Cryptocurrency, Blockchain, and a new economic world

OLLI

LATE SUMMER 2021

LECTURE 2

Bebo White - bebo.white@gmail.com

REGULATION

by **Kevin Helms**

Aug 8, 2021

69043

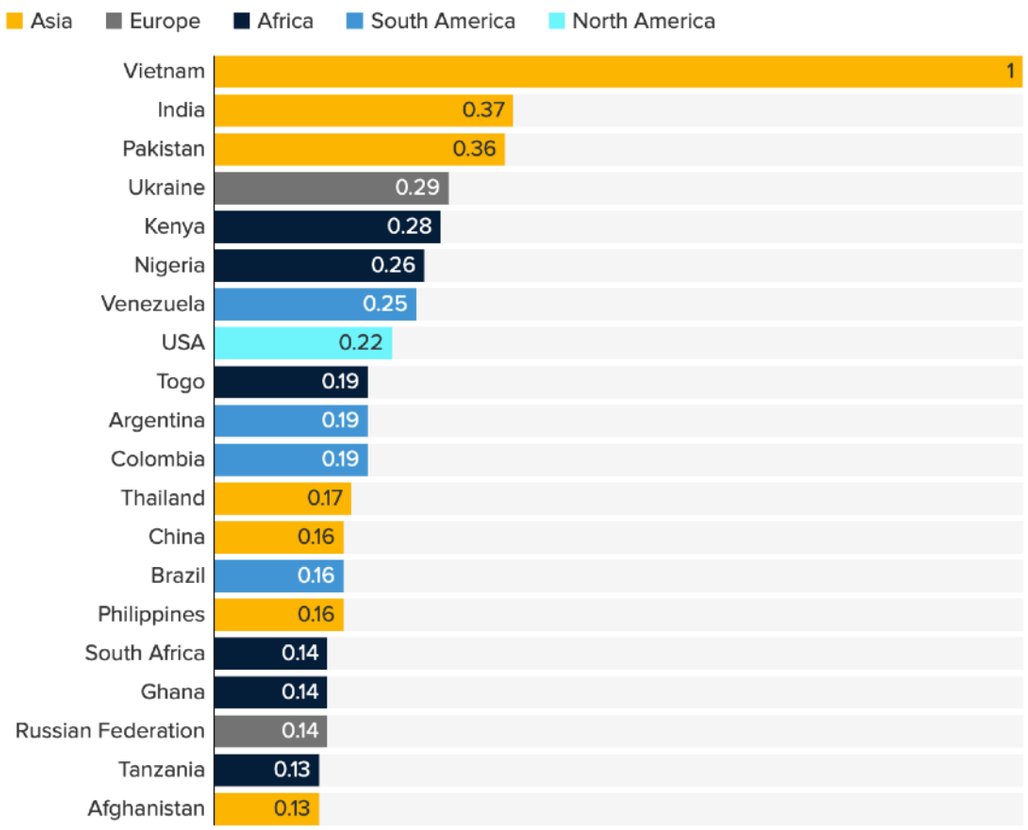
SEC Chairman Says Satoshi Nakamoto's Innovation Is Real, Crypto Rules Are Clear

The chairman of the U.S. Securities and Exchange Commission (SEC), Gary Gensler, says that Satoshi Nakamoto's innovation is real. "It has been and could continue to be a catalyst for change in the fields of finance and money," he said.

The Chainalysis 2021 Global Crypto Adoption Index

Top 20 countries, based on three metrics: Total crypto activity, trading activity of non-professional users, and peer-to-peer exchange trade volume. All are weighted by purchasing power parity per capita.

Countries are scored on a scale of 0 to 1.



Source: Chainalysis

CNBC

The Economist

Menu | Weekly edition | Search

Finance & economics

Aug 7th 2021 edition ›

The disaster scenario

What if bitcoin went to zero?

