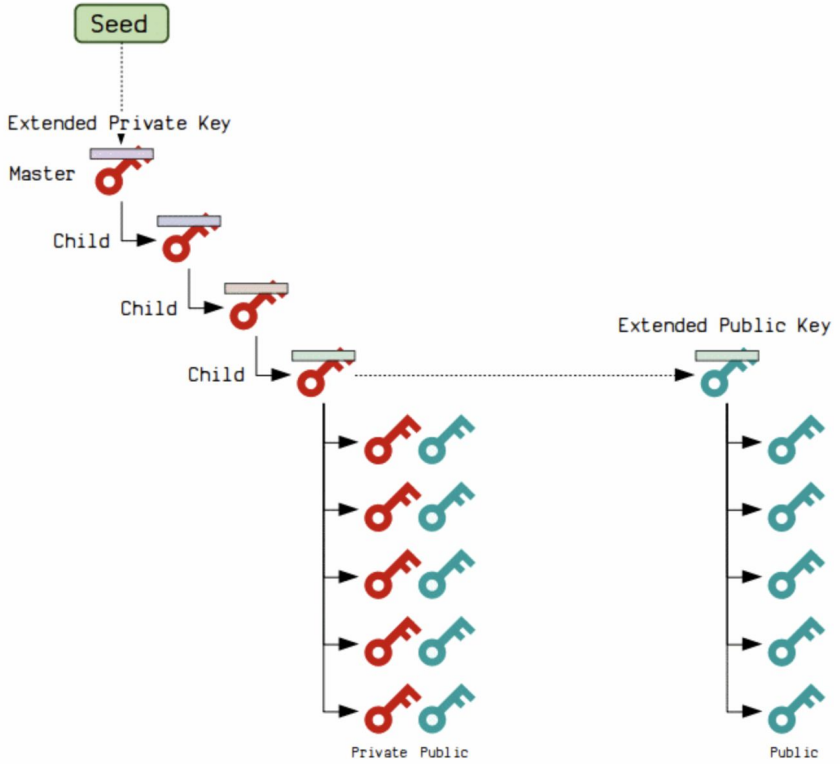
- Best practice is to never reuse pseudonyms, public keys

- Why?
  - Someone should not be able to determine how much bitcoin you own
  - Keys are computationally easy to generate anyways

- Wallet software will handle this

Hierarchical Deterministic (HD) Wallets

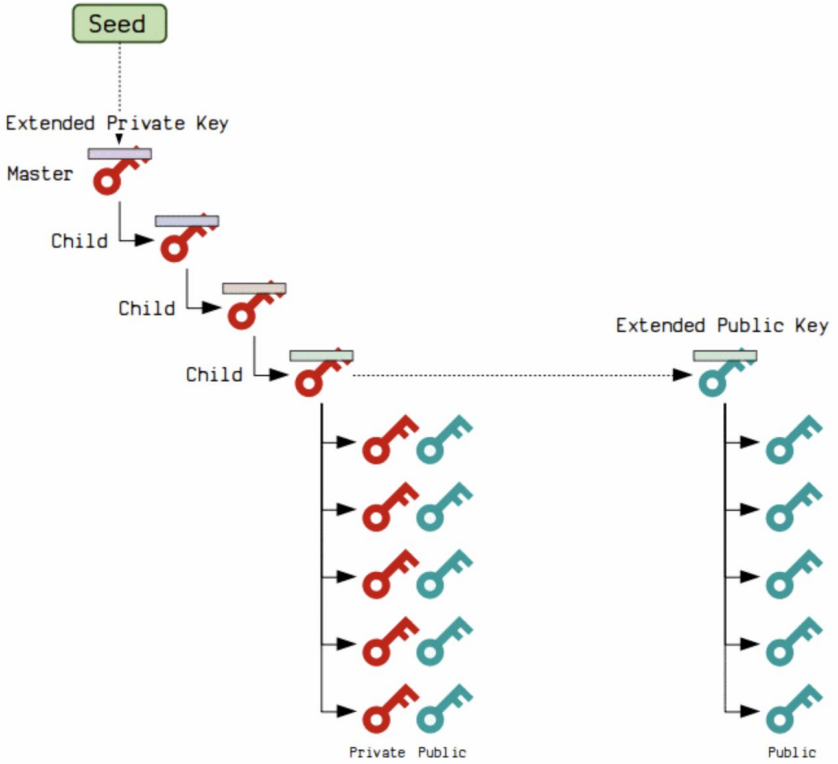
- Deterministic because all child keys are generated from a seed in the same way every time
- Hierarchical because you can organize the keys in a tree-like structure, with levels



AUTHOR: RUSTIE LIN
UPDATED BY: SEHYUN CHUNG

Hierarchical Deterministic (HD) Wallets

- Fewer points of failure: store/backup one master private key, then derive the entire tree of child keys (could also be considered a flaw)
- Access control: the tree-like structure allows the owner to allow someone access to only a part of a wallet, by delegating them a certain branch

