Cryptocurrency, Blockchain, and a new economic world

OLLI

LATE SUMMER 2021

LECTURE 3

Bebo White - bebo.white@gmail.com

ANOTHER CRYPTOLAND OLLI ADVENTURE

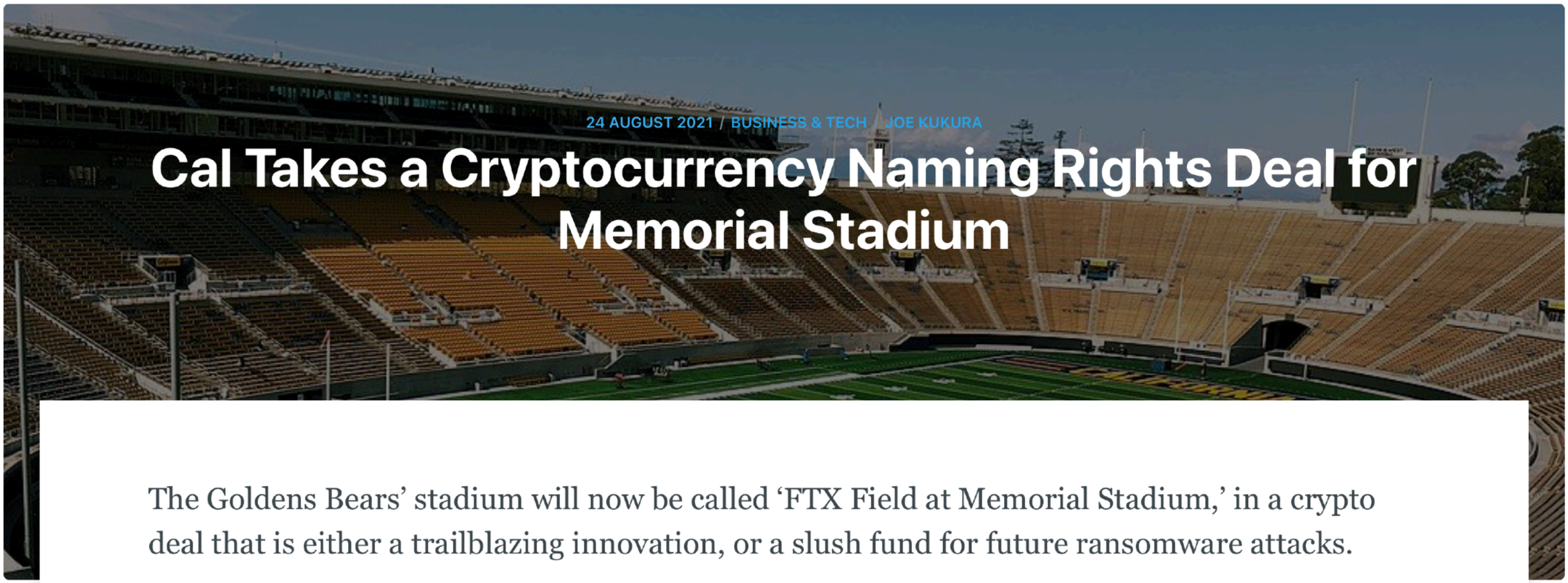
THE MYSTERIOUS DARK RECTANGLES ON THE SLIDES AND VIDEO

- artifacts from Zoom sharing screen (e.g., chat box and menus)
- apparently due to video optimization
- I will rely on Nick to keep track of questions in the chat box.

RE: PAUL KRUGMAN OP-ED

- I certainly don't want to pretend that I know more than Krugman or dismiss his opinions
- however, cryptocurrency is unprecedented in the history of money/economics/banking/finance and no one has experience with it
- cryptocurrency is such a controversial topic, we must consider all points of view
- it also gave me an excuse to discuss "the Long Nose!"

ANY CAL GRADS OUT THERE?



24 AUGUST 2021 / BUSINESS & TECH / JOE KUKURA

Cal Takes a Cryptocurrency Naming Rights Deal for Memorial Stadium

The Goldens Bears' stadium will now be called 'FTX Field at Memorial Stadium,' in a crypto deal that is either a trailblazing innovation, or a slush fund for future ransomware attacks.

Crypto bros will be even more un-'bear'-ably smug and mansplainy than usual today, as their form of alleged digital money has notched a new milestone. The Chronicle reports that UC Berkeley has struck a 10-year, $17.5 million stadium naming rights deal with a cryptocurrency exchange. The crypto exchange is called FTX, who already bought the naming rights to the Miami Heat arena earlier this year, and according to Cal Berkeley, this is the first ever cryptocurrency sponsorship of a college stadium name.

BIG WEEK FOR COINBASE

The Ratings Game

Coinbase is on its way to becoming 'one-stop shop' for all things crypto, analyst says

Published: Aug. 24, 2021 at 12:50 p.m. ET

By Emily Bary

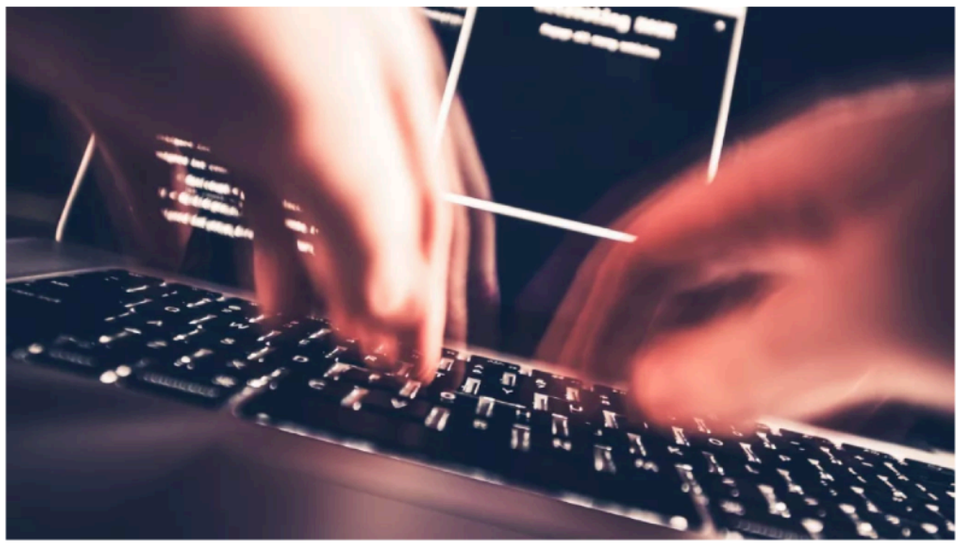
Company is seeing fast growth in its staking business and could continue to show momentum there

coinbase

Coinbase customers up in arms after hackers drain crypto wallets

By Anthony Spadafora about 22 hours ago

Another reason to store your crypto in a hardware wallet instead



(Image credit: Shutterstock)

An increasing number of users of the highly popular cryptocurrency exchange Coinbase have found their accounts on the platform empty after hackers managed to gain access to them and drain their cryptocurrency wallets.

MARKETS

Coinbase is buying $500 million in crypto and investing future profits into a crypto portfolio

PUBLISHED FRI, AUG 20 2021•8:55 AM EDT | UPDATED FRI, AUG 20 2021•9:53 AM EDT

Tanaya Macheel
@TANAYAMAC

SHARE

KEY POINTS

- CEO Brian Armstrong said he hopes to operate more of the company's operations using crypto, though it's mixed today.
- The company plans to invest in "Ethereum, Proof of Stake assets, DeFi tokens, and many other crypto assets supported for trading on our platform," finance chief Alesia Haas said in a blog post.

TRENDING NOW

WHAT DOES THIS MEAN?

