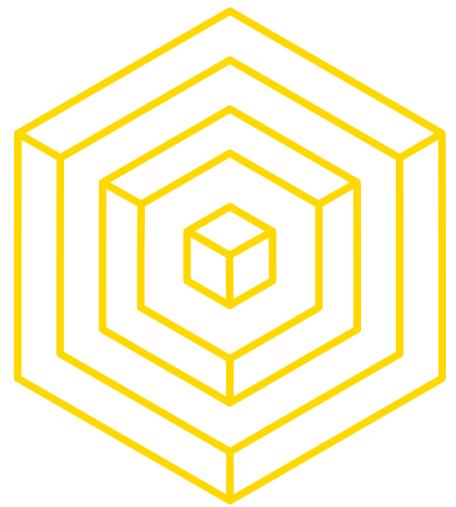


BITCOIN IRL: WALLETS, MINING, AND MORE

Noah Alcus
Jason Bi

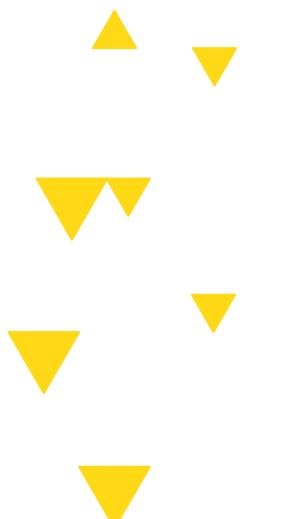


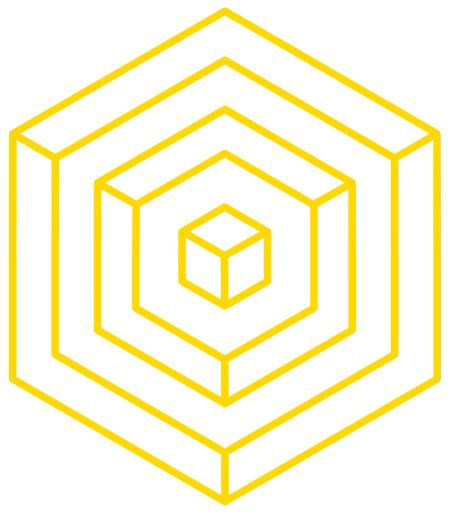
BLOCKCHAIN
AT BERKELEY



LECTURE OVERVIEW

- 1 ► **WALLET TYPES**
- 2 ► **WALLET MECHANICS**
- 3 ► **MINING**
- 4 ► **REAL WORLD MINING**
- 5 ► **CHANGING BITCOIN**

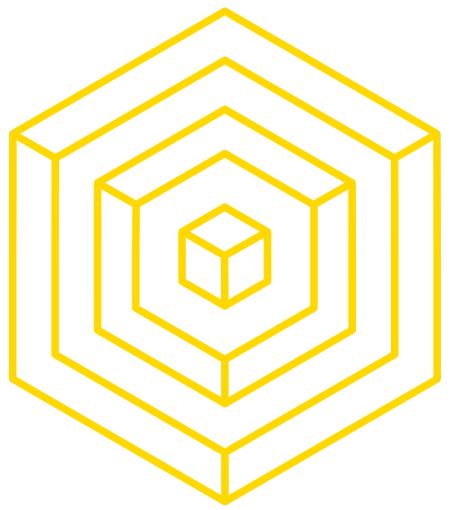




1

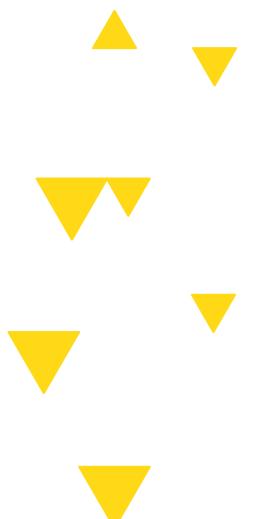
WALLET TYPES

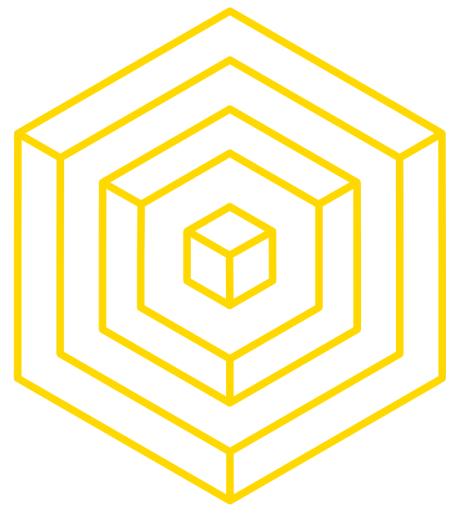
BLOCKCHAIN FUNDAMENTALS LECTURE 4



1.1

PUBLIC & PRIVATE KEY REVIEW

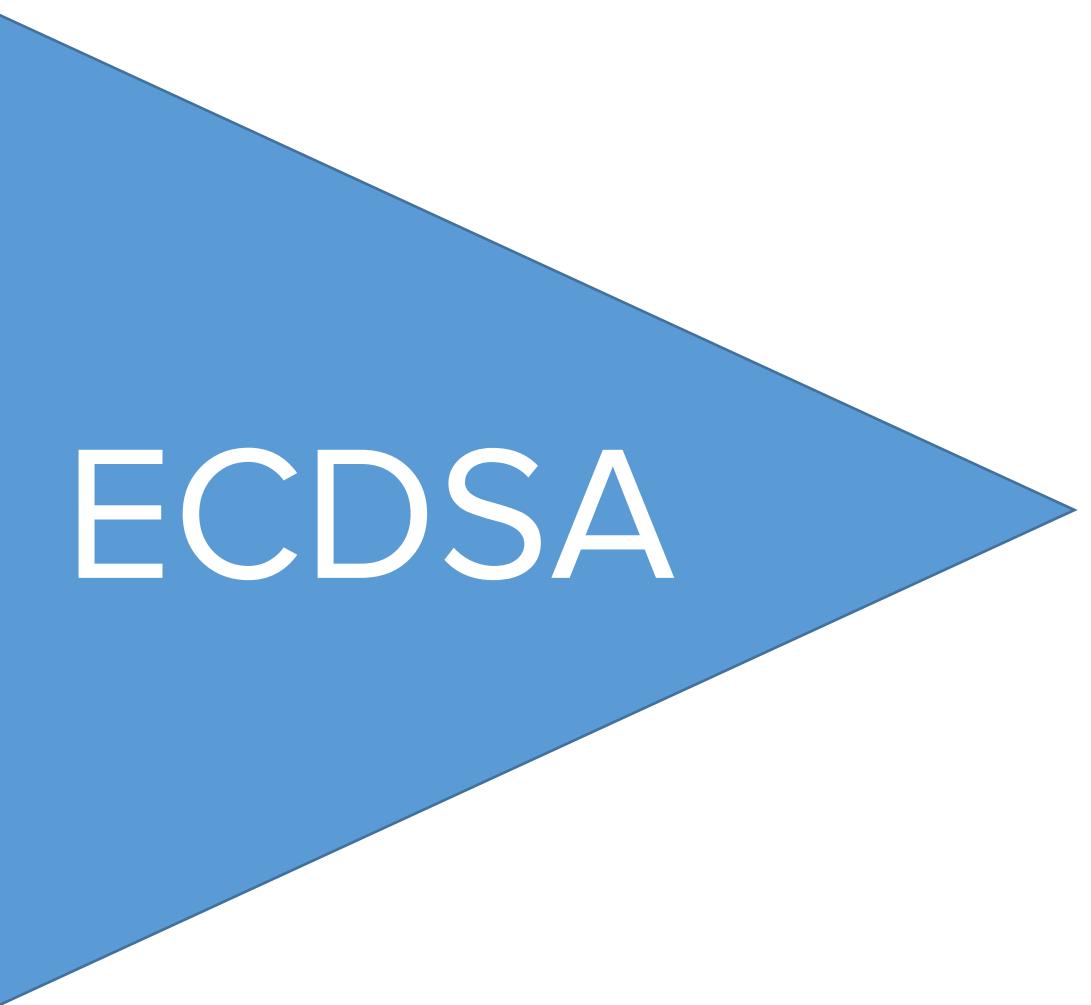




PUBLIC/PRIVATE KEY REVIEW

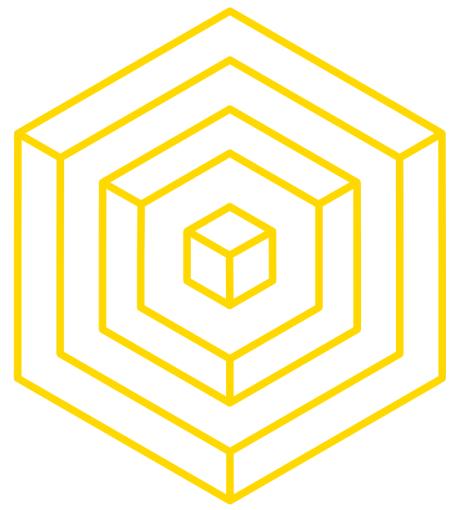
HOW TO GET YOUR PUBLIC KEY

a4552b084ed7314
415b9367502124b
f84be086a393bee
b0fb51294e2a378
3d0b



AUTHOR: SUNNY AGGARWAL

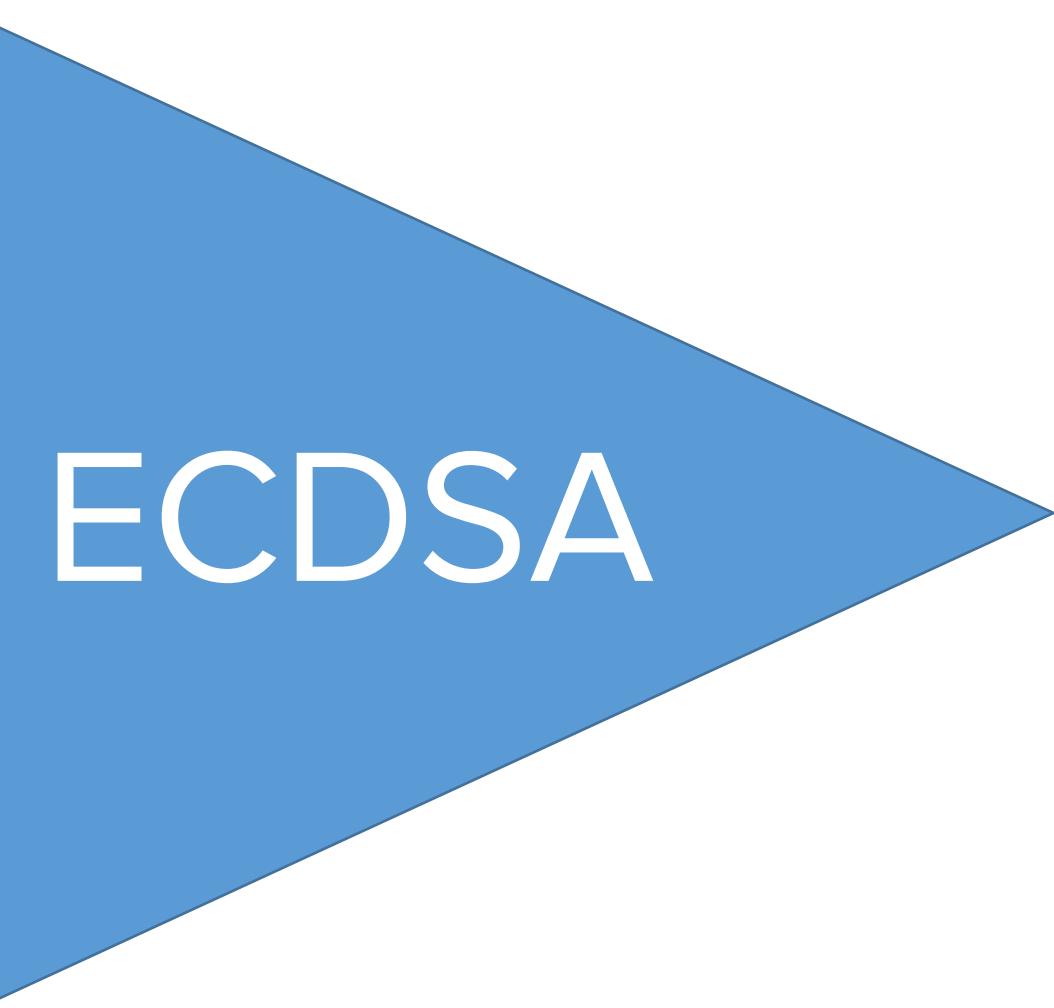
BLOCKCHAIN FUNDAMENTALS LECTURE 4



PUBLIC/PRIVATE KEY REVIEW

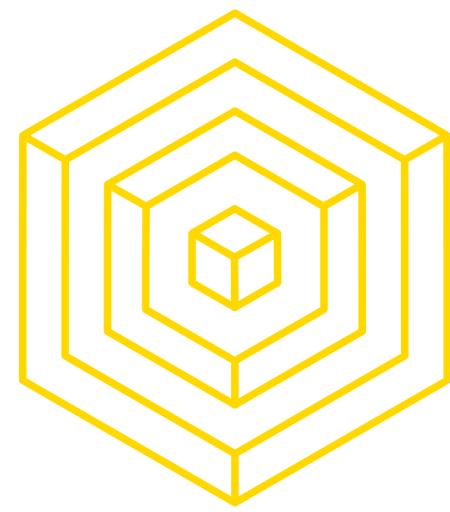
HOW TO GET YOUR PUBLIC KEY

a4552b084e
415b936750
f84be086a3
b0fb51294e2
3d0b



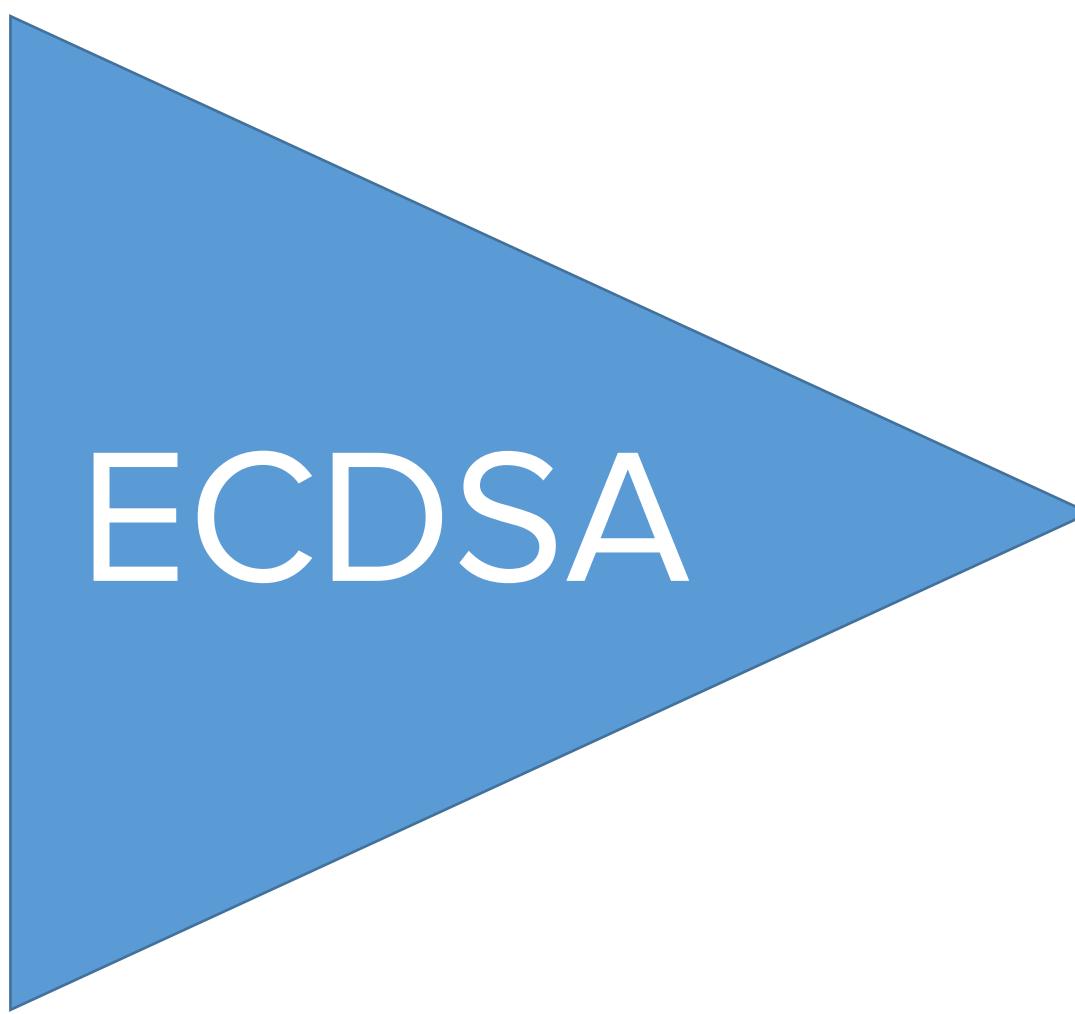
AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4

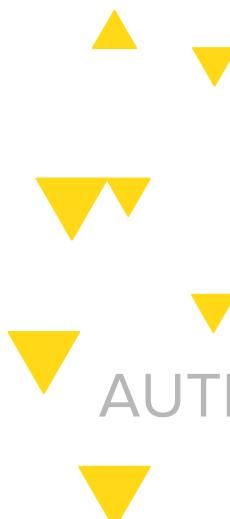


PUBLIC/PRIVATE KEY REVIEW

HOW TO GET YOUR PUBLIC KEY

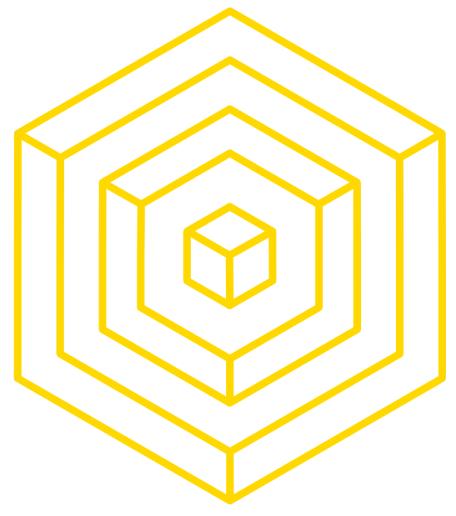


98cfe008e1fbfc74
770fb828531e18b
a4c19a0edd20ceb
8fc2396ba436ad6
a1c



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



PUBLIC/PRIVATE KEY REVIEW

BASE 58

ABCDEFGHIJKLMNOPQRSTUVWXYZ

26

abcdefghijklmnopqrstuvwxyz

26

1234567890

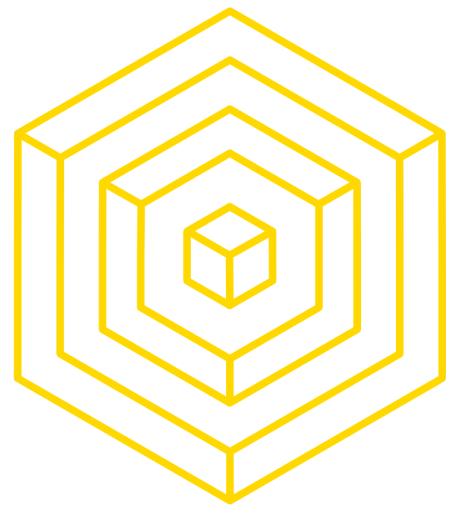
10

62



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



PUBLIC/PRIVATE KEY REVIEW

BASE 58

ABCDEFGH JKLMN PQRSTUWXYZ

abcdefghijklmn pqrstuvwxyz

123456789

24

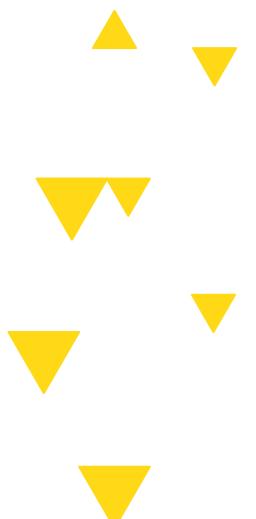
25

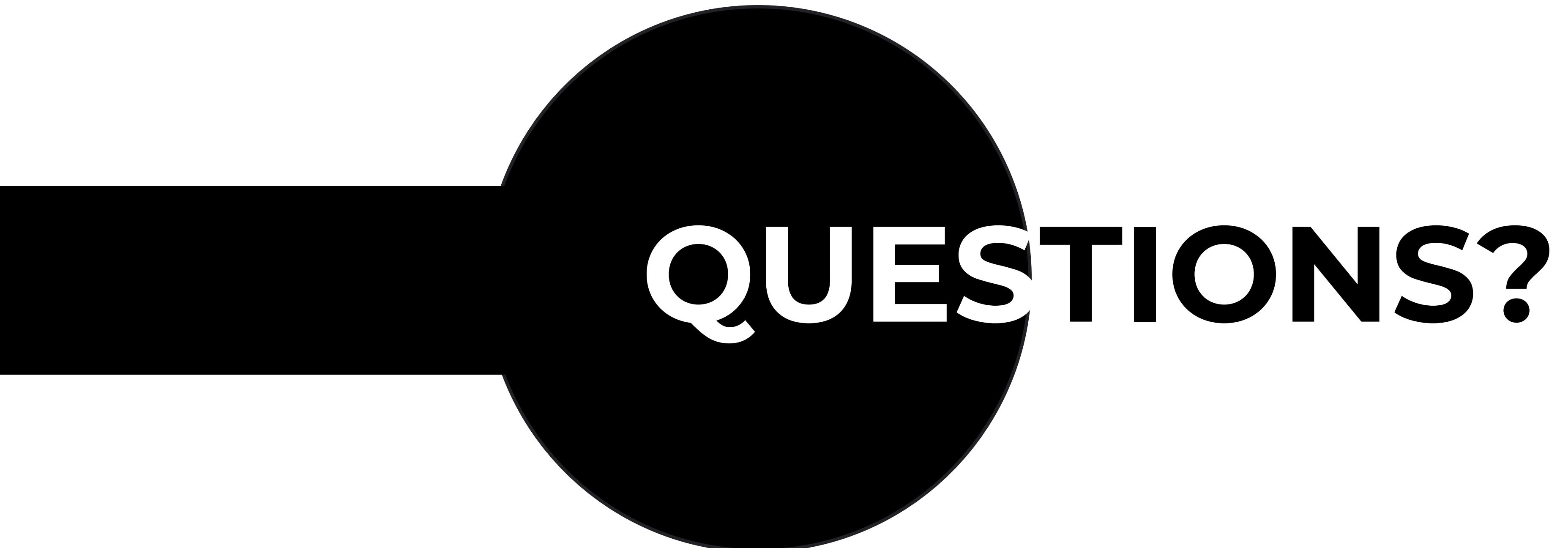
9

58

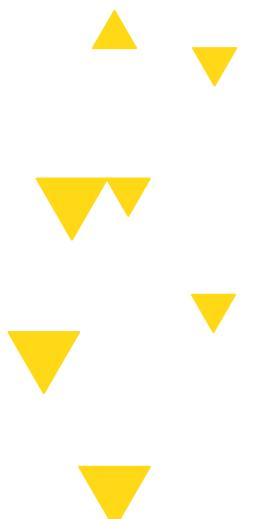
}

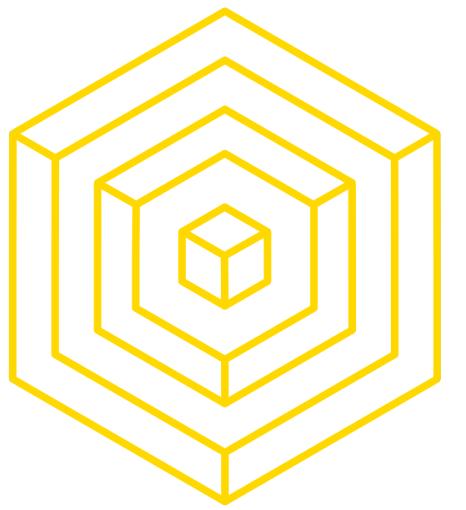
Omit 0, O, l, I



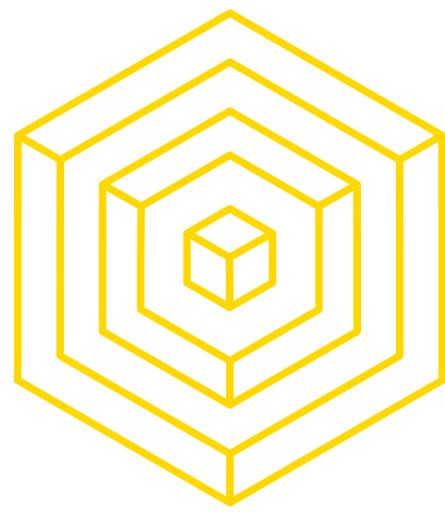


QUESTIONS?





1.2 **WALLETS**



BITCOIN WALLETS

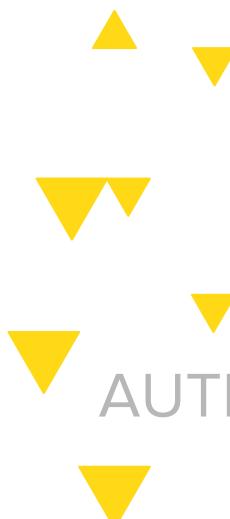
KEY MANAGEMENT

a4552b084ed7314415b936750212
4bf84be086a393beeb0fb51294e2
a3783d0b

98cfe008e1fbfc74770fb828531e18
ba4c19a0edd20ceb8fc2396ba436
ad6a1c

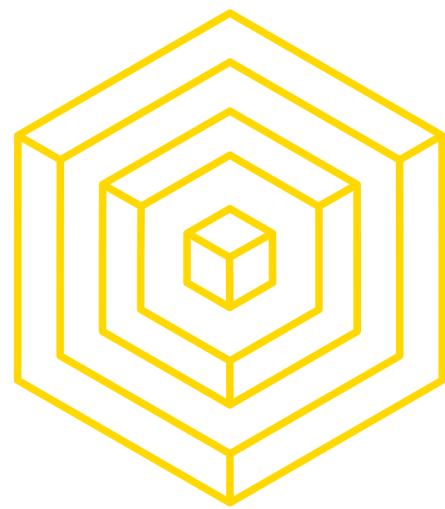
Operations depend on identity, so....

How do we manage all of our keys?



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

WALLET TYPES



What do wallets do?

- Keep track of your private key
- Store, send & receive, and list transactions

Wallet Forms

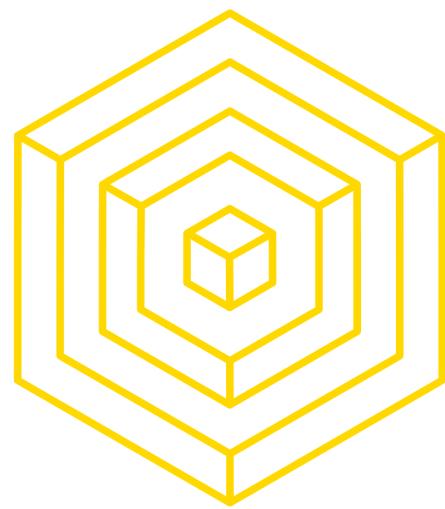
- Smartphone apps
 - [Mycelium](#), AirBitz
- Online web-wallets
 - Blockchain.info, coinbase.com
- Paper Wallets
 - [Bitcoinpaperwallet.com](#)
 - [Bitaddress.org](#)
- Hardware Wallets
 - [Ledger](#), [Trezor](#), [Case](#), [KeepKey](#)
- Brain Wallet

Cold Storage



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

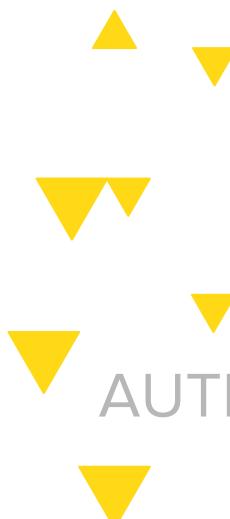
BRAIN WALLETS

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

Convenient way to memorize your private key.