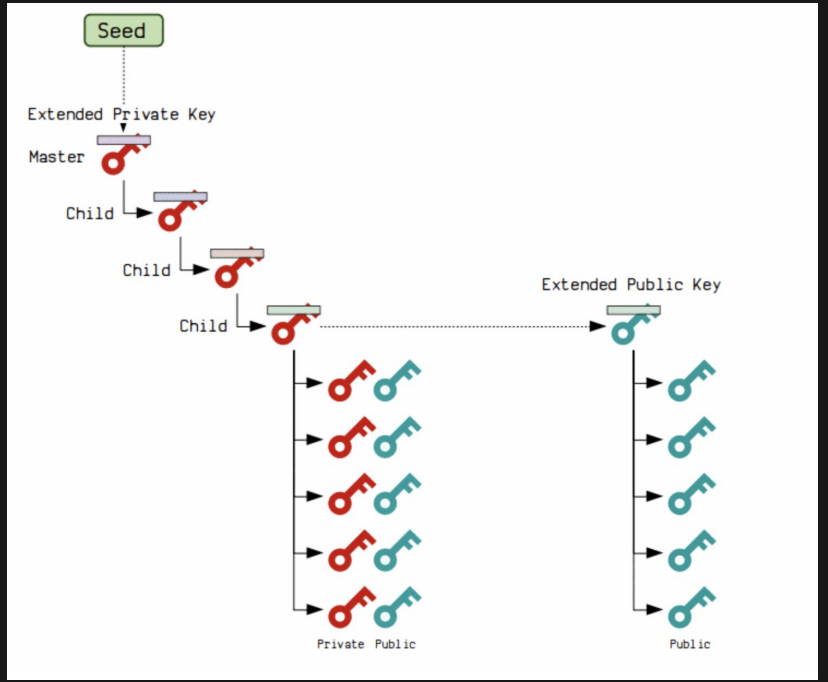


AUTHOR: SEHYUN CHUNG

WALLET MECHANICS

HD Wallets

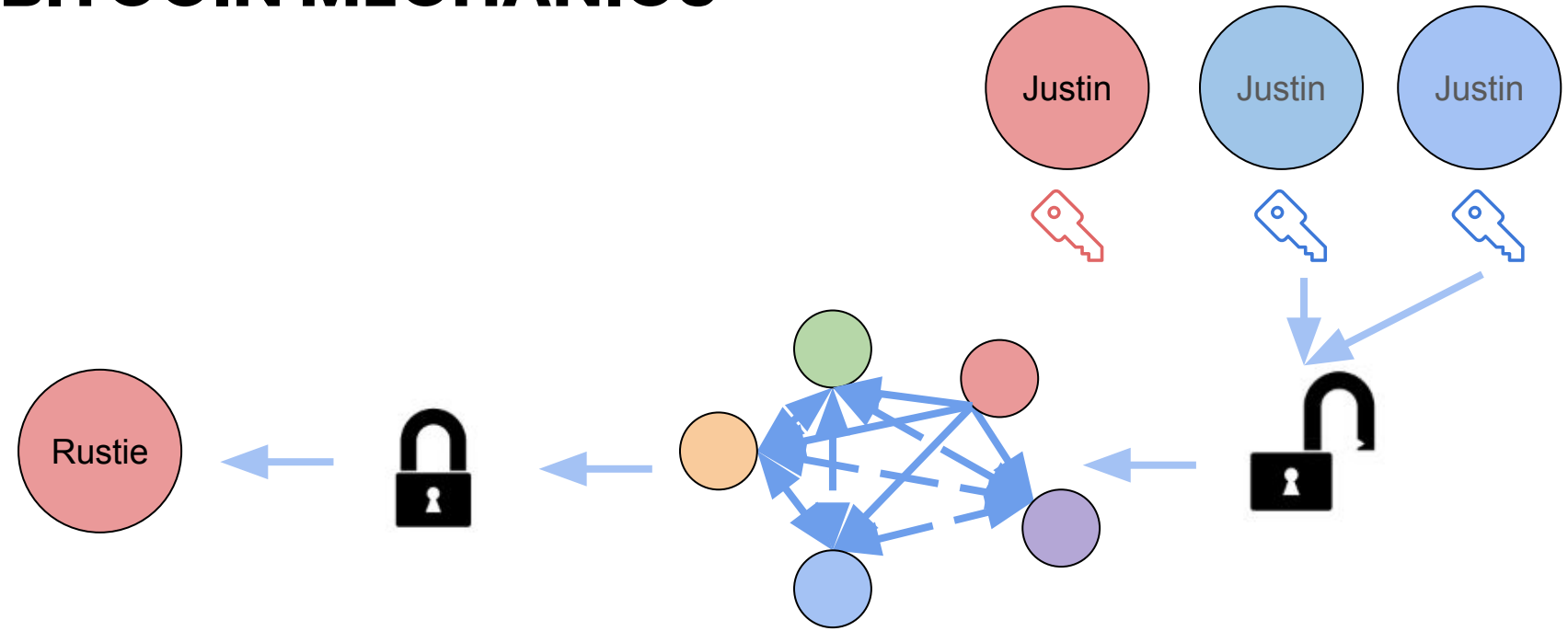
1. Start with a master private key
2. Generate child private keys by hashing your private key + index
3. Use the public key of the **master** private key to generate child public keys
4. By the nature of hash functions (same input **always** means same output), we only need the master key



AUTHOR: SEHYUN CHUNG

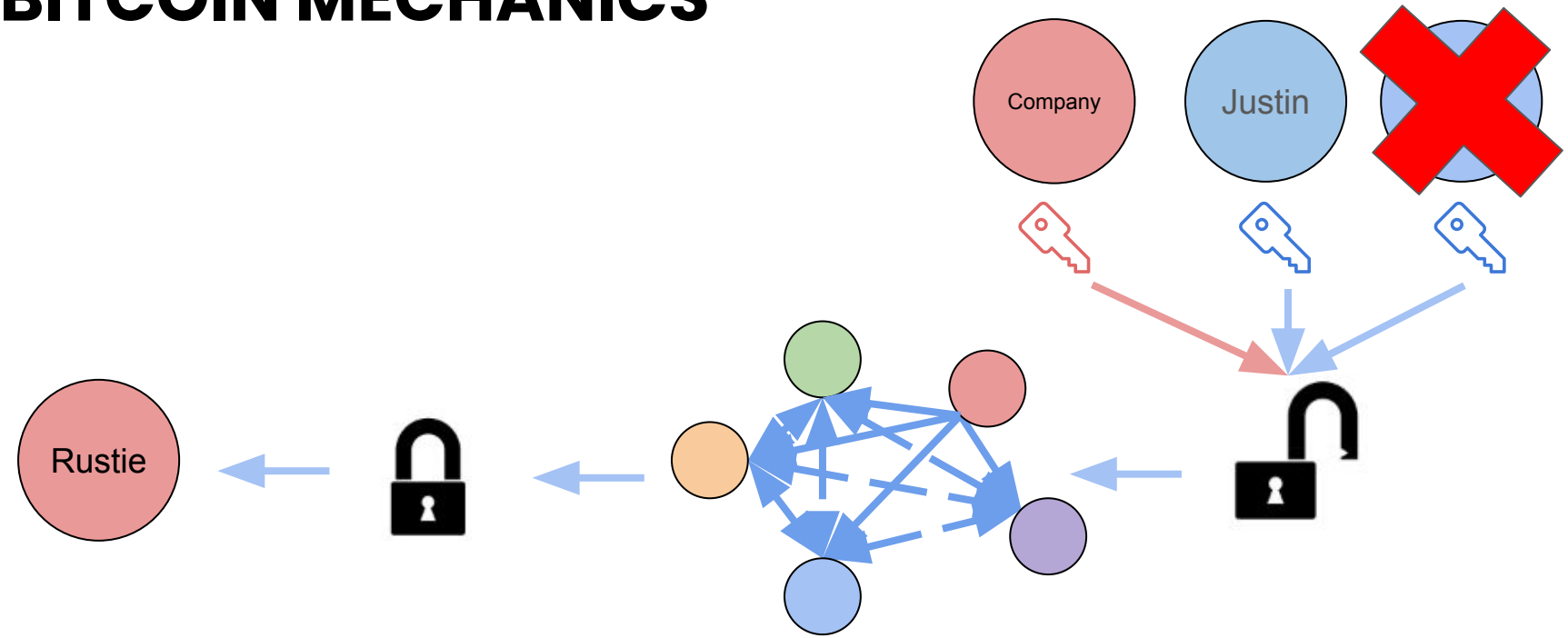
BLOCKCHAIN AT BERKELEY

BITCOIN MECHANICS



AUTHOR: RUSTIE LIN

BITCOIN MECHANICS



AUTHOR: RUSTIE LIN

WALLET BACKUPS

- **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

QUESTIONS?

BLOCKCHAIN
AT BERKELEY

Mining

RECIPE FOR MINING

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

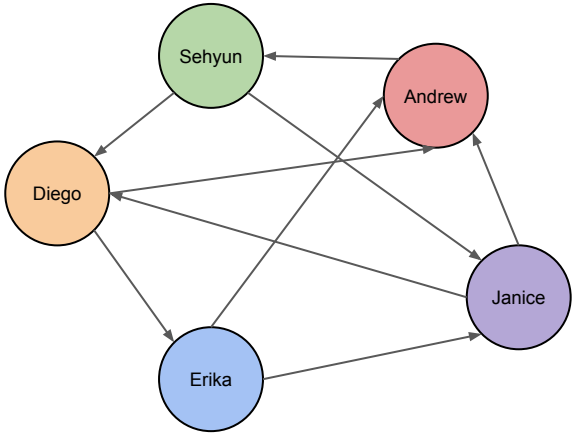
A full-fledged Bitcoin miner must:

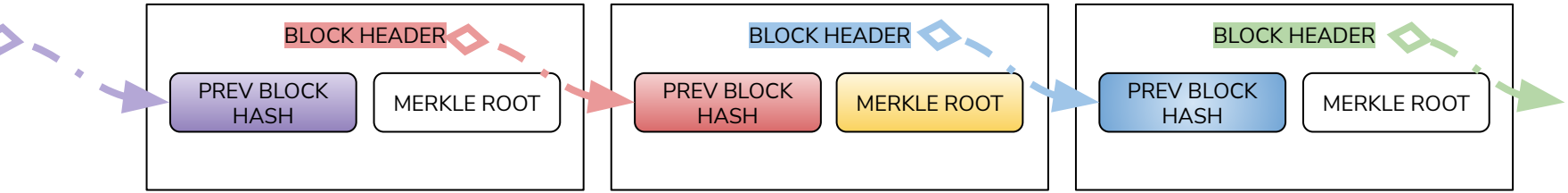
1. **Download** the entire Bitcoin blockchain
2. **Verify** incoming transactions
3. **Create** a block
4. **Find** a valid nonce
5. **Broadcast** your block
6. **Profit**!