Forbes

Aug 21, 2021, 06:30am EDT | 98,446 views

‘Urgent’ Warning Issued Over The Future Of Bitcoin Even As The Crypto Market Price Smashes Past $2 Trillion

Billy Bambrough Senior Contributor ⓘ
Crypto & Blockchain
I write about how bitcoin, crypto and blockchain can change the world.

Listen to this article now -04:04
Powered by Trinity Audio

Bitcoin and cryptocurrencies have seen a huge resurgence over the last year following the brutal so-called crypto winter that began in 2018.

The bitcoin price has this year climbed to never-before-seen highs, topping $60,000 per bitcoin before falling back slightly. Other smaller cryptocurrencies have risen at an even faster clip than bitcoin, with many making percentage gains into the thousands.

Now, as bitcoin and cryptocurrencies begin to carve out a place among traditional assets in investor portfolios, technologists have warned that advances in quantum computing could mean the encryption that underpins bitcoin is "fundamentally" undermined as soon as 2026—unless the software is updated.

The generation of public-private key pairs is based upon the factorization of very large numbers.

Reversing that factorization is very difficult (impossible?) for conventional computers to do. But, it’s the type of problem that quantum computers are very good at.

We should finish up the heavy "techie" background today!

NOW YOU UNDERSTAND HOW TO RECEIVE (GET PAID) AND SEND (PAY) WITH CRYPTOCURRENCY

- a wallet
- the role of your public (and private) keys
- security (including backing up/not losing your wallet and credentials


Crypto
Nation


Pay what you want
Lemonade
bitcoin
ACCEPTED HERE


LEMONAID
FOR SALE
25¢
OR
0.000023 BTC

SAN FRANCISCO, CA 94127

Hello Thomas, I'm going to cut to the chase. My name is RedTruth43 and I know about the secret you are keeping from your wife and everyone else. More importantly, I have *evidence* of what you have been hiding. I won't go into the specifics here in case your wife intercepts this, but you know what I am talking about.

You don't know me personally and nobody hired me to look into you. Nor did I go out looking to burn you. It is just your bad luck that I stumbled across your misadventures while working a job around San Francisco. I then put in more time than I probably should have looking into your life. Frankly, I am ready to forget all about you and let you get on with your life. And I am going to give you two options that will accomplish that very thing. Those two options are to either ignore this letter, or simply pay me $15,100. Let's examine those two options in more detail.

Option 1 is to ignore this letter. Let me tell you what will happen if you choose this path. I will take this evidence and send it to your wife. And as insurance against you intercepting it before your wife gets it, I will also send copies to her friends, family and to all your nearest neighbors. So, Thomas, even if you decide to come clean with your wife, it won't protect her from the humiliation she will feel when her friends and family find out your sordid details from me.

Option 2 is to pay me $15,100. We'll call this my "confidentiality fee". Now let me tell you what happens if you choose this path. Your secret remains your secret. You go on with your life as though none of this ever happened. Though you may want to do a better job at keeping your misdeeds secret in the future.

At this point you may be thinking, "I'll just go to the cops." Which is why I have taken steps to ensure this letter cannot be traced back to me. So that won't help, and it won't stop the evidence from destroying your life. I'm not looking to break your bank. I just want to be compensated for the time I put into investigating you.

So let's assume you have come to the obvious conclusion that your best option is to pay the fee. You will pay me anonymously using bitcoin. If you want me to keep your secret, then send $15,100 in **BITCOIN** to the ***Receiving Bitcoin Address*** listed at the bottom of this letter. **Payment MUST be received within 9 days of the post marked date on this letter's envelope**. Tell no one what you will be using the bitcoin for or they may not sell it to you. The procedure to obtain bitcoin can take a day or two so do not put it off. If I don't receive the bitcoin by the deadline, I will go ahead and release the evidence to everyone, and then the least you could do is tell your wife so she can prepare her friends and family before they find out.

Required Amount: $15,100

Receiving Bitcoin Address: 18NQEfGiiZtB4m4nLRvAhF5qPmJTk1TtUy

Explorer › Bitcoin Explorer › Address

Search your transaction, an address or a block

USD

Address

USD BTC

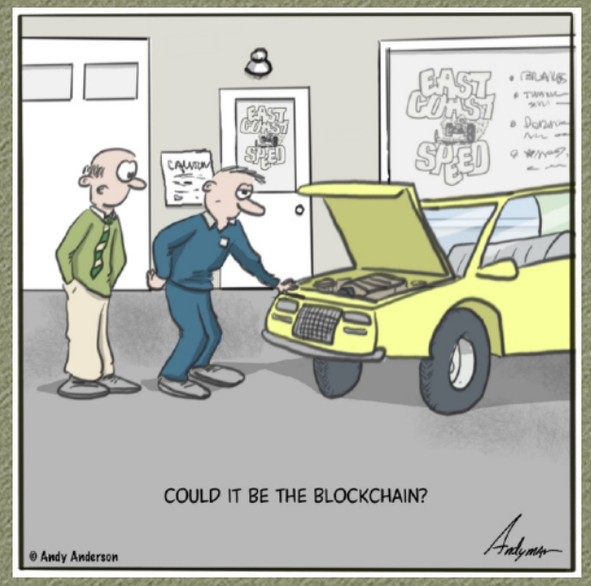
This address has transacted 0 times on the Bitcoin blockchain. It has received a total of 0.00000000 BTC ($0.00) and has sent a total of 0.00000000 BTC ($0.00). The current value of this address is 0.00000000 BTC ($0.00).

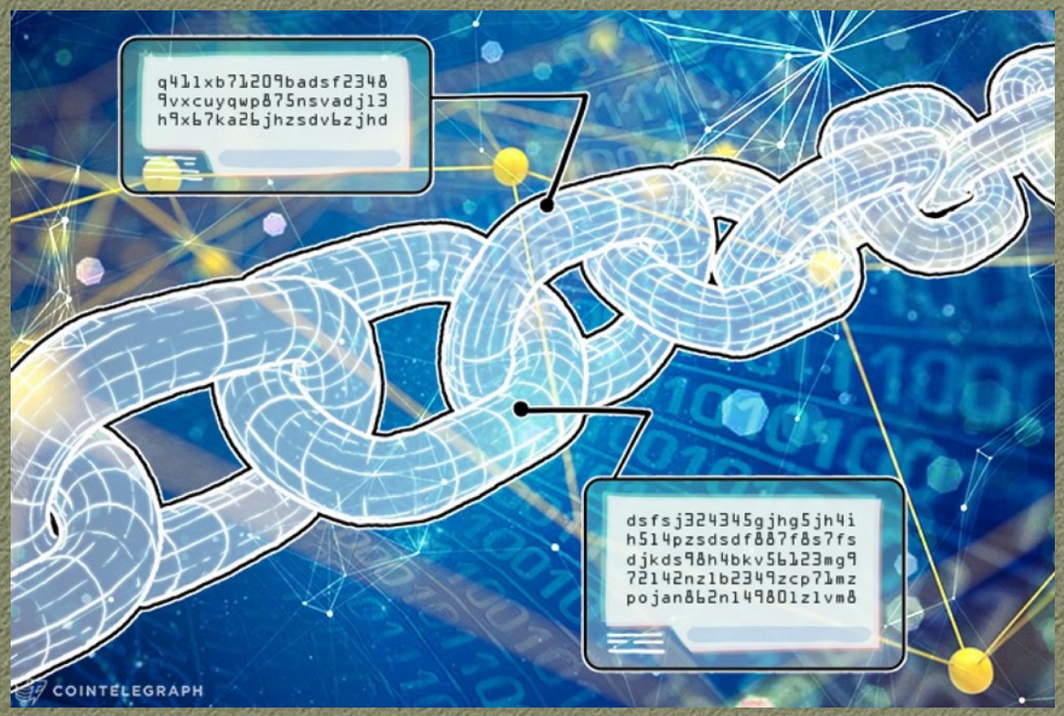
Address	18NQEfGiiZtB4m4nLRvAhF5qPmJTk1TtUy
Format	BASE58 (P2PKH)
Transactions	0
Total Received	0.00000000 BTC
Total Sent	0.00000000 BTC
Final Balance	0.00000000 BTC

- a gift certificate is a wallet (paper wallet)
- so has public and private keys
- typically recipient will “sweep” account
- other purposes?