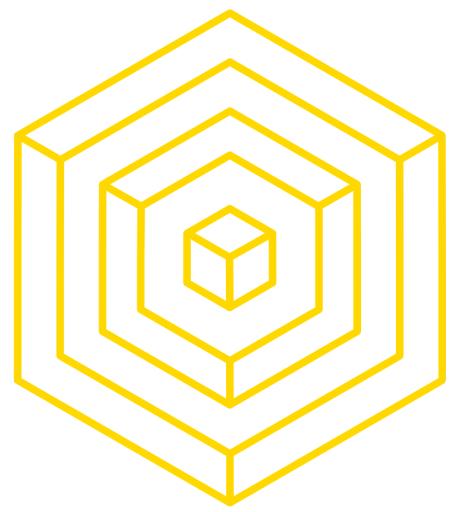
Easier to have something that you can turn into your private key

Not very secure, as humans aren't as random as we think we are.



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

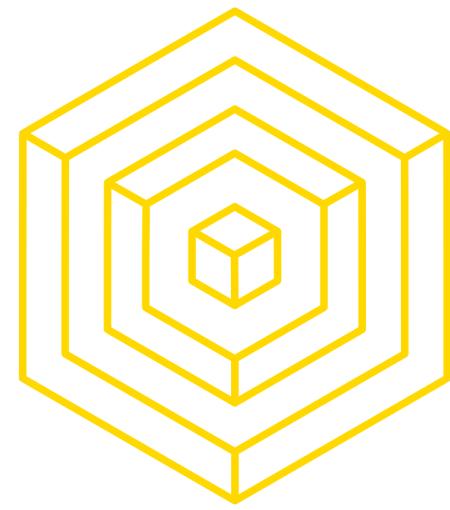
KEY STRETCHING

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



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

KEY STRETCHING

multi
sub
adjust
fuel
chain

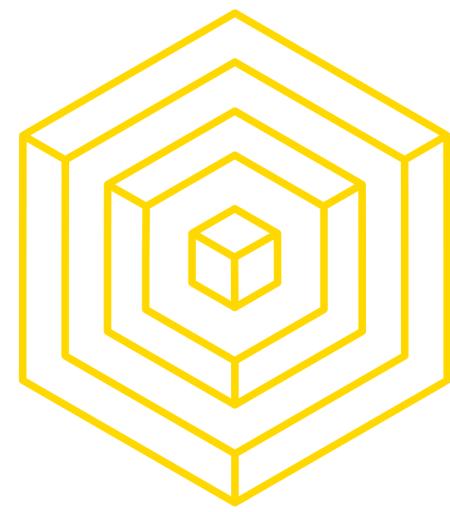


SHA-256



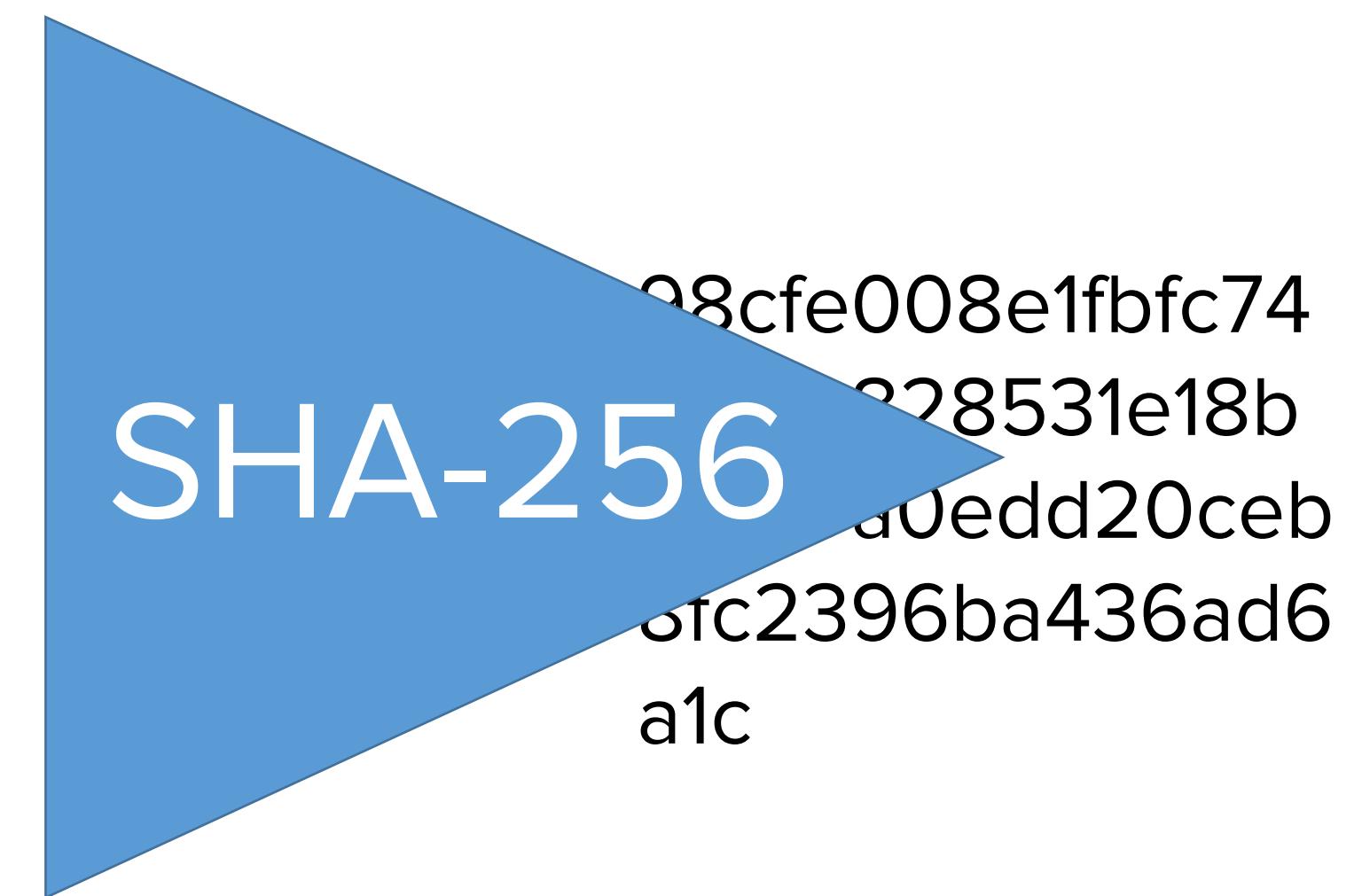
AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



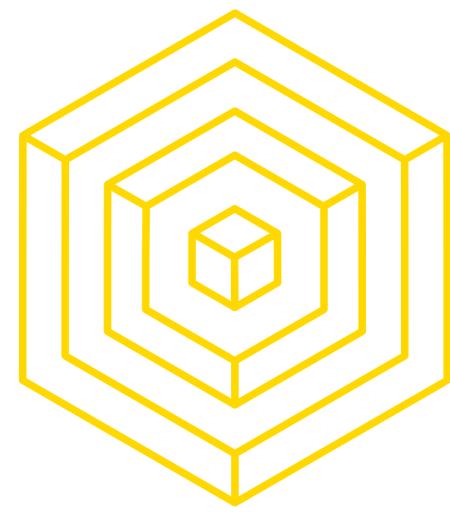
BITCOIN WALLETS

KEY STRETCHING



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

KEY STRETCHING

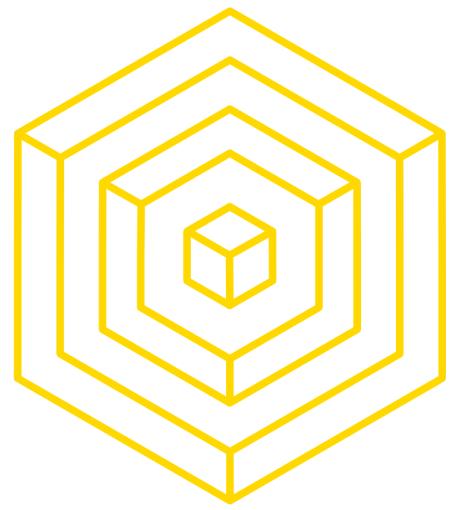


98cfe008e1fbfc74
770fb828531e18b
a4c19a0edd20ceb
8fc2396ba436ad6
a1c



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

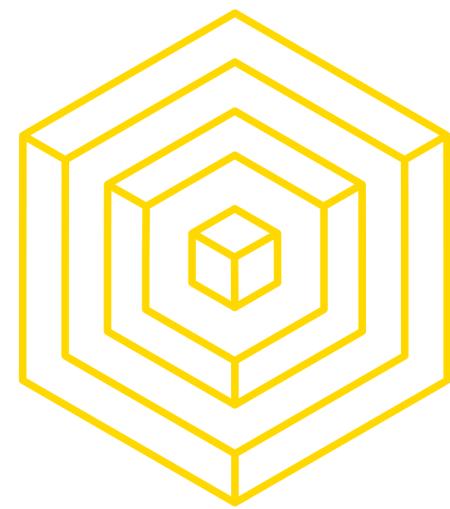
KEY STRETCHING

98cfe008e1fbfc74
770fb828531e18b
a4c19a0edd20ceb
8fc2396ba436ad6
a1c



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

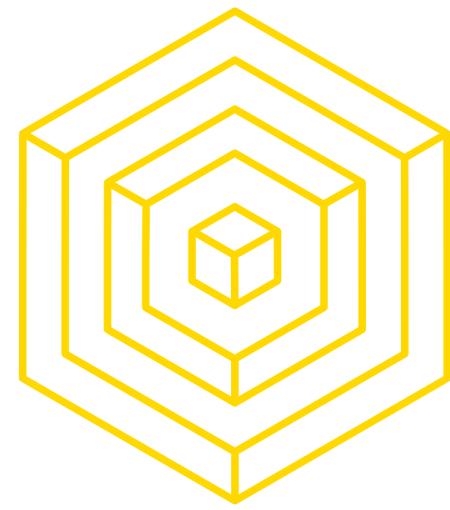
KEY STRETCHING

98cfe008e
770fb8285
a4c19a0ed
8fc2396ba
a1c



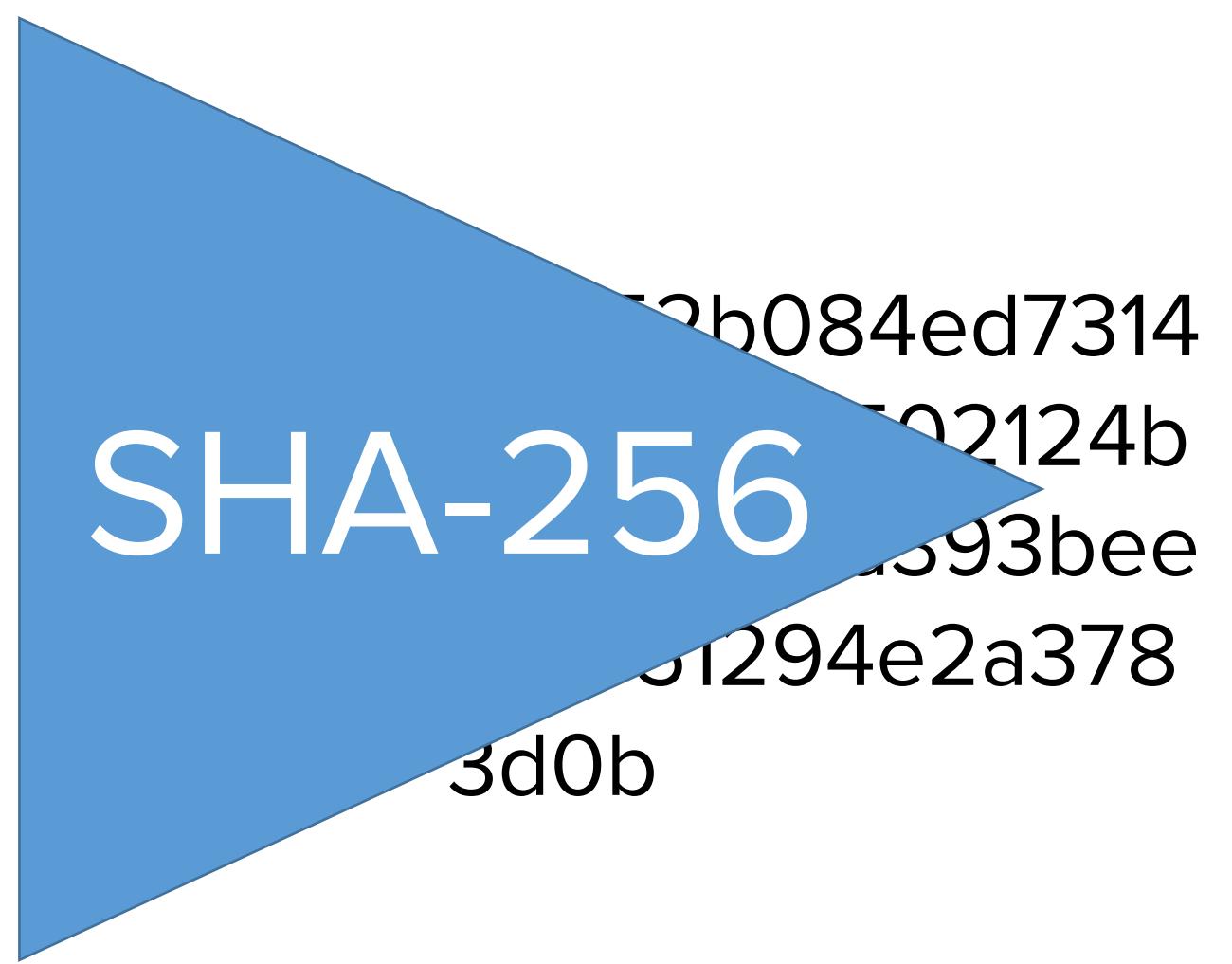
AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



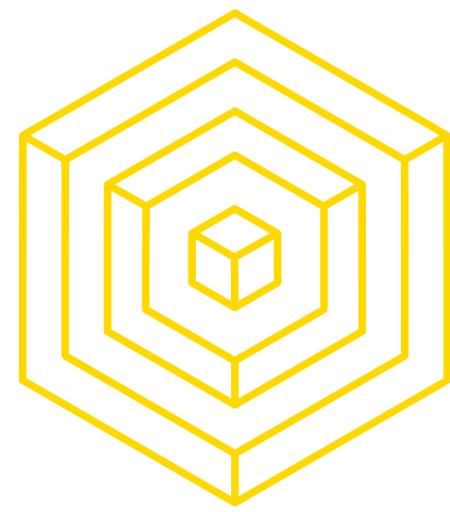
BITCOIN WALLETS

KEY STRETCHING



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4

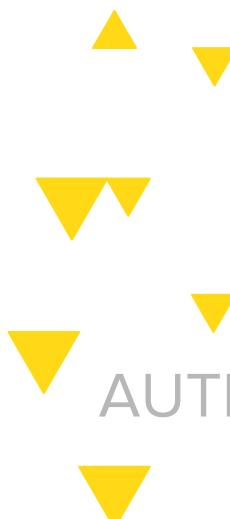


BITCOIN WALLETS

KEY STRETCHING

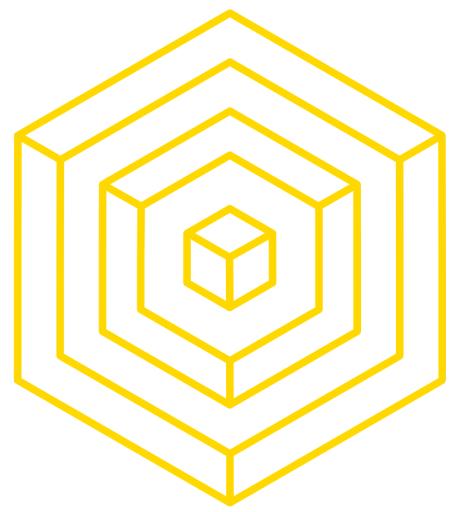


a4552b084ed7314
415b9367502124b
f84be086a393bee
b0fb51294e2a378
3d0b



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

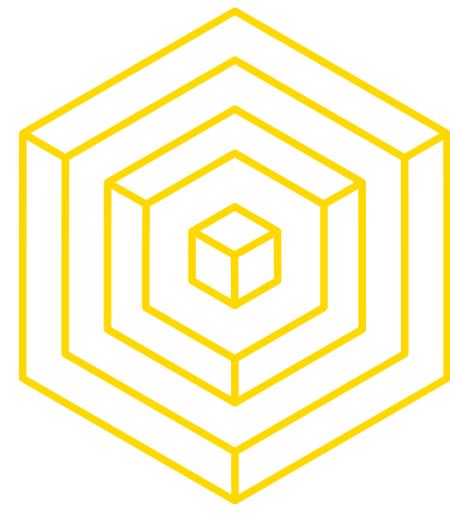
KEY STRETCHING

a4552b084ed7314
415b9367502124b
f84be086a393bee
b0fb51294e2a378
3d0b



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

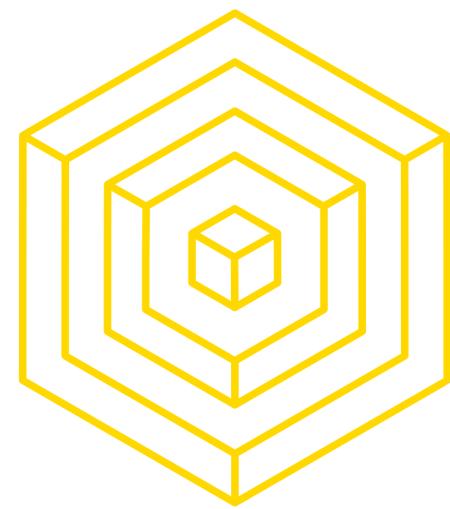
KEY STRETCHING

a4552b084
415b93675
f84be086a
b0fb51294
3d0b



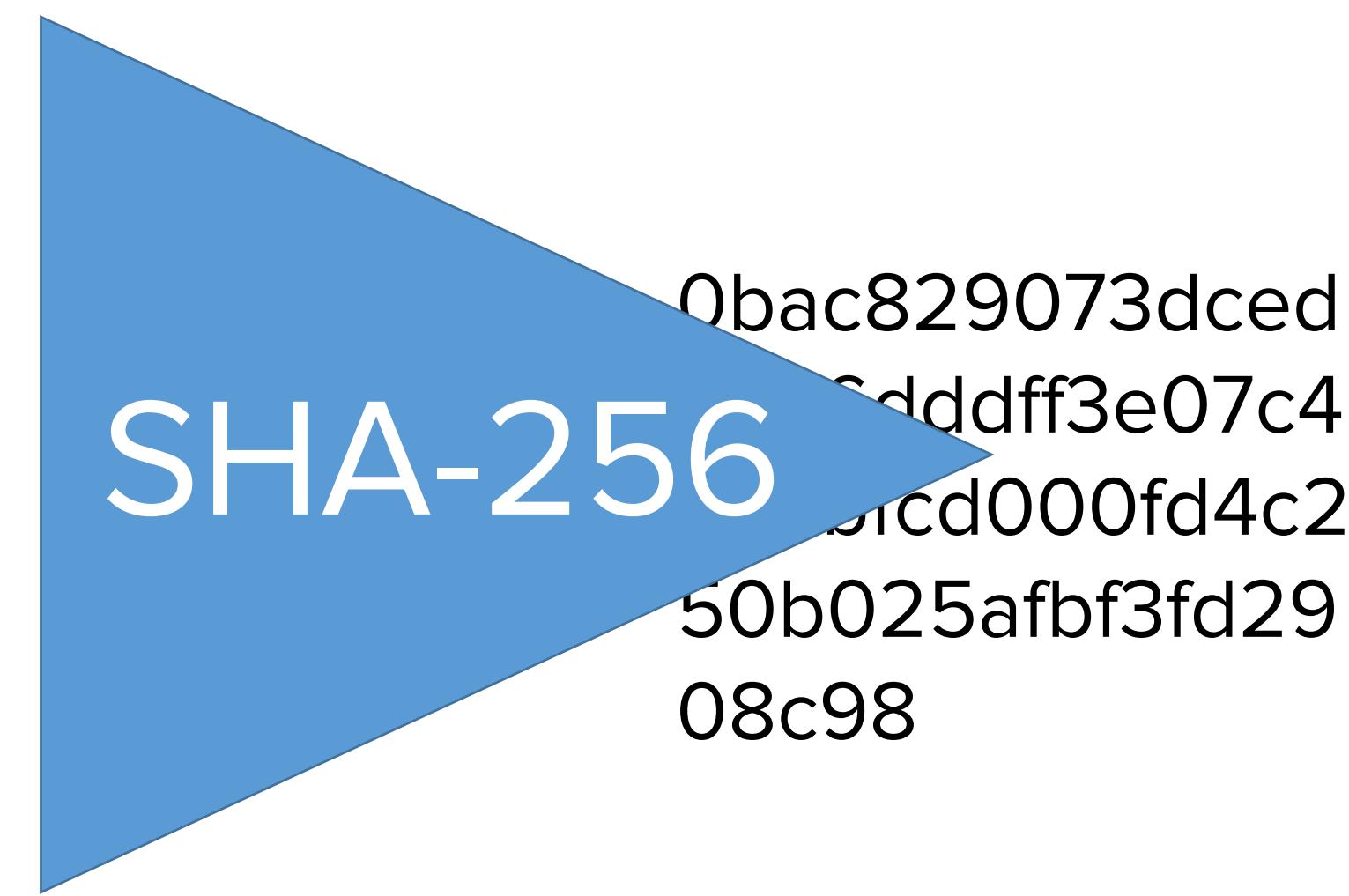
AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



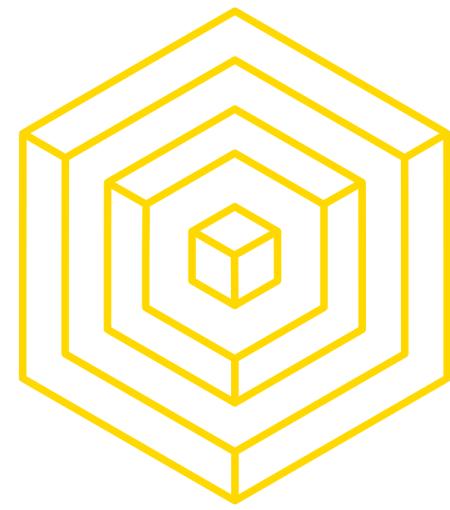
BITCOIN WALLETS

KEY STRETCHING



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

KEY STRETCHING

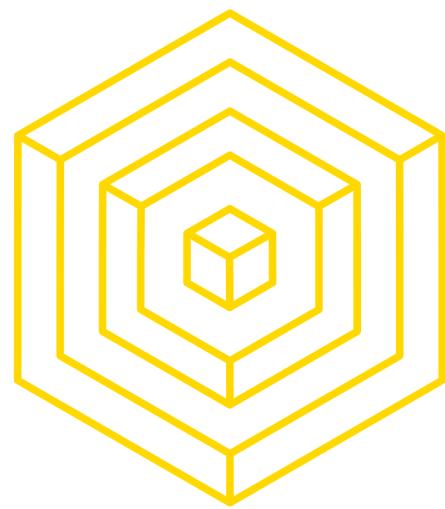


0bac829073dced
edb6dddff3e07c4
8d3bfcd000fd4c2
50b025afb3fd29
08c98



AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



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

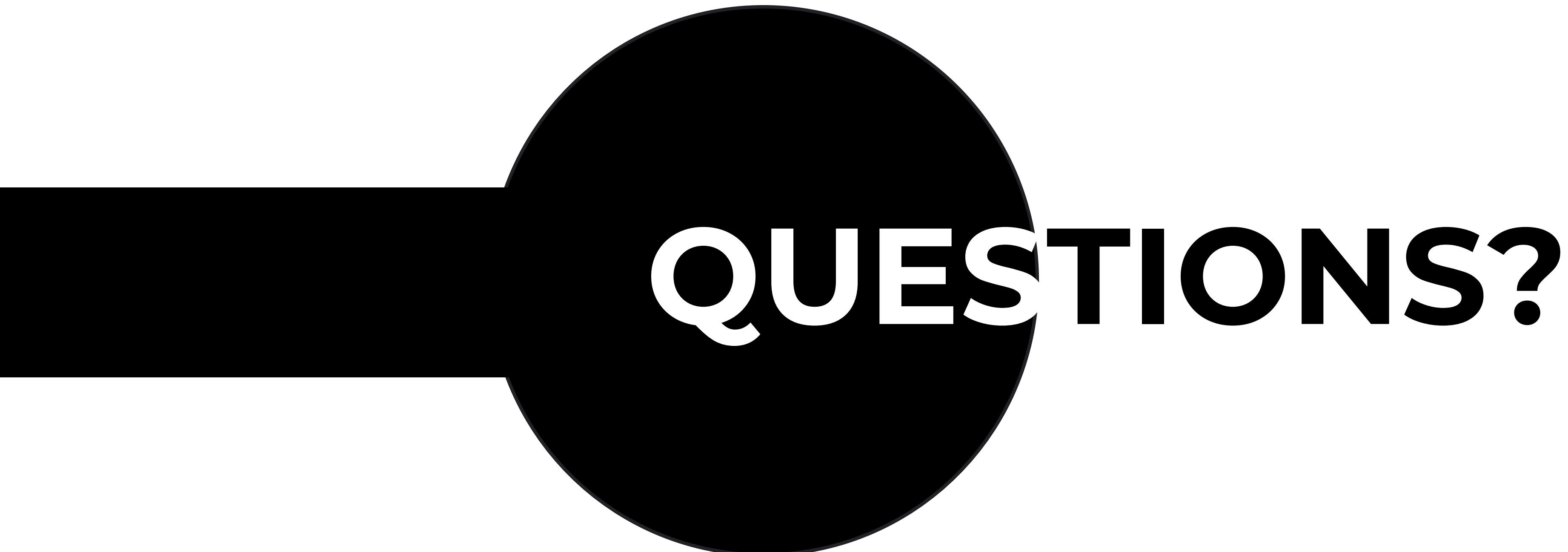
Who holds the private keys?

- You: mycelium, airbitz, blockchain.info
- Developer: coinbase.com

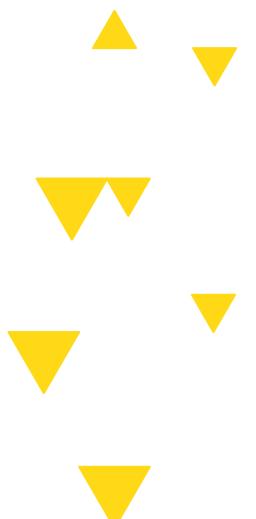


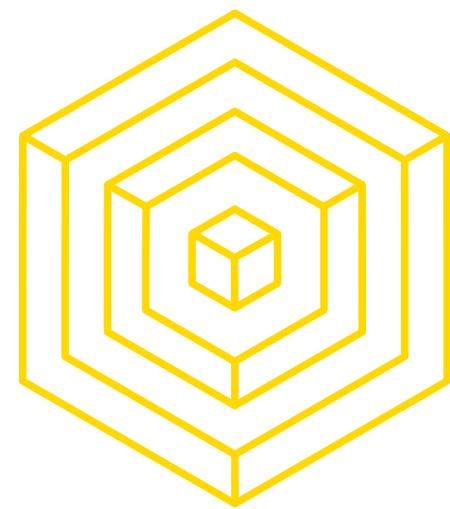
AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



QUESTIONS?