AUTHOR: NADIR AKHTAR
U[DATED: RUSTIE LIN

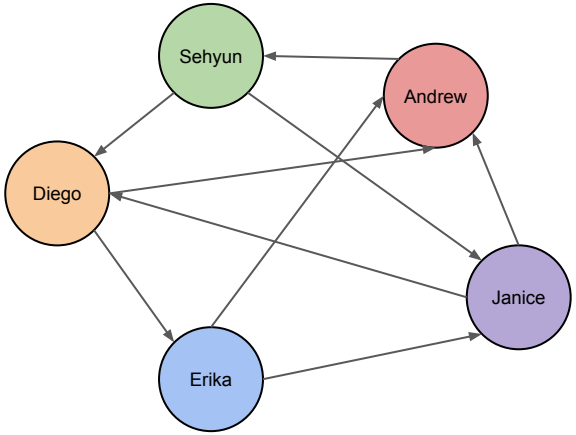
RECIPE FOR MINING

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



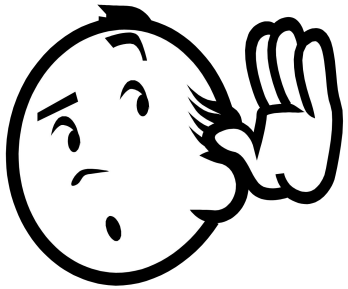


AUTHOR: RUSTIE LIN


Sehyun
Andrew
Diego
Janice
Erika

RECIPE FOR MINING

- 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



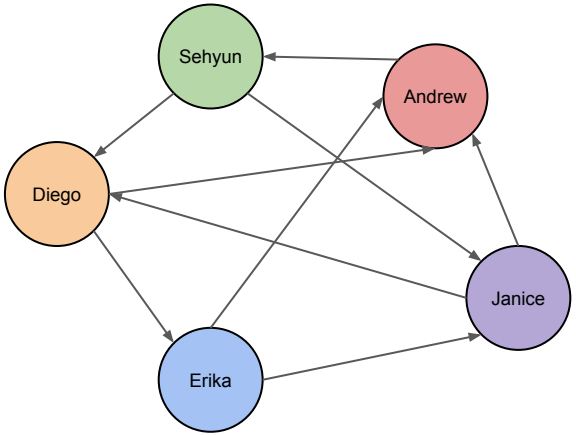
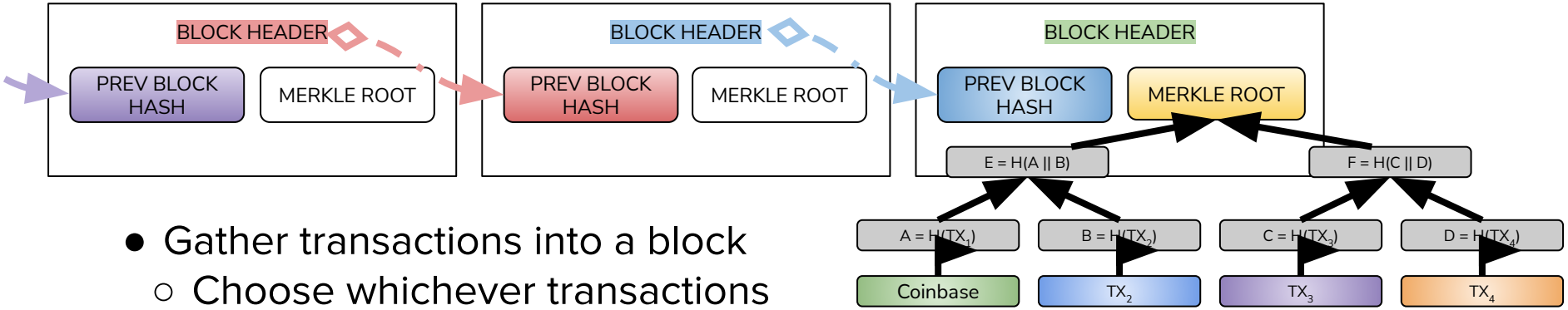


Image sources:
https://ru-clip.com/video/rVrb6rrRvNQ/what-is-a-mempool-and-how-to-speed-up-unconfirmed-transactions.html
https://englishinreims.wordpress.com/toeic-training/practice-toeic-listening-part-i/

AUTHOR: RUSTIE LIN

RECIPE FOR MINING

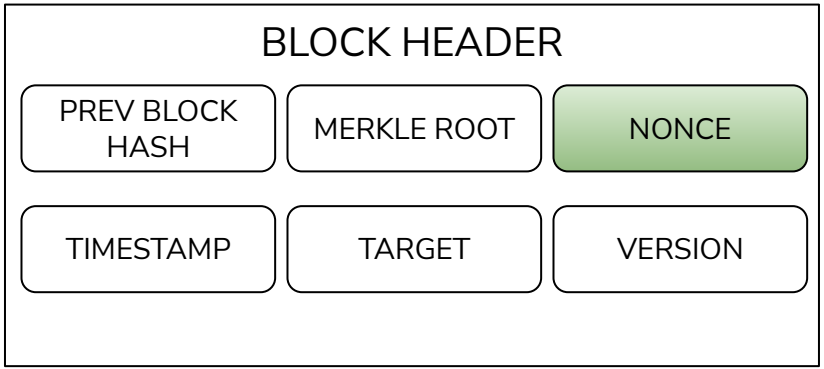


- Gather transactions into a block
  - Choose whichever transactions you want (most transaction fees)
- Get previous block hash and other necessary metadata