HASHING REMINDERS

- hash functions (e.g., SHA256, etc.) are publicly and freely available and proven robust (NSA and NIST) which is why they can be so generally used and trusted
- do not trust "home grown" hash function
- the military probably/certainly has hash functions that are secret
- remember that hashing is not encryption since it is only one-way (not reversible)
- "breaking" a hash function means finding more that one text string that yields the same hash value ("a collision")





RIDING ON THE BLOCKCHAIN

HOW THE BLOCKCHAIN AND CRYPTOCURRENCY WORK TOGETHER

"Perhaps one of the lasting disruptive legacies of the cryptocurrency discussion is blockchain"

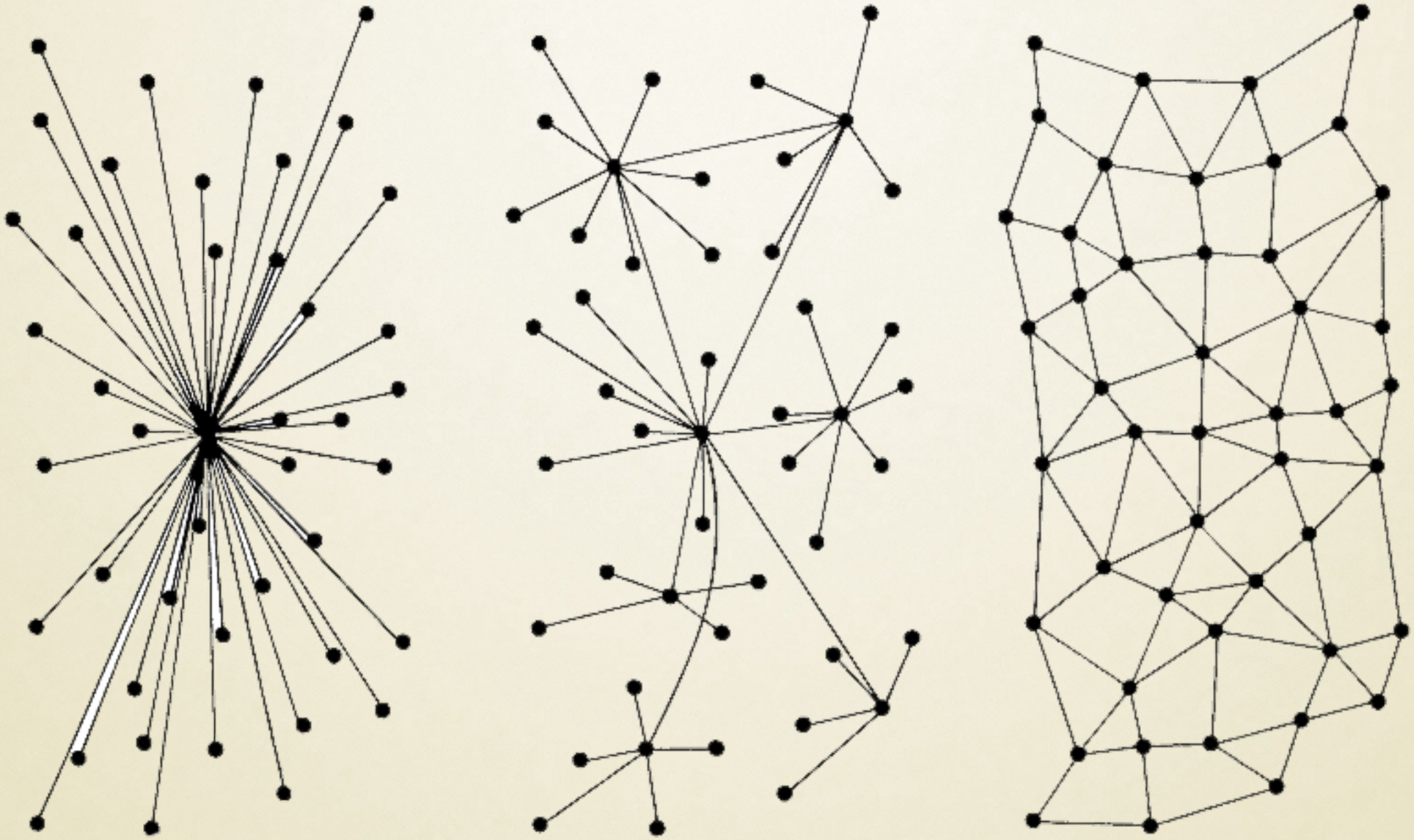
"Bitcoin and Blockchain? The equivalent of being the first to figure out that peanut butter and chocolate go well together."

-Jeff Flowers

WHAT HAPPENS WHEN YOU PUSH THE BUTTON OR ENTER YOUR KEY? - BLOCKCHAIN ENTERS THE PICTURE

- how does it work and what makes it special?
- its relationship with cryptocurrency
  - how cryptocurrency “mining” works - pros and cons
  - how it has shaped the post-bitcoin environment
  - crypto-economics and FinTech
- other (non-cryptocurrency) applications - hype or disruption?
- the future of blockchain technology

REMEMBER THIS?



a Peer-to-Peer (P2P) network

REMEMBER-

- the network is an infrastructure/platform (e.g., P2P)
- communication is defined by protocols (e.g., Bitcoin)
- applications/tasks operate on the platform (e.g., software applications like payments, etc.)

THE BITCOIN P2P NETWORK (1 OF 3)

- defines each of the nodes can play (by choice) different roles
- these roles defined by the node's software and hardware capability
- the simplest node is a client (e.g., a wallet)
  - what most of us have
  - for example, thin software (e.g., apps) on simple(?) computers (e.g., laptops, phones, etc.)
  - allows the sending and receiving of transactions

THE BITCOIN P2P NETWORK (2 OF 3)

- the most complex (and interesting) node is the mining node (or miner)
  - these nodes are capable of adding transactions to the Bitcoin blockchain through the process of mining
- nodes sometime collaborate to form mining pools
- complicated (?) software on sophisticated computing systems (e.g., clusters and high speed networks)
- often require extensive resource support (e.g., power, cooling, etc.)

THE BITCOIN P2P NETWORK (3 OF 3)

- fully-validating nodes (full nodes)
  - different from miners but they need each other
  - keep a full copy of the Blockchain (sort of like a storage device)
  - responsible for enforcing network rules (e.g., block size limit)
  - feed data to the miners
  - data intensive systems

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Fri Aug 27 2021 10:13:14 GMT-0700 (PDT).