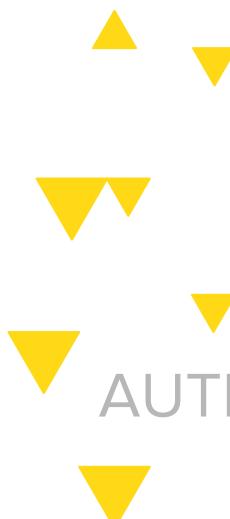




HOW DO I GET BITCOIN?

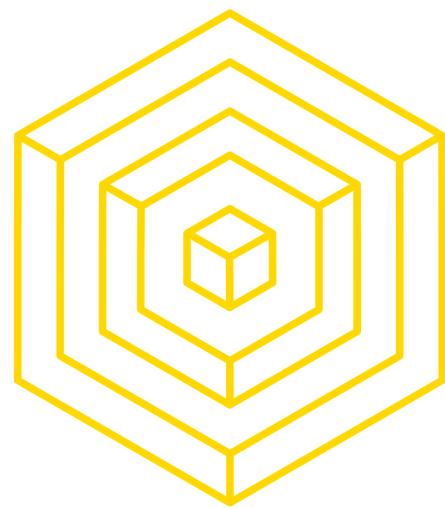
???????????

“But how do I get bitcoins?”



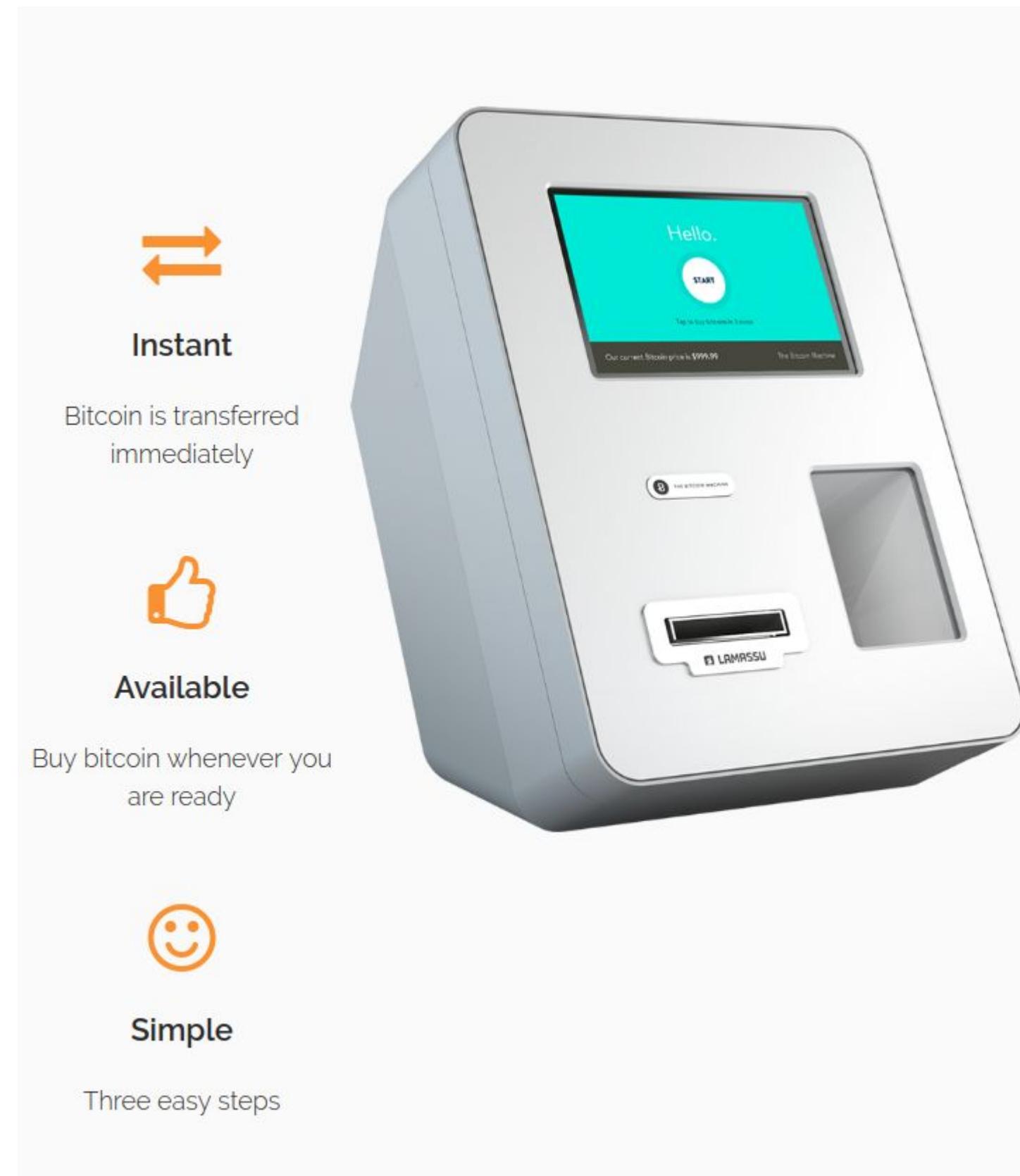
AUTHOR: RUSTIE LIN

BLOCKCHAIN FUNDAMENTALS LECTURE 4

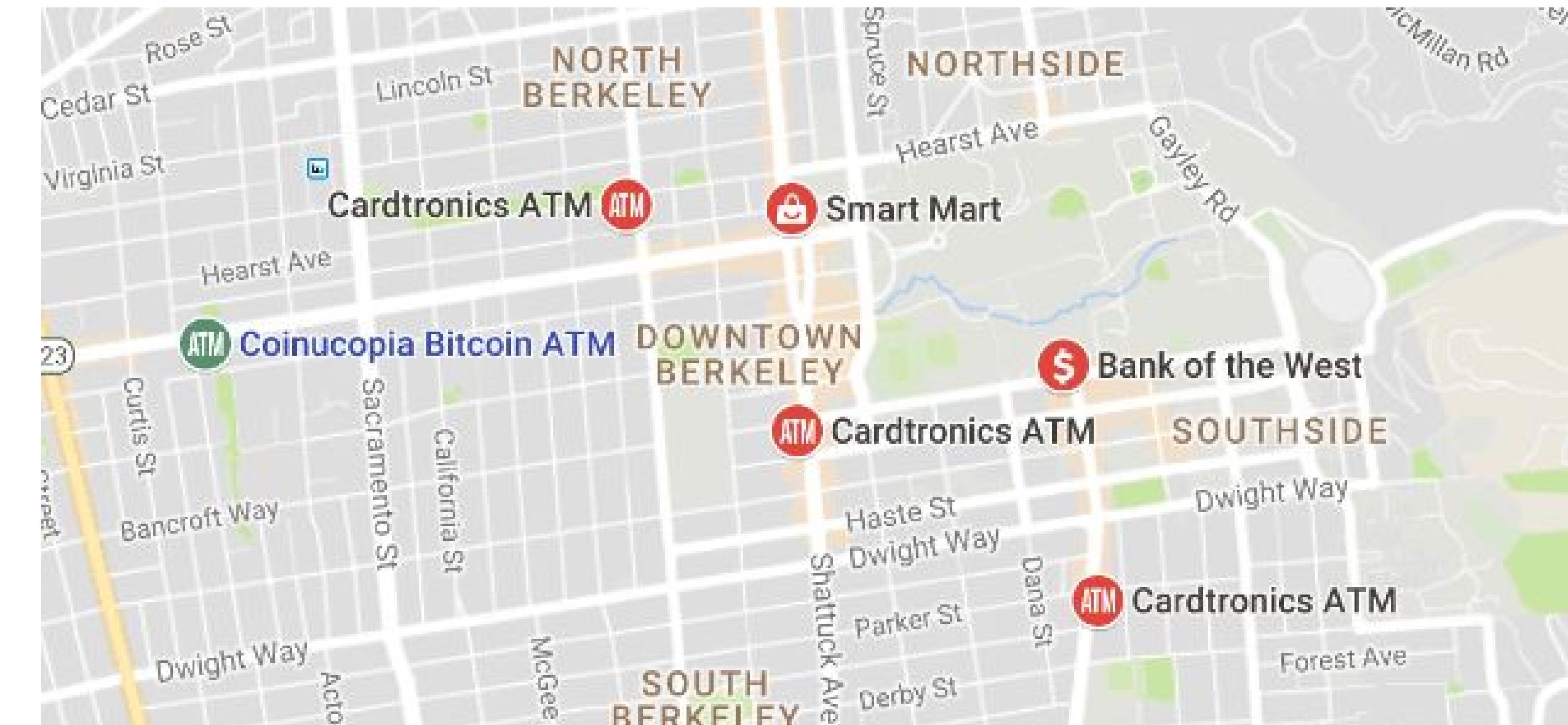


HOW DO I GET BITCOIN?

BITCOIN ATMS

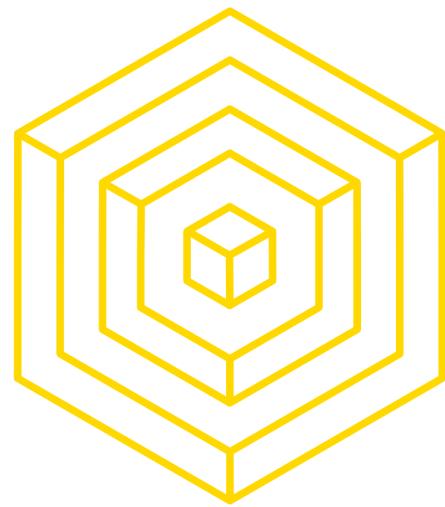


1250 University Ave.



AUTHOR: RUSTIE LIN

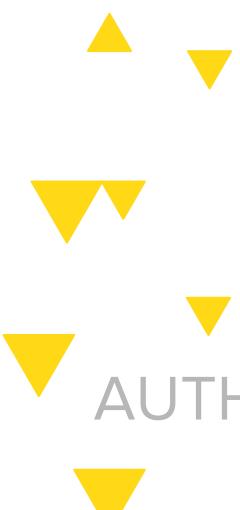
BLOCKCHAIN FUNDAMENTALS LECTURE 4



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.



AUTHOR: RUSTIE LIN



Bitcoin Exchanges

Places to buy bitcoin in exchange for other currencies.

Bitcoin Exchanges

Note: Exchanges provide highly varying degrees of safety, security, privacy, and control over your funds and information.
Perform your own due diligence and [choose a wallet](#) where you will keep your bitcoin before selecting an exchange.

International

Bisq
Bitstamp
Bitwage
Coinbase
Kraken
Local Bitcoins
Xapo

Europe

AnyCoin Direct
Bitcoin.de
BitPanda
BL3P
Paymium
The Rock Trading

Argentina

Ripio
SatoshiTango

Australia

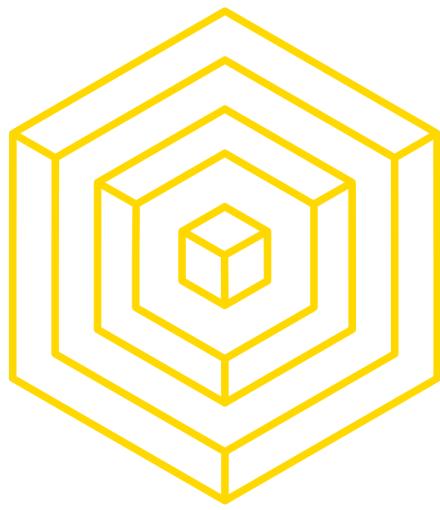
[Bitcoin Australia](#)
CoinJar
CoinLoft
CoinTree

Brazil

Foxbit
[Mercado Bitcoin](#)

Cambodia

[Bitcoin Cambodia](#)

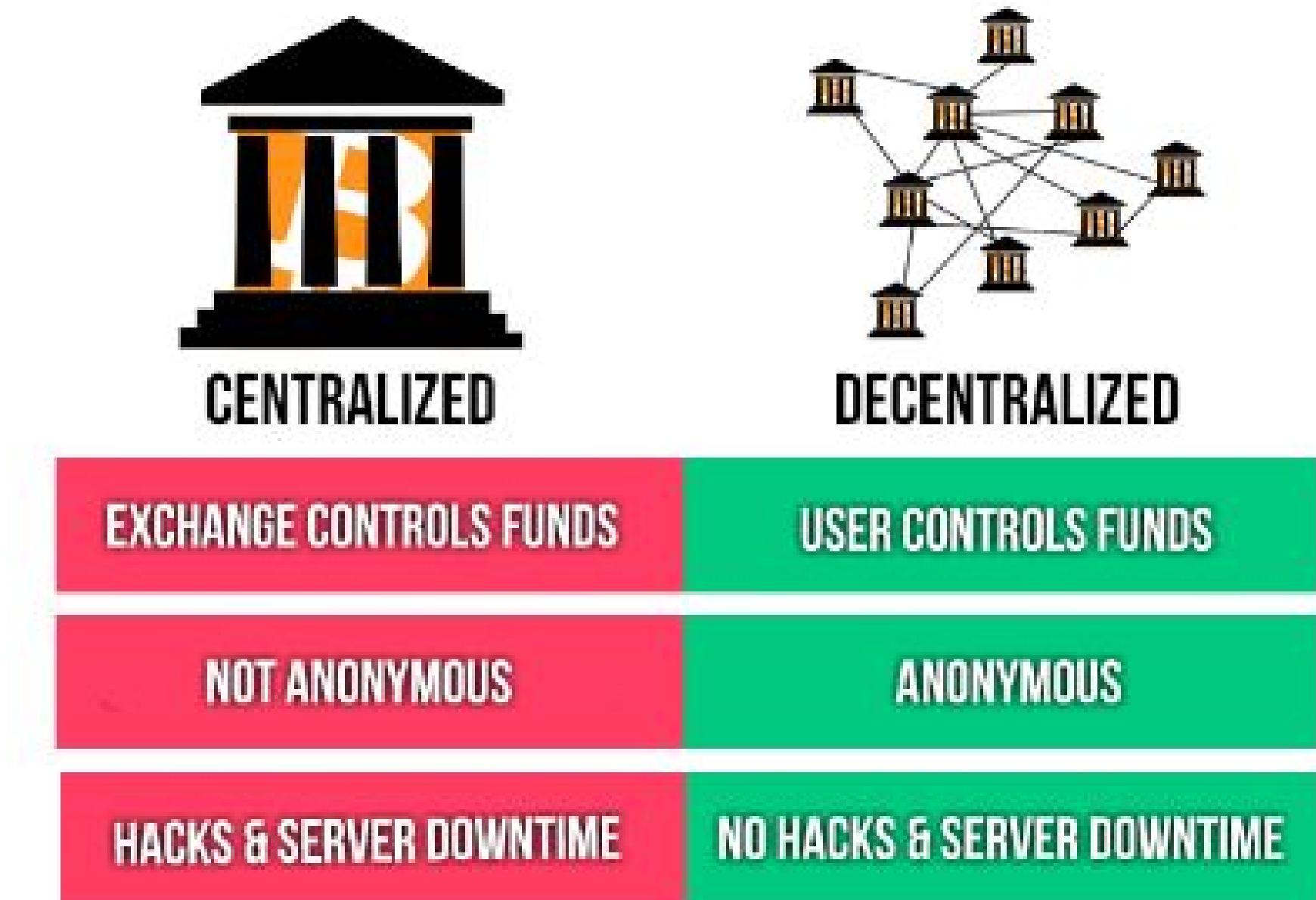


HOW DO I GET BITCOIN?

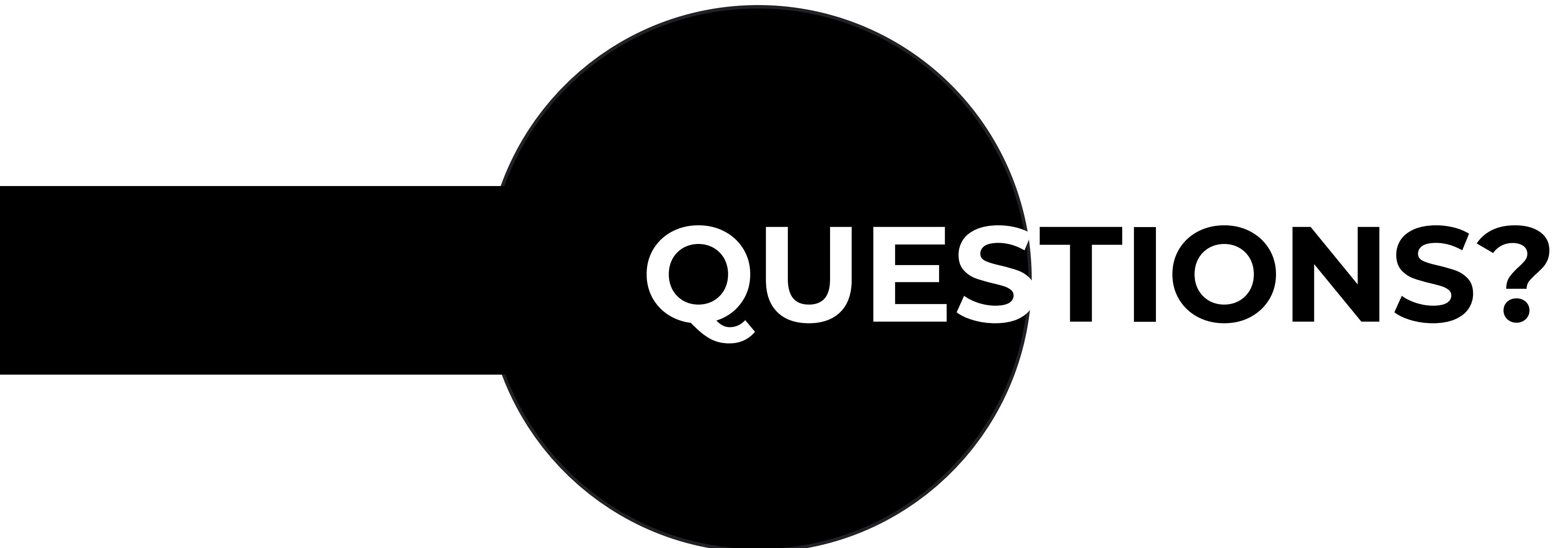
DECENTRALIZED EXCHANGES

Decentralized exchanges don't rely on a third party service to hold customer's funds

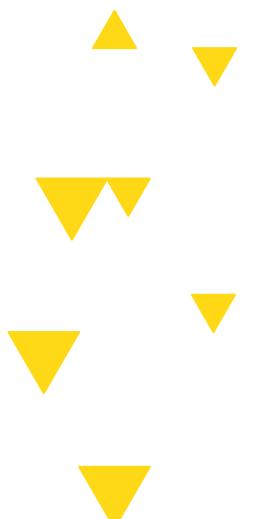
- Trades are P2P
 - Trustless
 - Bitshares, Bisq (ex Bitsquare),
Openledger, Airswap,
Etherdelta, etc.

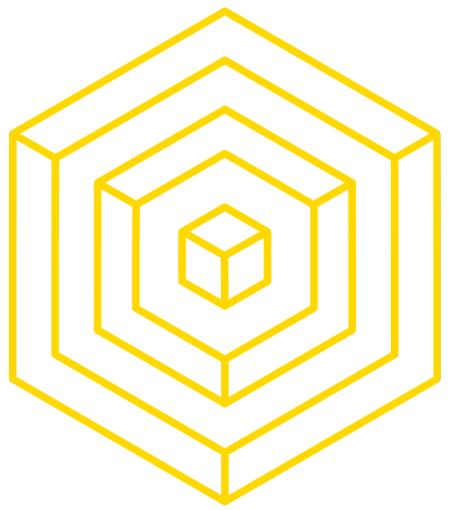


AUTHOR: RUSTIE LIN



QUESTIONS?

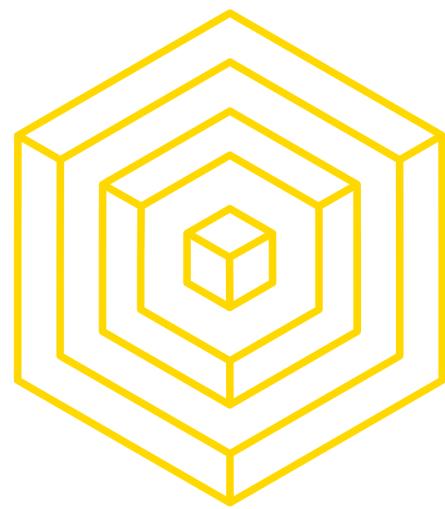




2

WALLET MECHANICS

BLOCKCHAIN FUNDAMENTALS LECTURE 4

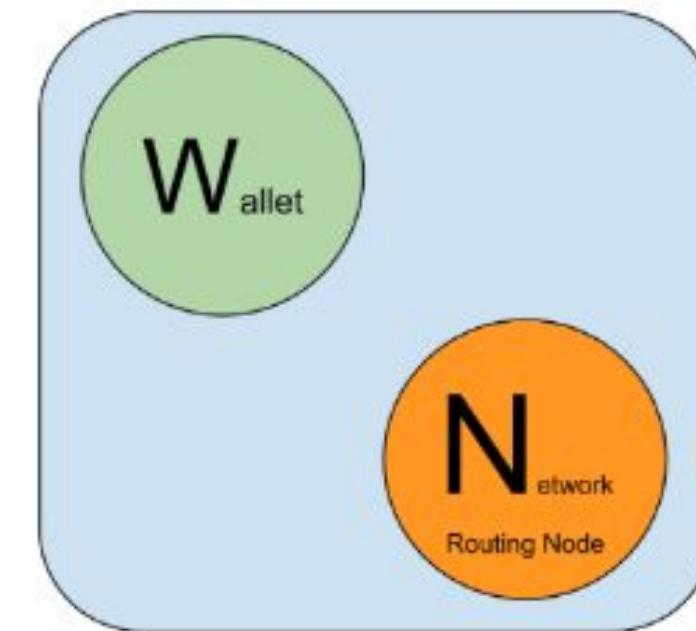


SIMPLE PAYMENT VERIFICATION

THIN CLIENTS

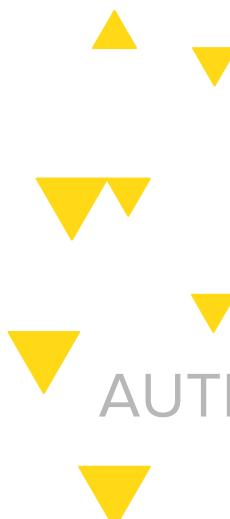
Simple Payment Verification (SPV) is method for verifying if particular transactions are included in a block without downloading the entire block

