BITCOIN IRL: WALLETS, MINING, AND MORE

Rustie Lin
Nadir Akhtar

LECTURE OVERVIEW

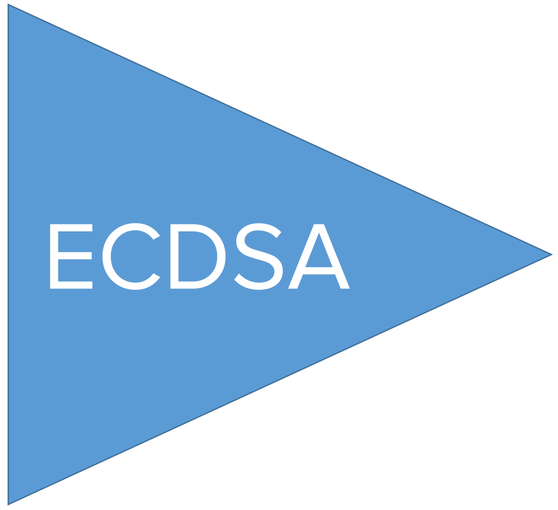
1. WALLET TYPES
2. WALLET MECHANICS
3. MINING INCENTIVES
4. REAL WORLD MINING
5. CHANGING BITCOIN

1 WALLET TYPES

PUBLIC/PRIVATE KEY REVIEW

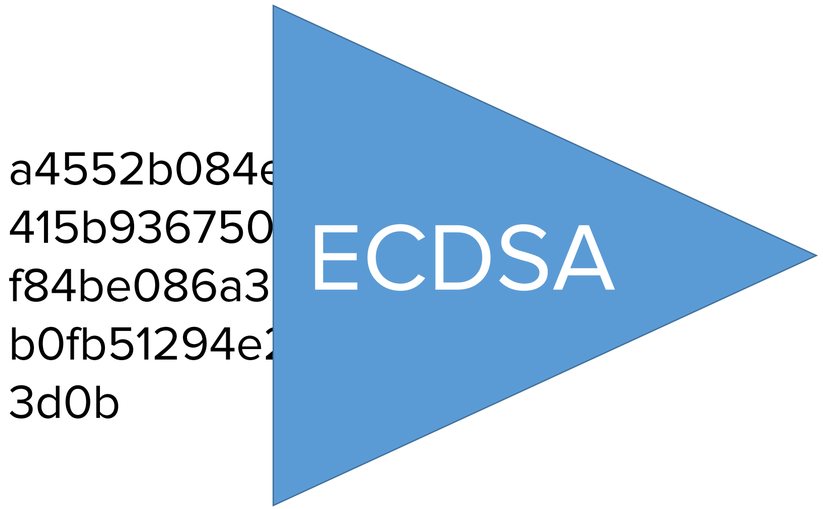
HOW TO GET YOUR PUBLIC KEY

a4552b084ed7314
415b9367502124b
f84be086a393bee
b0fb51294e2a378
3d0b



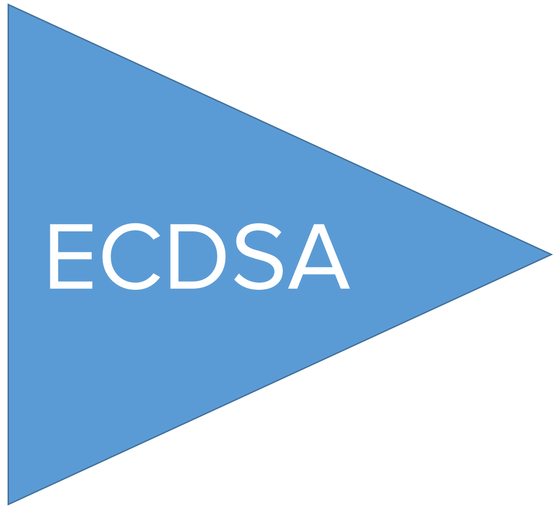
PUBLIC/PRIVATE KEY REVIEW

HOW TO GET YOUR PUBLIC KEY



PUBLIC/PRIVATE KEY REVIEW

HOW TO GET YOUR PUBLIC KEY



98cfe008e1fbfc74
770fb828531e18b
a4c19a0edd20ceb
8fc2396ba436ad6
a1c

PUBLIC/PRIVATE KEY REVIEW

BASE 58

ABCDEFGHIJKLMNOPQRSTUVWXYZ	26
abcdefghijklmnopqrstuvwxyz	26
1234567890	10
	62

PUBLIC/PRIVATE KEY REVIEW

BASE 58

ABCDEFGH JKLMN PQRSTUVWXYZ	24	Omit 0, O, l, I
abcdefghijklmn pqrstuvwxyz	25	
123456789	9	
	58	

BITCOIN WALLETS

KEY MANAGEMENT

a4552b084ed7314415b936750212
4bf84be086a393beeb0fb51294e2
a3783d0b

98cfe008e1fbfc74770fb828531e18
ba4c19a0edd20ceb8fc2396ba436
ad6a1c

Operations depend on identity, so....

How do we manage all of our keys?

BITCOIN WALLETS

WALLET TYPES

- What do wallets do?
  - Keep track of your private key
  - Store, send & receive, and list transactions
- 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

BRAIN WALLETS

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

- 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.
- No way to rate-limit brute force attempts.