AUTHOR: RUSTIE LIN

RECIPE FOR MINING

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

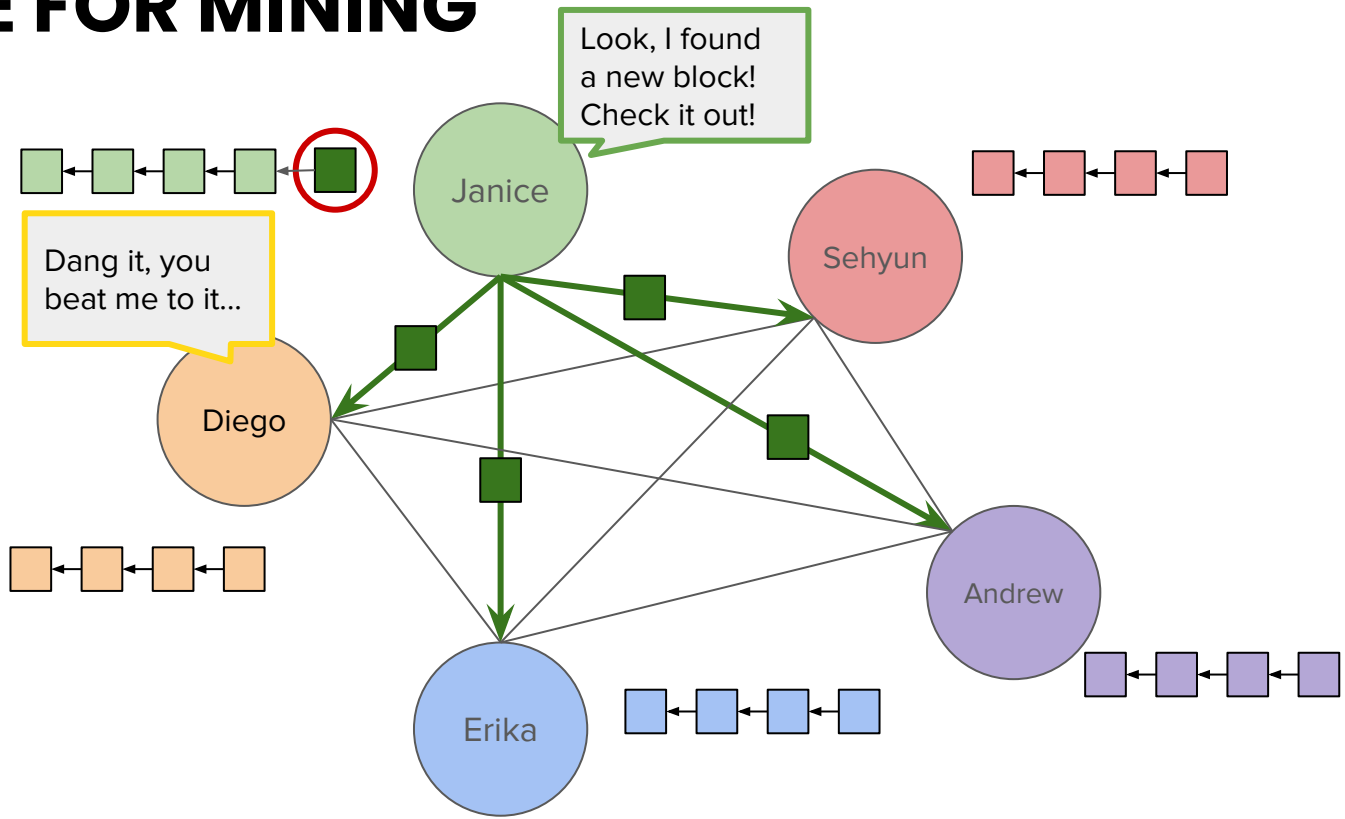



```
TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while (1) {
      header = makeBlockHeader(transactions, coinbase_nonce);
      for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++){
            if (SHA256(SHA256(makeBlock(header, header_nonce))) <
      TARGET)
            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

Figure 5.6 : CPU mining pseudocode.

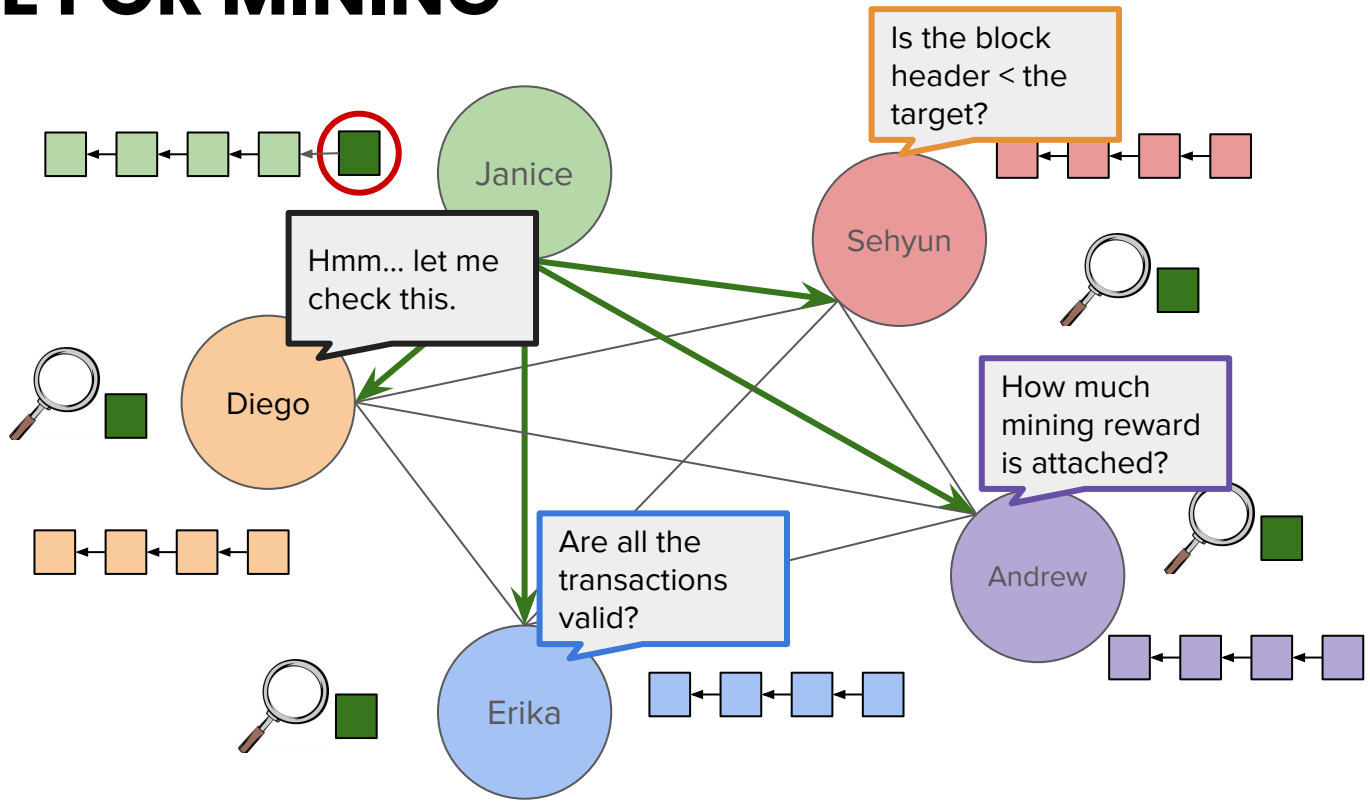
Image source: Mastering Bitcoin

RECIPE FOR MINING



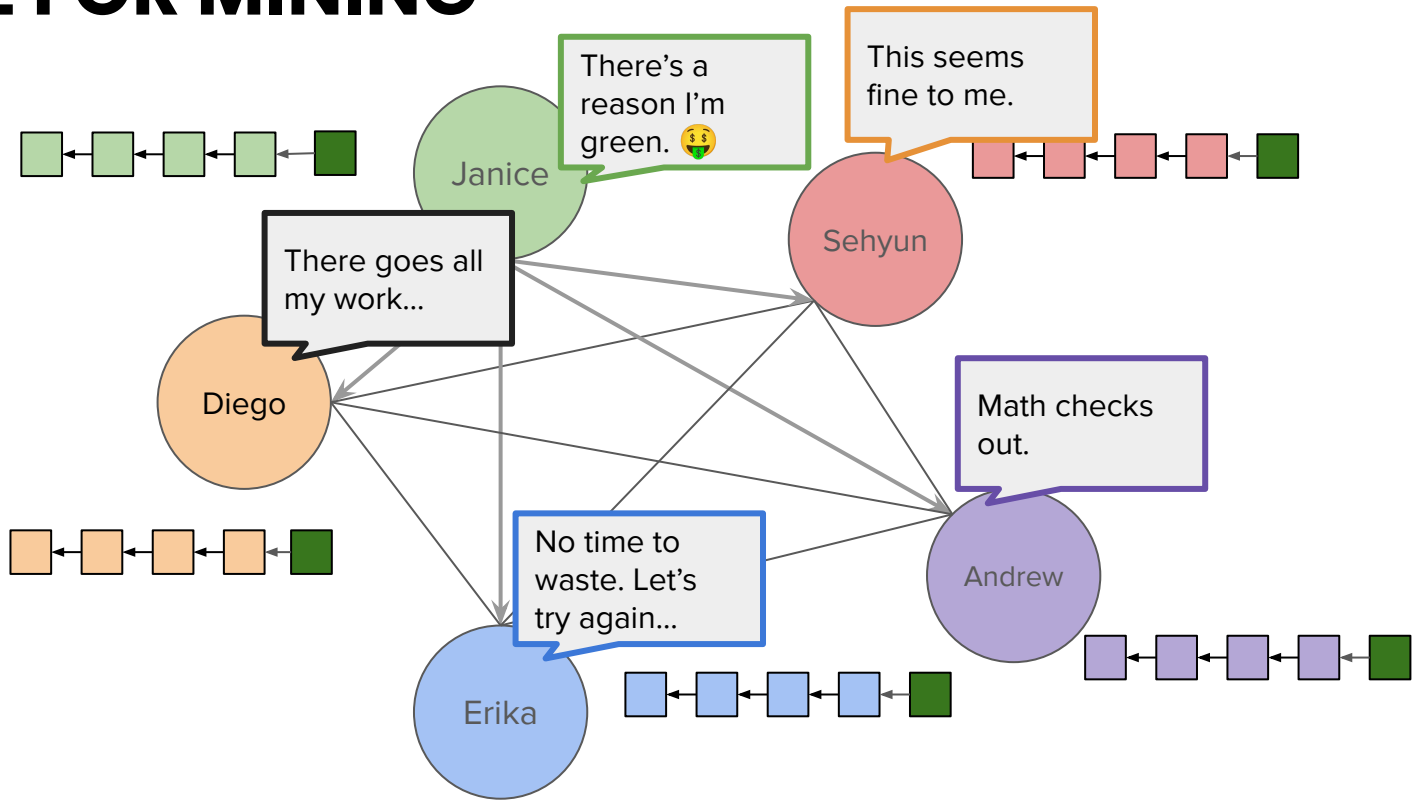
AUTHOR: JUSTIN YU

RECIPE FOR MINING



AUTHOR: JUSTIN YU

RECIPE FOR MINING



AUTHOR: JUSTIN YU

RECIPE FOR MINING

Remember: Mining is a competition

- Longest chain rules!
  - 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

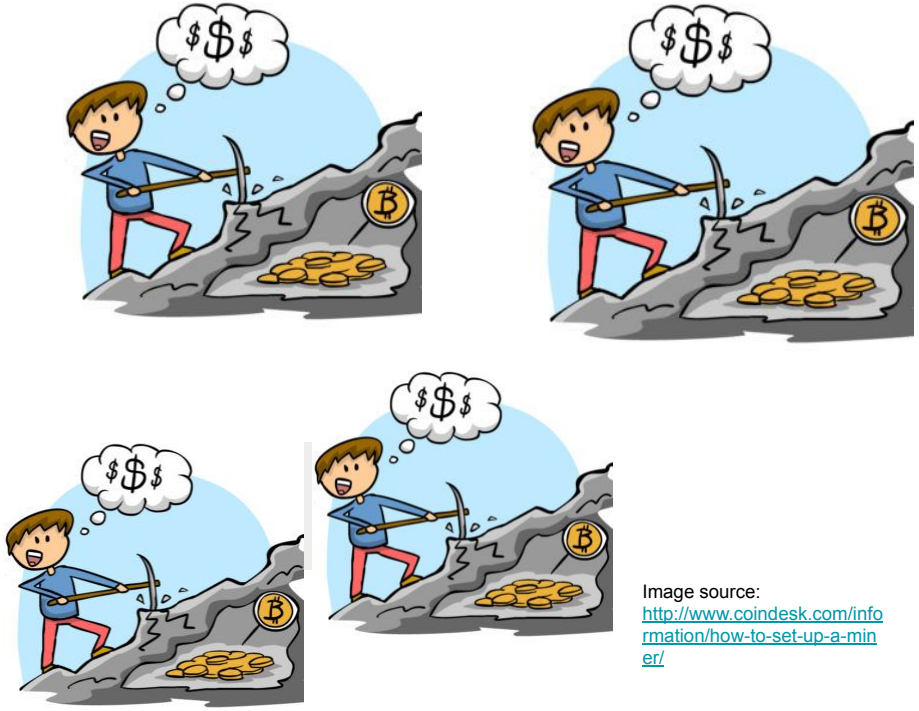


Image source: http://www.coindesk.com/information/how-to-set-up-a-miner/

QUESTIONS?

BLOCKCHAIN AT BERKELEY

Mining Incentives

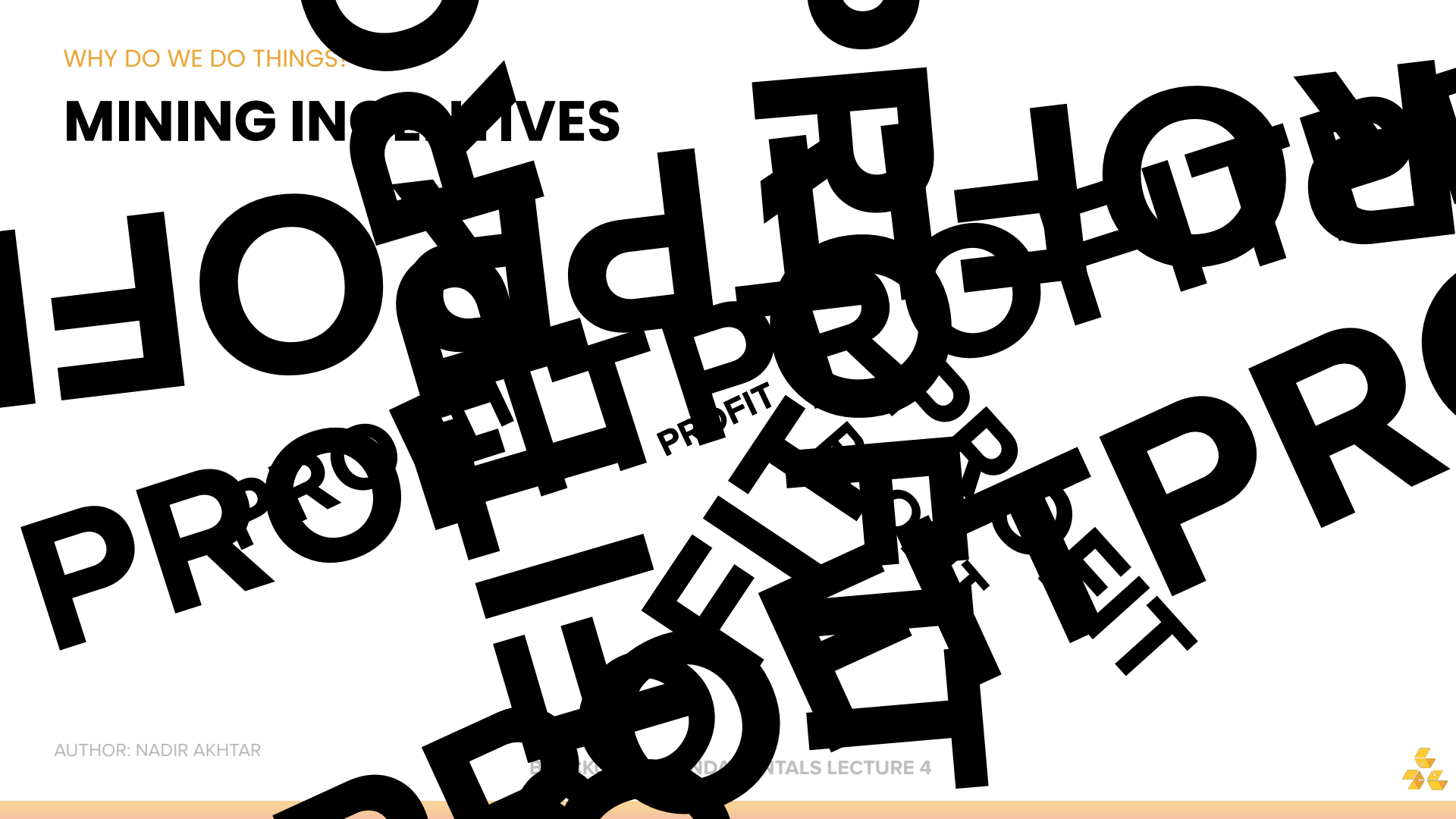
MINING INCENTIVES

PROFIT

AUTHOR: NADIR AKHTAR

WHY DO WE DO THINGS?

MINING INCENTIVES



AUTHOR: NADIR AKHTAR

WHAT IS PROFIT?

MINING INCENTIVES

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

PROFIT = REVENUE - COST

AUTHOR: NADIR AKHTAR

MINING INCENTIVES

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES

MINING_COST = FIXED_COSTS + VARIABLE_COSTS


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

AUTHOR: NADIR AKHTAR