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



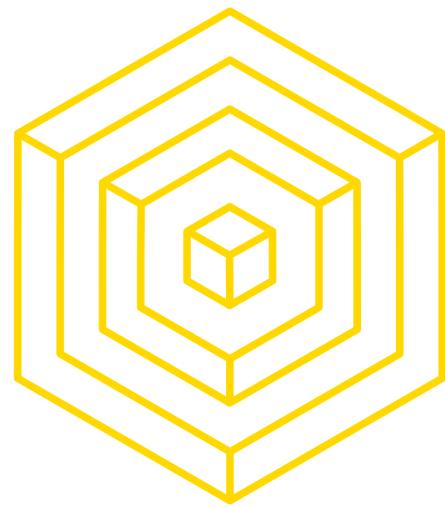
Lightweight (SPV) wallet

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



AUTHOR: RUSTIE LIN

BLOCKCHAIN FUNDAMENTALS LECTURE 4

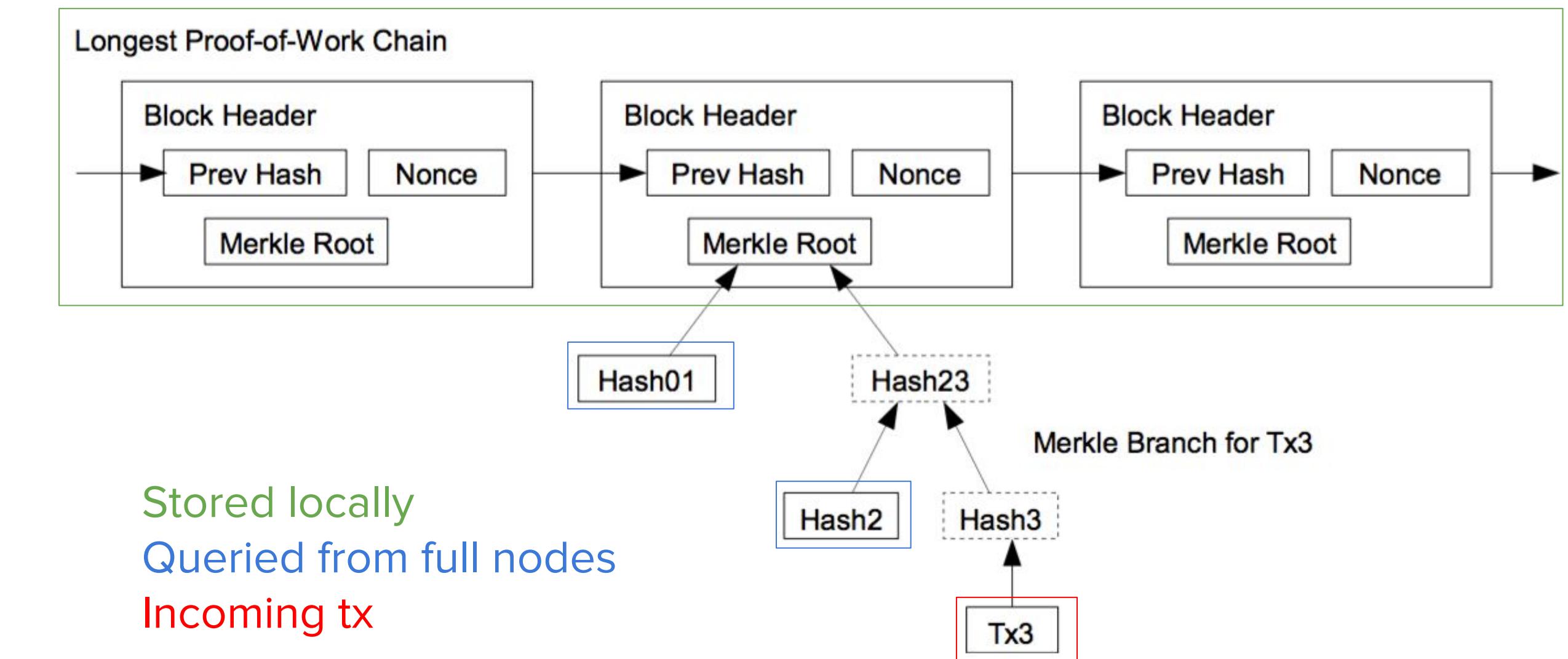


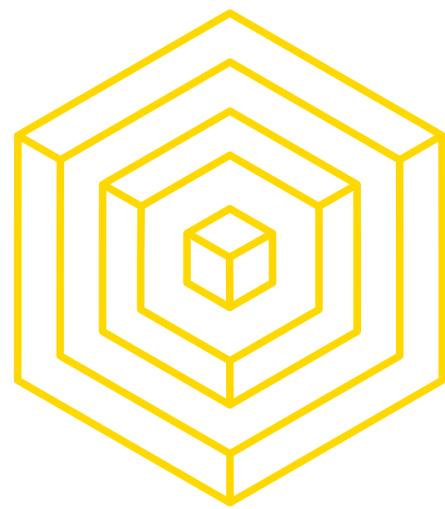
SIMPLE PAYMENT VERIFICATION

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

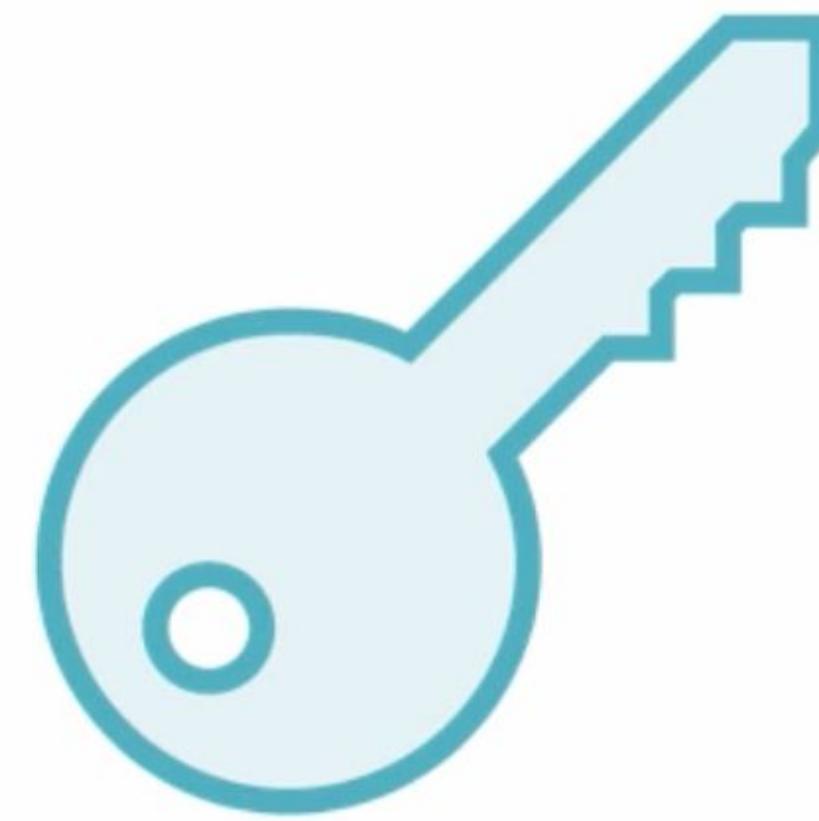




MULTISIGNATURE

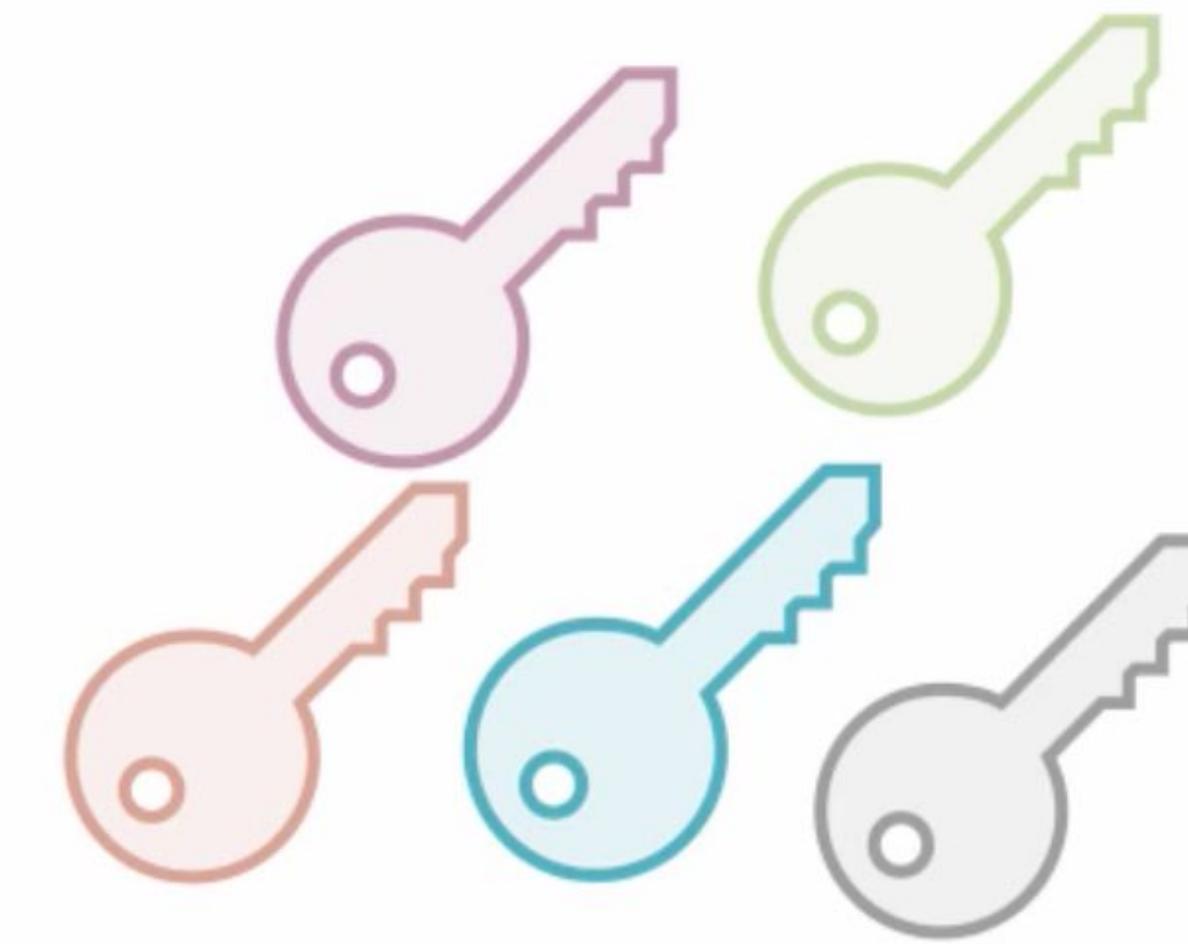
M-OF-N TRANSACTIONS

Multi-person Account Access



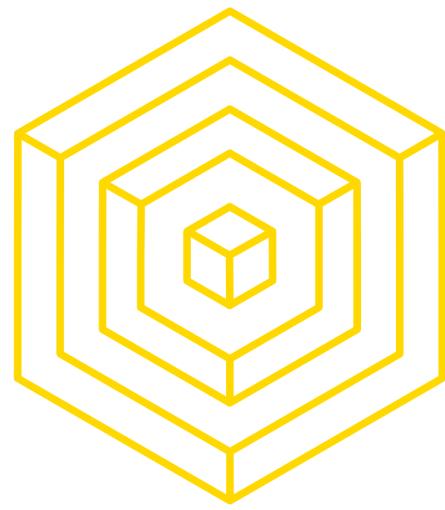
Regular Bitcoin Addresses

- ▲ Each account has 1 key (or seed)
- ▼ Any single person can steal funds



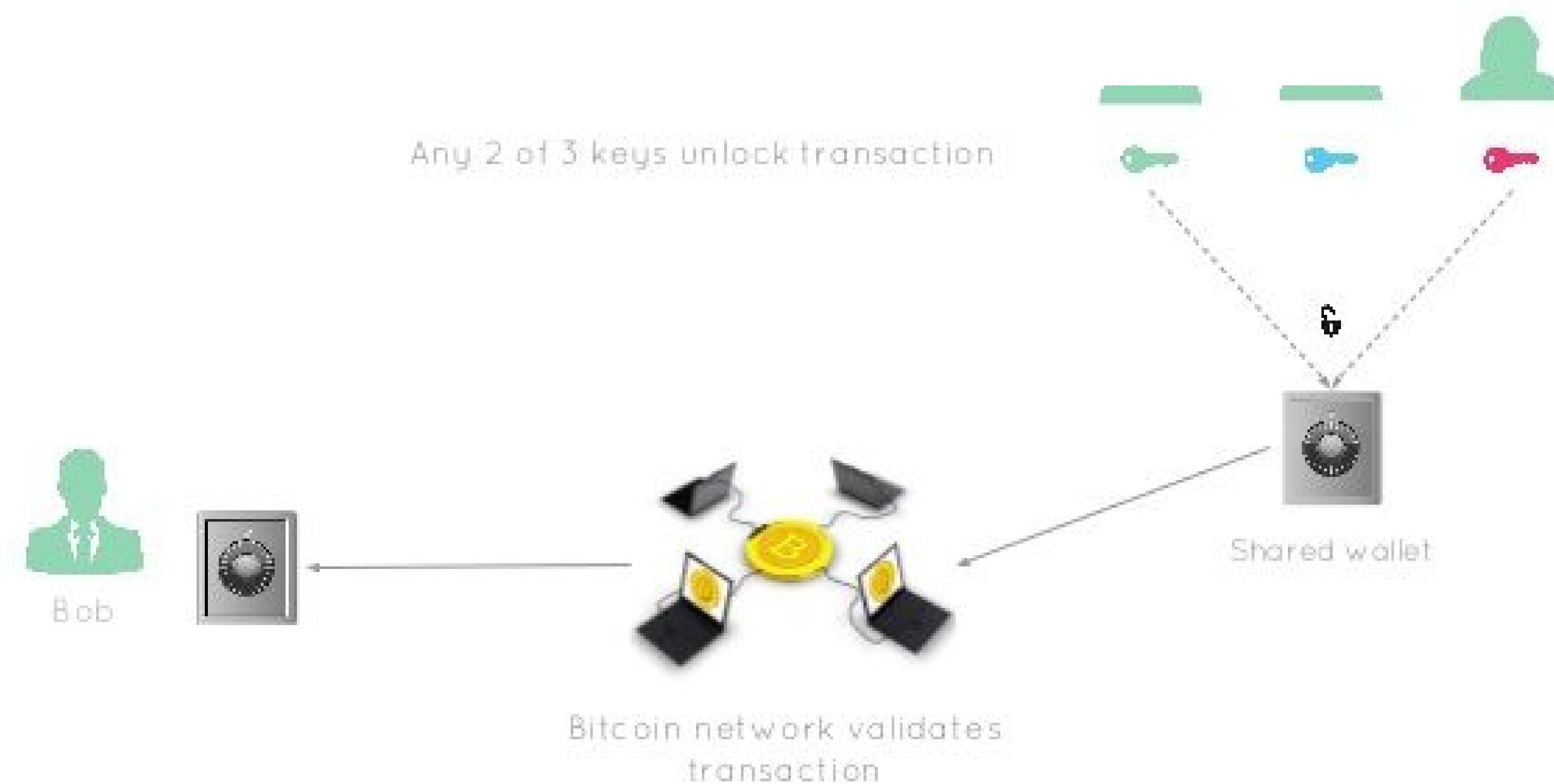
Multisignature Addresses

- Multiple signatures needed
- Ex: 3 of 5 signatures



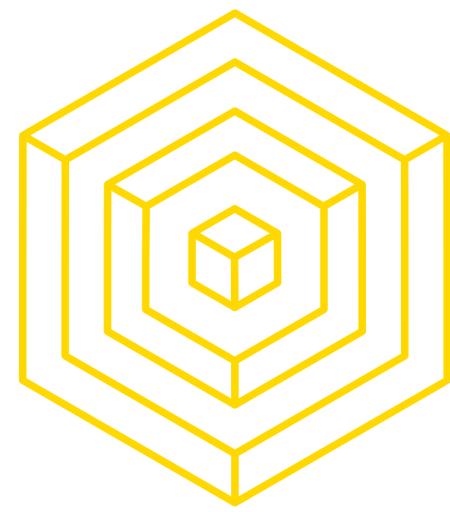
BITCOIN MECHANICS

MULTISIG TRANSACTION



AUTHOR: SUNNY AGGARWAL

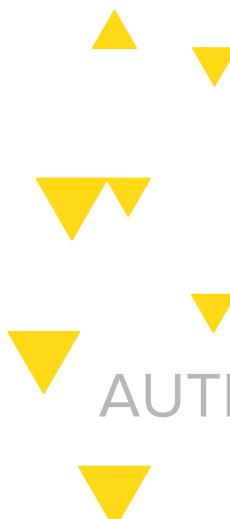
BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN MECHANICS

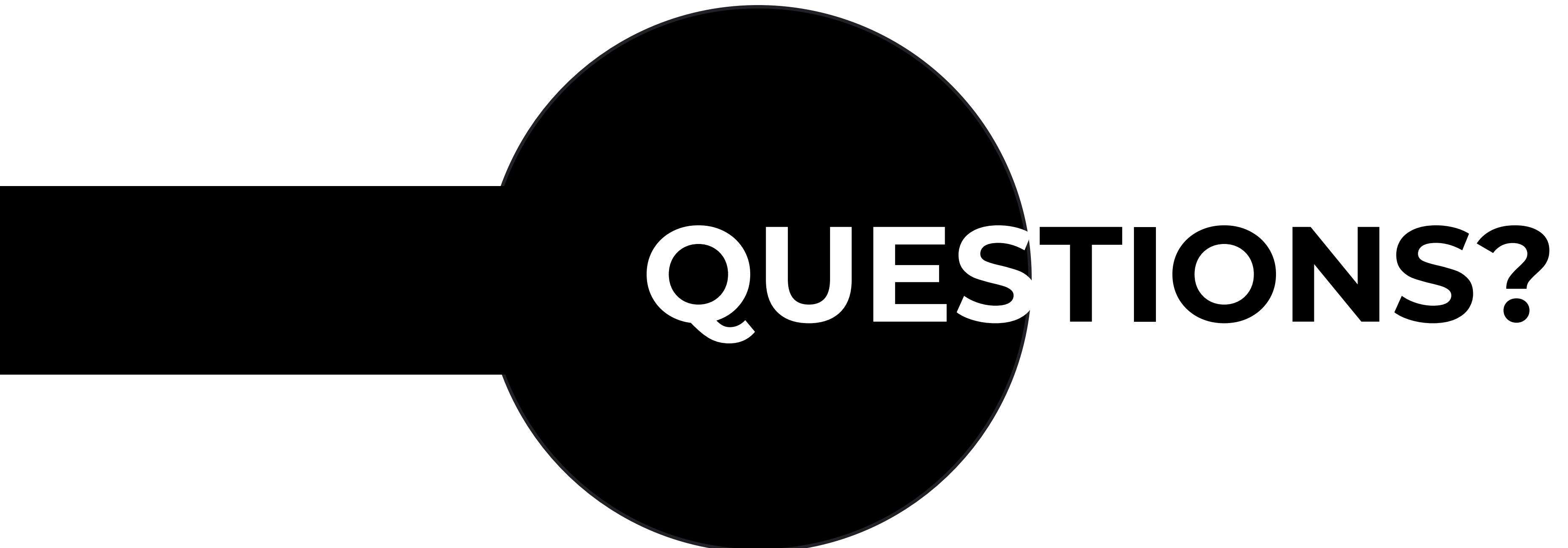
KEY GENERATION PRACTICES

- 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

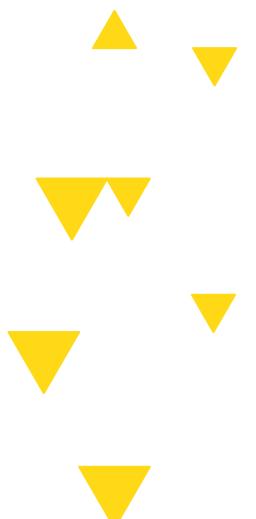


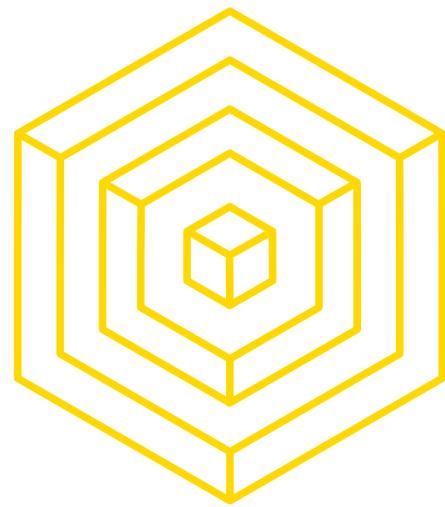
AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4



QUESTIONS?





WALLET BACKUPS

JBOK WALLETS

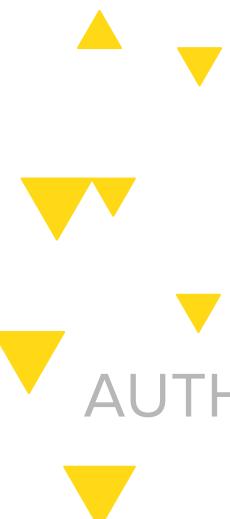


JBOK (Just a Bunch Of Keys)

New backup required for every new address

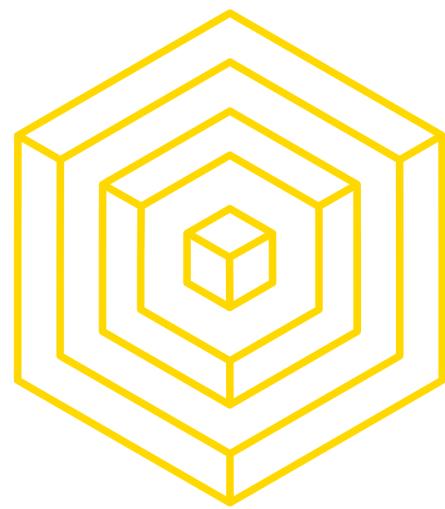
Or, generate a bunch of keys when first started

Not too convenient because you have to store
every key



AUTHOR: RUSTIE LIN

BLOCKCHAIN FUNDAMENTALS LECTURE 4



WALLET BACKUPS

HD WALLETS

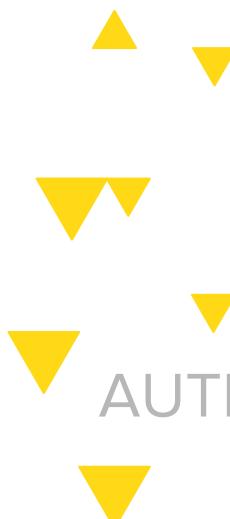


HD (Hierarchical Deterministic) Wallets

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

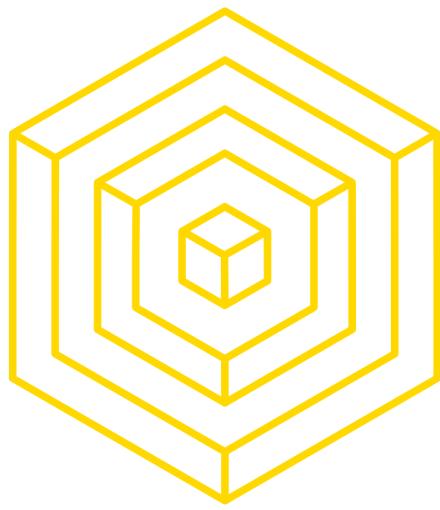
Use a one-way hash function with seed, index number, and optional chain code (just some more entropy)

Exchanges use these



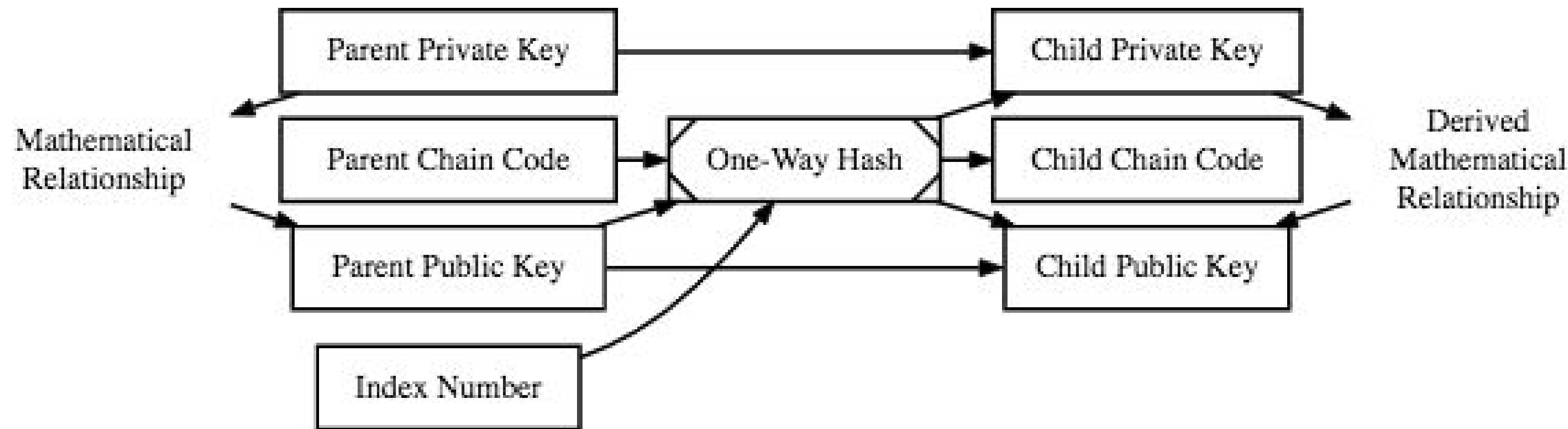
AUTHOR: RUSTIE LIN

BLOCKCHAIN FUNDAMENTALS LECTURE 4



BITCOIN WALLETS

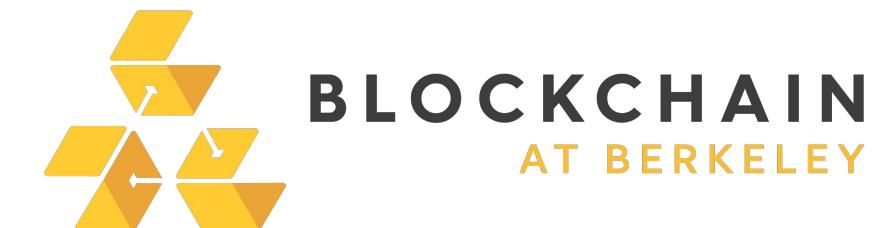
WALLET BACKUPS

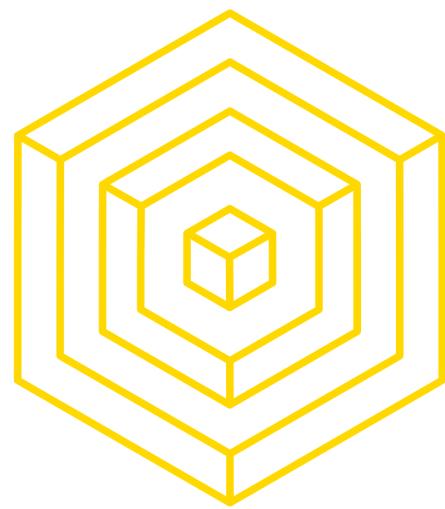


Normal Hierarchical Deterministic (HD) Key Derivation (BIP32)

AUTHOR: SUNNY AGGARWAL

BLOCKCHAIN FUNDAMENTALS LECTURE 4

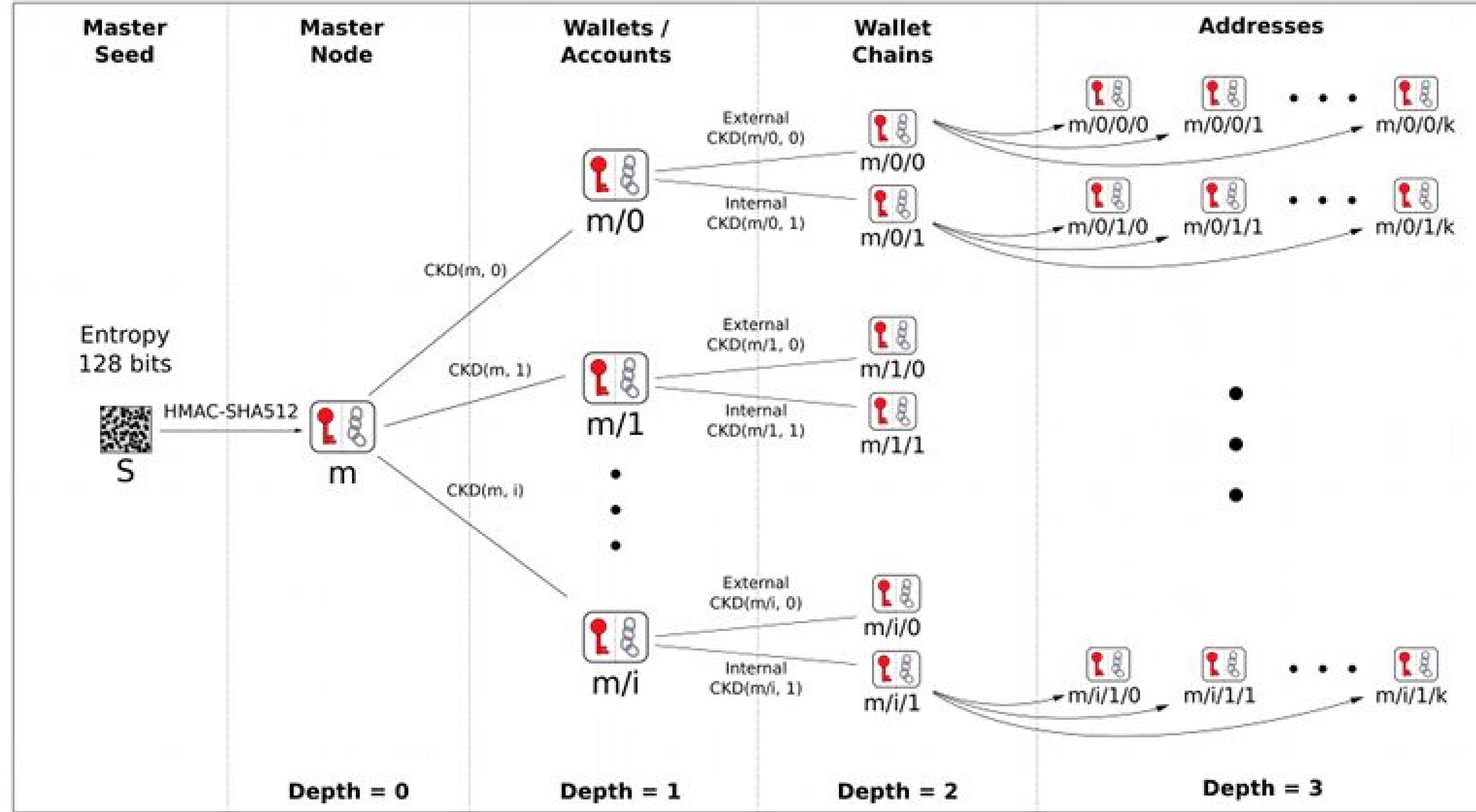


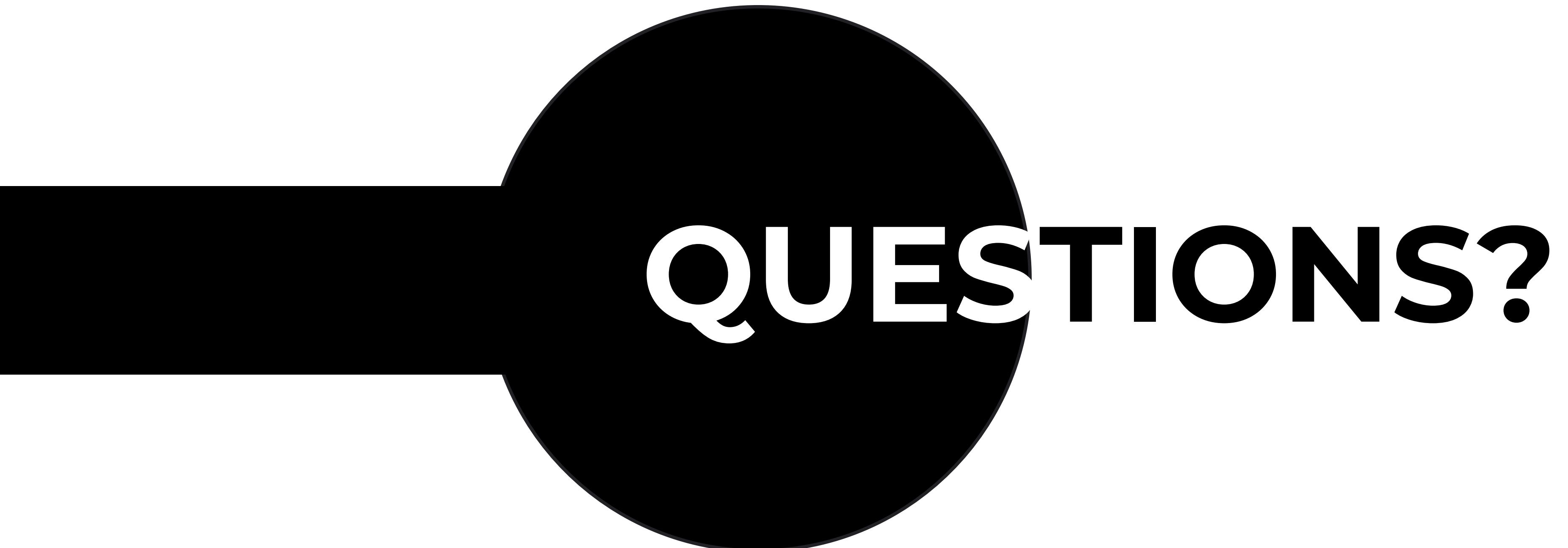


BITCOIN WALLETS

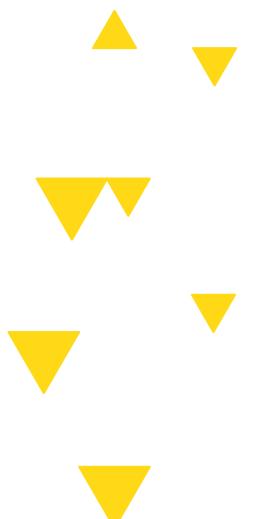
WALLET BACKUPS

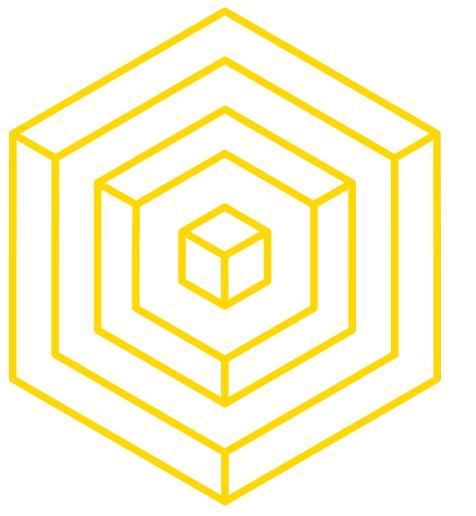
BIP 32 - Hierarchical Deterministic Wallets