BITCOIN WALLETS

KEY STRETCHING

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

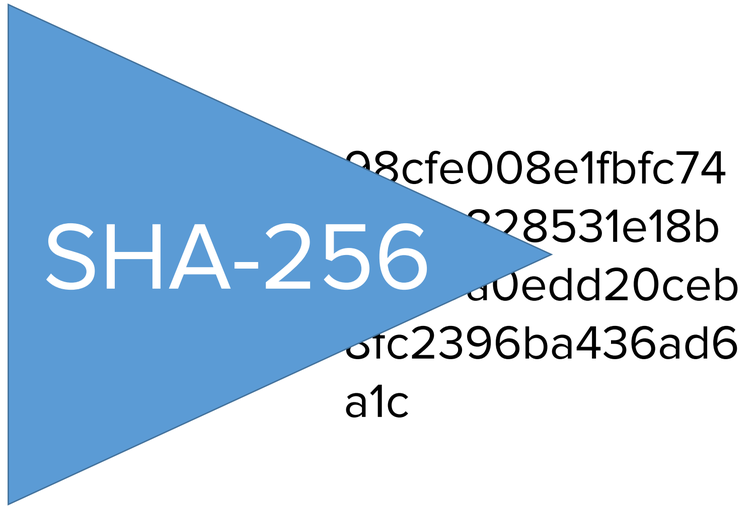
BITCOIN WALLETS

KEY STRETCHING

multi
subm
adjus
fuel r
chair

BITCOIN WALLETS

KEY STRETCHING



BITCOIN WALLETS

KEY STRETCHING

98cfe008e1fbfc74
770fb828531e18b
a4c19a0edd20ceb
8fc2396ba436ad6
a1c

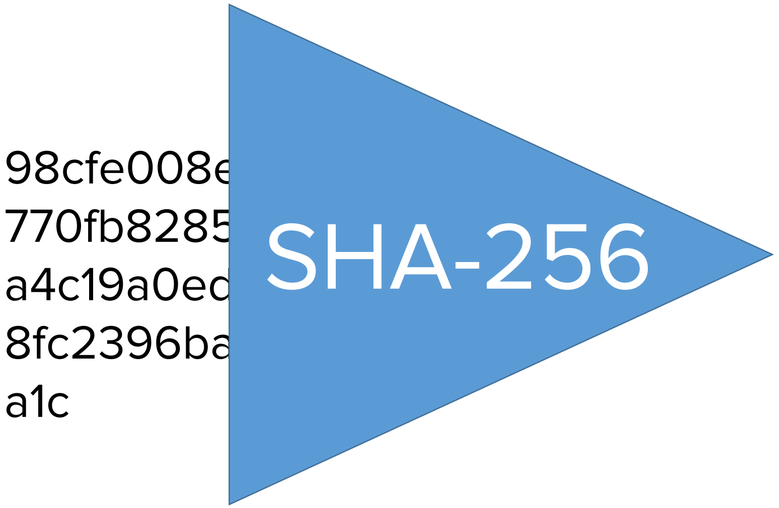
BITCOIN WALLETS

KEY STRETCHING

98cfe008e1fbfc74
770fb828531e18b
a4c19a0edd20ceb
8fc2396ba436ad6
a1c

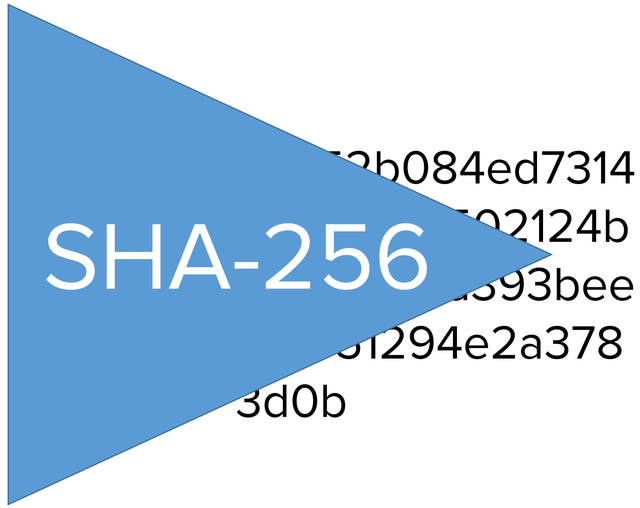
BITCOIN WALLETS

KEY STRETCHING



BITCOIN WALLETS

KEY STRETCHING



BITCOIN WALLETS

KEY STRETCHING

a4552b084ed7314
415b9367502124b
f84be086a393bee
b0fb51294e2a378
3d0b

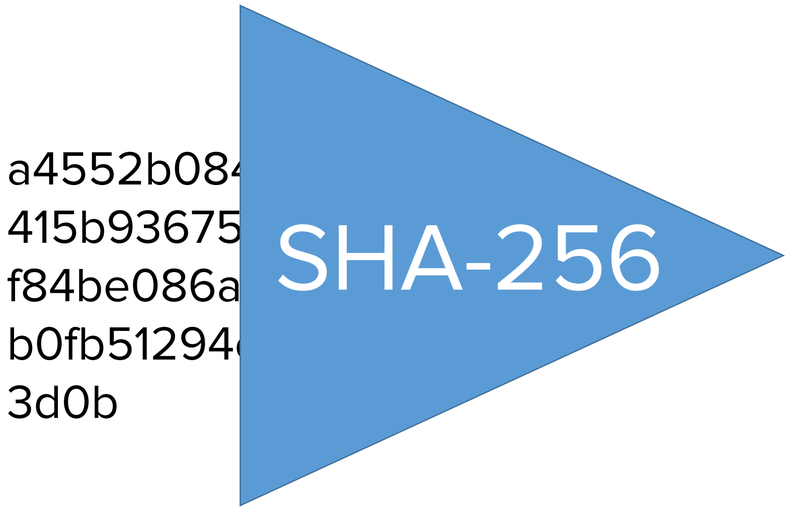
BITCOIN WALLETS

KEY STRETCHING

a4552b084ed7314
415b9367502124b
f84be086a393bee
b0fb51294e2a378
3d0b

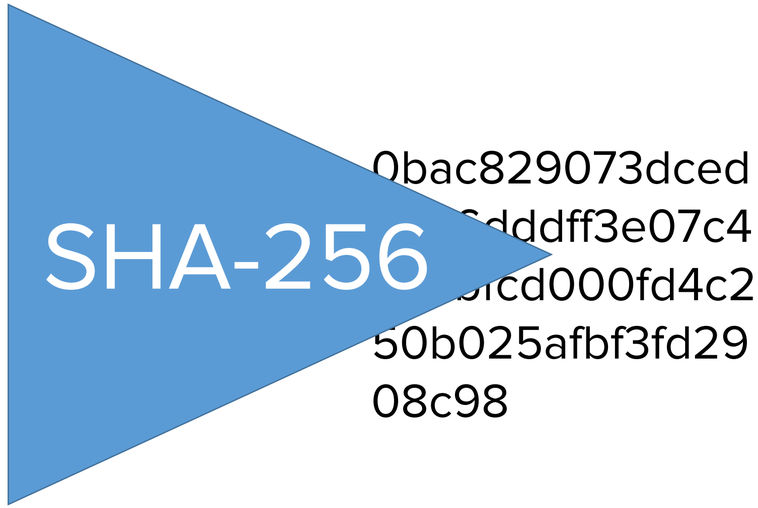
BITCOIN WALLETS

KEY STRETCHING



BITCOIN WALLETS

KEY STRETCHING



BITCOIN WALLETS

KEY STRETCHING

0bac829073dced
edb6dddff3e07c4
8d3bfcd000fd4c2
50b025afbf3fd29
08c98

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

BITCOIN WALLETS

WALLET OPTIONS

Coinbase Wallet

They hold private keys

Can call if you forget password

Mycelium & Electrum

You alone hold private keys

No recourse if lost

Case Wallet

2 / 3 Signatures

Device, Case service, & separate backup company

Green Address

2 / 2 Signatures

2-factor Authorization

Spending Limits

HOW DO I GET BITCOIN?

??????????

But how do I get bitcoins?

HOW DO I GET BITCOIN?

BITCOIN ATMS

Instant

Bitcoin is transferred immediately

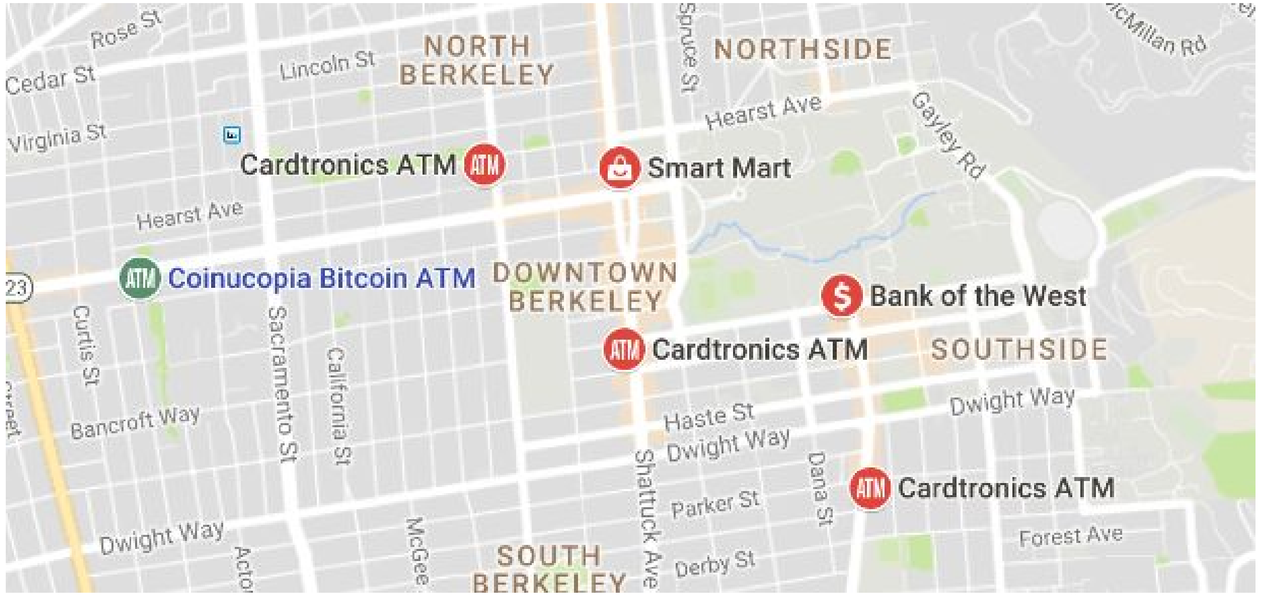
Available

Buy bitcoin whenever you are ready

Simple

Three easy steps

1250 University Ave.



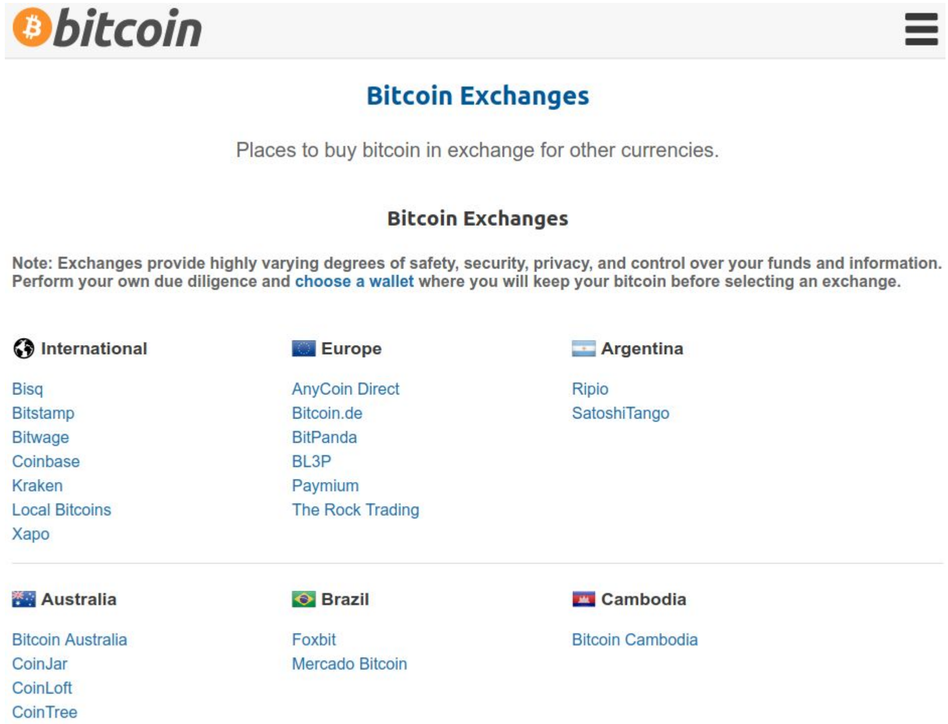
HOW DO I GET BITCOIN?

EXCHANGES

https://bitcoin.org/en/exchanges
(Do your own due diligence)

Trading between different types of currency

Centralized and decentralized exchanges, security, easy of access, etc.



HOW DO I GET BITCOIN?