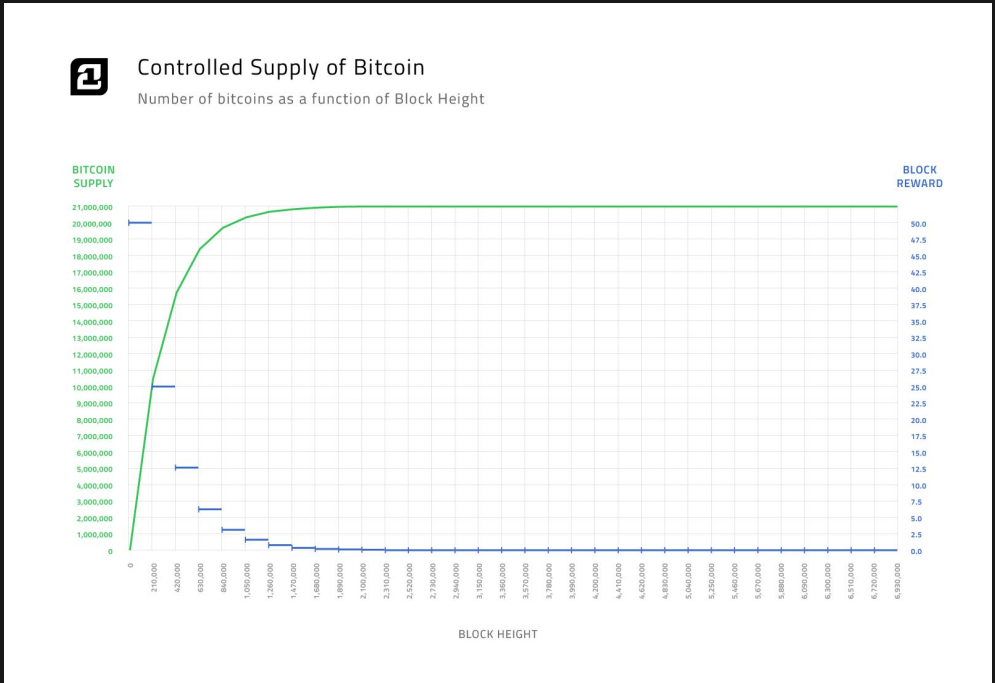
MINING INCENTIVES

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES

MINING_COST = FIXED_COSTS + VARIABLE_COSTS


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

AUTHOR: NADIR AKHTAR

BLOCK REWARD

MINING INCENTIVES



- Miner receives BTC for every confirmed block
  - Currently 6.25 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

AUTHOR: NADIR AKHTAR

BLOCK REWARD: RATIONALE

MINING INCENTIVES

- 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)

AUTHOR: NADIR AKHTAR

MINING INCENTIVES

How are miners incentivized to be honest in their mining? Why isn’t it in their best interest to mine empty blocks?

MINING INCENTIVES

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES

MINING_COST = FIXED_COSTS + VARIABLE_COSTS


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

AUTHOR: NADIR AKHTAR

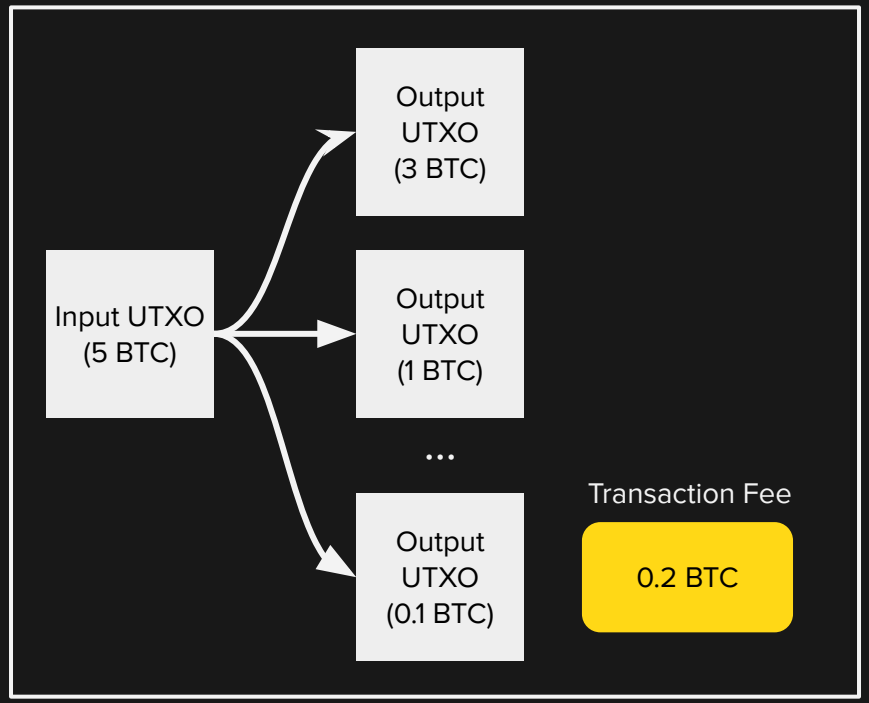
MINING INCENTIVES

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES

MINING_COST = FIXED_COSTS + VARIABLE_COSTS


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

AUTHOR: NADIR AKHTAR

TRANSACTION FEES

MINING INCENTIVES

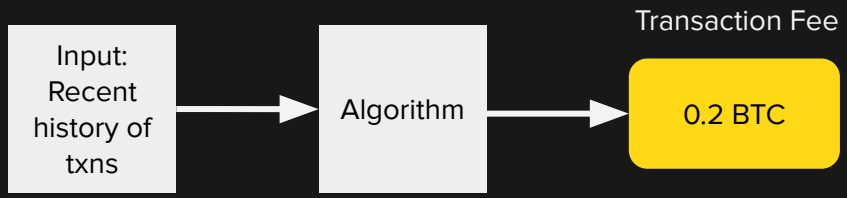


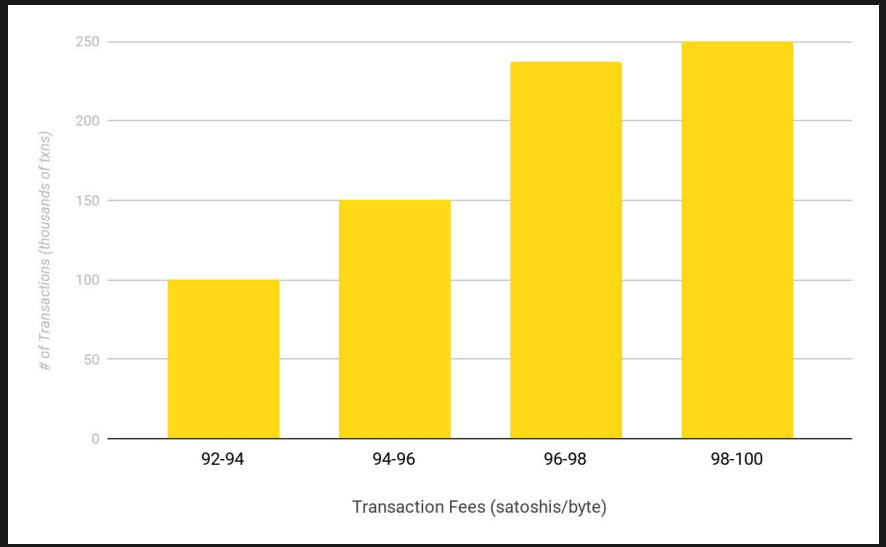
- Transaction creator sets the fee
  - Voluntary, but practically necessary
- Extra income for miners on top of block reward
  - Higher transaction fee → faster confirmation time, since more miners want to include your transaction
- `TX_FEE = INPUT - OUTPUT`
- When block reward becomes 0, TX fees will become the only source of revenue for miners