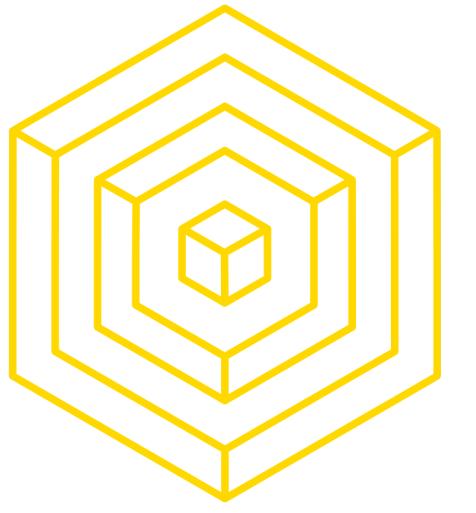
QUESTIONS?





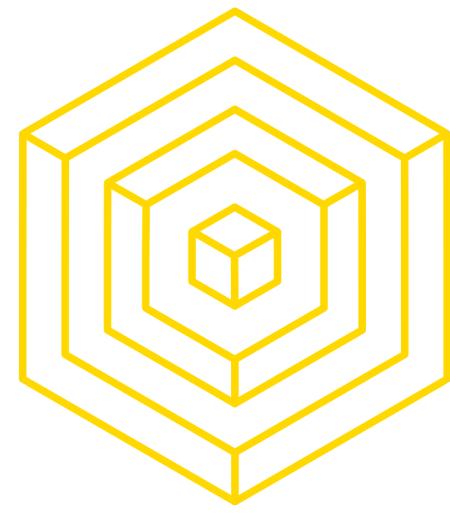
3 MINING

BLOCKCHAIN FUNDAMENTALS LECTURE 4



3.1

MINING REVIEW



MINING

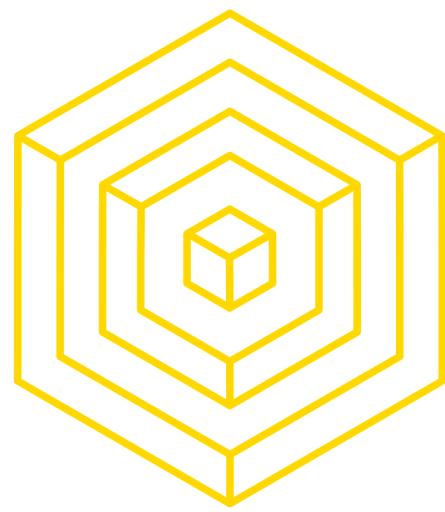
WHAT DOES MINING DO?

“So what does mining do?”



AUTHOR: JASON BI

BLOCKCHAIN FUNDAMENTALS LECTURE 4

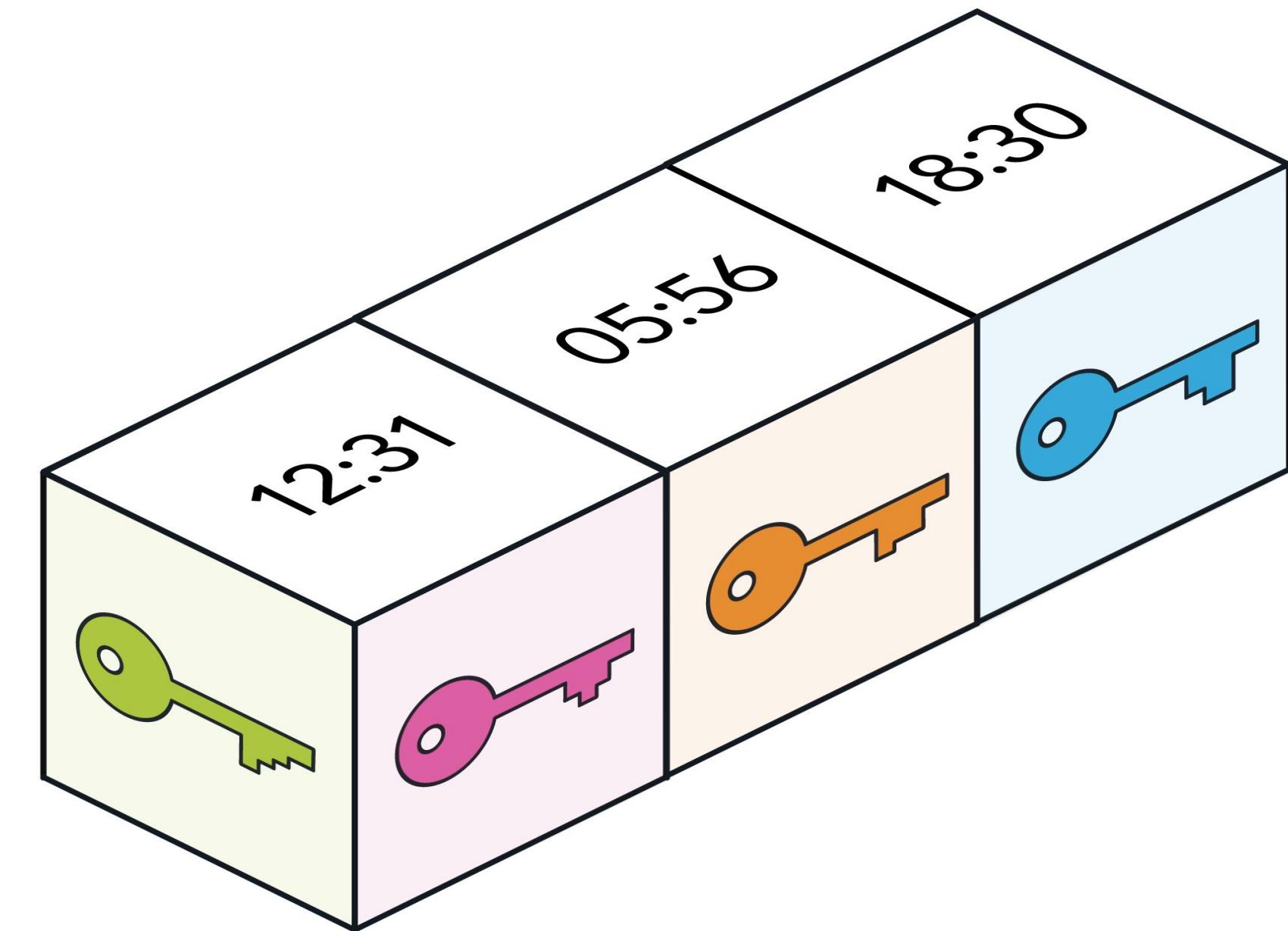


MINING

WHAT DOES MINING DO?

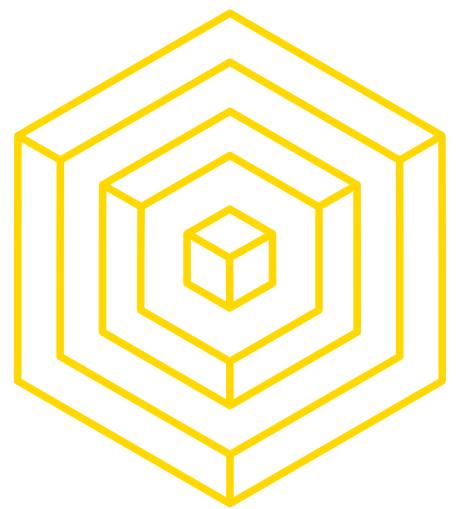
Mining updates the blockchain

- Transactions are bundled into blocks
- Blocks are verified
- New blocks are appended to the blockchain



 coindesk

◀ ▶
▼ ▼
▼ ▼
▼ AUTHOR: JASON BI
▼



MINING

WHAT DOES MINING DO?

Mining introduces new coins to the network

- Mining process decentralizes the coin minting process
- No central party issuing out coins/currency



AUTHOR: JASON BI



MINERS SERVE AS VERIFIERS

WHAT DOES A MINER DO?

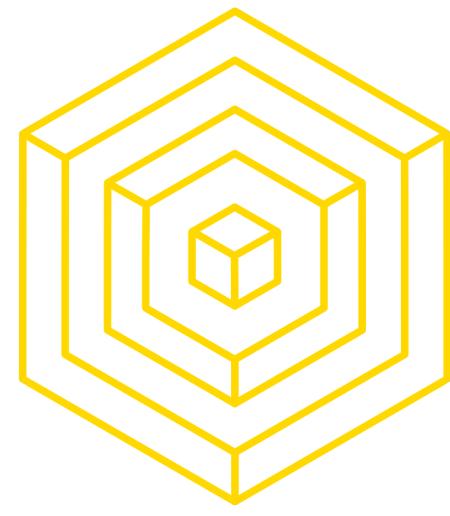
A full-fledged Bitcoin miner (“full node”) must:

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
5. **Hope** that your block is accepted by other nodes and not defeated by a competitor block
6. **Profit!**



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

AUTHOR: NADIR AKHTAR



MINING

THE PROOF OF WORK PROBLEM

BLOCK HEADER

PREV BLOCK HASH

NONCE

MERKLE ROOT



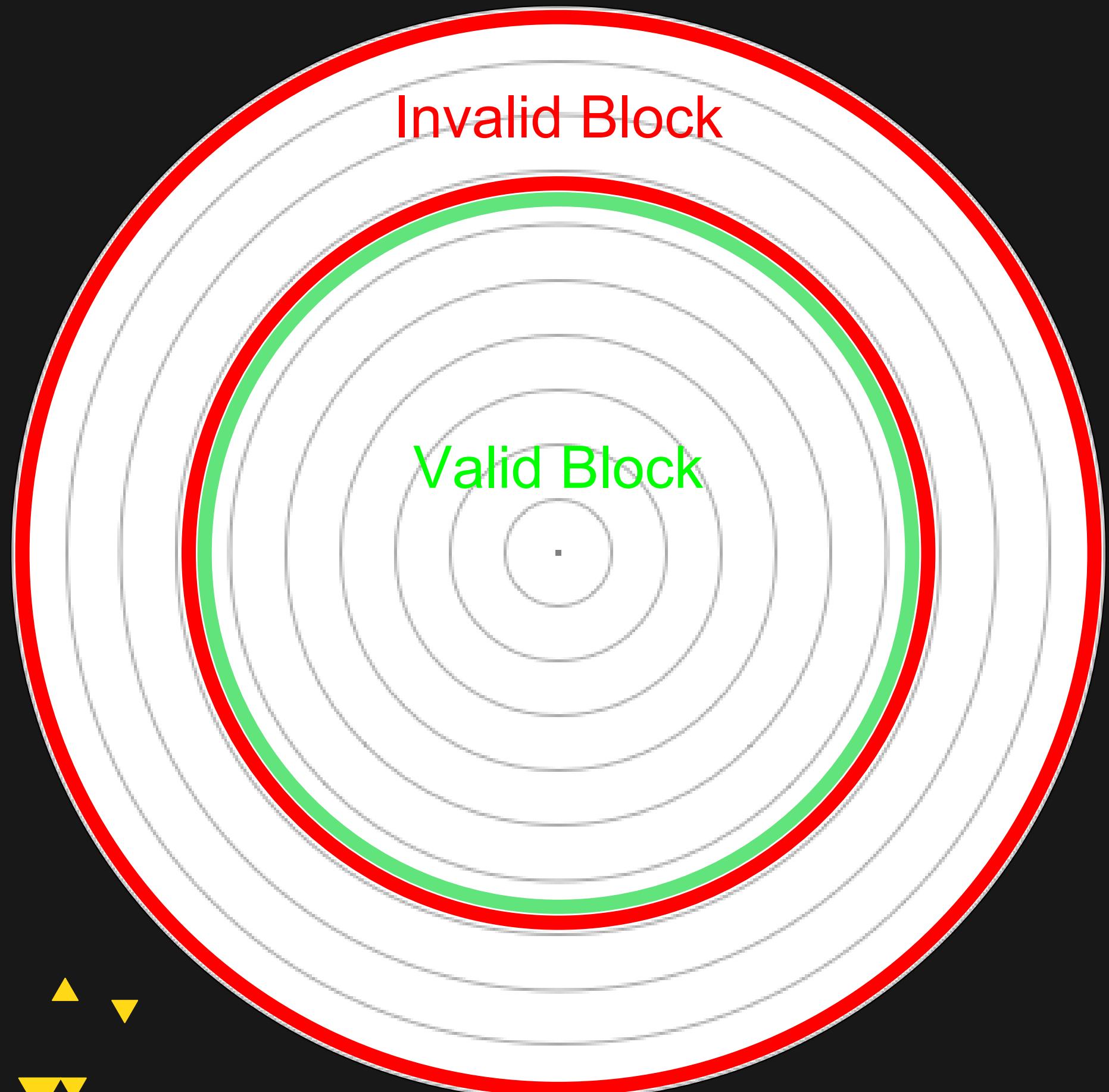
AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 3



MINING

THE PROOF OF WORK PROBLEM

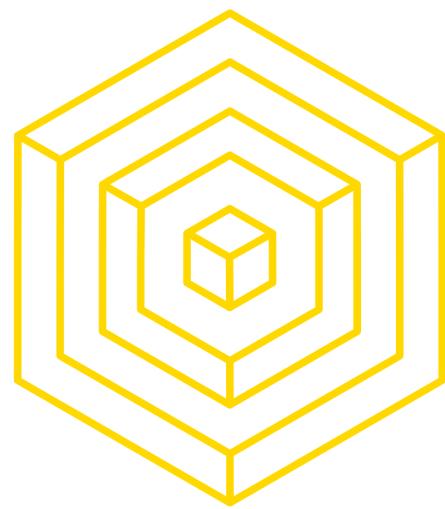


AUTHOR: JASON BI

Proof of Work Problem: Costly and time consuming to solve, easy to verify

-Goal: find the hash of a valid block header with value less than a target value

$-H(\text{prevBlockHash} \ || \ \text{merkleRoot} \ || \ \text{nonce}) < \text{target}$

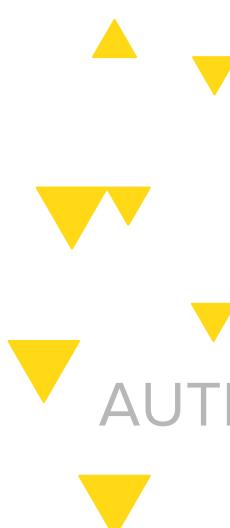


MINING

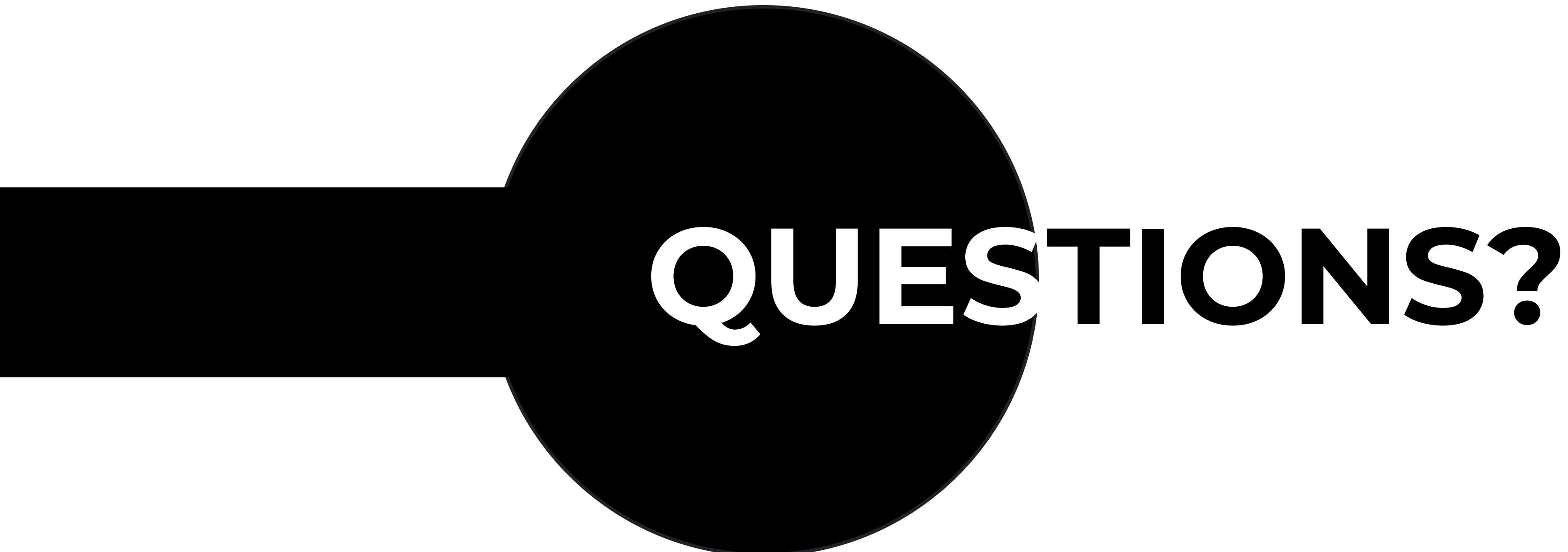
THE PROOF OF WORK PROBLEM

It helps to think of mining as a massive competition

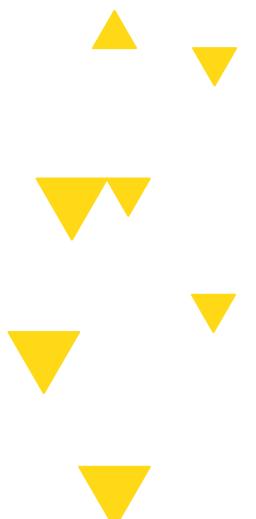
- A huge game of hungry hungry hippos in which each hippo is trying to eat one ball, specific to themselves
 - A random process
- The faster a hippo chomps the more likely it is to win
 - Calculating hashes faster increases chances of winning

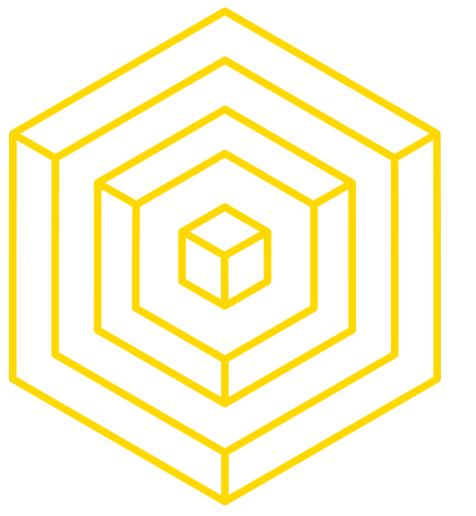


AUTHOR: JASON BI

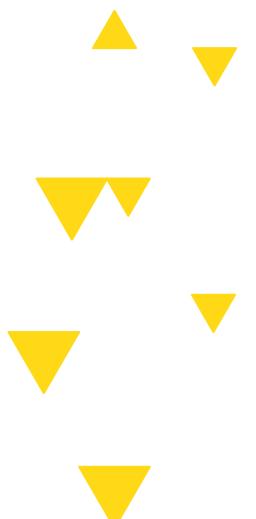


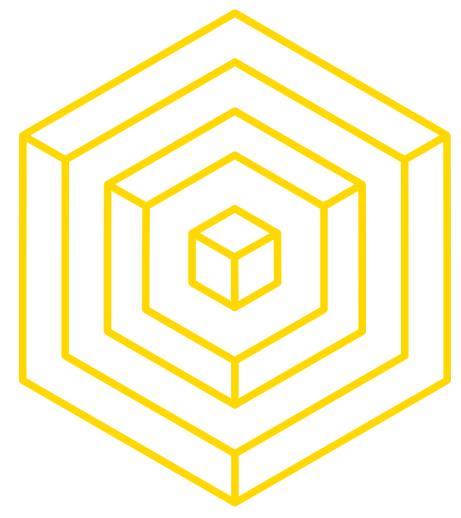
QUESTIONS?





3.2 MINING INCENTIVES





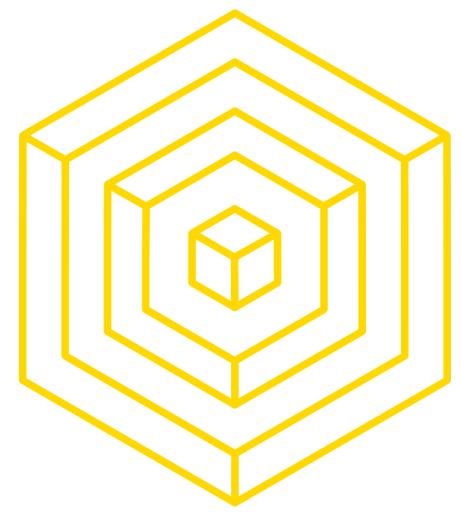
MINING INCENTIVES

WHY DO WE DO THINGS?



AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4



MINING INCENTIVES

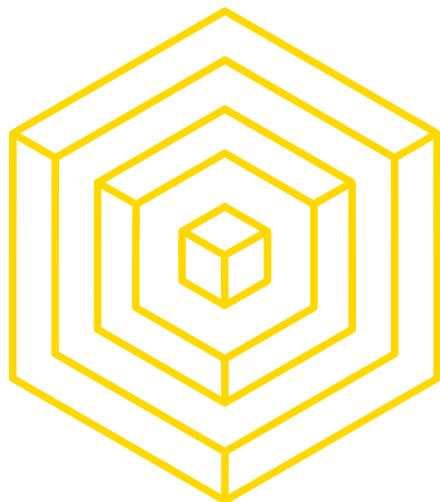
WHY DO WE DO THINGS?

PROFIT



AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4



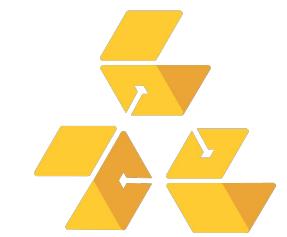
MINING INCENTIVES

WHY DO YOU DO THINGS?

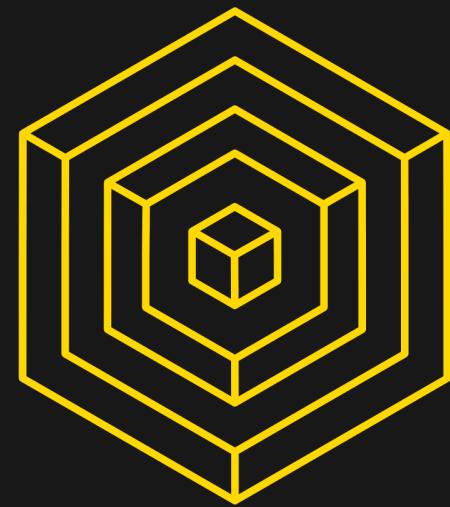
59

AUTHOR: NADIR AKHTAR

KCHAIN FUNDAMENTALS LECTURE 4



BLOCKCHAIN AT BERKELEY

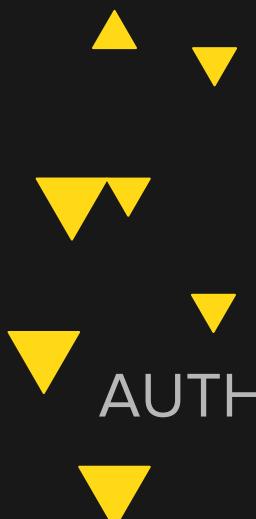


MINING INCENTIVES

WHAT IS PROFIT?