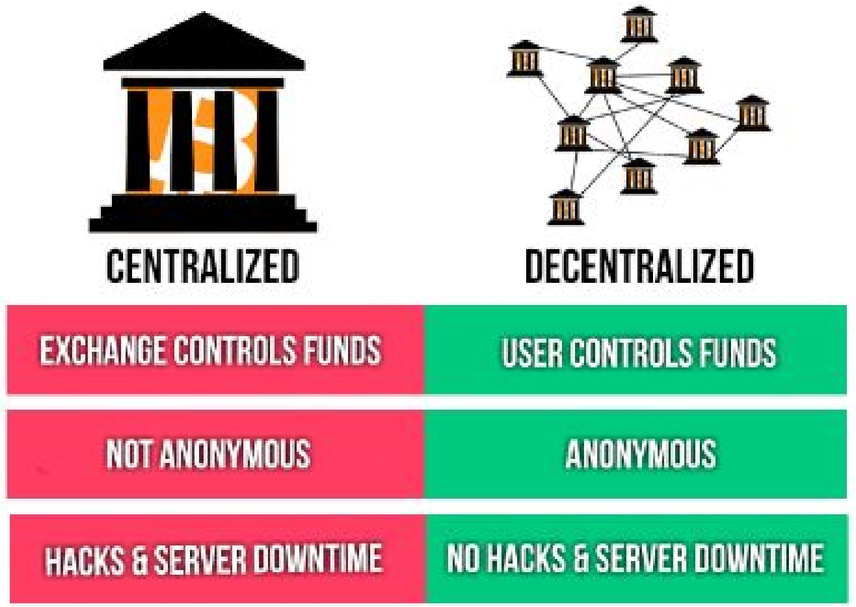
DECENTRALIZED EXCHANGES

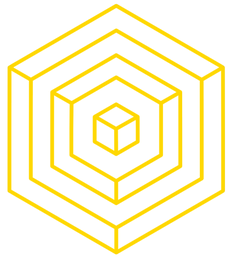
Don’t rely on a third party service to hold customer’s funds

Trades are P2P

Trustless

Bitsquare, Bitshares, Openledger, NXT, CounterParty, etc.





2 WALLET MECHANICS

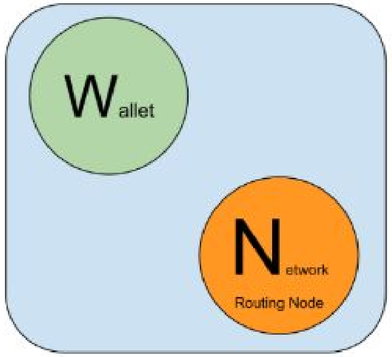
SIMPLE PAYMENT VERIFICATION

THIN CLIENTS

A 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



Lightweight (SPV) wallet

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

SIMPLE PAYMENT VERIFICATION

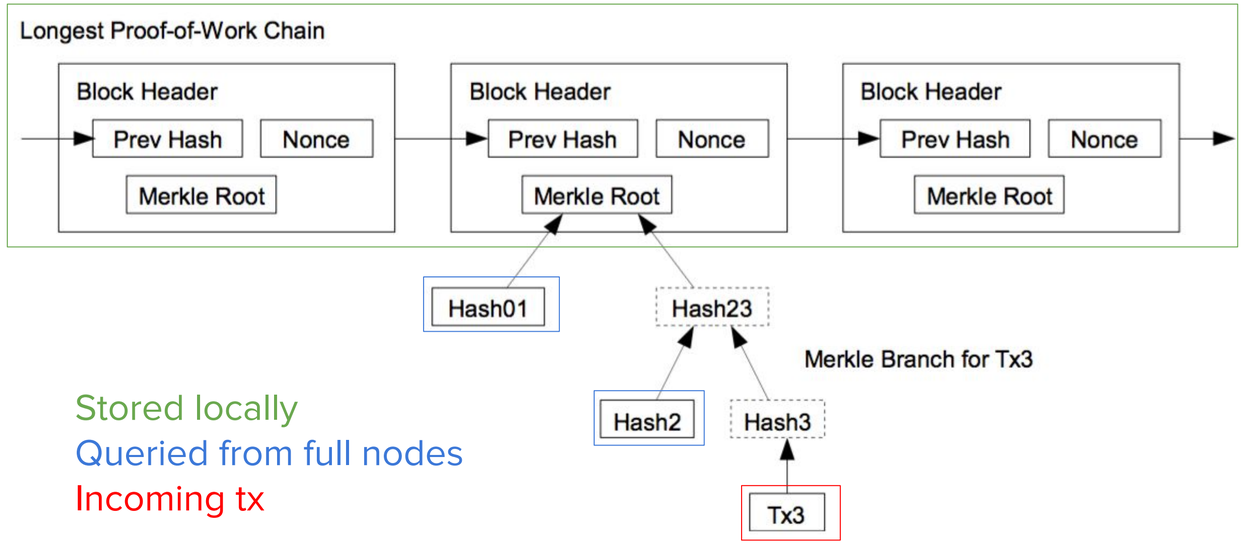
THIN CLIENTS

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



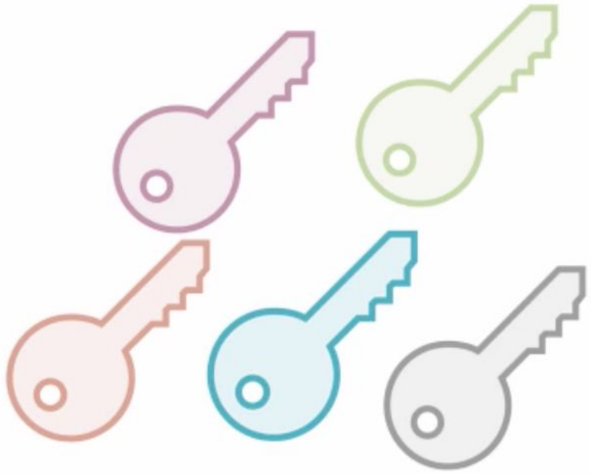
MULTISIGNATURE
M-OF-N TRANSACTIONS

Multi-person Account Access

Regular Bitcoin Addresses

Each account has 1 key (or seed)