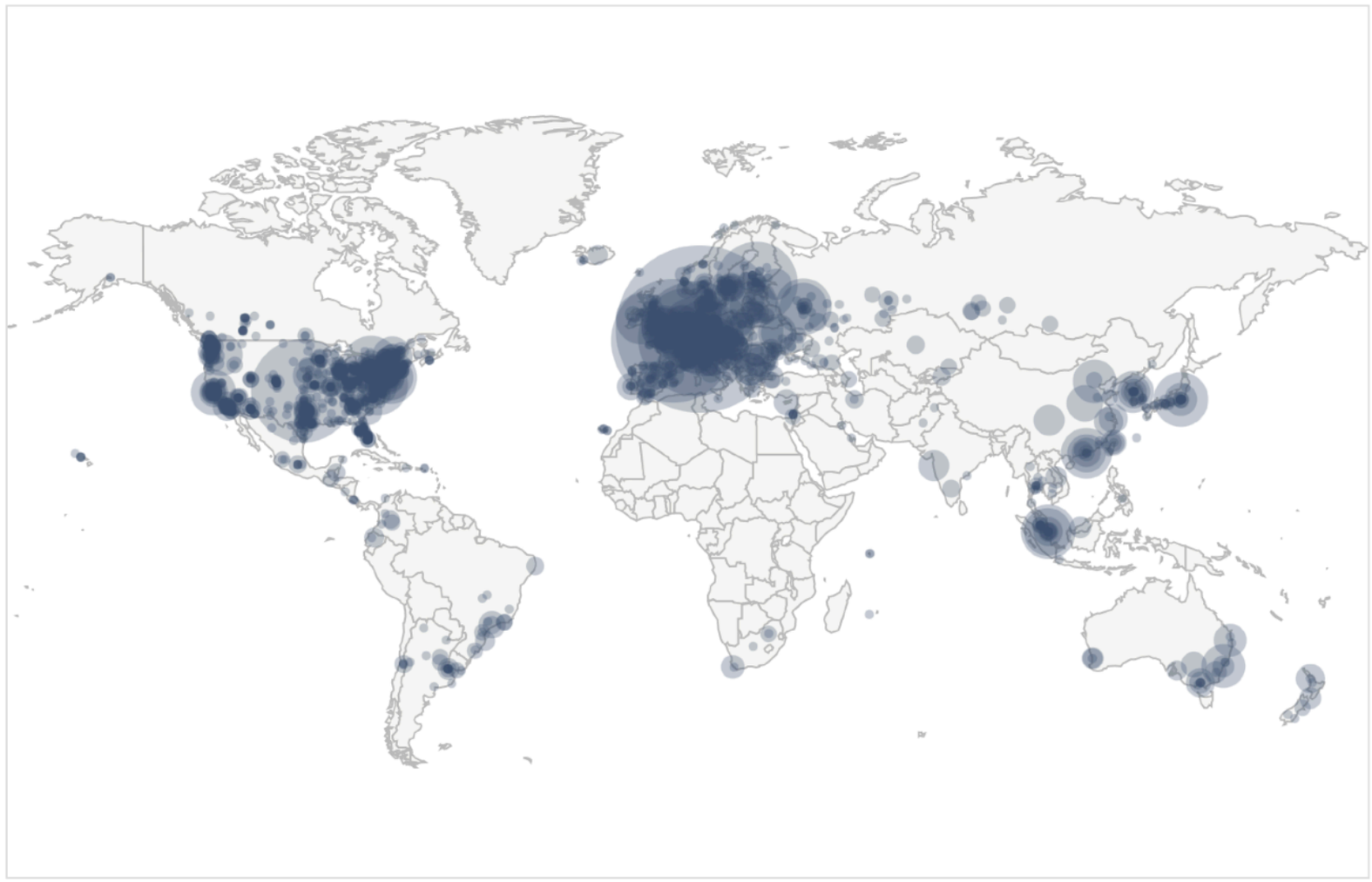
12038 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	4656 (38.68%)
2	United States	1836 (15.25%)
3	Germany	1764 (14.65%)
4	France	537 (4.46%)
5	Netherlands	400 (3.32%)
6	Canada	303 (2.52%)
7	United Kingdom	250 (2.08%)
8	Russian Federation	195 (1.62%)
9	Finland	184 (1.53%)
10	Switzerland	145 (1.20%)

More (86) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

JOIN THE NETWORK

Be part of the Bitcoin network by running a Bitcoin full node, e.g. Bitcoin Core.

2601:645:4200:5a1:23:6676:b2c7:bcd 8333 CHECK NODE

WHY MINING?

- in a classic sense, mining refers to expending labor which translates into value (commodity)
- effort mining + scarcity is proportional to perceived value
- applies to gold, diamonds, even rai
- mining introduces more of a commodity into a system "out of thin air"
- in Bitcoin it could be argued that the mining effort is that spent in computation

WHY IS MINING SO DIFFICULT?

- because of bitcoin's "public" structure, it needs a defense again malicious attacks
- uses "proof of work" (PoW) to make it computationally difficult to add to the blockchain
- has created a cost (equipment + operation) of mining and therefore a need to motivate mining

DEFINED FUNCTIONS OF MINERS (1 OF 2)

- book-keeping - synchronizes in real time the entire BTC blockchain

- network guardians - safeguards the network/ blockchain against hacks and validate each transaction

DEFINED FUNCTIONS OF MINERS (2 OF 2)

- settlement and clearing - the BTC network works as a settlement and clearing house for all transactions without depending upon any 3rd party service

- creation of new BTC - this new BTC is the miner's reward or payment for resource use; does not come out of anyone's "pocket;" transaction fees do come out of someone's "pocket"

CAN ANYONE BE A MINER?

- technically yes, BUT
  - requires running sophisticated software (not really a problem since software is open source, basically free and well supported)
  - requires access to extensive computing resources (has become that way)
  - questionable ROI (return on investment) are (hardware investment and maintenance) + resource (electricity) costs < (mining rewards + fees) ?

ts

AntMiner S3 441Gh/s @ 0.77W/Gh 28nm SHA-256 ASIC Miner

by AntMiner

★★★★½ 23 customer reviews

from $224.98 inc. tax + shipping

59 answered questions

Note: This item is only available from third-party sellers (see all offers).

Available from these sellers.

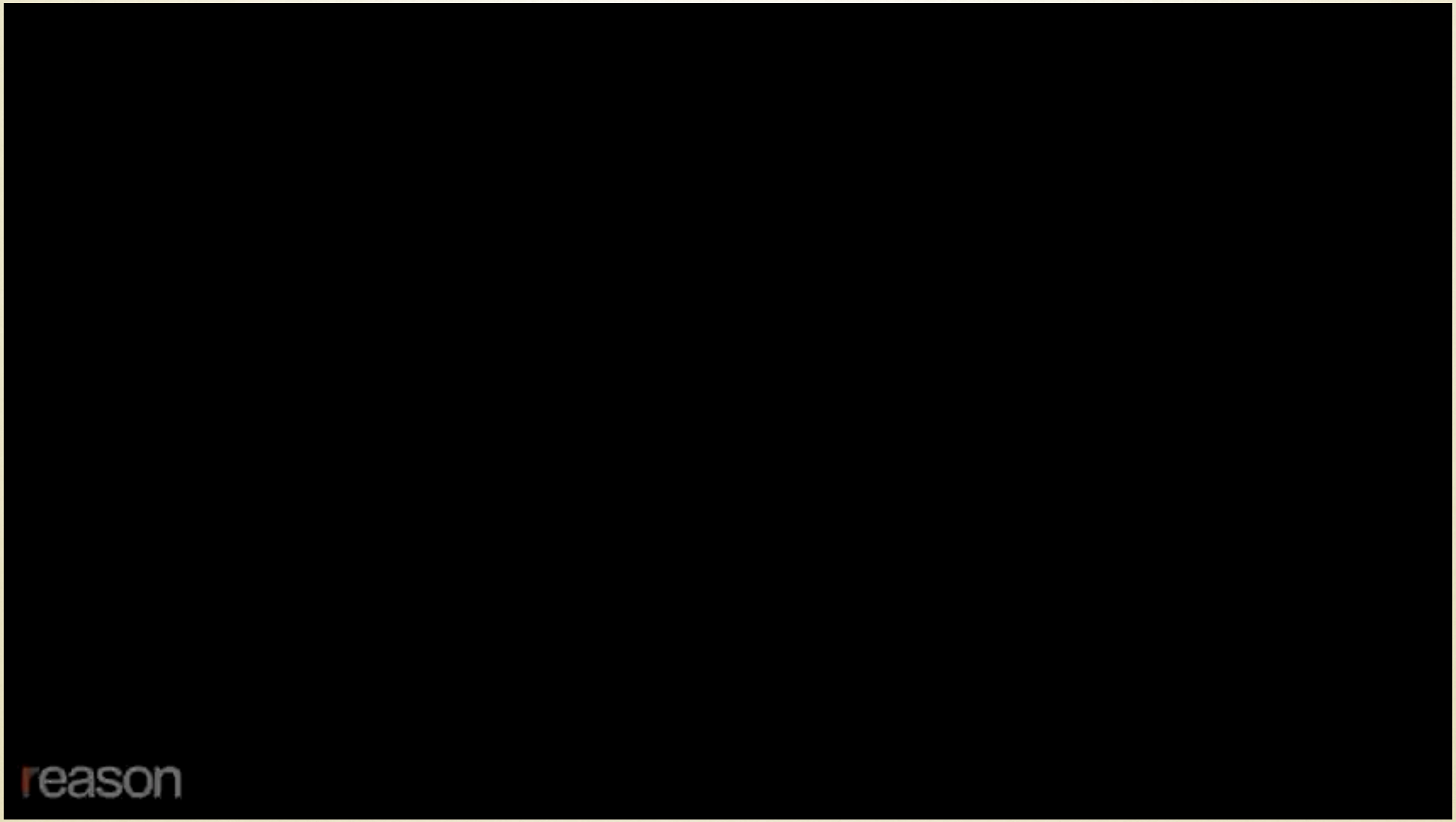
- 453GH/S BITCOIN MINER
- BM1382 28nm ASIC CHIPS x 32 chips
- Included: ATX Power Supply Jumper Switch w/ LED light for PSU, 7' Cat5 Network Cable, Bitmain Bumper Sticker and Orange Bitcoin Round Sticker
- Tech Support & Warranty Provided within USA by Bitmain 1-844-BIT-MAIN (844-248-6246)
- 12V power supply required (sold separately) Connector: PCI-E x 2