A thought experiment helps uncover the links between crypto and mainstream finance

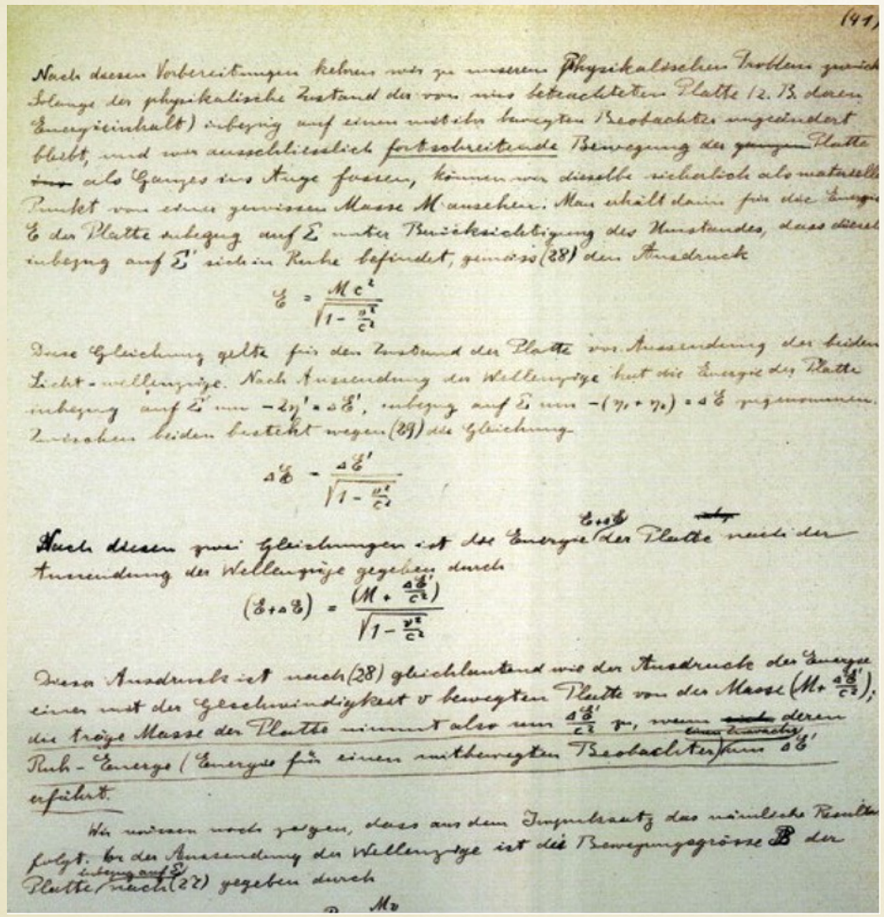
Satoshi Kambayashi

If I were giving homework assignments…

WHO IS/WAS SATOSHI?

- still no one knows
- many claims and suspicions, but no proof
- is in possession of > 980,000 bitcoins (> $46.75 billion) - none have been used (how could we know that?)
- why should we care?

HOW CAN A PAPER WRITTEN BY AN OBSCURE AND UNKNOWN AUTHOR MAKE A DIFFERENCE AND START A REVOLUTION?



(141)

Nach diesen Vorbereitungen kehren wir zu unserem physikalischen Problem zurück. Solange der physikalische Zustand der von uns betrachteten Platte (z. B. deren Energieinhalt) bezogen auf einen mit ihr bewegten Beobachter ungeändert bleibt, und wir ausschließlich fortschreitende Bewegung der ~~ganzen~~ Platte als Ganzes ins Auge fassen, können wir dieselbe nichtsdestoweniger als materiellen Punkt von einer gewissen Masse M ansehen. Man erhält dann für die Energie E der Platte bezogen auf Σ unter Berücksichtigung des Umstandes, daß dieselbe bezogen auf Σ' sich in Ruhe befindet, gemäß (28) den Ausdruck

$$E = \frac{Mc^2}{\sqrt{1-\frac{v^2}{c^2}}}$$

Diese Gleichung gelte für den Zustand der Platte vor Aussendung der beiden Licht-Wellenzüge. Nach Aussendung der Wellenzüge hat die Energie der Platte bezogen auf Σ' nun $= E' + \Delta E'$, bezogen auf Σ nun $= (\eta_1 + \eta_2) + \Delta E$ genommen. Zwischen beiden besteht wegen (29) die Gleichung