Any single person can steal funds



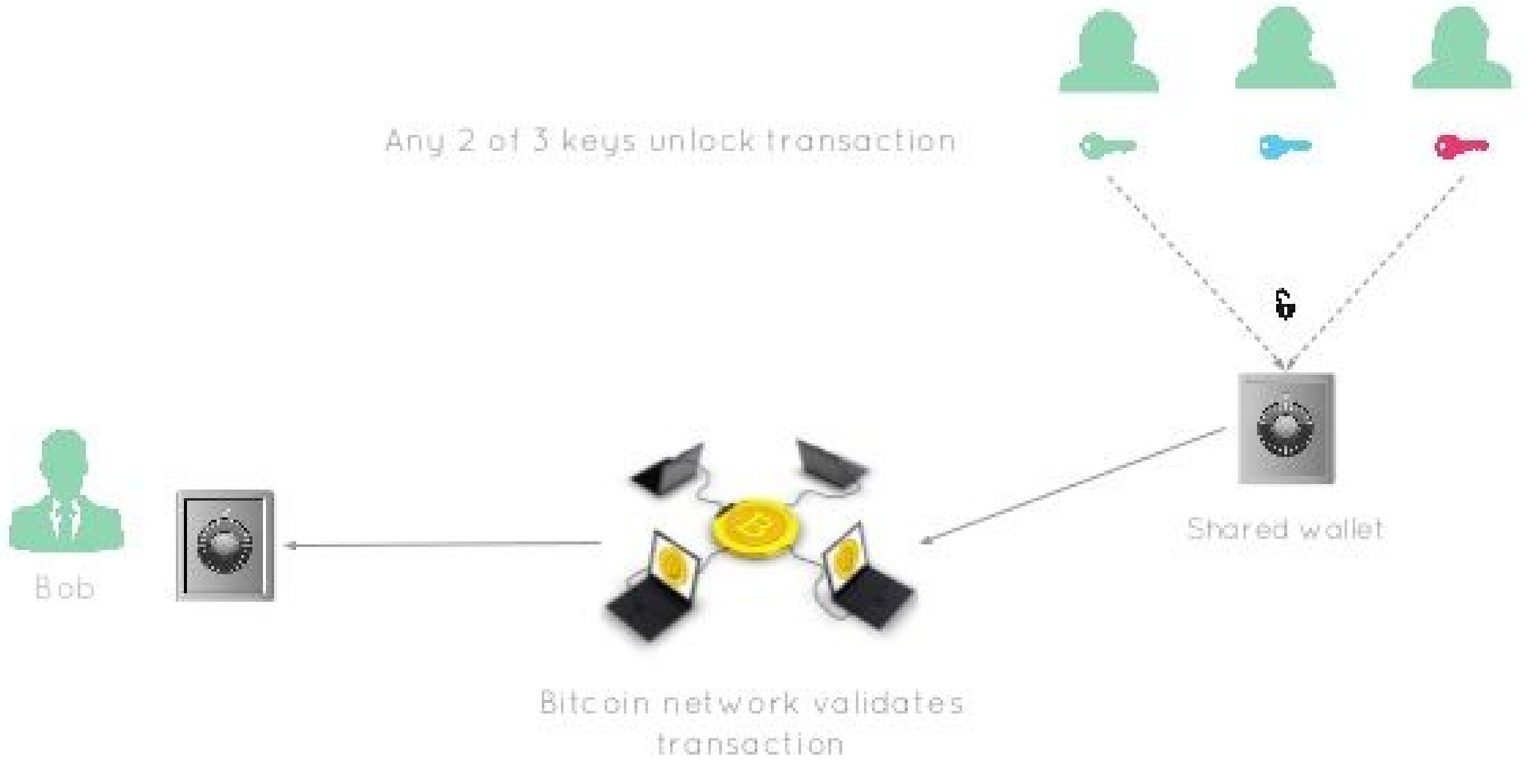
Multisignature Addresses

Multiple signatures needed

Ex: 3 of 5 signatures

BITCOIN MECHANICS

MULTISIG TRANSACTION



BITCOIN MECHANICS

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 address

Or, generate a bunch of keys when first started

Not too convenient because you have to store every key

WALLET BACKUPS

HD WALLETS

HD (Hierarchical Deterministic) Wallets

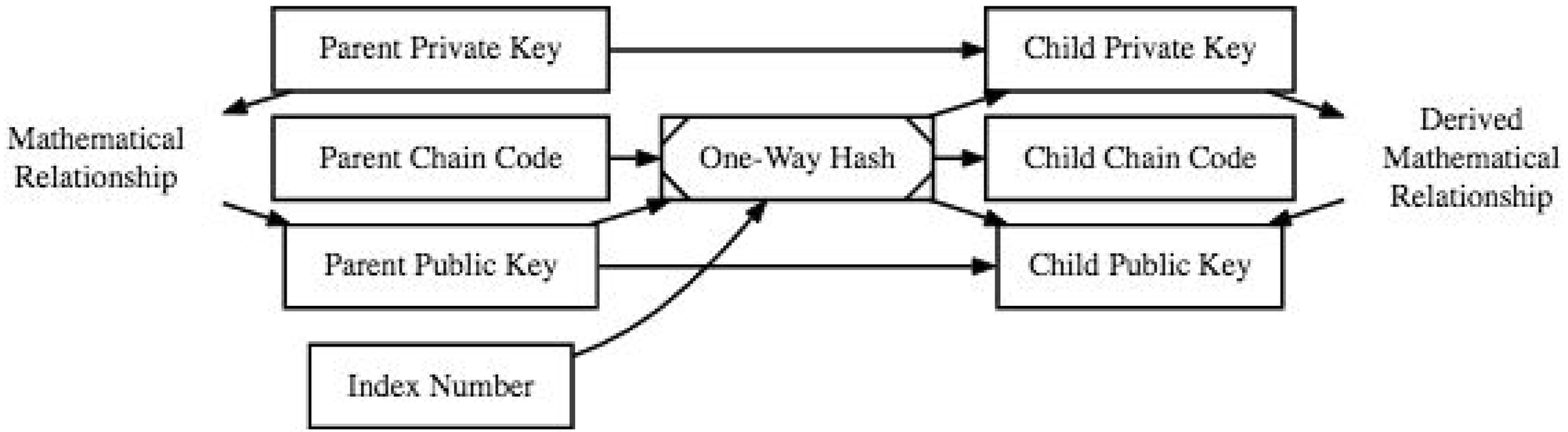
Deterministic, and more convenient to know a seed, or master key

Use a one-way hash function with seed, index number, and optional chain code (just some more entropy)

Exchanges use these

BITCOIN WALLETS

WALLET BACKUPS

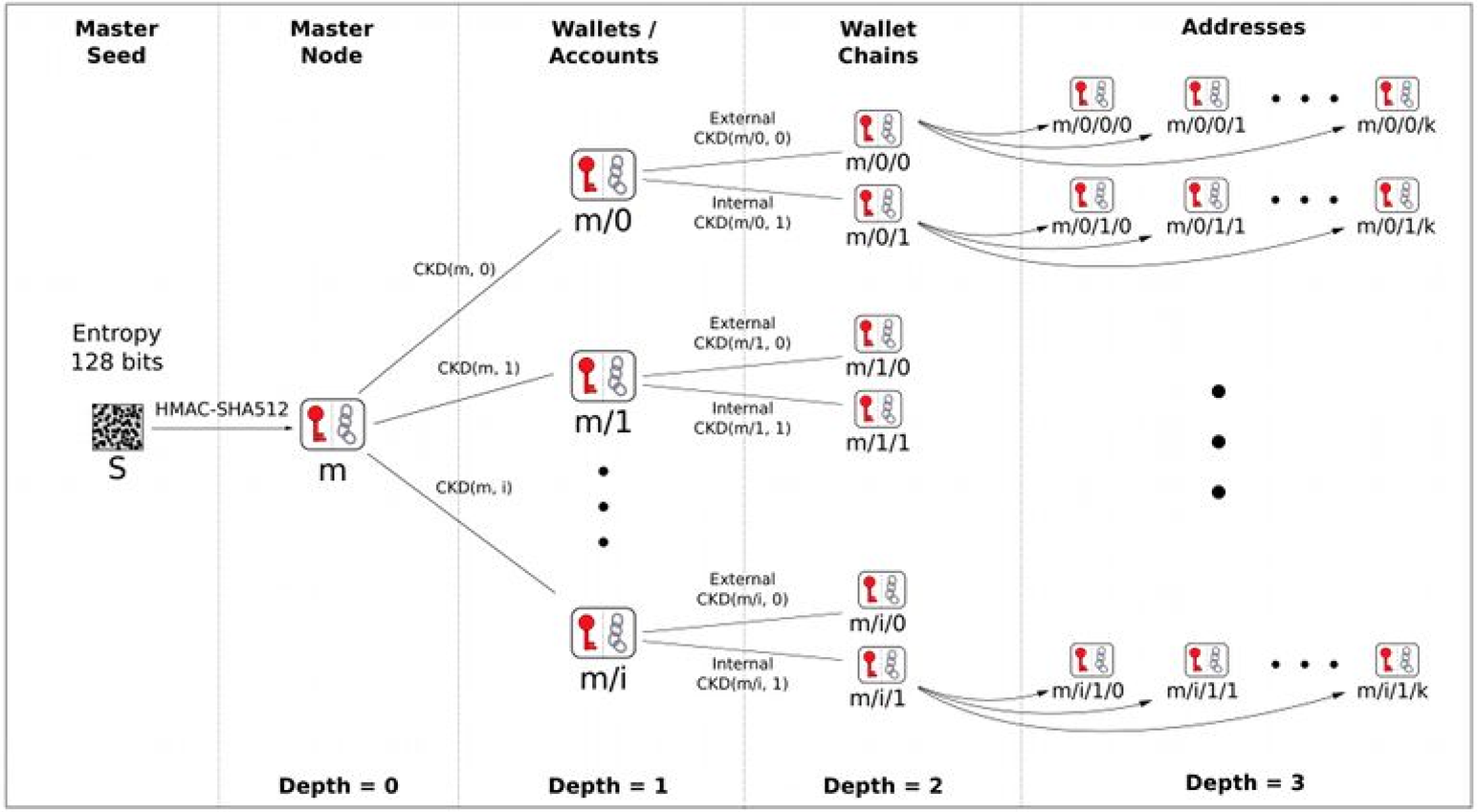


Normal Hierarchical Deterministic (HD) Key Derivation (BIP32)

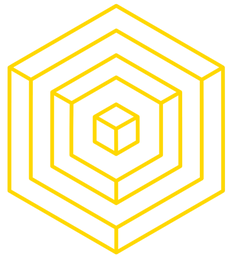
BITCOIN WALLETS

WALLET BACKUPS

BIP 32 - Hierarchical Deterministic Wallets



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



3 MINING INCENTIVES

MINING INCENTIVES

WHY DO WE DO THINGS?

MINING INCENTIVES

WHY DO WE DO THINGS?

PROFIT

MINING INCENTIVES

WHY DO [illegible] THINGS?

MINING INCENTIVES

WHAT IS PROFIT?

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

PROFIT = REVENUE - COST

MINING INCENTIVES

WHAT DOES A MINER DO?