› See more product details

Used (1) from $219.99 + $5.49 shipping

Report incorrect product information.

Remember that 441Gh/sec specification
ASIC = “application-specific integrated circuit)


reason

WHAT ELSE IS A POOR MINER WANNABE TO DO?

- mining in "the cloud" (e.g., Amazon Web Services)?
  - ROI isn't there
- join a "mining pool" and share the profits?
  - takes computing expertise
- cryptojacking?
  - installing malware on other people's computers and creating a distributed computing network
  - like SETI@Home but involuntary and illegal
  - used by "bad actors" and "rogue states"

Use computers at work? - NO!

Announcements

- The recent surge in cryptocurrency (e.g., Bitcoin and Ethereum) values has fueled a sharp increase in incidents involving cryptocurrency mining at Stanford. Per university policy, Stanford resources must not be used for personal financial gain. Community members are prohibited from using university resources (including computing equipment, network services and electricity) for cryptocurrency mining activities outside of faculty-sanctioned research and course work. **Learn more**.

BIT COIN information

1 (877) 778-7984

Scan the bar code & Start Mining Today!

Call for a free consultation.

SHA-256 CLOUD MINING.

Online cloud mining allows you to invest in bitcoin and other online currency.

You can invest any dollar about and watch your money grow within days.

Withdrawal your money at anytime. You are your own investor, there is no middle man.

Cloud mining allows you to lease the use of the mining equipment (computers & the software) there is nothing you need to purchase, no setup cost, just an easy to use website. Create an account invest any dollar amount and see results within days.

Scan the bar code, visit the site and call with any questions.

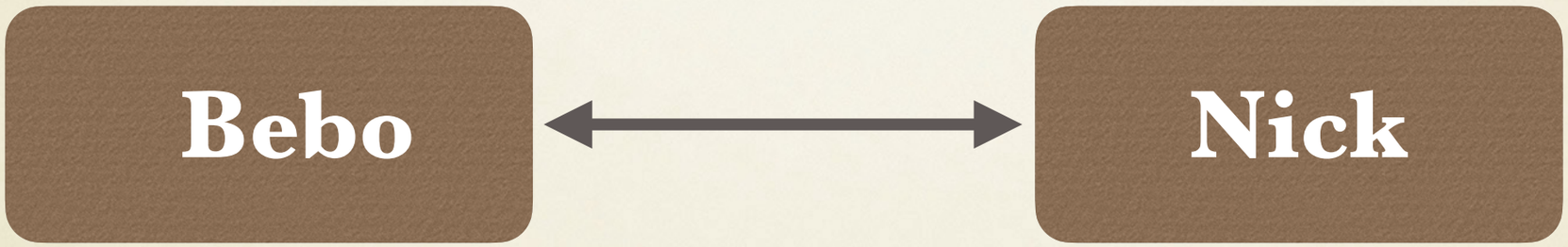
Stocks are limited so don't delay! SHA-256 CLOUD MINING.

Be scammed into renting/leasing mining equipment? - NO!

IN SATOSHI'S WORLD

"the primary function of mining is not for the reward, but rather keeping the network safe and executing transactions smoothly"

WHAT HAPPENS IN A TRANSACTION (1 OF 3)



- Bebo and Nick want to do business
- they both have wallets (clients)
- public key is available for recipient
- their wallets create a transaction
- transaction contains all necessary data (date, amount, etc.)

WHAT HAPPENS IN A TRANSACTION (2 OF 3)

Arthur | **Bruce** | **Charlie** | **David**

- Arthur, Bruce, Charlie, and David are miners
- they probably don't know one another
- they are running mining software on their computers
- they want to add the Bebo-Nick transaction to the blockchain
- Bebo and Nick are anxious for verification
- what do Arthur, Bruce, Charlie and David do?

WHAT HAPPENS IN A TRANSACTION (3 OF 3)

- Arthur, Bruce, Charlie and David each combine all the transactions that have occurred in the past 10 minutes (available from the BTC network full nodes) into a block (hence blockchain)
- blocks are approximately 1Mb in size
- this block includes the Bebo-Nick transaction plus others
- how do Arthur, Bruce, Charlie and David reach consensus on who gets to add the block to the blockchain thereby collecting the reward (new BTC) and transaction fees?

CONSIDER

- if cryptography helps accomplish communication in the presence of adversaries over a network

- what about how to reach agreement in the presence of adversaries over a network?

- consensus

- <another tech digression>

SATOSHI TURNED TO A CLASSIC COMPUTER SCIENCE EXERCISE - “THE BYZANTINE GENERALS PROBLEM”

The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. [**Computer-Communication Networks**]: Distributed Systems—*network operating systems*; D.4.4 [**Operating Systems**]: Communications Management—*network communication*; D.4.5 [**Operating Systems**]: Reliability—*fault tolerance*

General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

1. INTRODUCTION

A reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behavior that is often overlooked—namely, sending conflicting information to different parts of the system. The problem of coping with this type of failure is expressed abstractly as the Byzantine Generals Problem. We devote the major part of the paper to a discussion of this abstract problem and conclude by indicating how our solutions can be used in implementing a reliable computer system.

We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals

This research was supported in part by the National Aeronautics and Space Administration under contract NAS1-15428 Mod. 3, the Ballistic Missile Defense Systems Command under contract DASG60-78-C-0046, and the Army Research Office under contract DAAG29-79-C-0102.
Authors' address: Computer Science Laboratory, SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025.

Generals have surrounded a city and are ready to attack.

How can they reach consensus on an attack plan given insecure communications and possible treachery?

A bad choice will be disastrous.