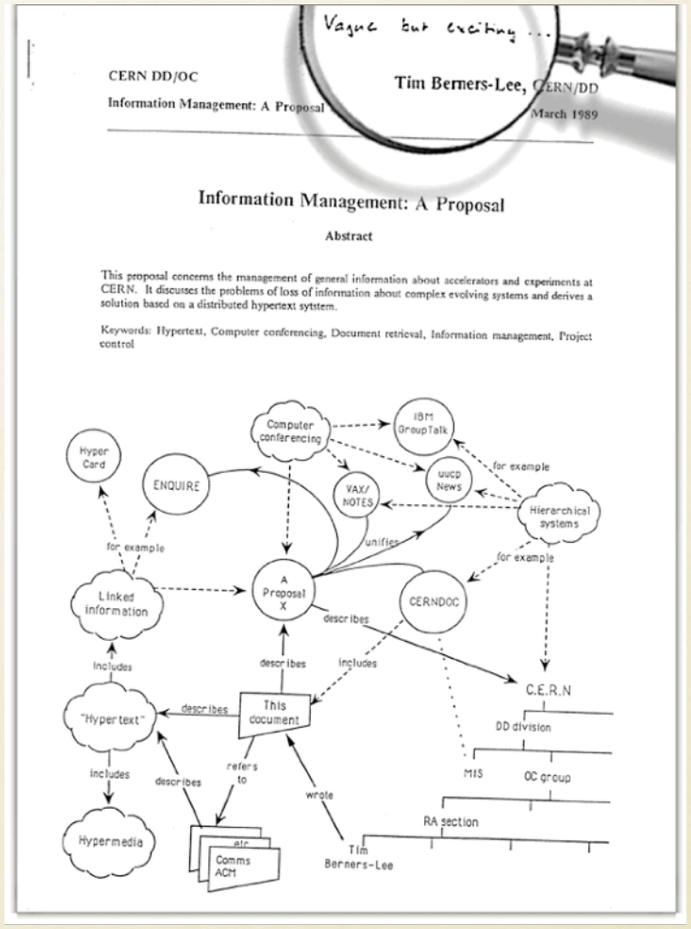
$$\Delta E = \frac{\Delta E'}{\sqrt{1-\frac{v^2}{c^2}}}$$

Nach diesen zwei Gleichungen ist die Energie ~~bezogen~~ der Platte ~~nach~~ nach der Aussendung der Wellenzüge gegeben durch

$$(E + \Delta E) = \frac{(M + \frac{\Delta E'}{c^2})}{\sqrt{1-\frac{v^2}{c^2}}}$$

Dieser Ausdruck ist nach (28) gleichlautend wie der Ausdruck der Energie einer mit der Geschwindigkeit v bewegten Platte von der Masse $(M + \frac{\Delta E'}{c^2})$; die träge Masse der Platte nimmt also um $\frac{\Delta E'}{c^2}$ zu, wenn ~~sich~~ deren Ruh-Energie (Energie für einen mitbewegten Beobachter) $\Delta E'$ erfährt.

Wir wollen noch zeigen, daß aus dem Impulssatz das nämliche Resultat folgt. Bei der Aussendung der Wellenzüge ist die Bewegungsgröße B der Platte (bezogen auf Σ) nach (22) gegeben durch



Vague but exciting ...

CERN DD/OC

Tim Berners-Lee, CERN/DD

Information Management: A Proposal

March 1989

Information Management: A Proposal

Abstract

This proposal concerns the management of general information about accelerators and experiments at CERN. It discusses the problems of loss of information about complex evolving systems and derives a solution based on a distributed hypertext sytstem.

Keywords: Hypertext, Computer conferencing, Document retrieval, Information management, Project control

1905 Because the world was **1989** ready for it

WHAT GENERALLY IS BITCOIN (AND OTHER CRYPTOCURRENCIES)?