AUTHOR: NADIR AKHTAR
UPDATED: JUSTIN YU

TRANSACTION FEES

FEE ESTIMATION ALGORITHM





- Input: past transaction data grouped into “buckets”
- One bucket represents a range of transaction fees (e.g. 0.00000097 BTC - 0.00000099 BTC)
- Identifies the lowest fee rate bucket where all transactions are confirmed
- Output: the lowest fee rate bucket. This is the transaction fee you should use to ensure your transaction is put into a block.

AUTHOR: SEHYUN CHUNG
SOURCE: MORCOS

BLOCKCHAIN AT BERKELEY

FEE BUMPING

- “bumping” up the transaction of an **already broadcast** transaction

Why do we need to do this?

- transaction can get **stuck** in the mempool
- if the fee associated with a transaction is too low, no miner will want to pick it up
- caused by naive fee estimation algorithms, a spike in minimum fees, etc.

FEE BUMPING SOLUTIONS

- Replace by Fee (RBF)
  - the user signs a replacement transaction with the same inputs, but pays additional fees
  - the additional fee may come from the change output
- Child Pays for Parent (CPPP)
  - the user creates a new transaction which spends one or more of the outputs of the stuck transaction
  - attaches a large fee
  - this works because miners package together ancestor and descendant transactions

QUESTIONS?

MINING INCENTIVES

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES

MINING_COST = FIXED_COSTS + VARIABLE_COSTS


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

AUTHOR: NADIR AKHTAR

MINING INCENTIVES

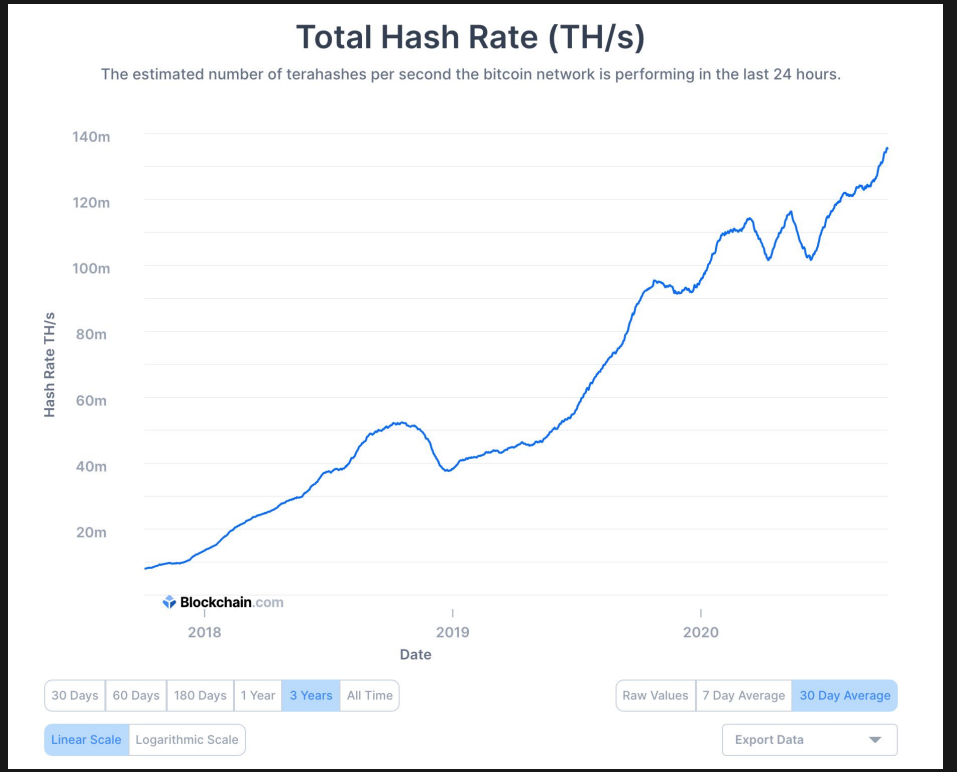
```
MINING_REVENUE = BLOCK_REWARD + TX_FEES