BGP solution

- General(s) Arthur, Bruce, Charlie and David
- receive their order from “on high”
- defined some restrictions and protocol:
  - each general requires 10 minutes to create a message - the time to compose it + seal it with the official seal
  - message contains new order plus entire history of previous messages

SCENARIO (1 OF 4)

- Gen. Arthur sends message to Gen. Bruce to attack and the message reaches Gen. Bruce after 10 minutes and says “Gen. Arthur orders attack at 4 AM”
- Gen. Bruce sends message to Gen. Charlie and also takes 10 minutes. So Gen. Charlie receives message “Gen. Bruce orders attack at 4 AM|Gen. Arthur orders attack at 4 AM”

SCENARIO (2 OF 4)

- Gen. Charlie receives the message, but in fact Gen. Charlie is a traitor

- Gen. Charlie changes message to “Gen. Charlie orders attack at 3 AM”

- but Gen. Charlie has to also change messages of Gen. Arthur and Gen. Bruce which takes him 20 minutes for a total of 30 minutes.

SCENARIO (3 OF 4)

- Gen. David will either receive-

1. “Gen. Charlie orders attack at 3 AM | Gen. Bruce orders attack at 4 AM | Gen. Arthur orders attack at 4 AM” in 10 minutes. Since all messages are not in synch, Gen. David will realize that Gen. Charlie is corrupt and let the other generals know.

2. “Gen. Charlie orders attack at 3 AM | General Bruce orders attack at 3 AM | General Arthur orders attack at 3 AM” in 30 minutes. Since message was received after 30 minutes, Gen. David realizes that Gen. Charlie is corrupt.

SCENARIO (4 OF 4)

- the only way for Gen. Charlie to succeed in his treachery is to prepare all 3 messages in just 10 minutes which is supposedly impossible

- Generals Arthur, Bruce and David are able to reach consensus in the threat of Gen. Charlie's attempted treachery

- Gen. Charlie's failure to complete the required task in 10 minutes is what allows him to be detected

BACK TO MINERS INSTEAD OF GENERALS - THE BASICS OF MINING (1 OF 2)

- Arthur, Bruce, Charlie and David need to be able to reach consensus (agreement) on who gets to add the block (that contains the Bebo-Nick transaction) to the blockchain
- like the Byzantine generals they must demonstrate "proof of work" (PoW)
- this PoW is accomplished by solving a problem whose difficulty suggests that a solution can be found in 10 minutes
- the solution cannot be faked, so all miners have to agree on its correctness

BACK TO MINERS INSTEAD OF GENERALS - THE BASICS OF MINING (2 OF 2)

- the problem solver gets a reward in BTC and the "right" to add the new block to the blockchain
- the BTC reward is created "out of thin air" and adds to the total in circulation
- Bebo & Nick's transaction appears on the blockchain and is therefore verified by historical ledger record (like a credit/ debit)
- the reward payment is also recorded on the blockchain
- the losers try again on a new block

MINING SPECIFICS (1 OF 2)

1. collect all the transactions that have occurred in the last 10 minutes into a "block" of size 1Mb (megabyte)
2. create a block header that contains
    a. hash of transactions
    b. time stamp
    c. hash pointer of previous block - why?
    d. transaction fee information
    e. other administrative information
3. work on the "puzzle" ("Proof of Work")

THE MYSTERIOUS MINING PUZZLE (1 OF 2)

1. hash the block header
2. if value is < prescribed target, go to Step 4.
3. add random value to block header, hash again and go to Step 2.
4. broadcast solution to other miners (illustrates PoW and leads to consensus); solving miner "wins"

MINING PUZZLE PARAMETERS

- given the nature of "hashing," puzzle solution can only be found via "brute force"
- puzzle difficulty is adjusted every 2016 blocks - if difficulty goes up, then target goes down and vice-versa
- goal is to keep the average block creation time at 10 minutes, maintain the block size limit, and keep the transaction rate at approximately 7 per second

THE MYSTERIOUS MINING PUZZLE (2 OF 2)

5. if consensus then add new block to blockchain
6. go to Step 1.

- "losing" miners go to Step 1.
- Bebo & Nick's transaction is validated and recorded and appears on the blockchain

THINK ABOUT IT THIS WAY...

given a string of characters, what arbitrary string of characters can you add to it such that the hash of the resulting string

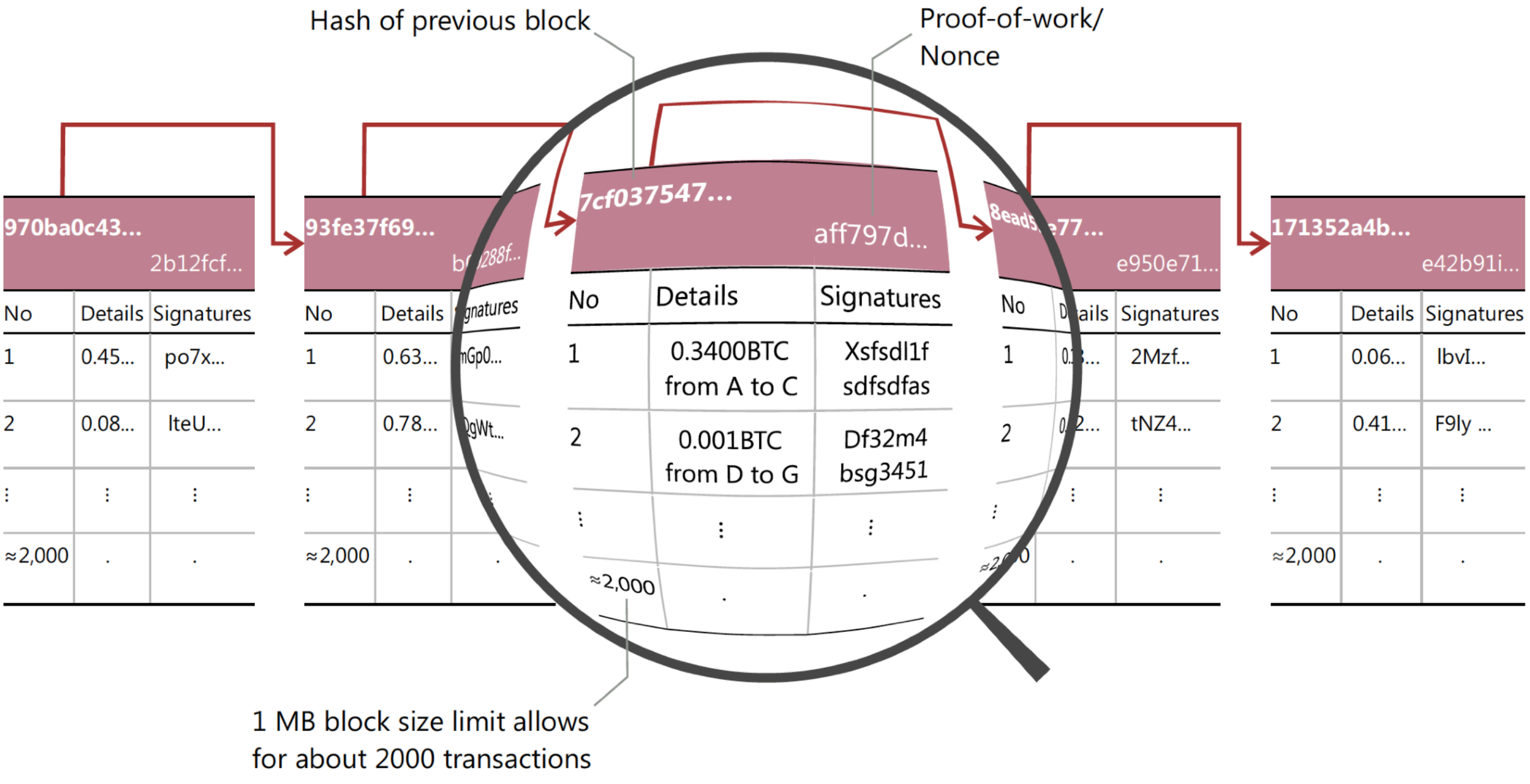
begins with 0?

begins with 00?

begins with 000?

etc.

this can only be done by “brute force”/“trial and error” that uses up a lot of computer power



(ref:Bank for International Settlements)

Bitcoin

Blockchain information for Bitcoin (BTC) including historical prices, the most recently mined blocks, the mempool size of unconfirmed transactions, and data for the latest transactions.