- "Bitcoin" is the protocol; "bitcoins" are the units (BTC); one (and first) example of a cryptocurrency
- called cryptocurrency since cryptographic methods are used to make it viable
- value is represented by an entry in a ledger that is duplicated worldwide and very computationally difficult (impossible?) to modify - this ledger is the "BTC Blockchain;" likewise "Ethereum" is the ledger; "Ether" is the currency
- generic terminology for Blockchain is "Distributed Ledger Technology" (DLT)
- value units and ledgers are specifically designed for a digital/networked society
- deliberately decentralized and independent of state/fiat currencies (some exceptions discussed later)
- can be used anonymously (like fiat currencies but unlike credit cards, PayPal, etc.)

DISINTERMEDIATION

- “third parties” are no longer needed to
  - establish identity or prove creditworthiness
  - distribute media
  - mediate communication between parties
  - mediate transfers of value
- assuming the blockchain doesn’t qualify as a”third party”

SATOSHI'S RESPONSE TO MICROPAYMENTS?

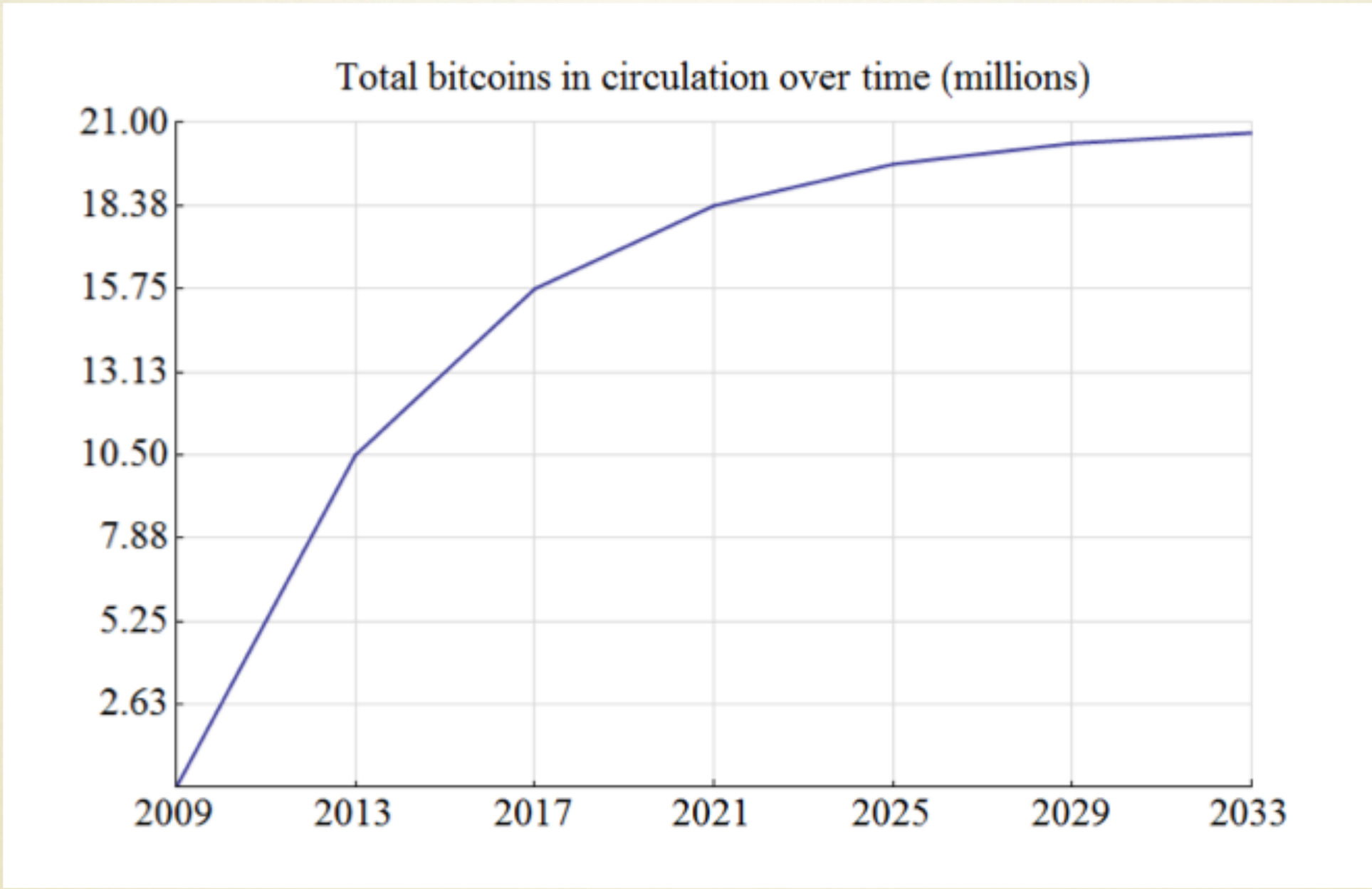
- 1 bitcoin (BTC) is divided into satoshi (SAT)
- 1 SAT = .000000001 BTC (one hundred millionth)
- to put into perspective, for 1 SAT = 1¢ , 1 BTC = $1,000,000
- as the value of BTC increases, it is likely that most transactions will be in SAT
- 1 bit = one millionth or 10^{-6} BTC (not universally accepted)