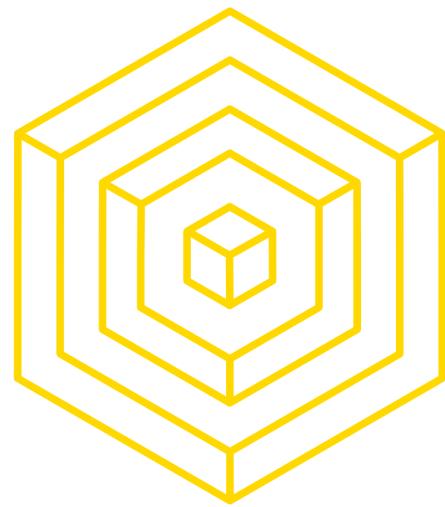
```
if revenue > cost:  
    return "$$$$"
```

$$\text{PROFIT} = \text{REVENUE} - \text{COST}$$



AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4



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()
```

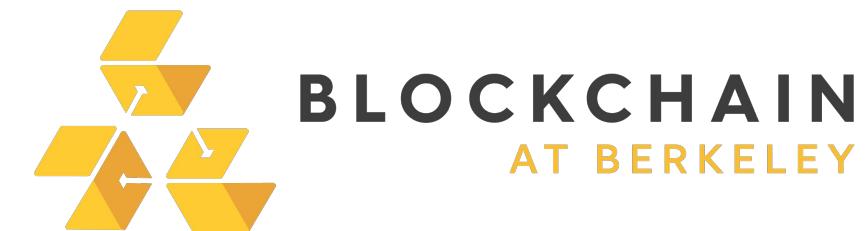


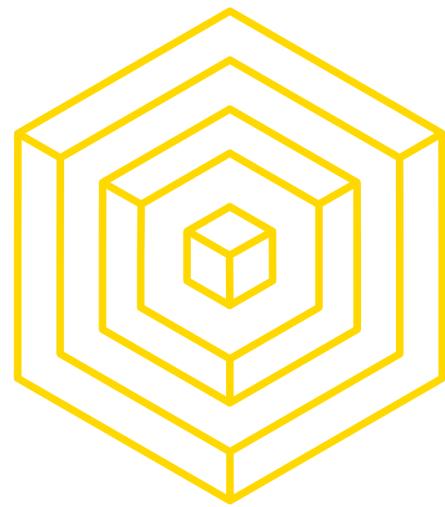
Image source: <https://profitbitcoin.com/>



AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4





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()
```

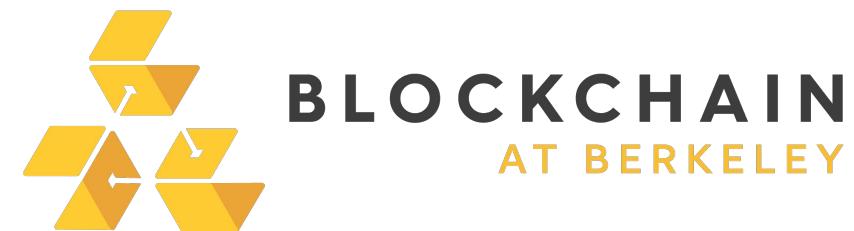


Image source: <https://profitbitcoin.com/>



AUTHOR: NADIR AKHTAR

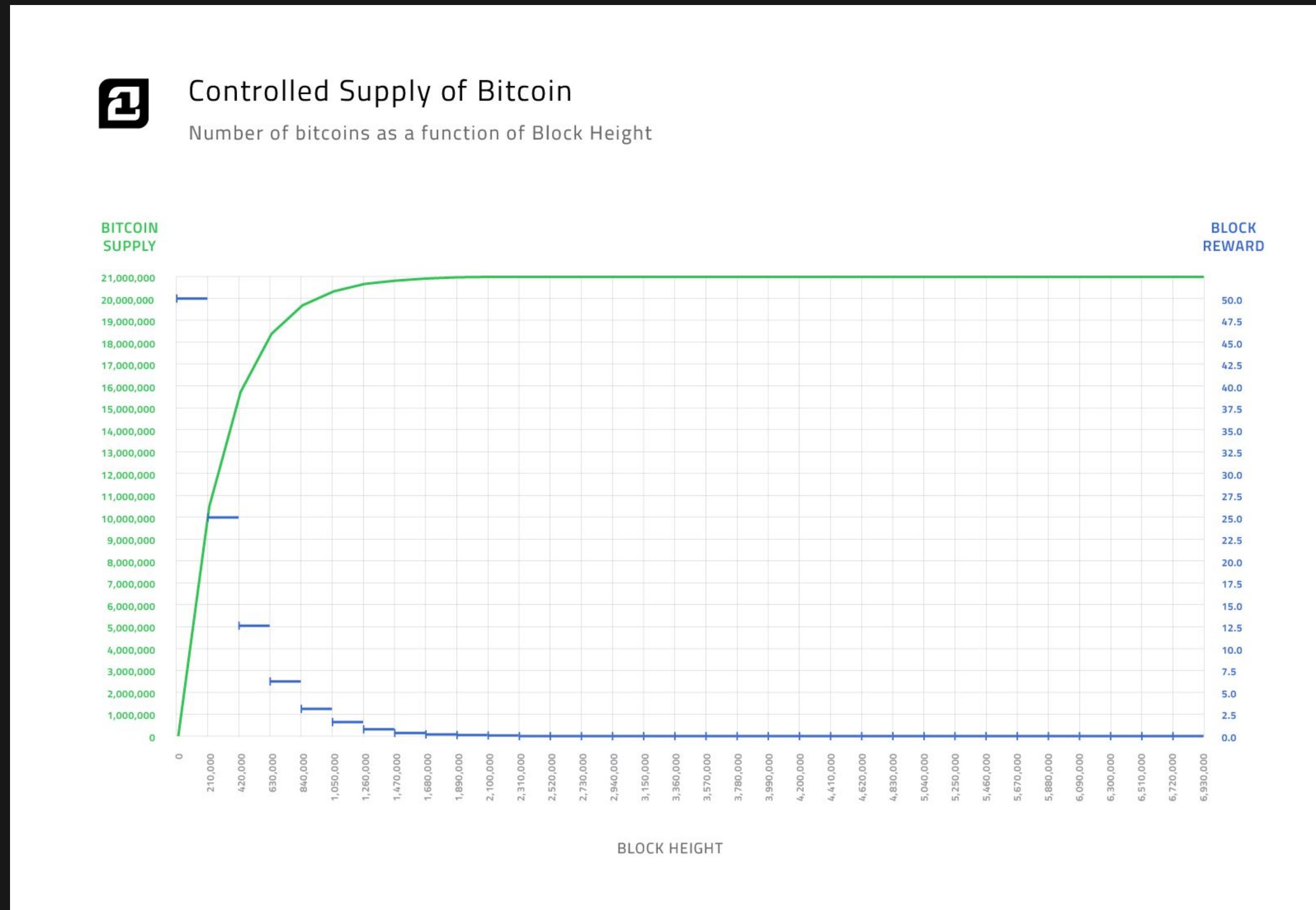
BLOCKCHAIN FUNDAMENTALS LECTURE 4





MINING INCENTIVES

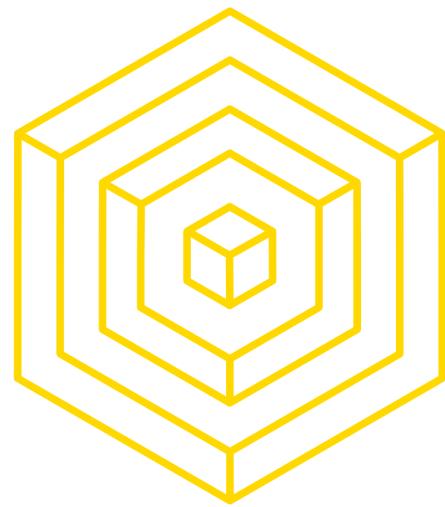
BLOCK REWARD



- 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



AUTHOR: NADIR AKHTAR



MINING INCENTIVES

HOW TO PROFIT FROM MINING

MINING_REVENUE = *BLOCK_REWARD* + TX_FEES

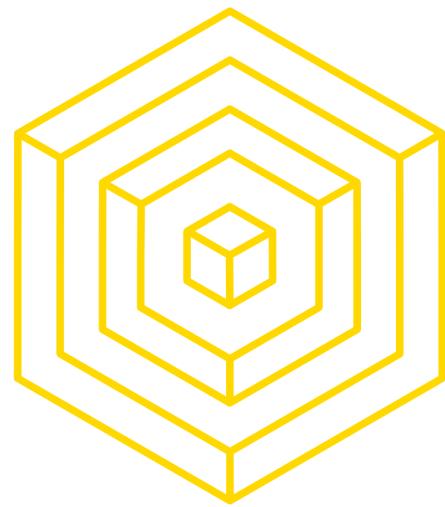
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

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



AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4



MINING INCENTIVES

HOW TO PROFIT FROM MINING

MINING_REVENUE = *BLOCK_REWARD* + *TX_FEES*

MINING_COST = FIXED_COSTS + VARIABLE_COSTS

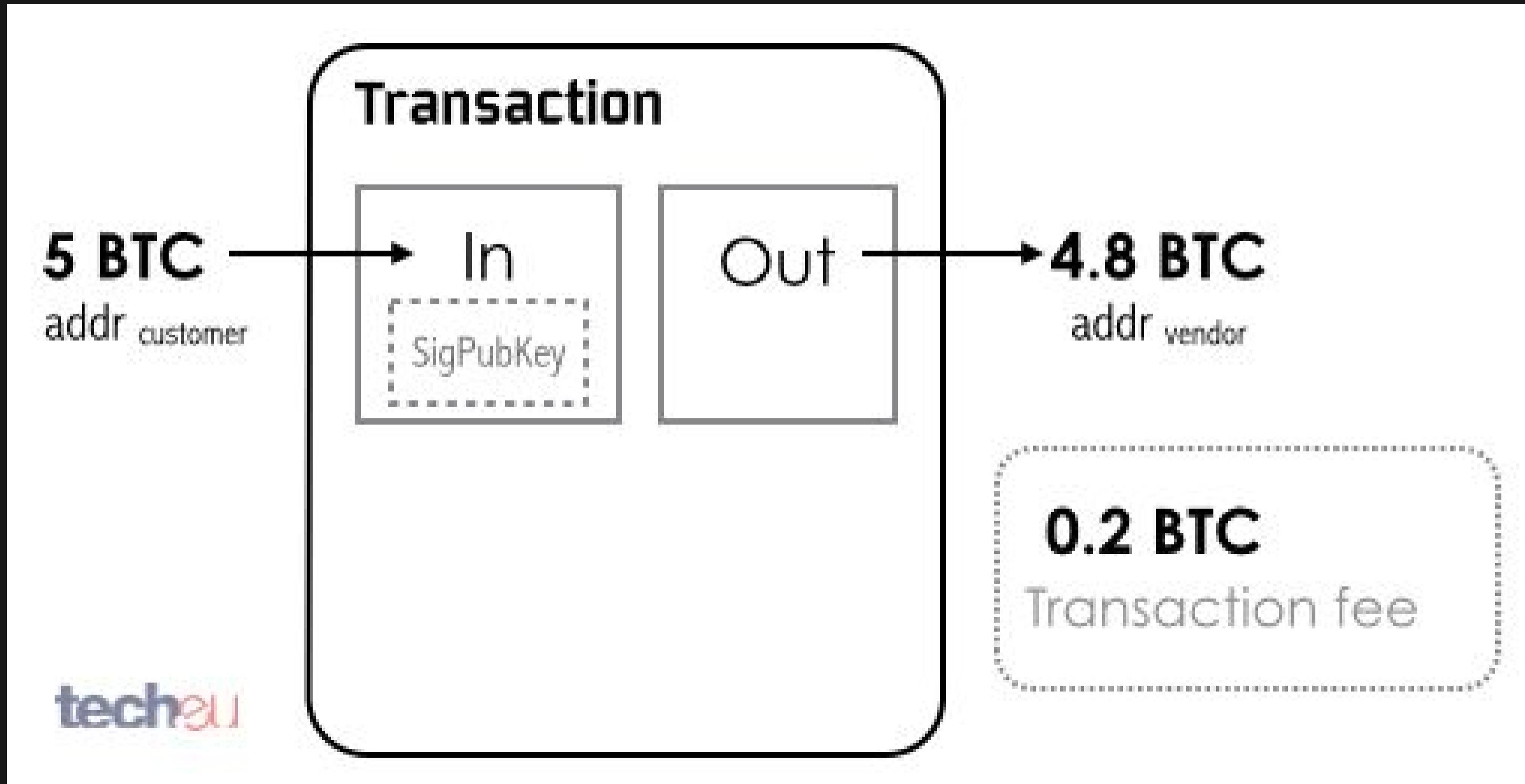
```
if MINING_REVENUE > MINING_COST:  
    miner.get_profit()
```





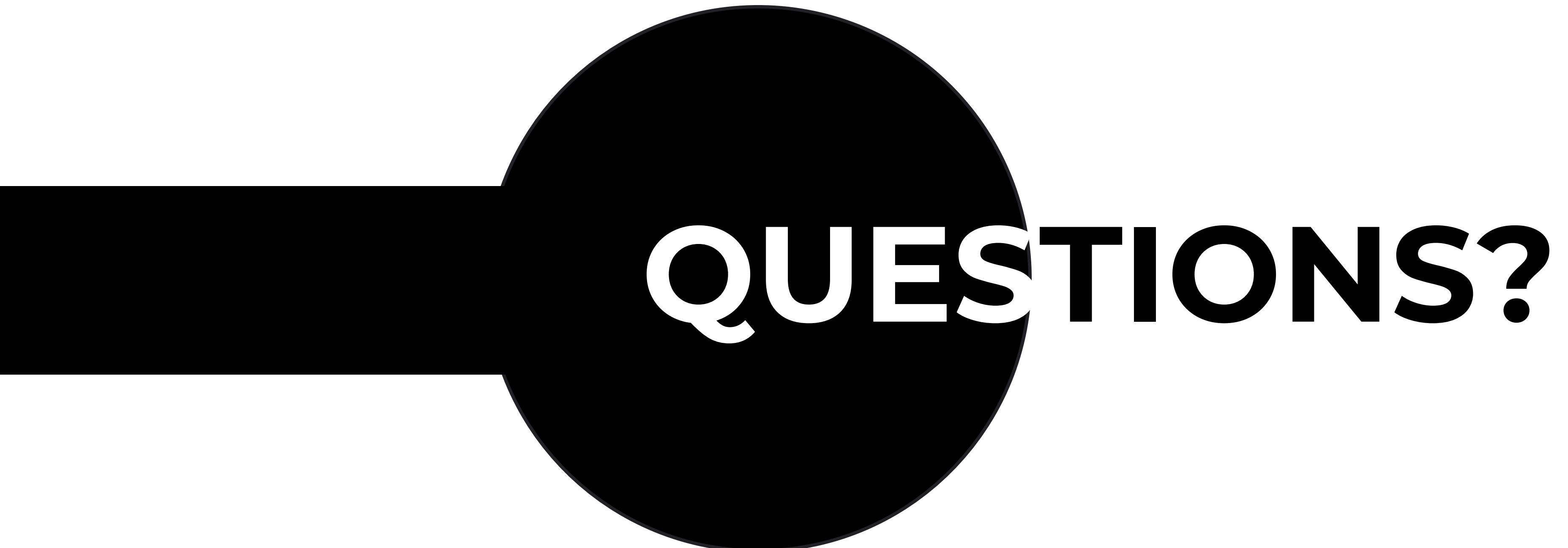
MINING INCENTIVES

TRANSACTION FEES

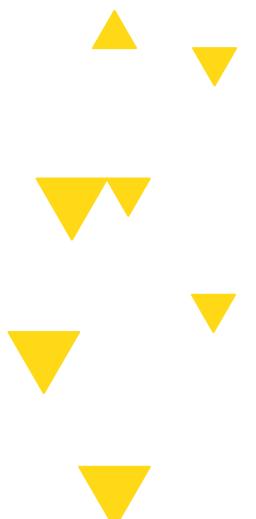


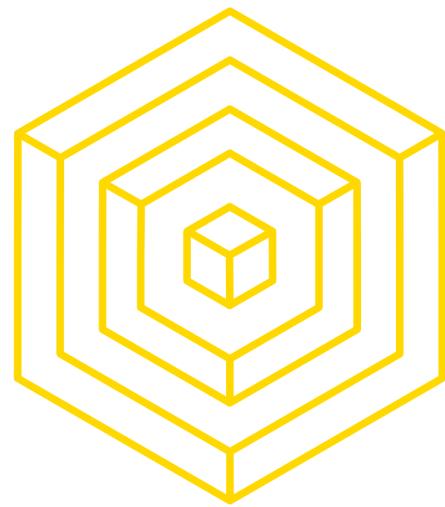
- Tx creator sets tx fee
 - Voluntary, but practically necessary...
- Extra income for miners on top of block reward (esp. as reward diminishes)
 - Higher transaction fee \Rightarrow faster confirmation time
- $\text{TX_FEE} = \text{INPUT} - \text{OUTPUT}$
- **When block reward becomes 0, TX fees will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

AUTHOR: NADIR AKHTAR



QUESTIONS?





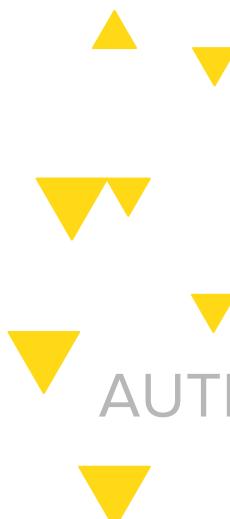
MINING INCENTIVES

HOW TO PROFIT FROM MINING

MINING_REVENUE = *BLOCK_REWARD* + *TX_FEES*

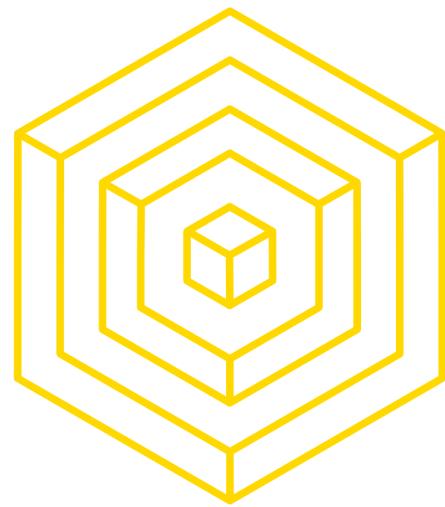
MINING_COST = FIXED_COSTS + VARIABLE_COSTS

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



AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4



MINING INCENTIVES

HOW TO PROFIT FROM MINING

MINING_REVENUE = *BLOCK_REWARD* + *TX_FEES*

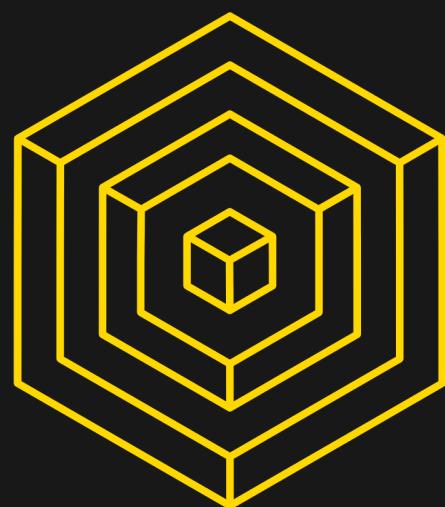
MINING_COST = *FIXED_COSTS* + VARIABLE_COSTS

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



AUTHOR: NADIR AKHTAR

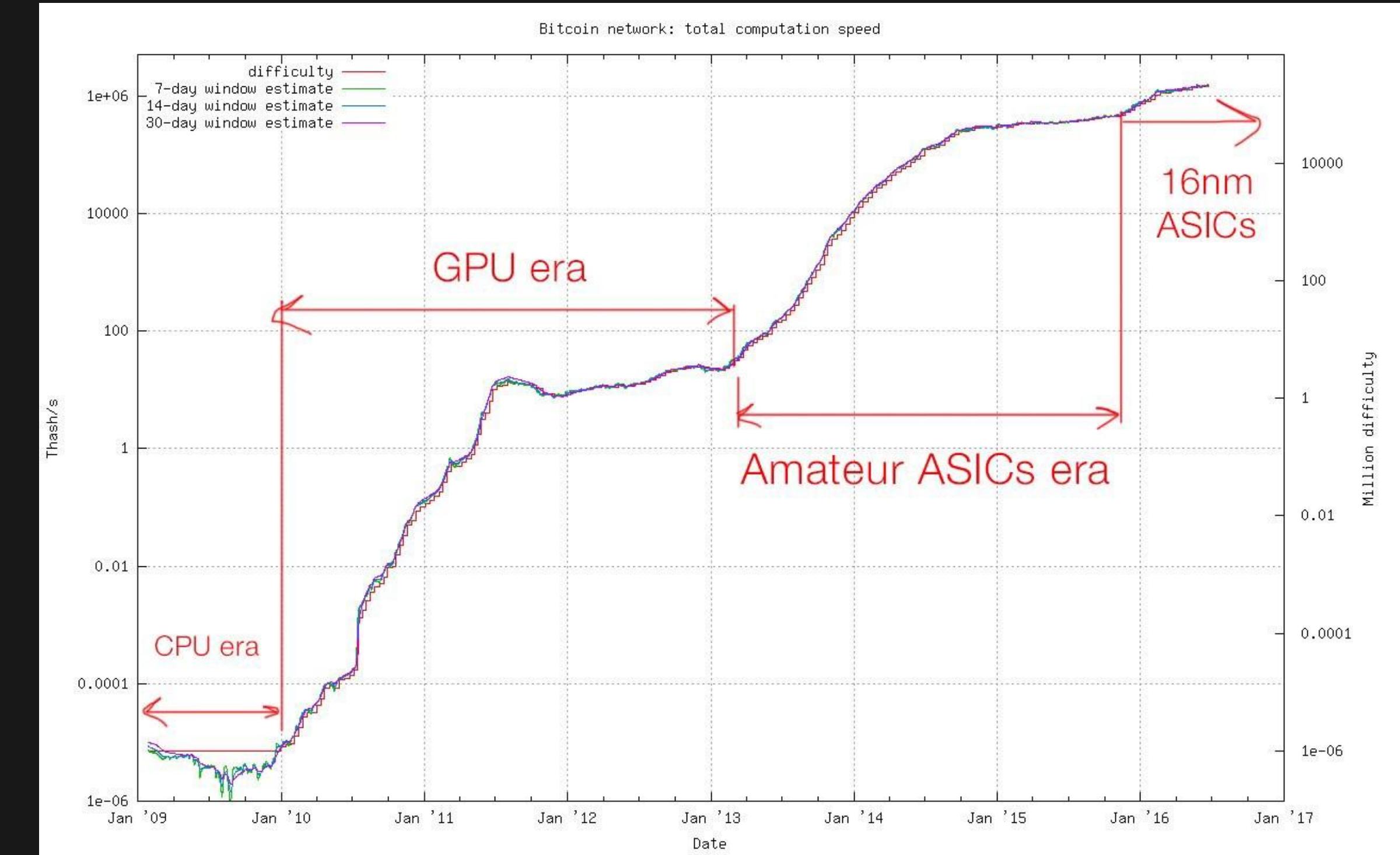
BLOCKCHAIN FUNDAMENTALS LECTURE 4



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





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



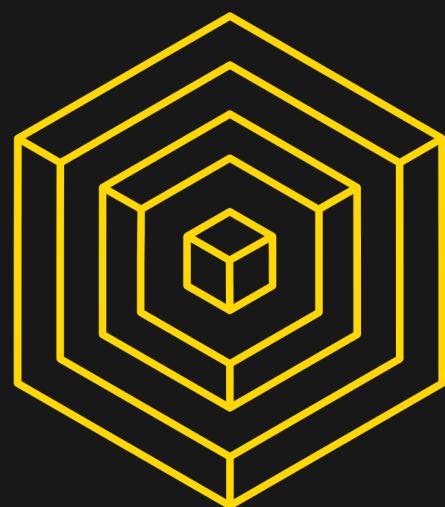


MINING INCENTIVES

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

- Field Programmable Gate Arrays
 - 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

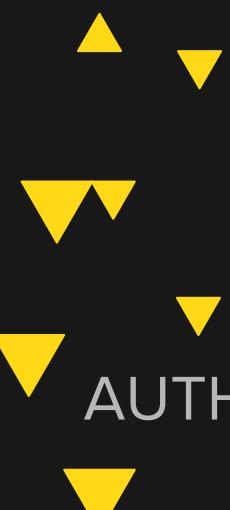


MINING INCENTIVES

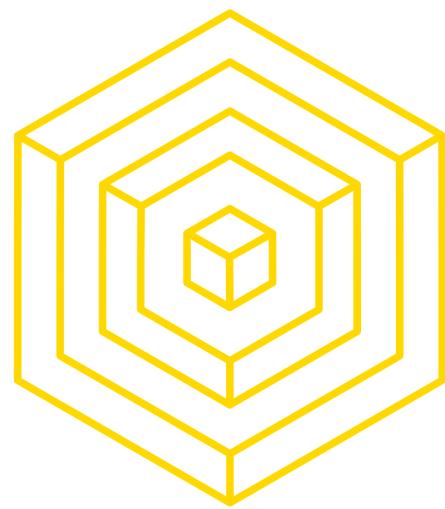
FIXED COST: ASIC MINING

	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

- **Application-Specific Integrated Circuit**
 - 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



AUTHOR: NADIR AKHTAR



MINING INCENTIVES

HOW TO PROFIT FROM MINING

MINING_REVENUE = *BLOCK_REWARD* + *TX_FEES*

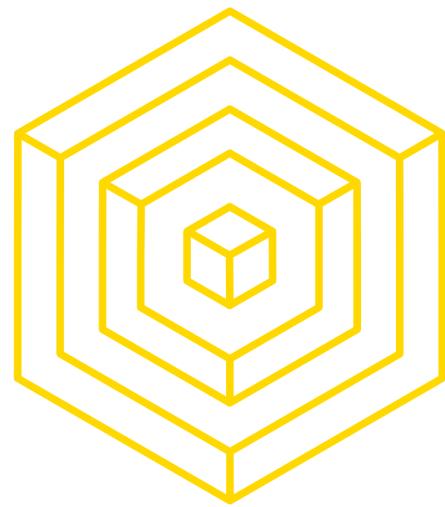
MINING_COST = *FIXED_COSTS* + VARIABLE_COSTS

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



AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4



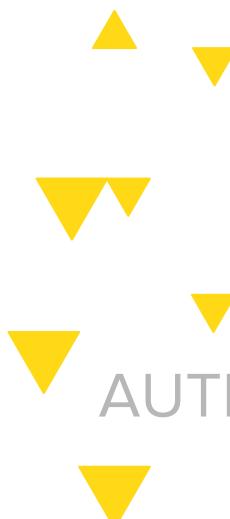
MINING INCENTIVES

HOW TO PROFIT FROM MINING

MINING_REVENUE = *BLOCK_REWARD* + *TX_FEES*

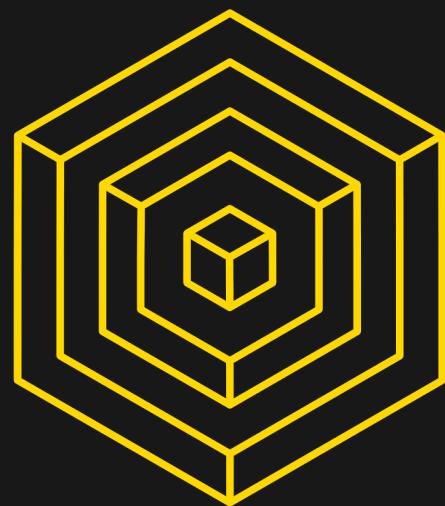
MINING_COST = *FIXED_COSTS* + *VARIABLE_COSTS*

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



AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4



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!