$49,200.22	147.700 EH/s	275,135	5.270m BTC	96,800 BTC
Price →	Estimated Hash Rate →	Transactions (24hrs) →	Transaction Volume →	Transaction Volume (Est) →

Price

The price of Bitcoin over the last day

1 Day

View All Prices →

Mempool Size (Bytes)

The aggregate size of unconfirmed transactions in bytes

1 Day

View All Charts →

Latest Blocks

The most recently mined blocks

Height	Mined	Miner	Size
697314	6 minutes	Unknown	41,677 bytes

Latest Transactions

The most recently published unconfirmed transactions

Hash	Time	Amount (BTC)	Amount (USD)
a9c979375c51bafda53e5...	20:42	0.01017291 BTC	$500.51

MINING VOCABULARY (1 OF 2)

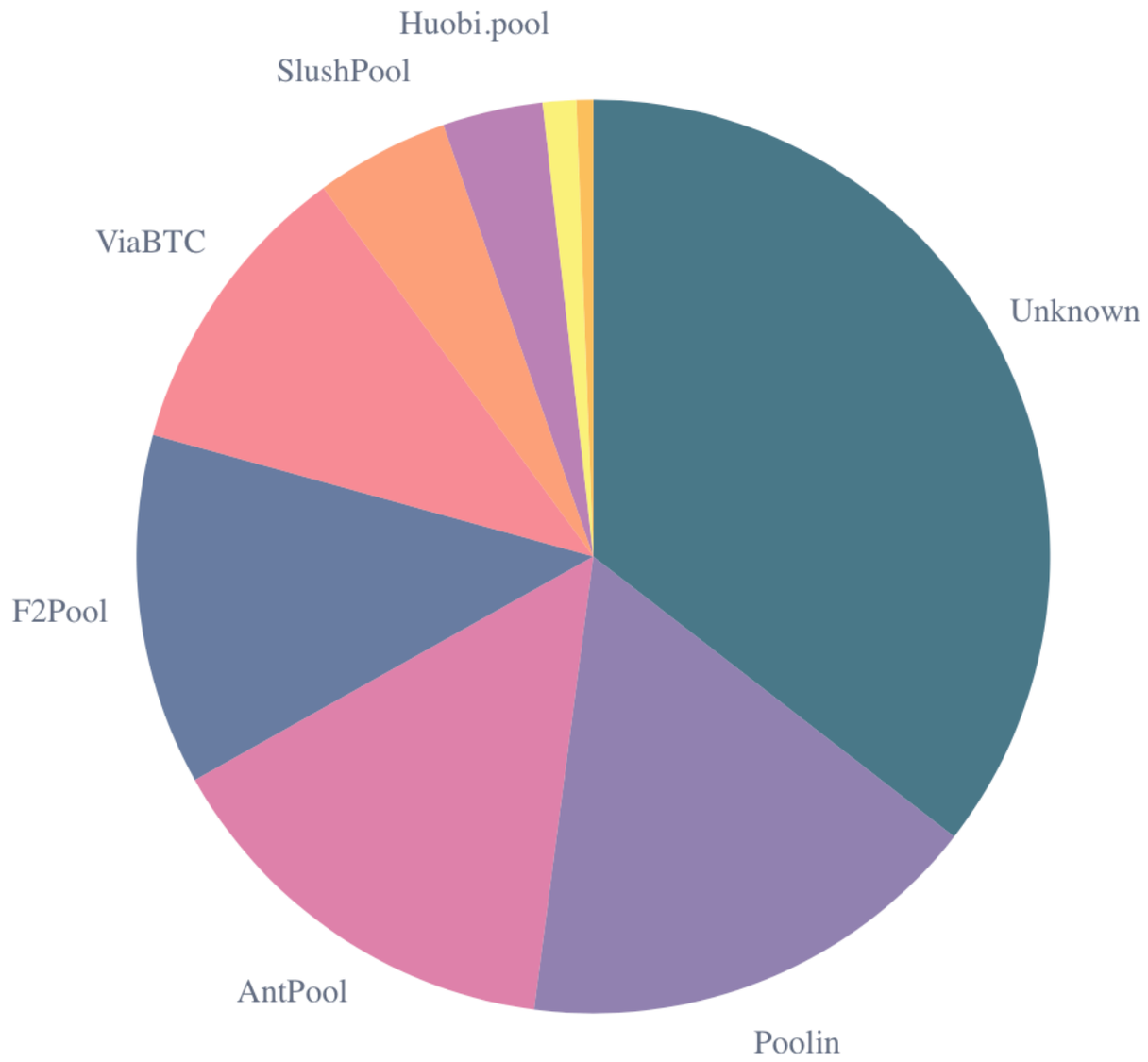
- hashrate - number of hash operations the BTC network (e.g. all the miners) is performing per second; measured in TH/sec - 10^{12} (trillion) hashes per second; indicator of all computing resources available and/or dedicated
- difficulty - a value used to illustrate how hard it is to solve the PoW problem; recalculated every 2016 blocks; based on hashrate
- block reward - started at 25 BTC/block; halves every 210,000 blocks;

MINING VOCABULARY (2 OF 2)

- mining rig - specialized computer systems of high-performance CPUs designed to optimize mining
- mining pool - miners pooling resources to increase hashrate share
- 51% attack - hypothetical attack scenario where a group of miners (or pools) control more than 50% of the hashrate; theoretically they could block transaction confirmation

Hashrate Distribution

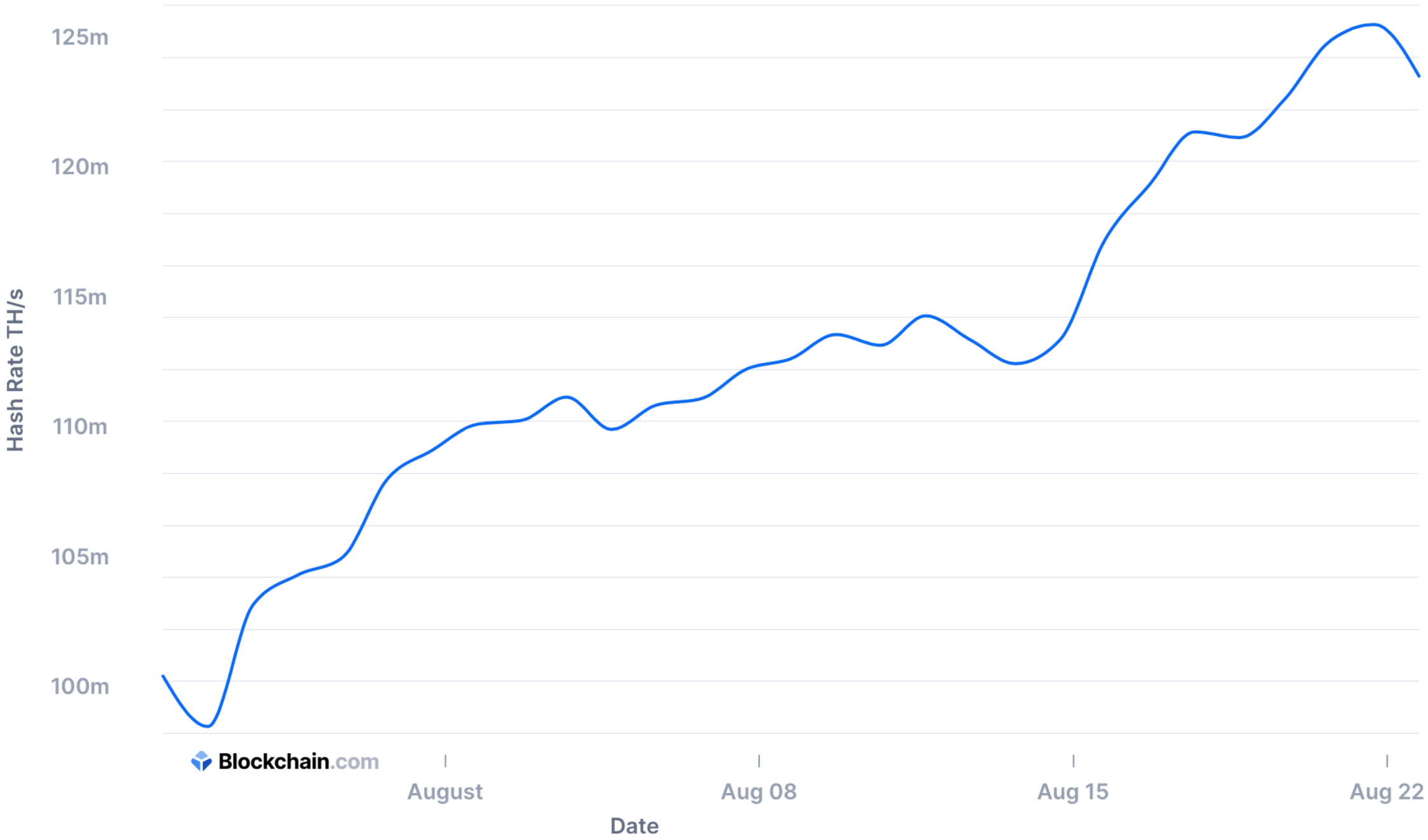
An estimation of hashrate distribution amongst the largest mining pools.