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

- A full-fledged Bitcoin miner (“full node”) must:
  1. **Download** the entire Bitcoin blockchain to store the entire transaction history
  2. **Verify** incoming transactions by checking signatures and confirming the existence of valid bitcoins
  3. **Create** a block using collected valid transactions
  4. **Find** a valid nonce to create a valid block header (the “mining” part)
  5. **Hope** that your block is accepted by other nodes and not defeated by a competitor block
  6. **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

HOW TO PROFIT FROM MINING

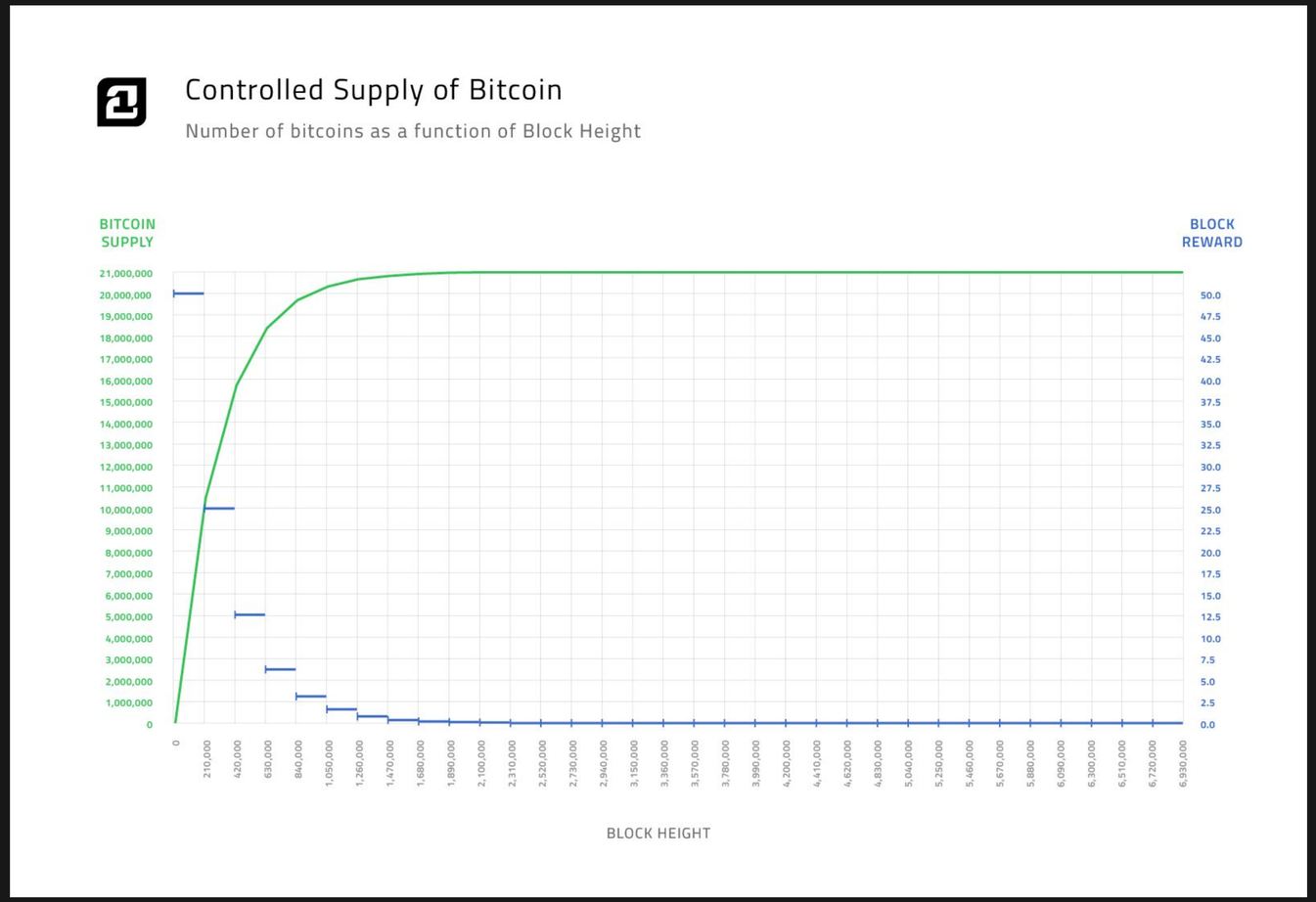
```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

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

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

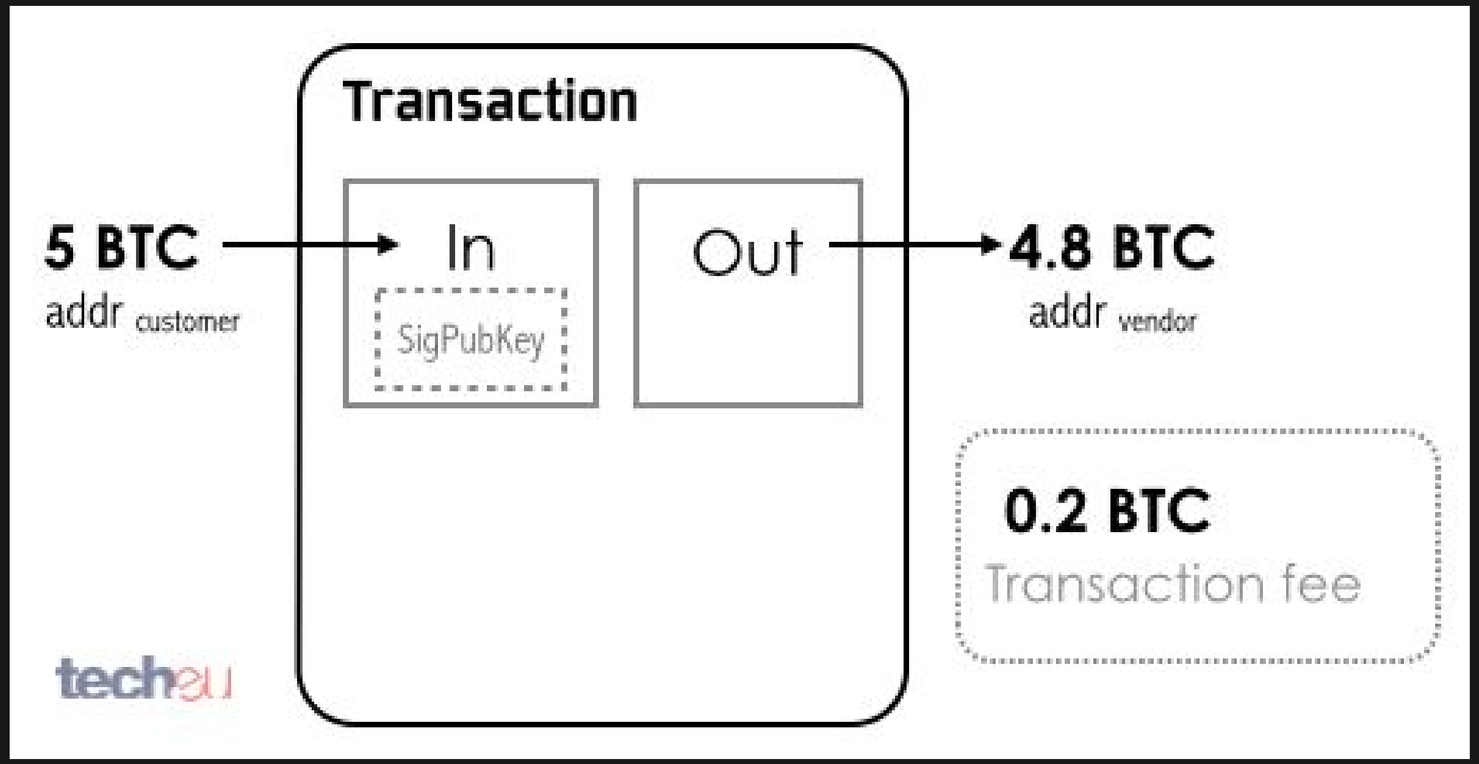
HOW TO PROFIT FROM MINING

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

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

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()
```

MINING INCENTIVES

HOW TO PROFIT FROM MINING

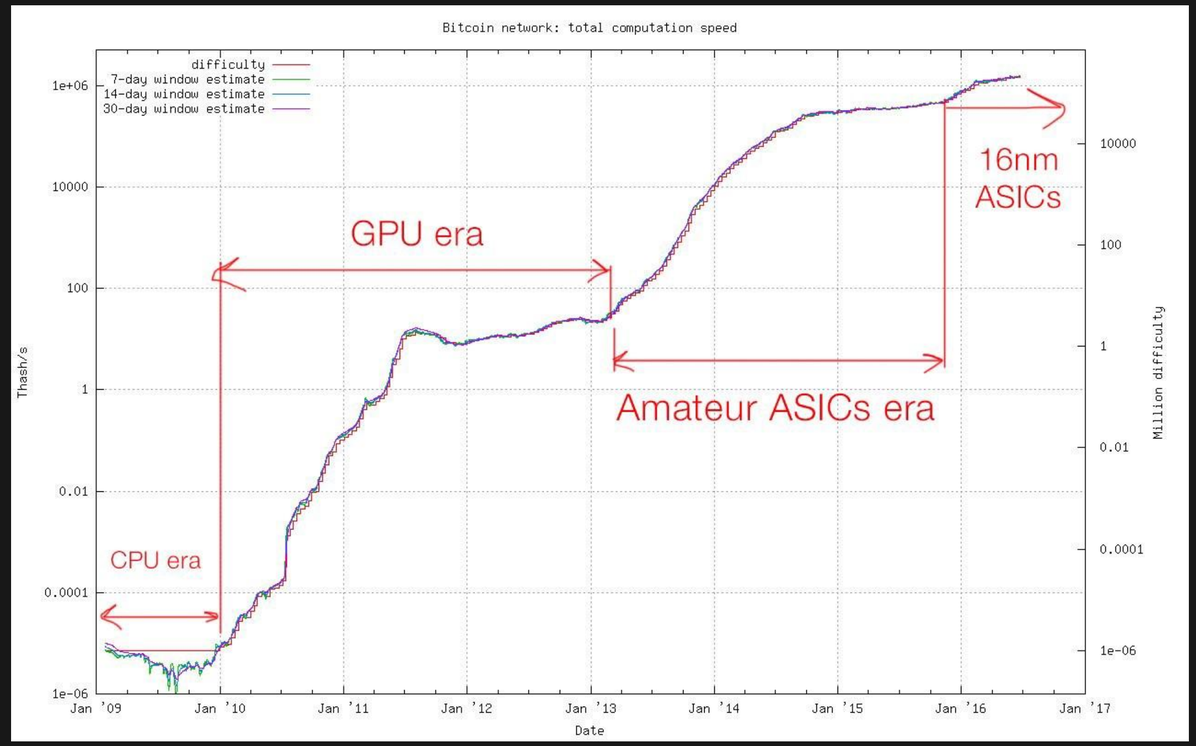
```
MINING_REVENUE = BLOCK_REWARD + TX_FEES
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

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

MINING INCENTIVES

FIXED COST: HARDWARE COSTS

	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
AS OF 9/26/17

MINING INCENTIVES

FIXED COST: CPU 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