MINING_COST = FIXED_COSTS + VARIABLE_COSTS


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

AUTHOR: NADIR AKHTAR

FIXED COST: HARDWARE COSTS

MINING INCENTIVES

	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



AUTHOR: NADIR AKHTAR

BLOCKCHAIN AT BERKELEY

FIXED COST: CPU MINING

MINING INCENTIVES

	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

```
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

FIXED COST: GPU MINING

MINING INCENTIVES

	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

- 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

AUTHOR: NADIR AKHTAR

FIXED COST: FPGA MINING

MINING INCENTIVES

	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**!

AUTHOR: NADIR AKHTAR

FIXED COST: ASIC MINING

MINING INCENTIVES

	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

- **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
- Antminer S9 (53 TH/s): $1500

AUTHOR: NADIR AKHTAR

MINING INCENTIVES

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES

MINING_COST = FIXED_COSTS + VARIABLE_COSTS


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

AUTHOR: NADIR AKHTAR

MINING INCENTIVES

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES

MINING_COST = FIXED_COSTS + VARIABLE_COSTS


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


OPERATING COSTS

MINING INCENTIVES

- 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!

AUTHOR: MAX FANG

MINING INCENTIVES

```
MINING_REVENUE = BLOCK_REWARD + TX_FEES

MINING_COST = FIXED_COSTS + VARIABLE_COSTS


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

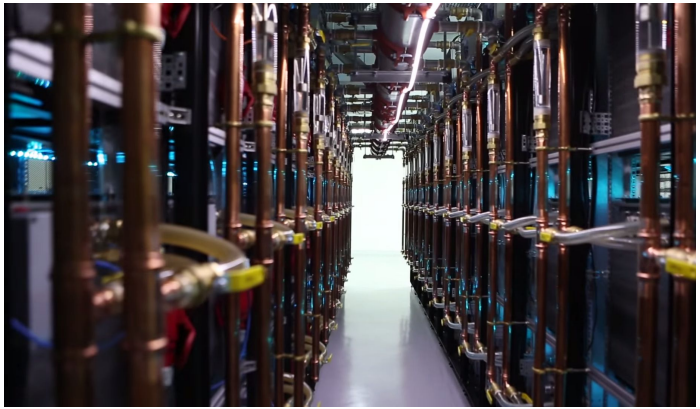

QUESTIONS?

BLOCKCHAIN
AT BERKELEY

Real Word Mining

CHINESE ASIC MINING FARM

REAL WORLD MINING



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

AUTHOR: NADIR AKHTAR

REAL WORLD MINING

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

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

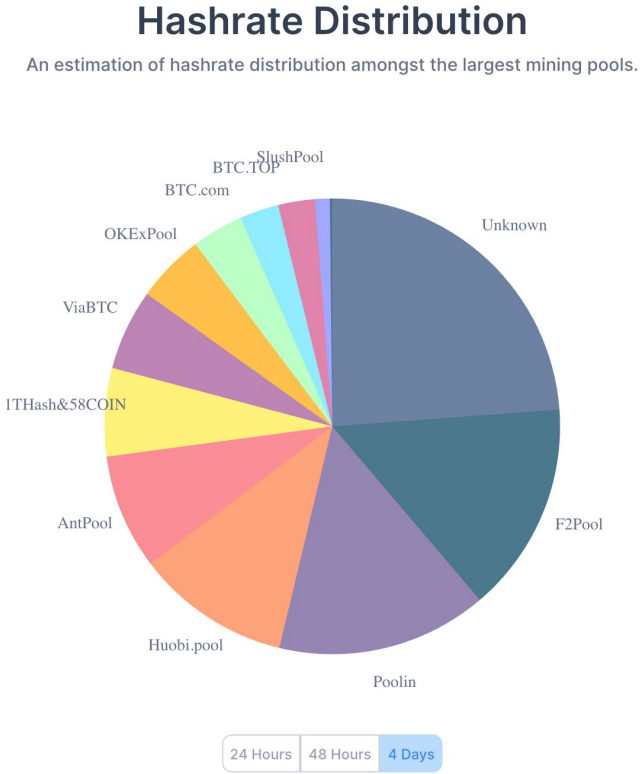
AUTHOR: MAX FANG

REAL WORLD MINING

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

Source: https://www.blockchain.com/charts/pools (10/2/2020)



AUTHOR: MAX FANG

QUESTIONS?

REAL WORLD MINING

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

POOL REWARDS

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
    a. Not a problem if pool is sufficiently large
3. Lower risk for pool operators - only pay out when reward is found
    a. Individuals thus incentivized to submit valid blocks

AUTHOR: MAX FANG

REAL WORLD MINING

- **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.

AUTHOR: MAX FANG

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

REAL WORLD MINING

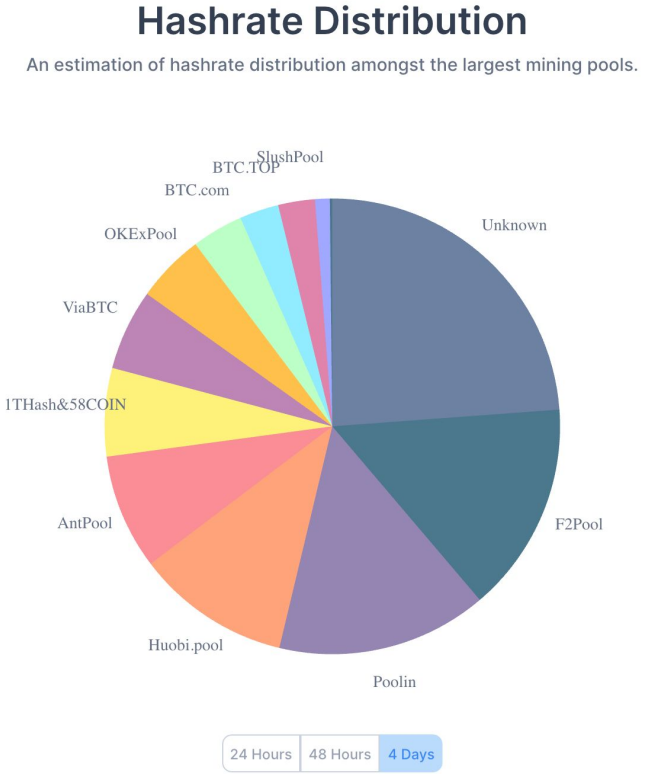
Pros

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

Cons

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

Source: https://www.blockchain.com/charts/pools (10/2/2020)



AUTHOR: MAX FANG
UPDATED: BRIAN HO

REAL WORLD MINING

Quick facts:

- Today's (10/08/19) network hashrate:
  94, 509, 815 TH/s

- Mining Reward / yr = (1 yr / 10 mins) * 12.5 = **657k BTC / yr**

- Assume **constant price of Bitcoin** of $10,000

Suppose you want to start mining today.

- Antminer S17: Costs $1500, **53 TH/s**
- **% of network hashrate** = (53 TH/s) /

  (94, 509, 815 TH/s) = **0.000000560788316**

Expected Annual Reward

- 0.000000560788316 * 657k /yr
  ≃ 0.36843 BTC / yr ≃ **$3,053/ yr**

AUTHOR: MAX FANG
UPDATED: BRIAN HO

REAL WORLD MINING

Solo mining

- 1 block 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 ⅛ network hashrate
  - Pool finds every 6th block ≃ 1 per hr
- $1530.72 /yr / 8760 hrs/yr
  ≃ **$0.17 every hour**

Paradox:

- The more secure Bitcoin gets, the greater the appeal for mining pools and centralization of computation power

AUTHOR: MAX FANG
UPDATED: BRIAN HO

QUESTIONS?