(blockchain.com)

Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.



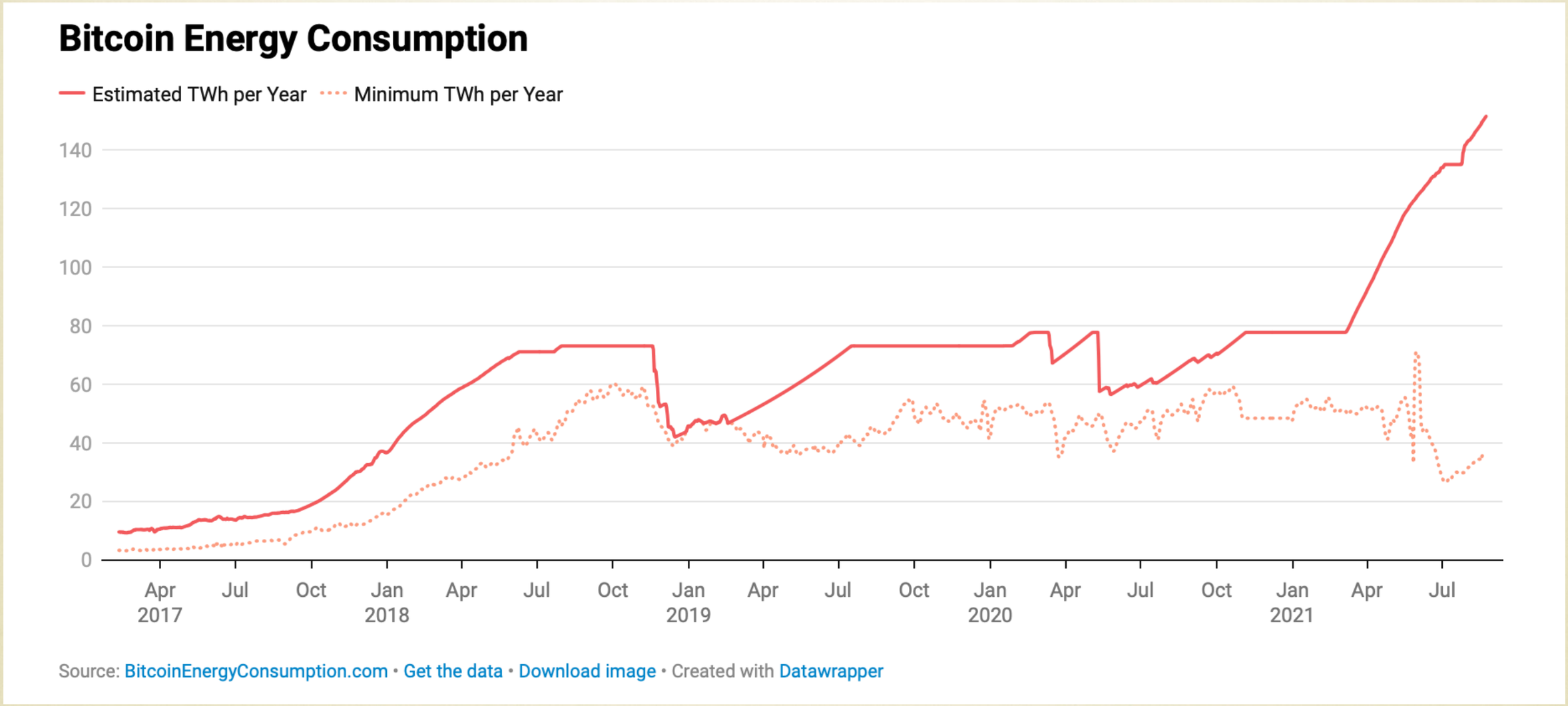
30 Days | 60 Days | 180 Days | 1 Year | 3 Years | All Time

Raw Values | 7 Day Average | 30 Day Average

TERAHASHES AREN'T CHEAP - THERE ARE DEFINITELY MINING ISSUES

- mining requires huge use of computational resources and therefore has an appreciable energy/ environmental impact - is this a "show stopper?"
- miners are a 'new center of power' - if five (estimated) mining pools control the creation of blocks, how is that centralized?
- is it possible to make PoW and consensus less compute-intensive?

THE RESOURCE AND ENVIRONMENTAL IMPACT IS WELL DOCUMENTED (1/2)



"It's an extremely inefficient way of conducting transactions, and the amount of energy that's consumed in processing those transactions is staggering" - Janet Yellen

THE RESOURCE AND ENVIRONMENTAL IMPACT IS WELL DOCUMENTED (2/2)

Annualized Total Bitcoin Footprints

Carbon Footprint	Electrical Energy	Electronic Waste
72.00 Mt CO2	151.57 TWh	7.98 kt
Comparable to the carbon footprint of **Greece**.	Comparable to the power consumption of **Malaysia**.	Comparable to the e-waste generation of **Luxembourg**.

Single Bitcoin Transaction Footprints

Carbon Footprint	Electrical Energy	Electronic Waste
807.83 kgCO2	1700.69 kWh	89.50 grams
Equivalent to the carbon footprint of **1,790,424** VISA transactions or **134,638** hours of watching Youtube.	Equivalent to the power consumption of an average U.S. household over **58.29** days.	Equivalent to the weight of **1.38** 'C'-size batteries or **1.95** golf balls. (Find more info on e-waste here.)

These numbers are ridiculously frightening!

THIS IMPACT IS CLEARLY NOT ACCEPTABLE OR SUSTAINABLE

- is this impact a sufficient reason to discount bitcoin/ cryptocurrency? - maybe!
- this impact is coming directly from the computational requirements of the BTC PoW algorithm
- what are alternative consensus mechanisms to PoW (if any) that result in less environmental impact?
  - an ongoing research area
  - one of the issues driving the development of new cryptocurrencies (alternatives to BTC)

Questions? Comments?
bebo.white@gmail.com