```
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	1 billion	152,357
ASIC	14 trillion	10.88

- Order of magnitude faster than CPUs
  - Implying larger consumption of energy and higher production of heat
- Most common ~5 years ago
- Viable for mining Zcash and Ethereum
  - (For now...)
- 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	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
  - Manufacturing ASICs takes large upfront capital, inducing production centralization
- Antminer S9 (14 TH/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()
```

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

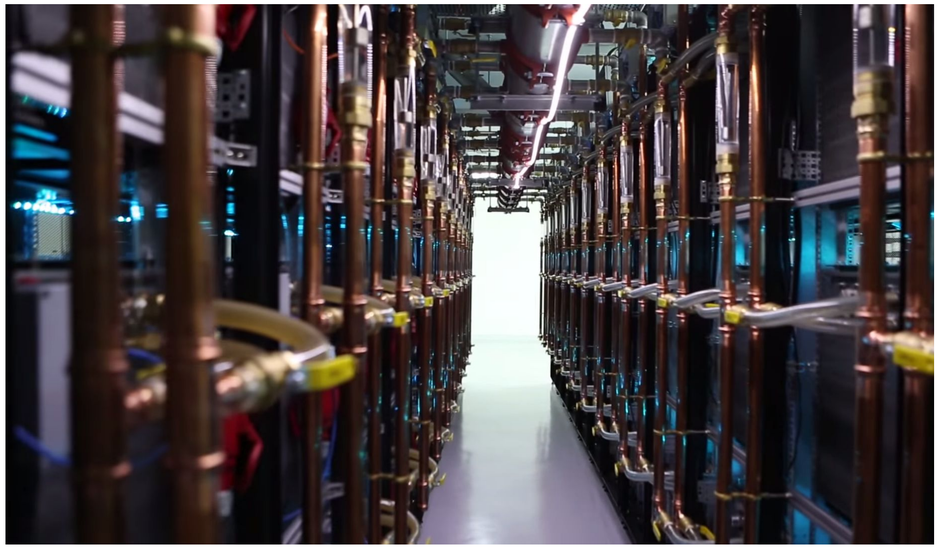
OPERATING COSTS

- 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!

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

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

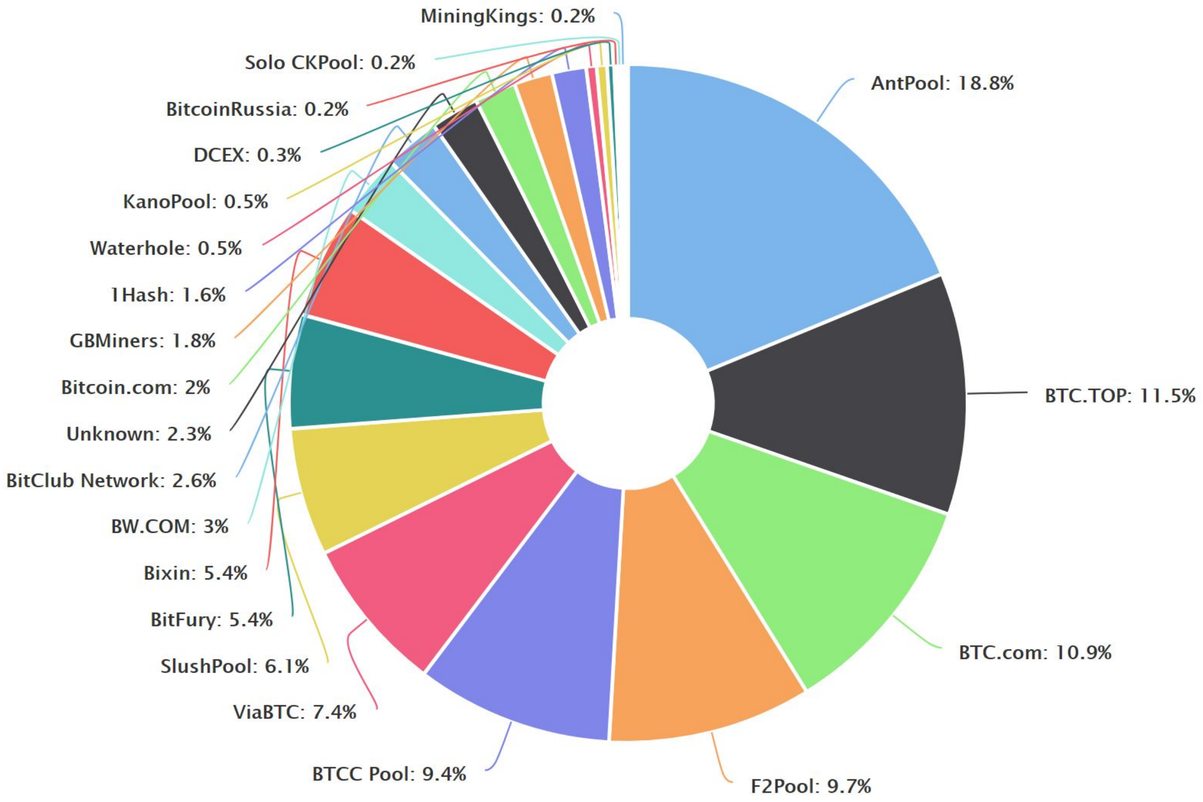
REAL WORLD MINING

MINING POOLS

Source:
blockchain.info (8/21/17)

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 POOLS

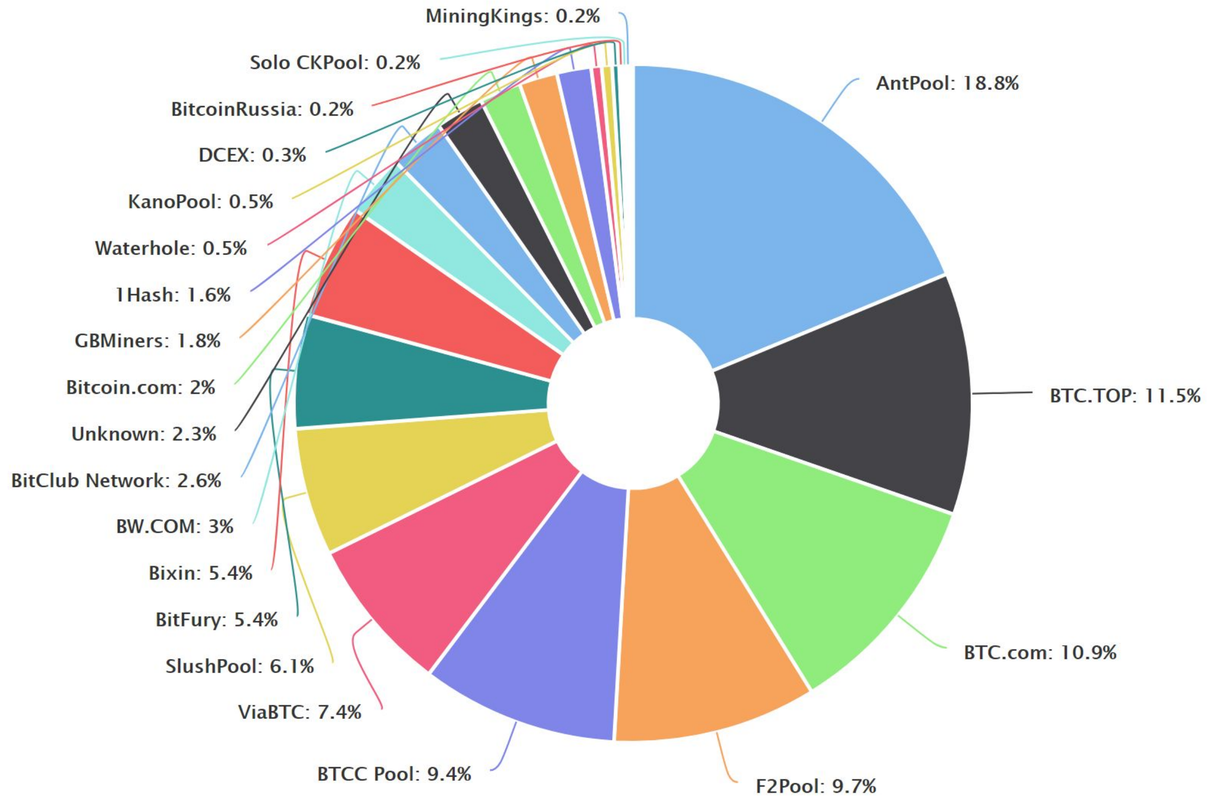
Source:
blockchain.info (8/21/17)

Pros

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

Cons

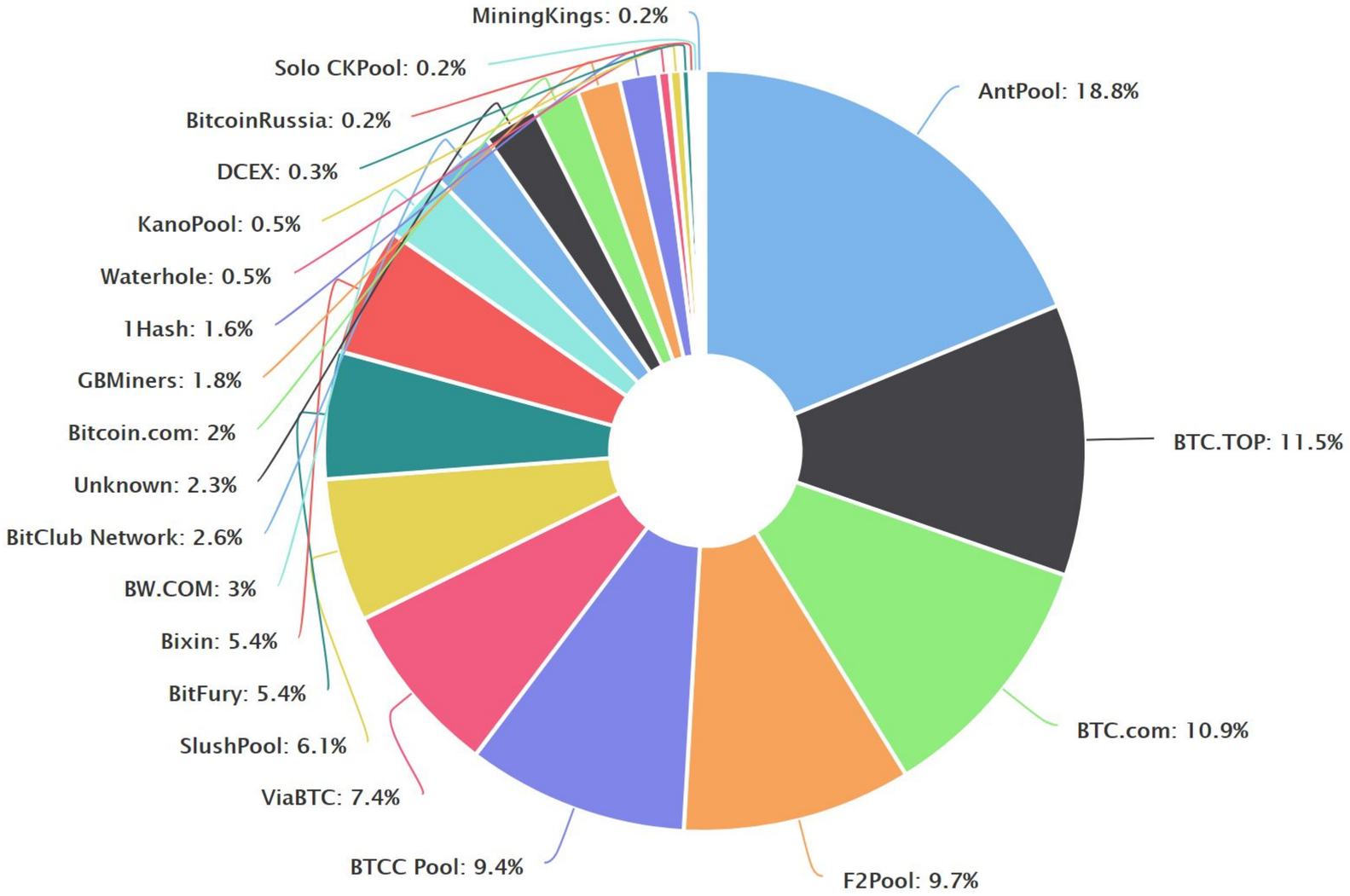
- Pool manager must be trusted
- Centralized
- Enables a multitude of attacks



REAL WORLD MINING

MINING POOLS

Source: blockchain.info (8/21/17)



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 network hashrate: **7,257,882 TH/s**
- Mining Reward / yr = (1 yr / 10 mins) * 12.5 = **657k BTC / yr**
- Assume constant price of $4000

Suppose you want to start mining today.

- Antminer S9: Costs $3000, **14 TH/s**
- **% of network hashrate** = (14 TH/s) / (7,257,882 TH/s) = **0.000192893%**

Expected Annual Reward

- 0.000192893% * 657k /yr
  ≃ 1.27 BTC / yr ≃ **$5080/yr**

Solo mining

- 1 block mined per 571853 blocks
  ⇒ 12.5 BTC every 3972 days
  ⇒ **$50000 once every 10.9 years**

Mining with mining pool

- Assume pool has ⅛ network hashrate
  - Pool finds every 6th block ≃ 1 per hour
- $5080 / 8760 hrs/yr
  ≃ **$0.58 every hour**

Paradox:

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

AUTHOR: MAX FANG
UPDATED BY NADIR AKHTAR

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

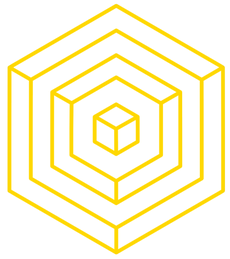
Pool pays out **at every share submitted.** By default will be proportional to work done by individuals

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



5 CHANGING BITCOIN

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”
  - 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

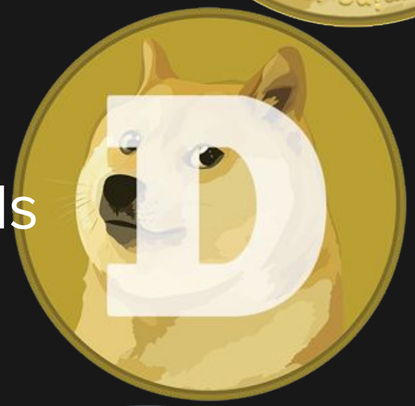
SCRYPT

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

AUTHOR: MAX FANG

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
```