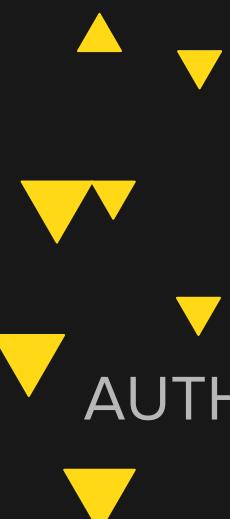
◀ ▶
▼
▼ ▼
▼ AUTHOR: MAX FANG



MINING INCENTIVES

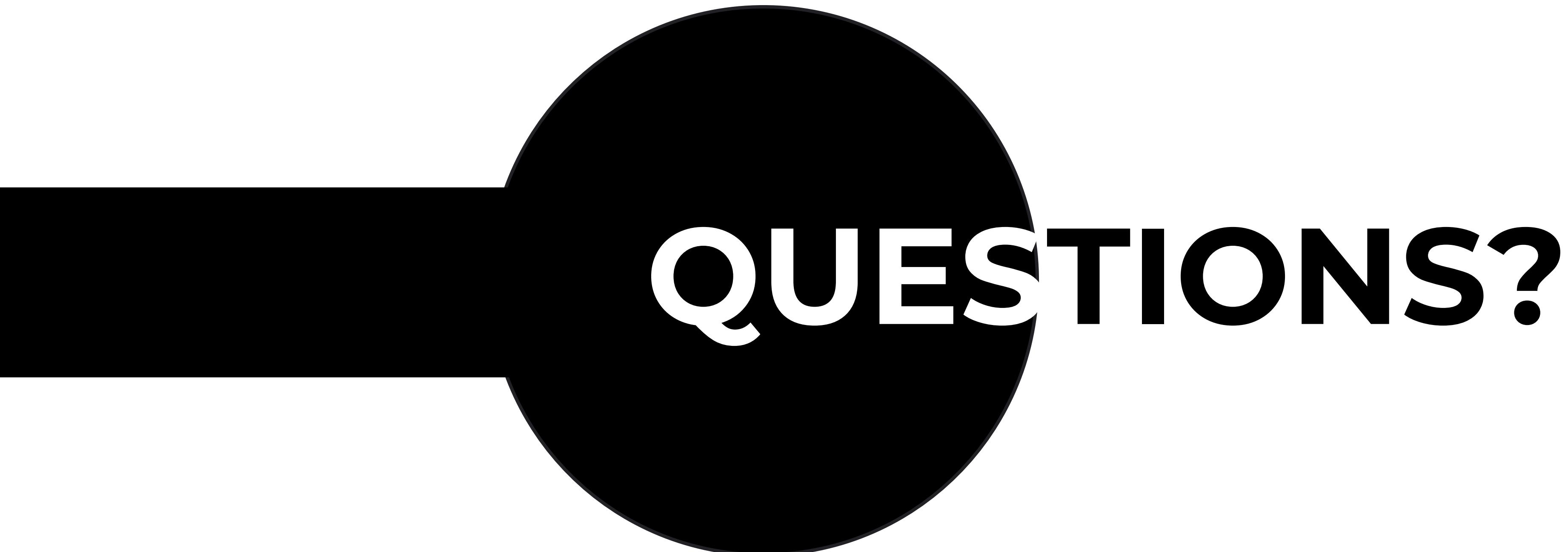
BLOCK REWARD: RATIONALE

- 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)

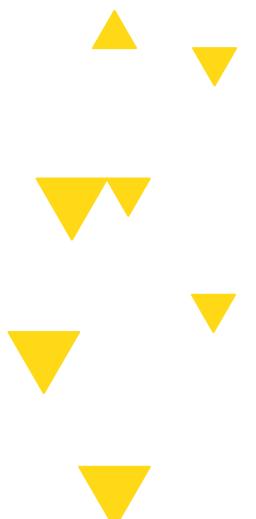


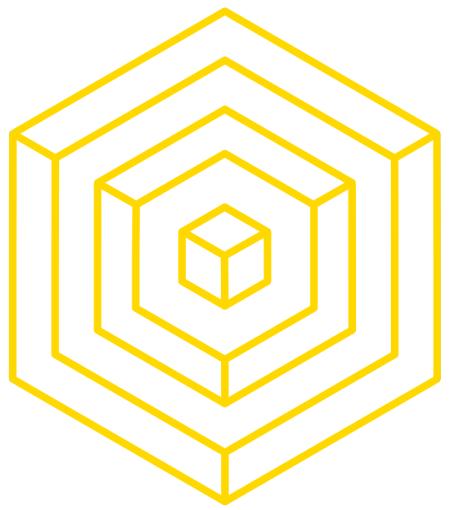
AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4



QUESTIONS?

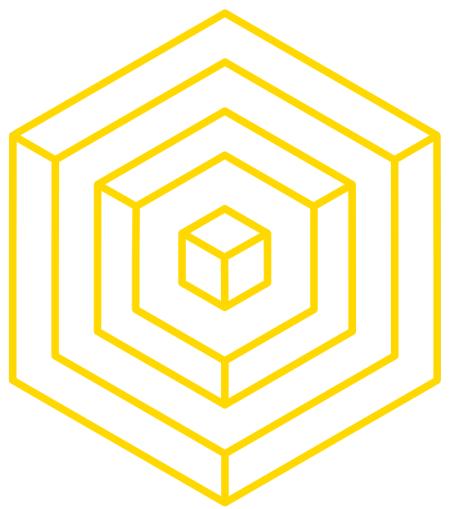




4

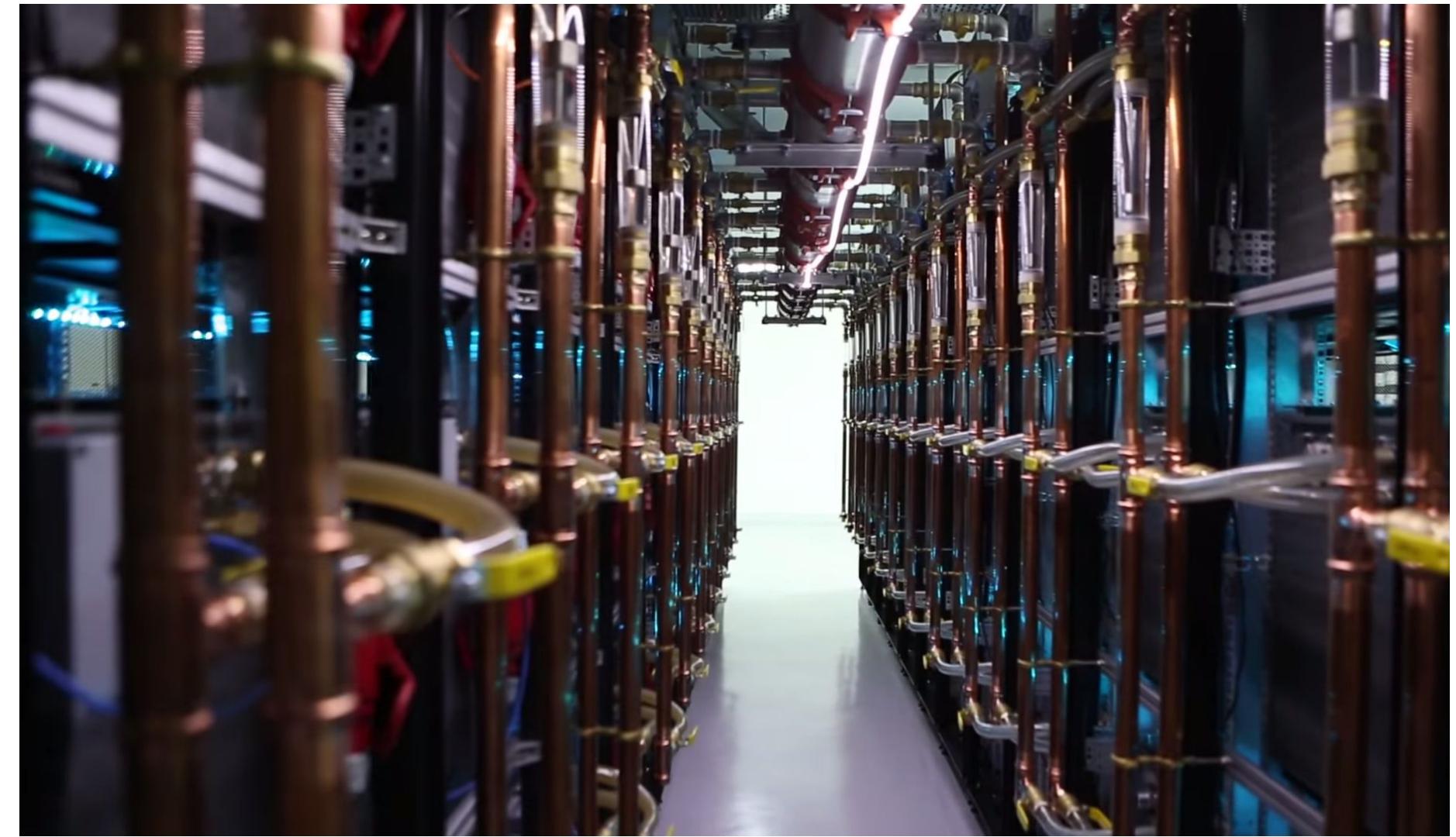
REAL WORLD MINING

BLOCKCHAIN FUNDAMENTALS LECTURE 4



REAL WORLD MINING

CHINESE ASIC MINING FARM

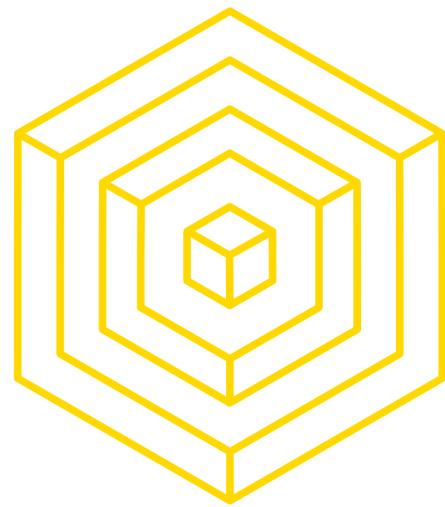


Source: https://www.theregister.co.uk/2014/08/12/chinese_bitcoin_farms_from_scifi_to_scuzzy/



AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4



REAL WORLD MINING

ASICS



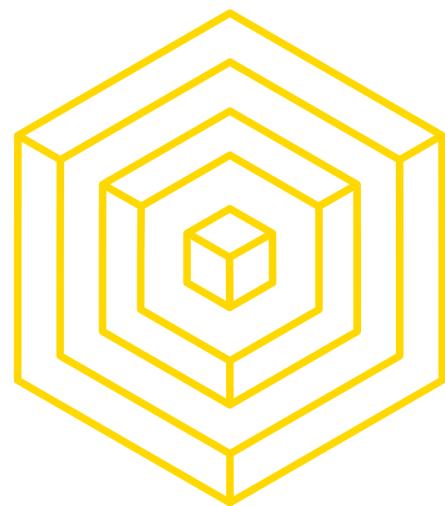
Source:

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

Source: https://sc01.alicdn.com/kf/HTB18YN_JFXXXXcqXFXXq6xFXXXw/221223714/HTB18YN_JFXXXXcqXFXXq6xFXXXw.jpg

AUTHOR: NADIR AKHTAR

BLOCKCHAIN FUNDAMENTALS LECTURE 4



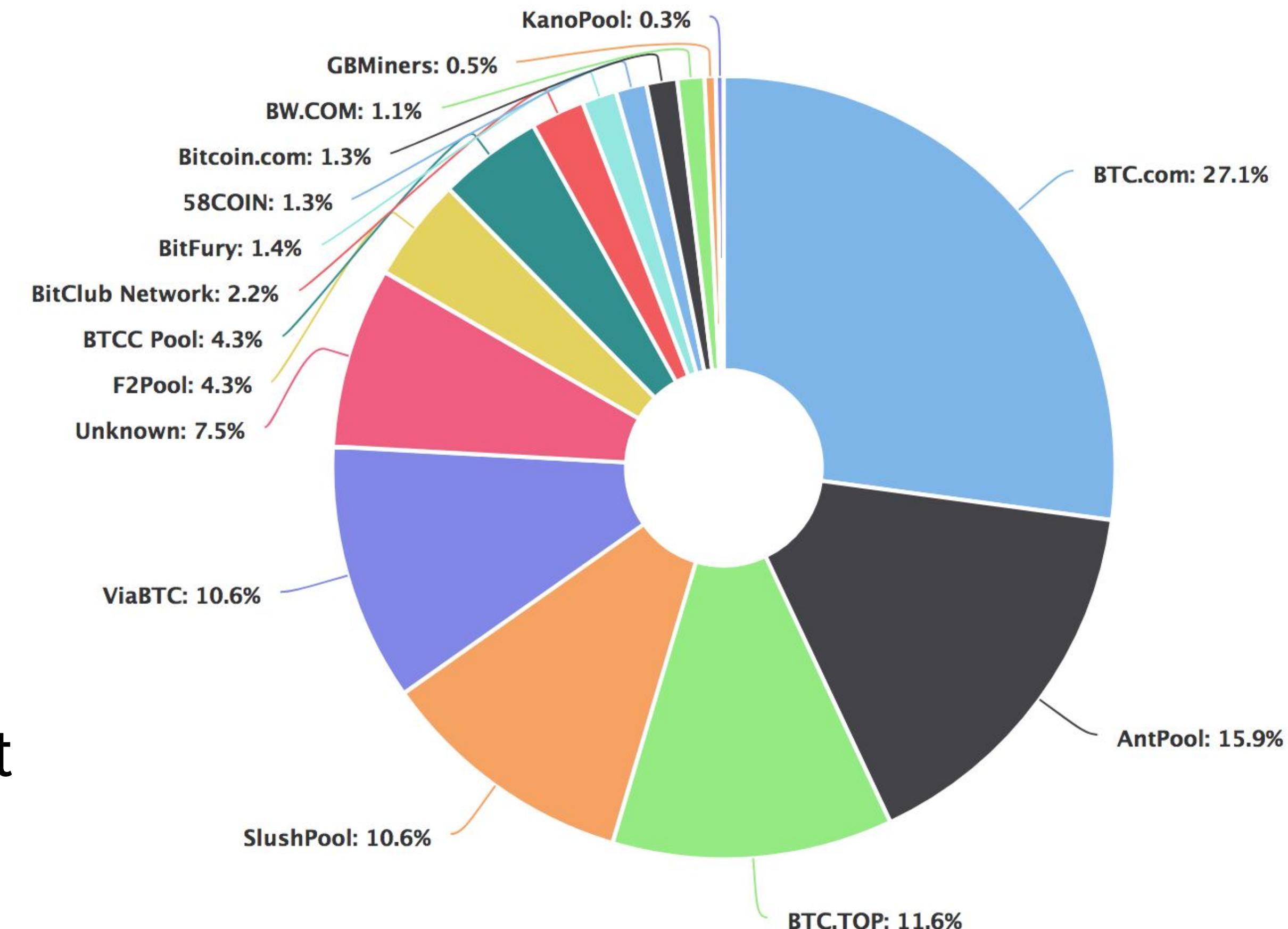
REAL WORLD MINING

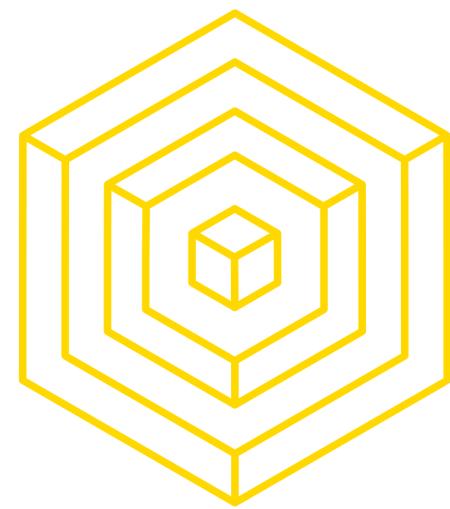
MINING POOLS

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:
blockchain.info (2/16/18)





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

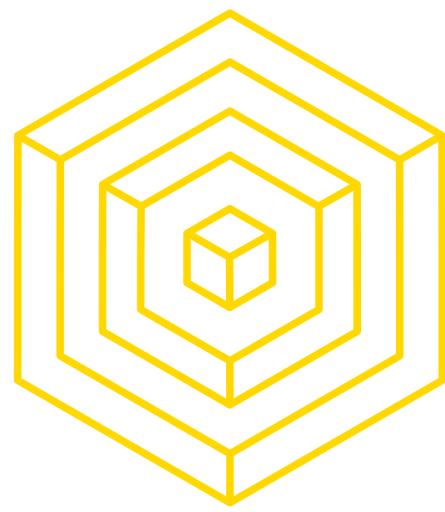
FAQ: Why can't someone submit shares in a pool and keep the reward of the valid block for themselves?

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



AUTHOR: MAX FANG

BLOCKCHAIN FUNDAMENTALS LECTURE 4



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

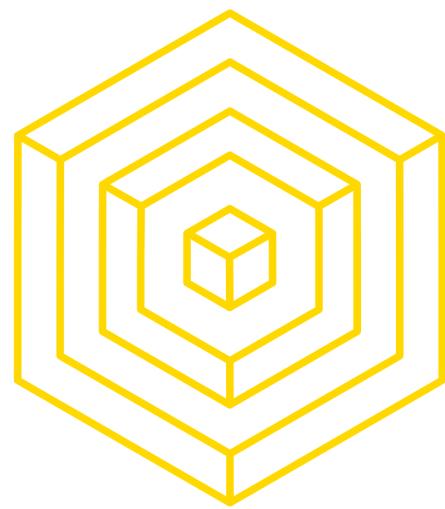


AUTHOR: MAX FANG

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



REAL WORLD MINING

MINING POOLS

Source:
blockchain.info (2/16/18)

Pros

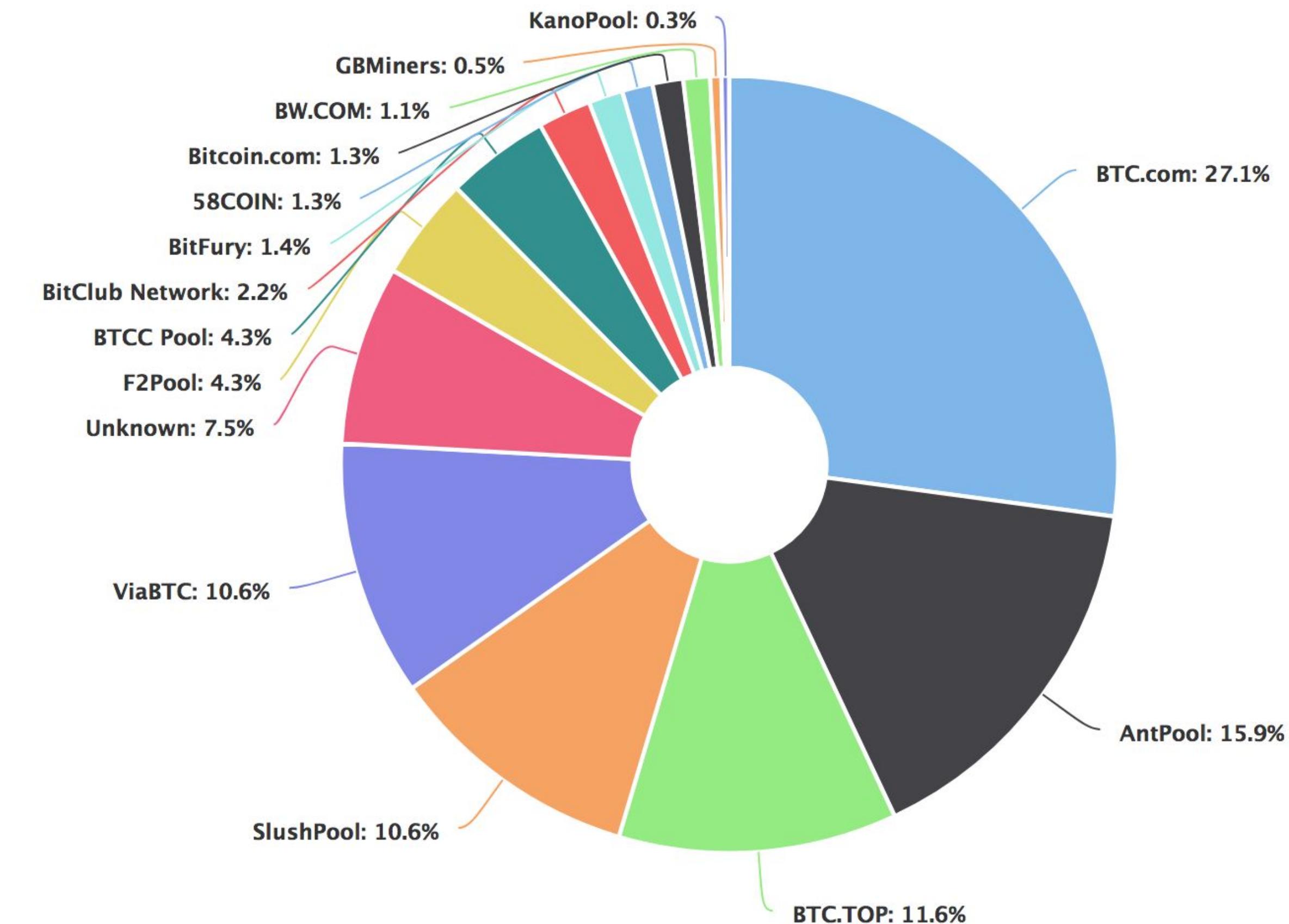
- Allows individual miners to participate
- Easy to upgrade software changes

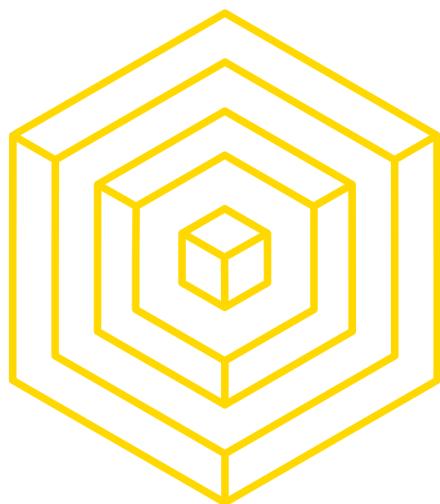
Cons

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



AUTHOR: MAX FANG





REAL WORLD MINING

MINING POOLS

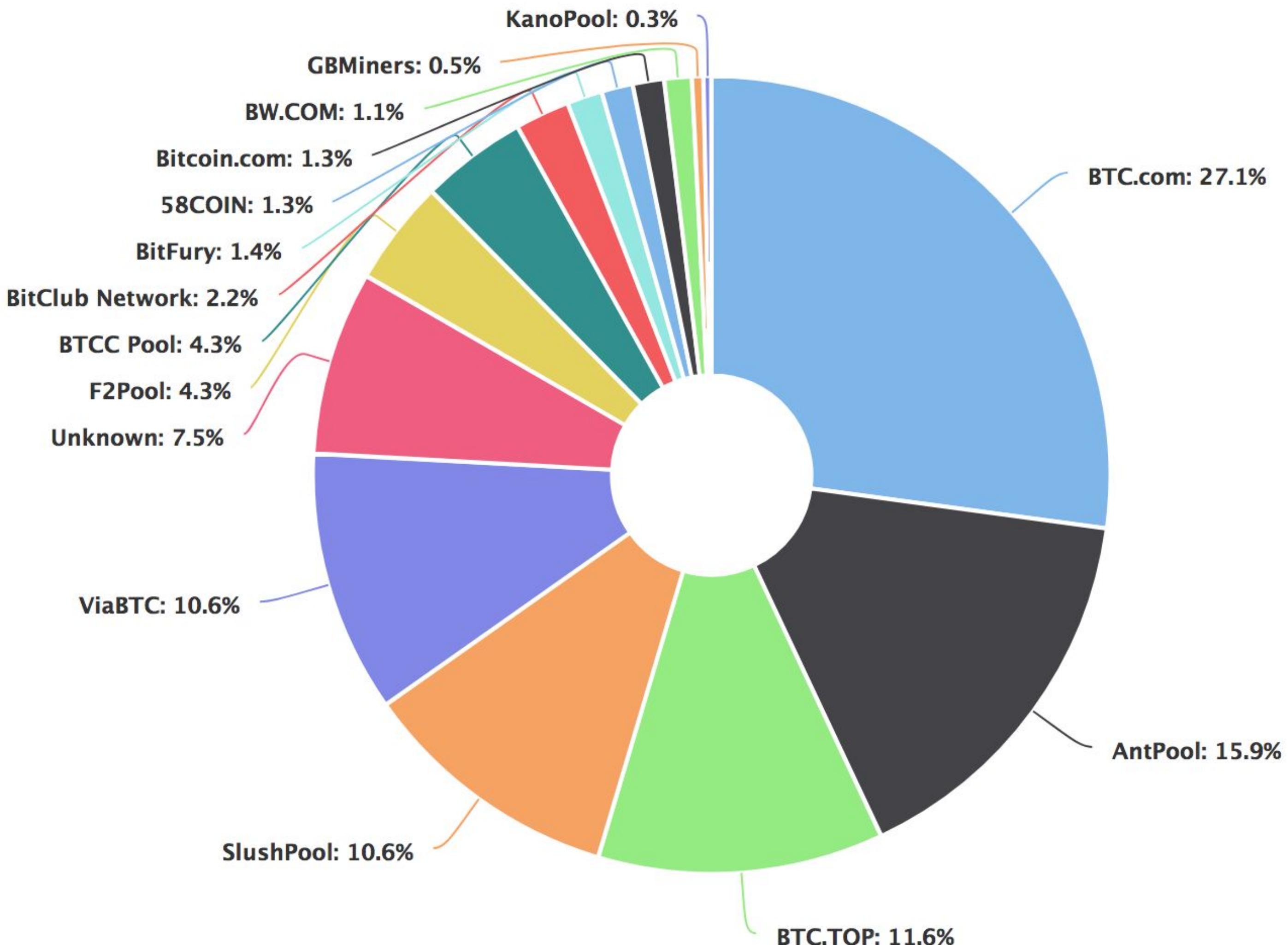
Community exhibits backlash against large mining pools

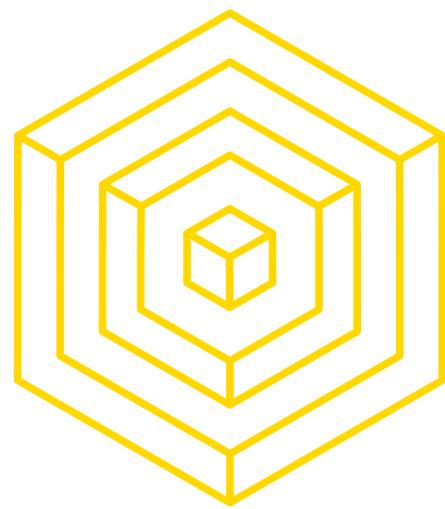
- Ex: GHash.io in 2014

Single entity might be participating in multiple pools

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

Source:
blockchain.info (2/16/18)





REAL WORLD MINING

MINING POOLS

Quick facts

- Today's (2/15/18) network hashrate:
25,579,249 TH/s
- Mining Reward / yr = $(1 \text{ yr} / 10 \text{ mins}) * 12.5 =$
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** = $(14 \text{ TH/s}) / (25,579,249 \text{ TH/s}) = 0.0000005473186\%$

Expected Annual Reward

- $0.0000005473186 * 657k / \text{yr}$
 $\approx 0.35958832 \text{ BTC / yr} \approx \$3623.11 / \text{yr}$