BLOCKCHAIN AT BERKELEY

Changing Bitcoin

DECENTRALIZING MINING

- 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_JFXXXXcqXFXXq6xXFXXXw/221223714/HTB18YN_JFXXXXcqXFXXq6xXFXXXw.jpg

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

DECENTRALIZING MINING

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

DECENTRALIZING MINING

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

SCRYPT

DECENTRALIZING MINING

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

AUTHOR: MAX FANG

SCRYPT

DECENTRALIZING MINING

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

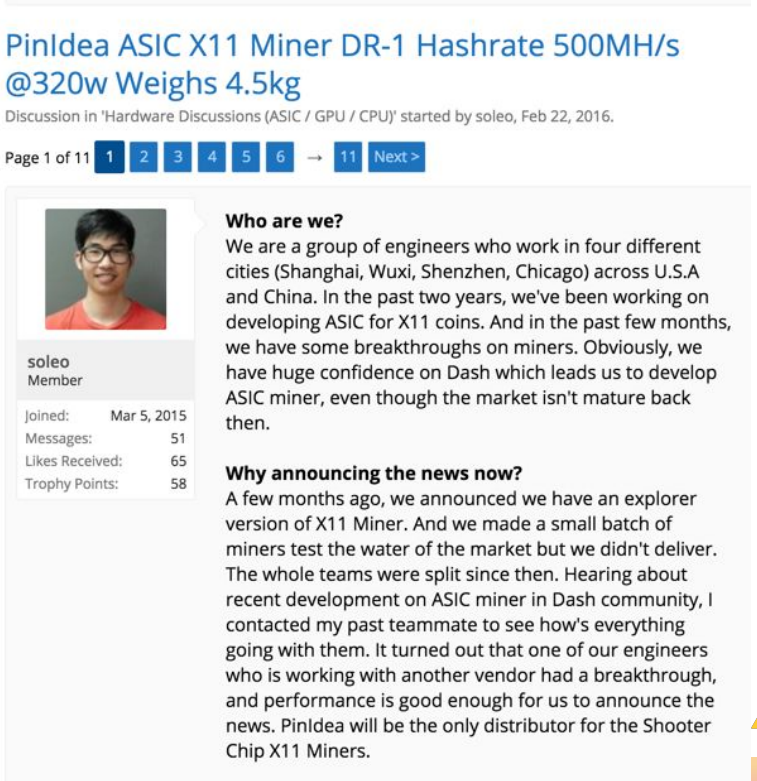
```
1 def scrypt(N, seed):
2     V = [0] * N  // initialize memory buffer of length N

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

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

10  return X
```

AUTHOR: MAX FANG

BLOCKCHAIN AT BERKELEY

DECENTRALIZING MINING

- **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.

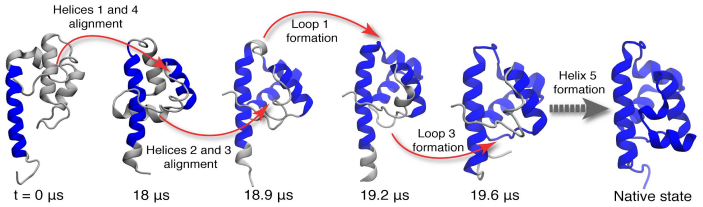
Mike Hearn, Bitcoin Core developer: “There’s really no such thing as an ASIC-resistant algorithm.”

DECENTRALIZING MINING

- 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

AUTHOR: MAX FANG

PROOF-OF-USEFUL-WORK



- "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

AUTHOR: MAX FANG

PROOF-OF-USEFUL-WORK

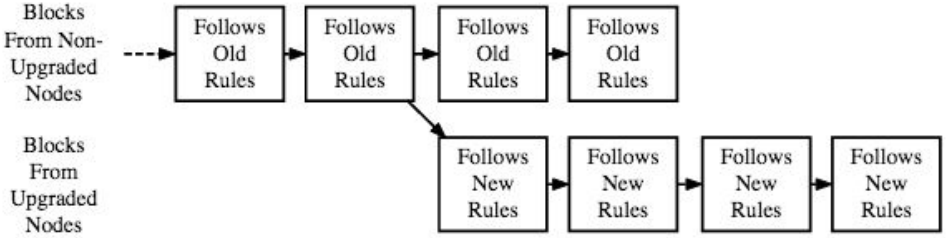
- Most distributed computing problems are unsuitable for proof-of-work
  - Fixed amount of data
    - Missing an inexhaustible puzzle space
  - Potential solutions not equally likely
    - Missing an equiprobable solution space
  - Cannot rely on central entity to delegate tasks
    - Missing decentralized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

CONSENSUS UPDATES

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

CONSENSUS UPDATES

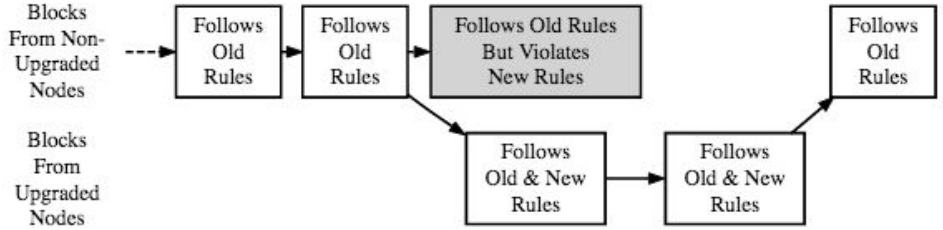
Hard Fork



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

Source: Bitcoin.org Developer Guide

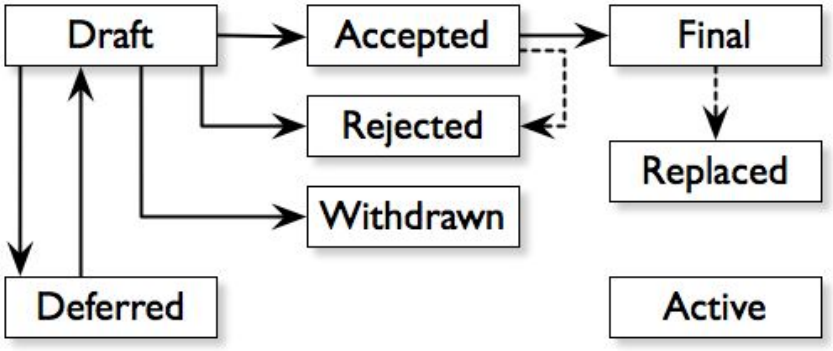
Soft Fork



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

CONSENSUS UPDATES

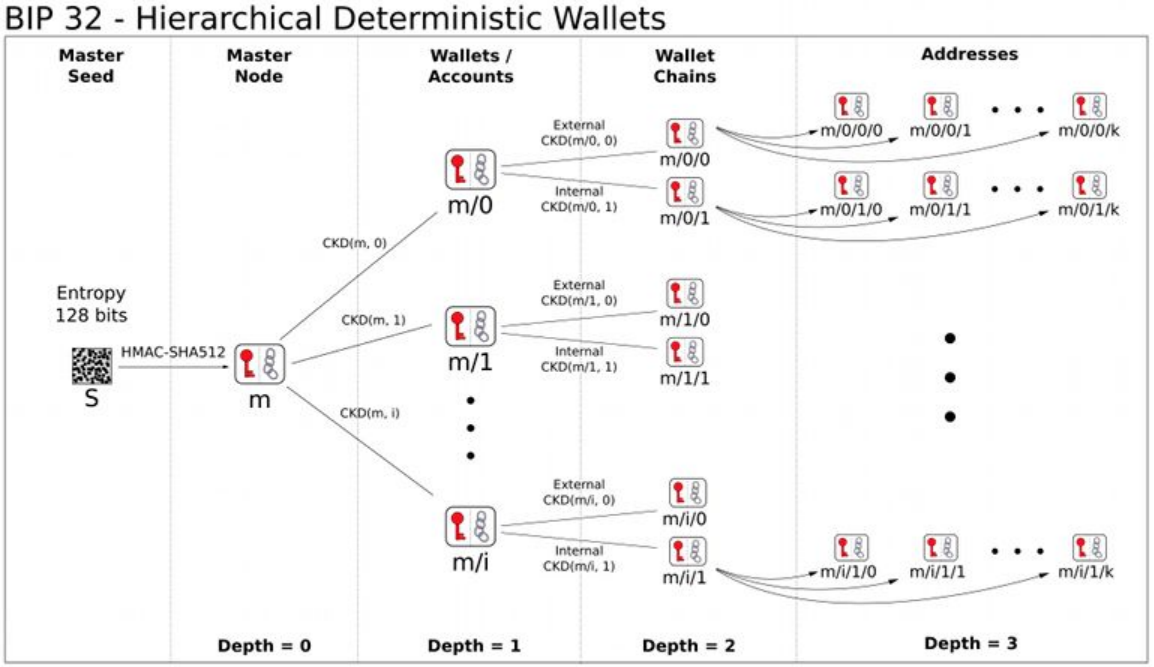
- **BIP:** Bitcoin Improvement Proposal
  - Three types:
    - Standards Track BIPs
    - Informational BIPs
    - Process BIPs
- First BIP proposed by Amir Taaki on 2011-08-19
- Signal support for a BIP by including reference in block when mining



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

QUESTIONS?

BITCOIN WALLETS



AUTHOR: SUNNY AGGARWAL