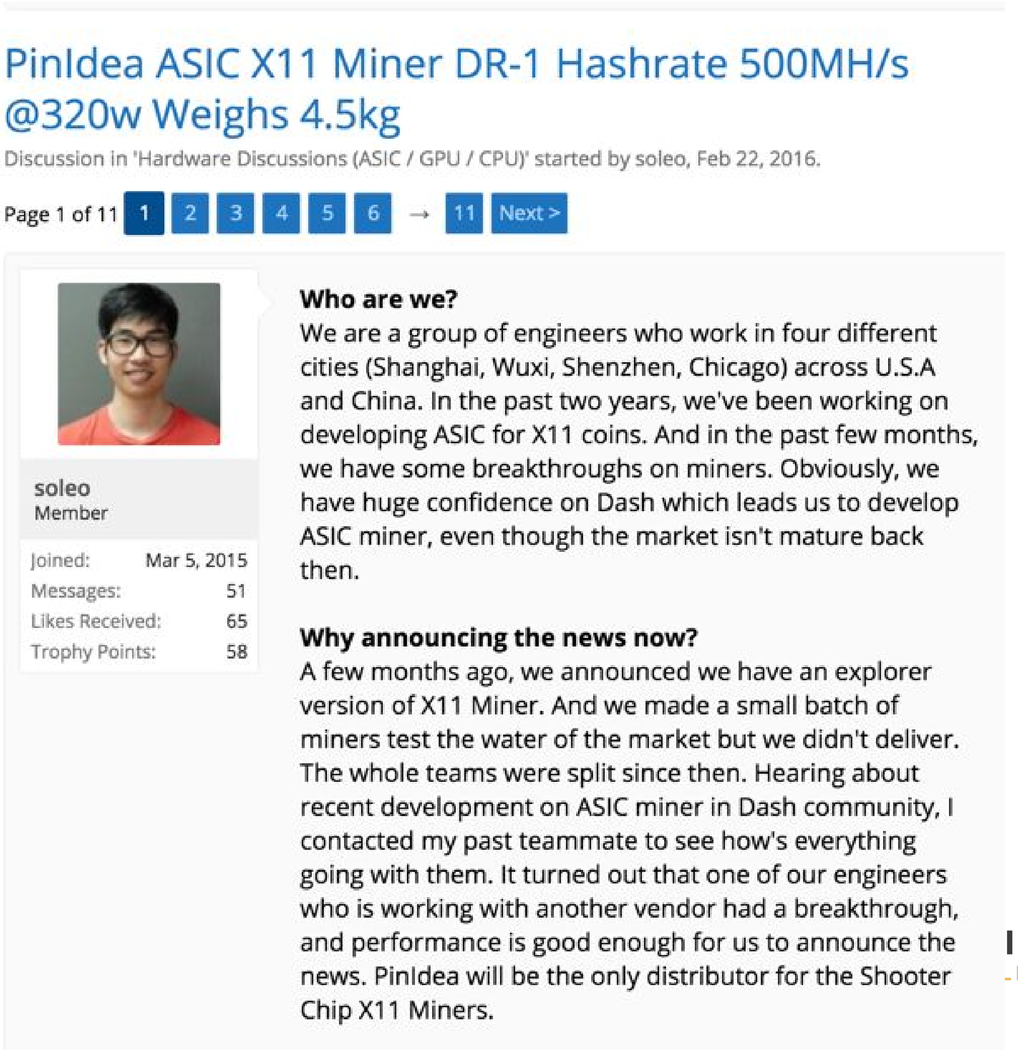
AUTHOR: MAX FANG

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
  - Easy to work around
  - Not implemented

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



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.