Solo mining

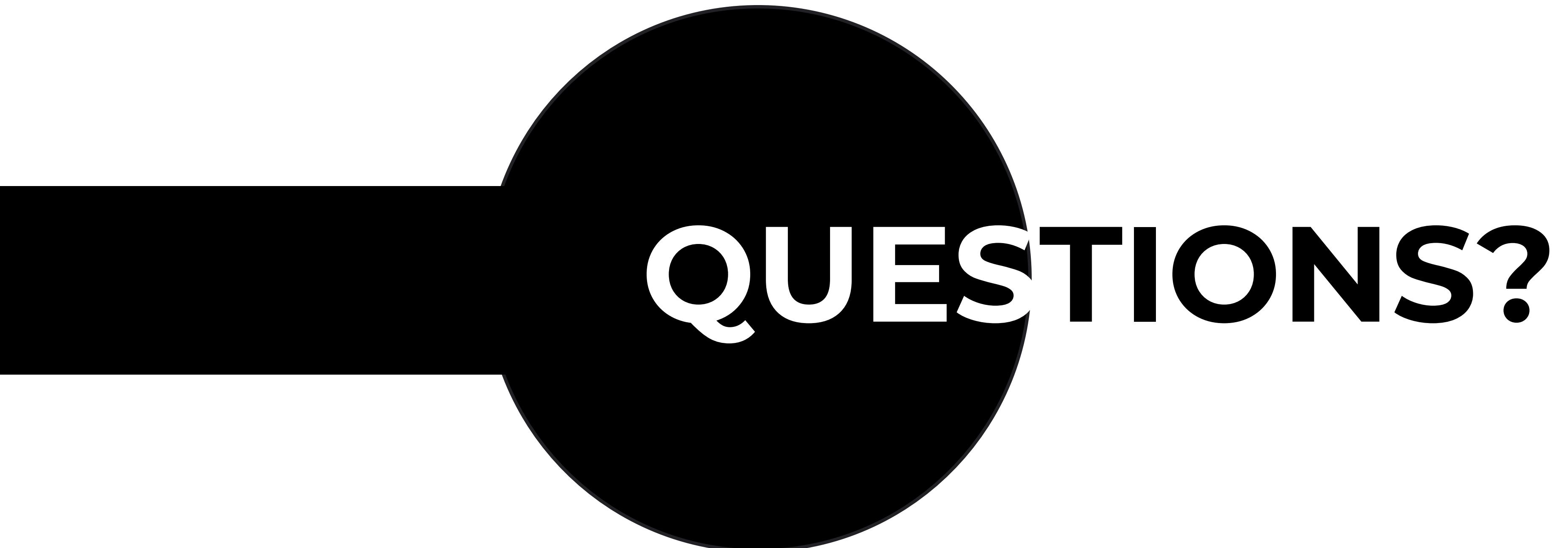
- 1 block mined per 1,827,089 blocks
 $\Rightarrow 12.5 \text{ BTC every } 12,688 \text{ days}$
 $\Rightarrow \$125,000 \text{ once every } 34.8 \text{ years}$

Mining with mining pool

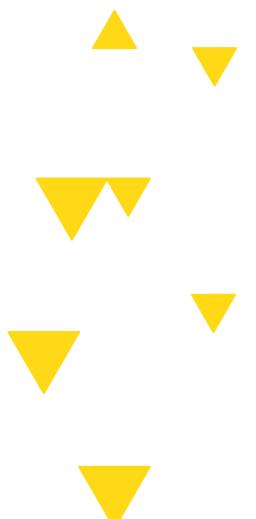
- Assume pool has $\frac{1}{6}$ network hashrate
 - Pool finds every 6th block ≈ 1 per hr
- $\$10,000 / 8760 \text{ hrs/yr} \approx \0.42 every hour

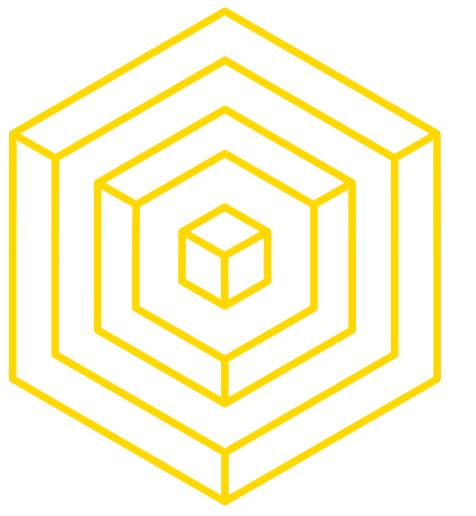
Paradox:

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



QUESTIONS?

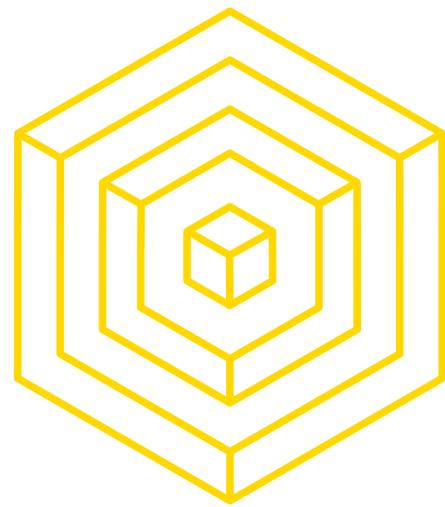




5

CHANGING BITCOIN

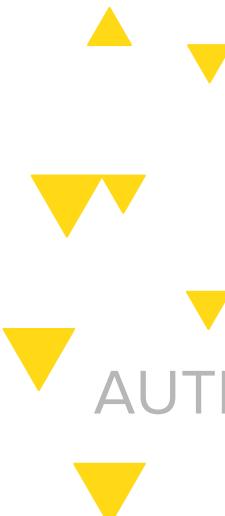
BLOCKCHAIN FUNDAMENTALS LECTURE 4



DECENTRALIZING MINING

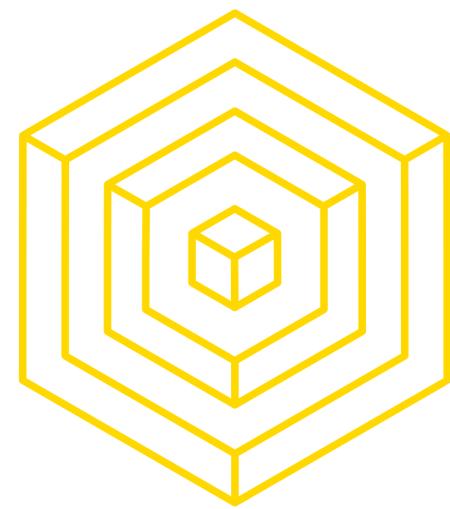
PUZZLE REQUIREMENTS REVIEW

- 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



AUTHOR: MAX FANG

BLOCKCHAIN FUNDAMENTALS LECTURE 4



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:

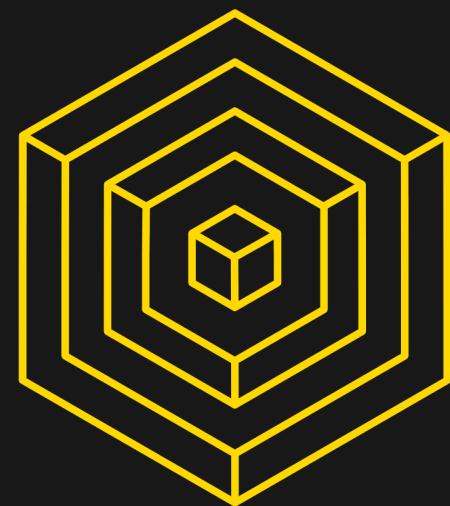
- Used for hashing passwords
- Hard to brute-force

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!



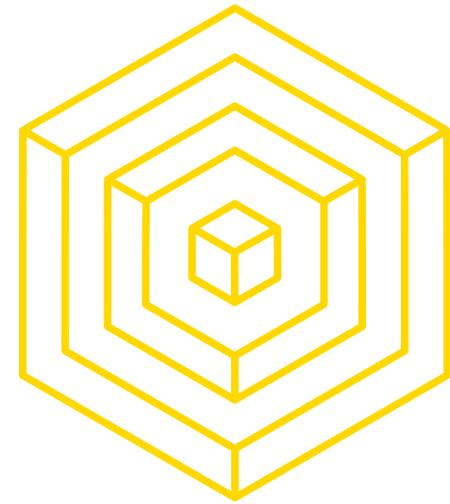
AUTHOR: MAX FANG

Figure 8.1: Scrypt pseudocode

```

1 def scrypt(N, seed):
2     V = [0] * N // initialize memory buffer of length N
3
4     // Fill up memory buffer with pseudorandom data
5     V[0] = seed
6     for i = 1 to N:
7         V[i] = SHA-256(V[i-1])
8
9     // Access memory buffer in a pseudorandom order
10    X = SHA-256(V[N-1])
11    for i = 1 to N:
12        j = X % N // Choose a random index based on X
13        X = SHA-256(X ^ V[j]) // Update X based on this index
14
15    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
 - Easy to work around
 - Not implemented

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

AUTHOR: MAX FANG

[Pinldea 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

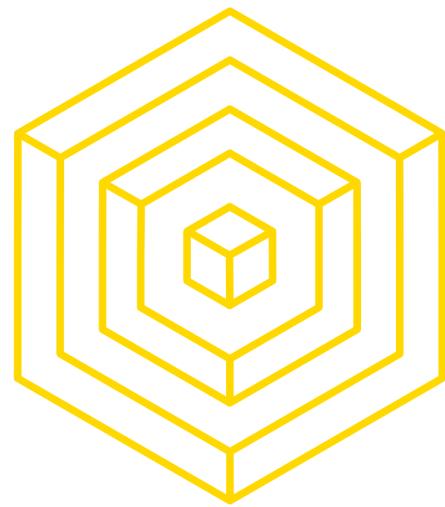
Joined: Mar 5, 2015
Messages: 51
Likes Received: 65
Trophy Points: 58

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. Pinldea will be the only distributor for the Shooter Chip X11 Miners.

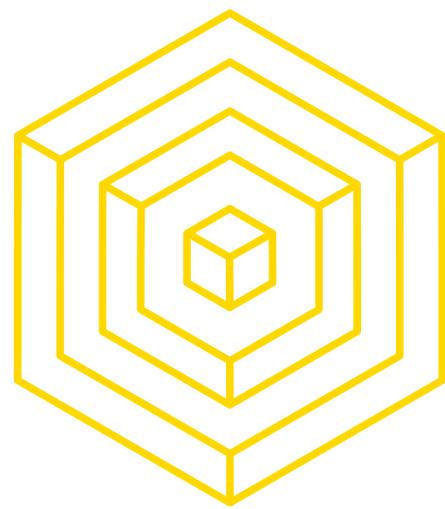


DECENTRALIZING MINING

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





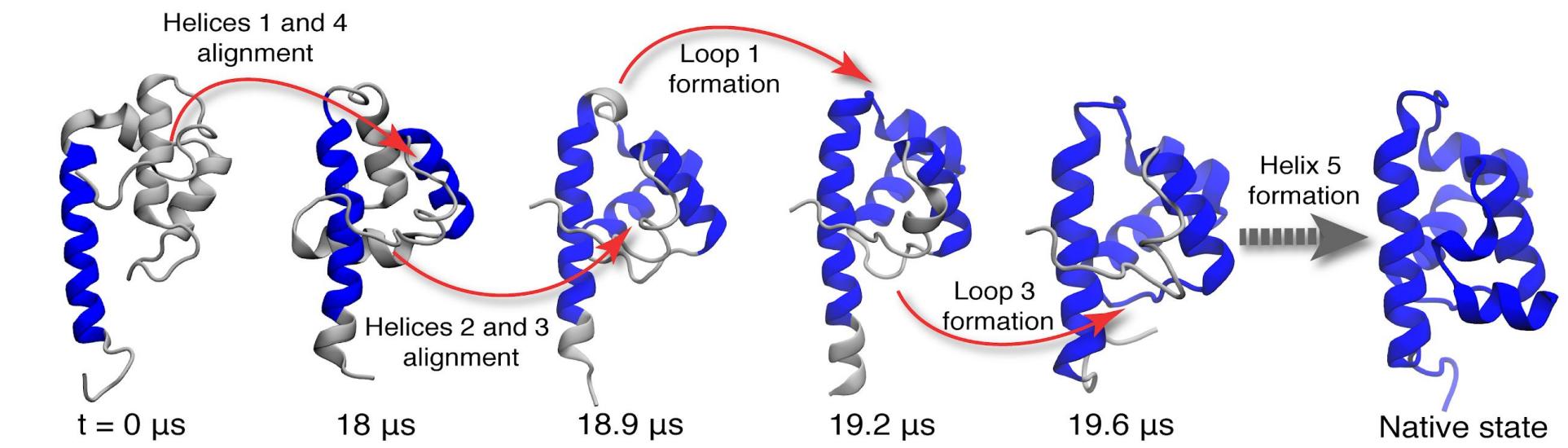
EXTRA: PROOF-OF-USEFUL-WORK

NOT A PUZZLING CONCEPT

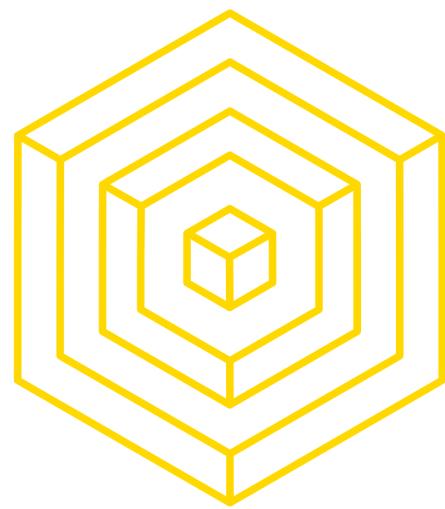
- “Repurpose” computing power

- 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



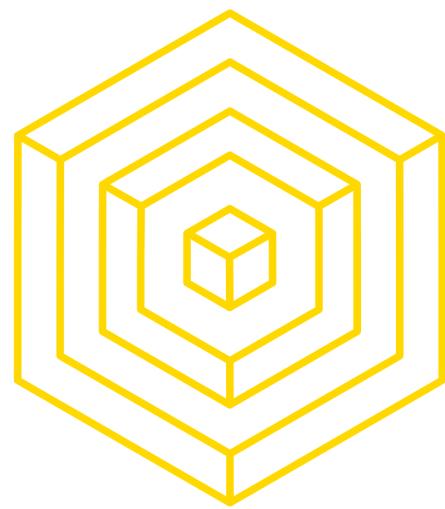
EXTRA: PROOF-OF-USEFUL-WORK

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**



AUTHOR: MAX FANG



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



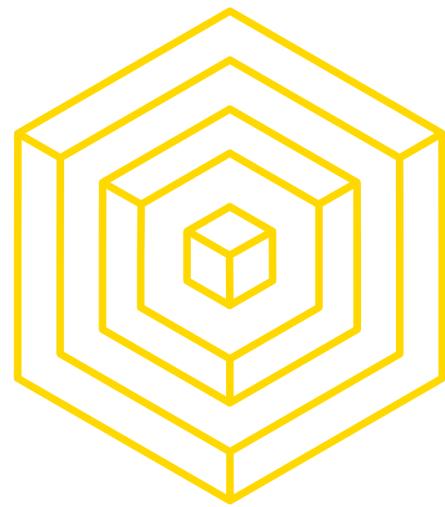
BitcoinCore
Helping you keep Bitcoin decentralized

[Download Bitcoin Core](#)



AUTHOR: NADIR AKHTAR

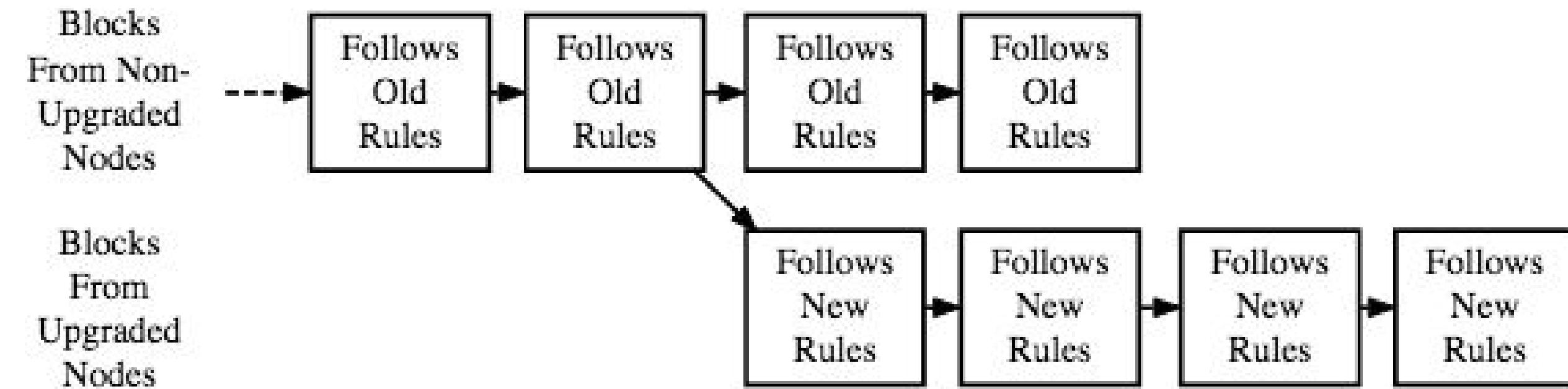
BLOCKCHAIN FUNDAMENTALS LECTURE 4



CONSENSUS UPDATES

FORKS

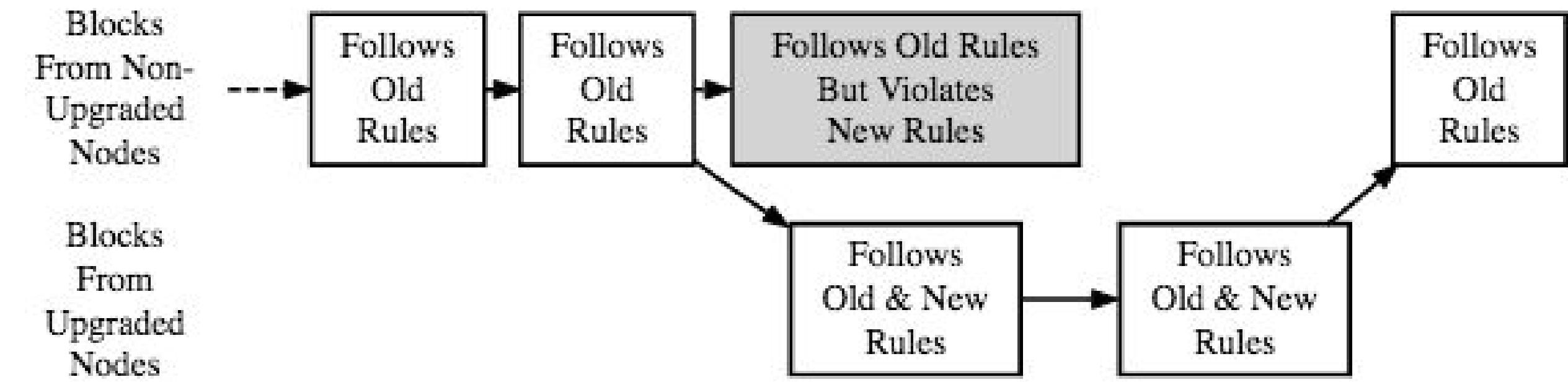
Hard Fork



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

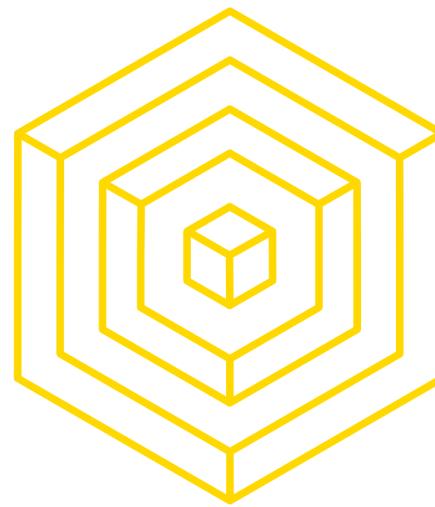
Source: Bitcoin.org Developer Guide

Soft Fork



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

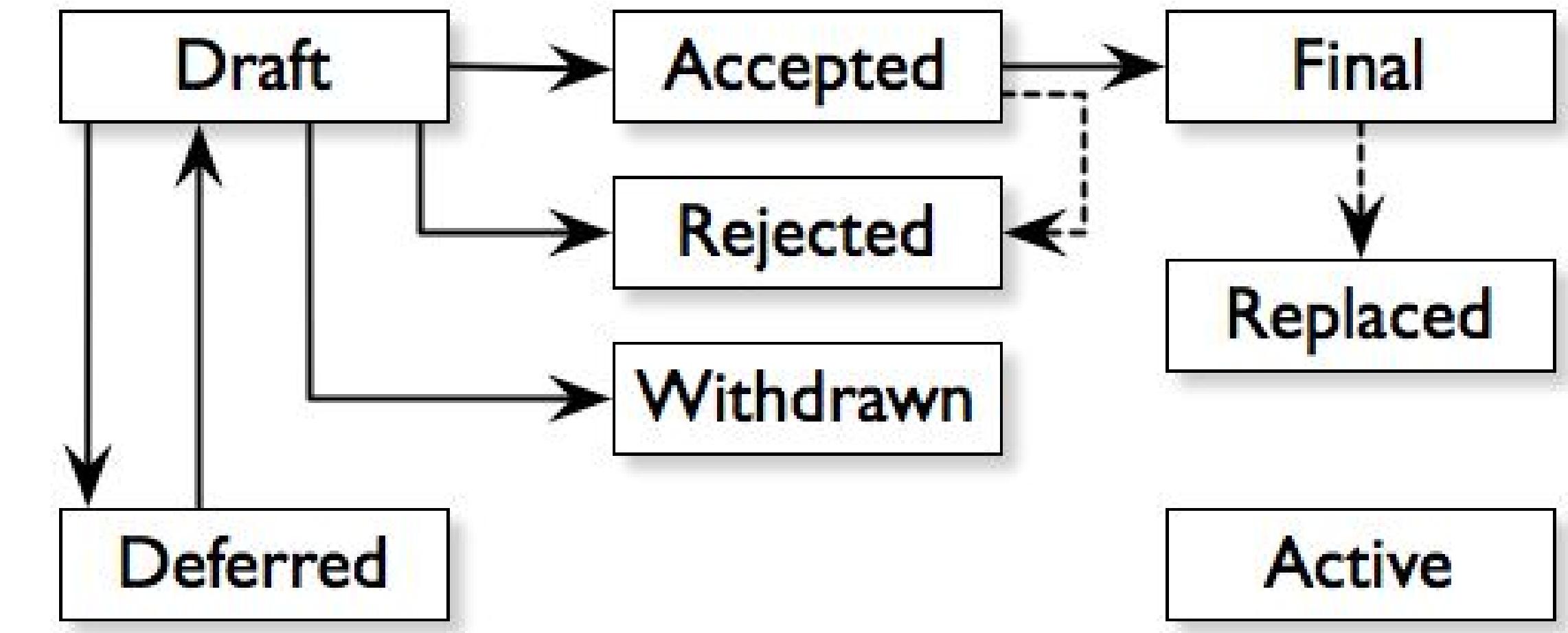
AUTHOR: MAX FANG



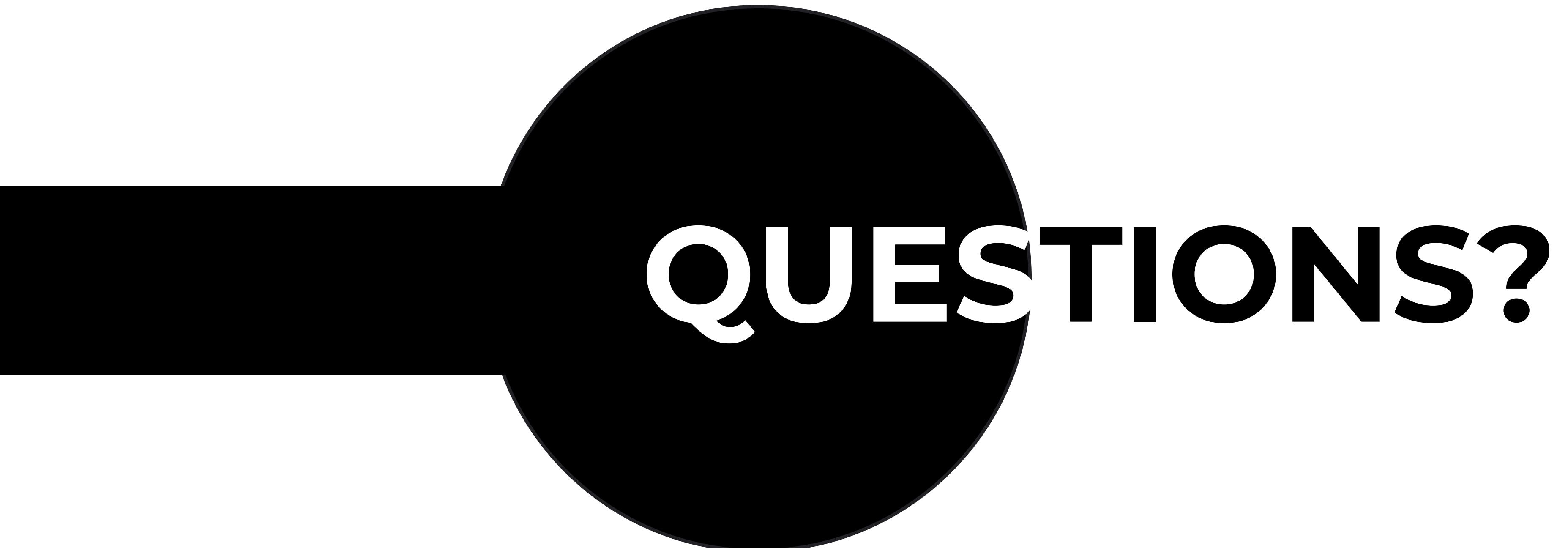
CONSENSUS UPDATES

BITCOIN IMPROVEMENT PROPOSAL (BIP)

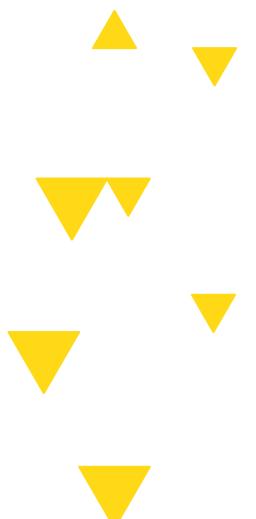
- **BIP:** Bitcoin Improvement Proposal
 - Three types:
 - Standards Track BIPs
 - Informational BIPs
 - Process BIPs
- First BIP proposed by Amir Taaki on 2011-08-19
- Signal support for a BIP by including reference in block when mining

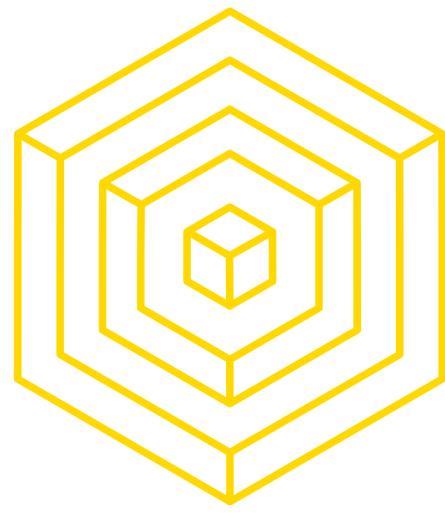


Source: https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals



QUESTIONS?





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)