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

NON-OUTSOURCEABLE PUZZLES

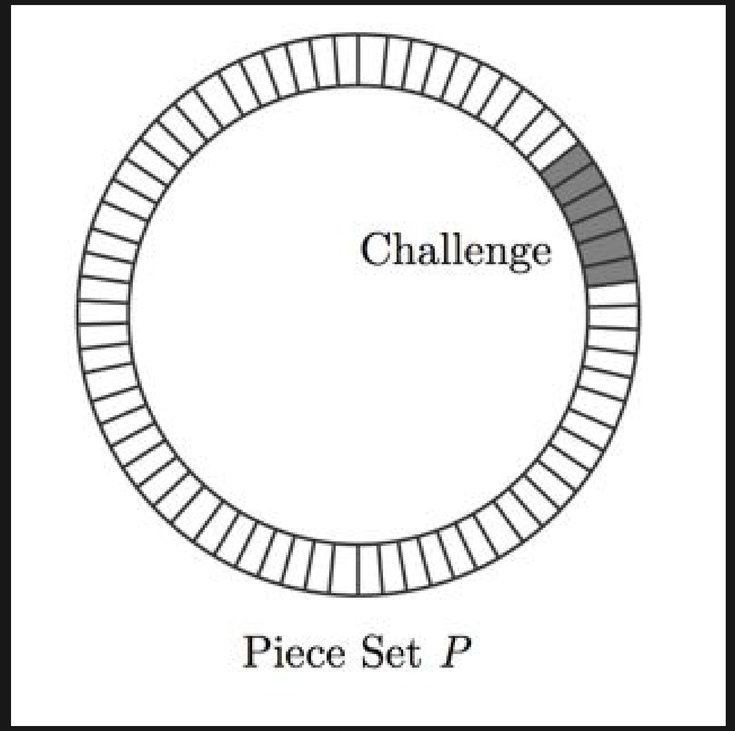
FILECOIN

Image source:
https://filecoin.io/images/filecoin-logo.svg

Filecoin

Allows you to store a large amount of data in a decentralized manner, maintained by a blockchain

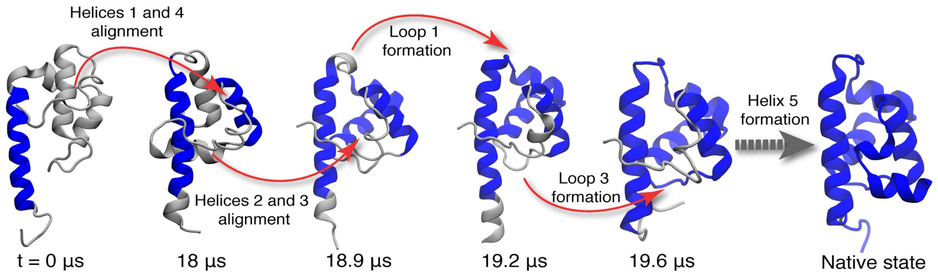
- Maintains a growing set of data pieces **P** and implements **proofs-of-retrievability** as part of its consensus algorithm
  - Finding the solution to the partial hash-preimage puzzle (the standard PoW) yields a partially mined block B', which contains the PoW
- The PoW solution is used as source of randomness; chooses a range of pieces as the **Challenge**, where the number of pieces chosen is a tunable difficulty parameter
- To fully mine the block, must provide:
  - Proof of retrievability of the **challenge**
  - Pieces specified by **Put** transactions
  - Pieces specified by **Get** transactions
- Correctly aligned incentives: No hoarding, even distribution, etc.



AUTHOR: MAX FANG

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

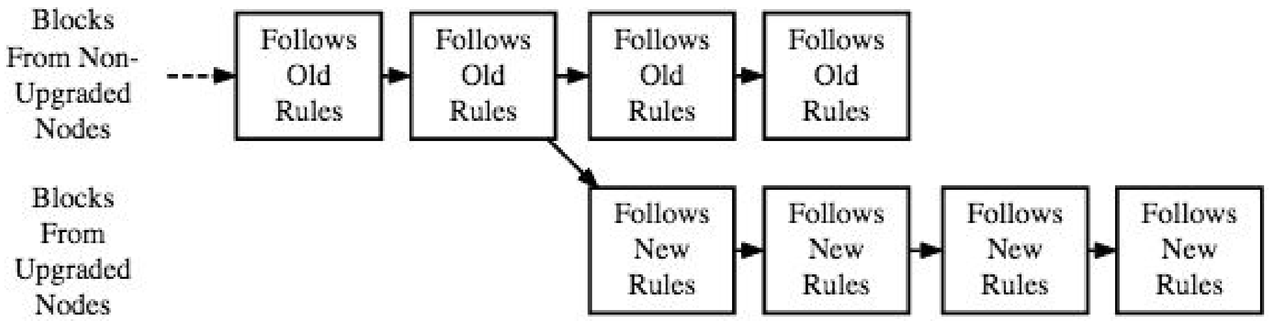
BITCOIN CORE

- **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

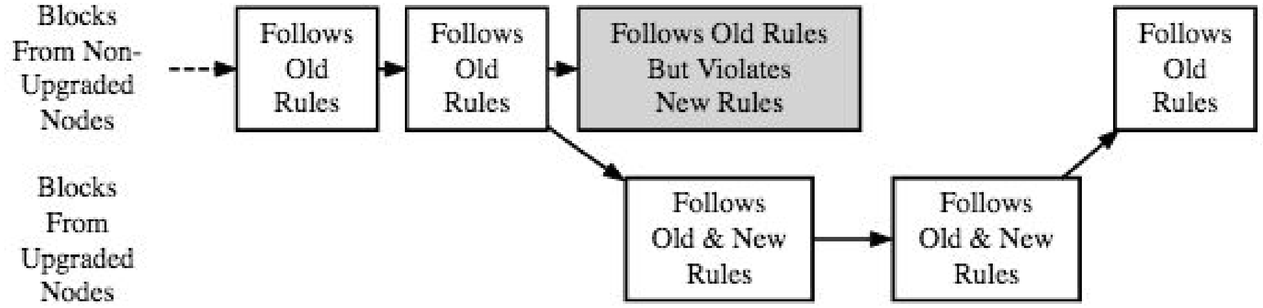
Hard Fork



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

Source: Bitcoin.org Developer Guide

Soft Fork

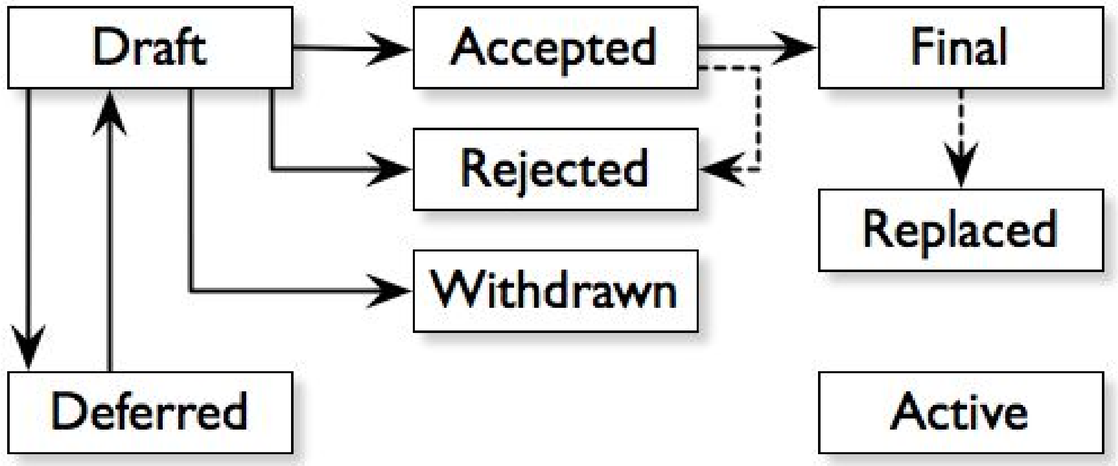


A Soft Fork: Blocks Violating New Rules Are Made Stale By The Upgraded Mining Majority

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

HOMEWORK

- Readings:
  - https://www.coindesk.com/viabtc-mystery-miner-bitcoin-scaling-future/
  - https://www.coindesk.com/antbleed-bitcoins-newest-new-controversy-explained/
  - Ethereum whitepaper up to “Miscellanea...”: https://github.com/ethereum/wiki/wiki/White-Paper
  - (Optional) https://medium.com/bitcoinfoundation/verified-chatlogs-why-jihan-and-jiang-want-to-block-segwit-at-all-cost-bbf068c5ce0f
  - (Optional) https://bitcoinwisdom.com/bitcoin/difficulty
    - Play around with different variables!
- HW:
  - Argue! Debate on one of two topics (check Piazza for submission instructions):
    - ASIC-Resistance
    - Who controls Bitcoin (if anyone)