FUNGIBILITY

- BTC is *fungible*, (i.e., they can be traded or exchanged, one for another)
- one BTC is always equal in value to another BTC
- 1 SAT will always be equal to .000000001 BTC and equal to another SAT
- if your wallet has 5 BTC, you can spend parts of it however you wish (just like fiat currency)
- what would *non-fungibility* mean?

SATOSHI'S RESPONSE TO MONEY SUPPLY AND INFLATION?

- the protocol dictates that the maximum number of BTC (ever) = $21*10^6$ = 21 million
- maximum number of SAT = $2.1*10^{15}$ = 2,100,000,000,000,000
- to put into perspective, the amount of $US in the world = 10^{12} = 1,000,000,000,000
- new BTC are introduced via "mining" (more about that process later)
- some economists attribute BTC volatility to the fixed limit



Never more than 21 million created - no inflation -
includes coin lost or unavailable - what's wrong with no inflation?

Lost Bitcoin: 3.7 million Bitcoin are probably gone forever

Around 20% of currently minted Bitcoin—worth a small fortune—are gone forever, and can never be retrieved. Here's where they went.

By Daniel Phillips

4 min read • Jan 3, 2021

AROUND 3.7 MILLION BITCOIN ARE LOST FOREVER (IMAGE: SHUTTERSTOCK)

WHY DOES BITCOIN/ CRYPTOCURRENCY WORRY SO MANY OR MAKE THEM ANGRY?

(I welcome your comments on the following discussion - this is where I play economist…)

WHY DID THE CYPHERPUNKS/SATOSHI THINK THAT THE 2008 FINANCIAL CRISIS DEMONSTRATED A NEED FOR CHANGE?

- how could a stable, people-centric financial system allow the following:
  - a combination of speculation in financial markets, focusing particularly on property transactions and the availability of cheap credit
  - unsustainable borrowing to finance one-way bets on rising property prices leading to a widening gap between incomes and debt and an increase in global inflation
    - borrowers struggling to repay mortgages as property prices fell leading to a collapse in the value of assets (devaluation) held by many financial institutions
    - an ongoing belief that a reduction in regulations and confidence that markets are efficient
    - the need for an enormous bail-out as governments were forced to inject billions of dollars into affected banks to avoid a collapse of the financial system
- it wasn't simply the desire for a digital currency for the Internet world

CRYPTO DECODED

Second-largest U.S. mortgage lender will accept payment in bitcoin

PUBLISHED THU, AUG 19 2021•6:58 PM EDT

MacKenzie Sigalos
@KENZIESIGALOS

KEY POINTS

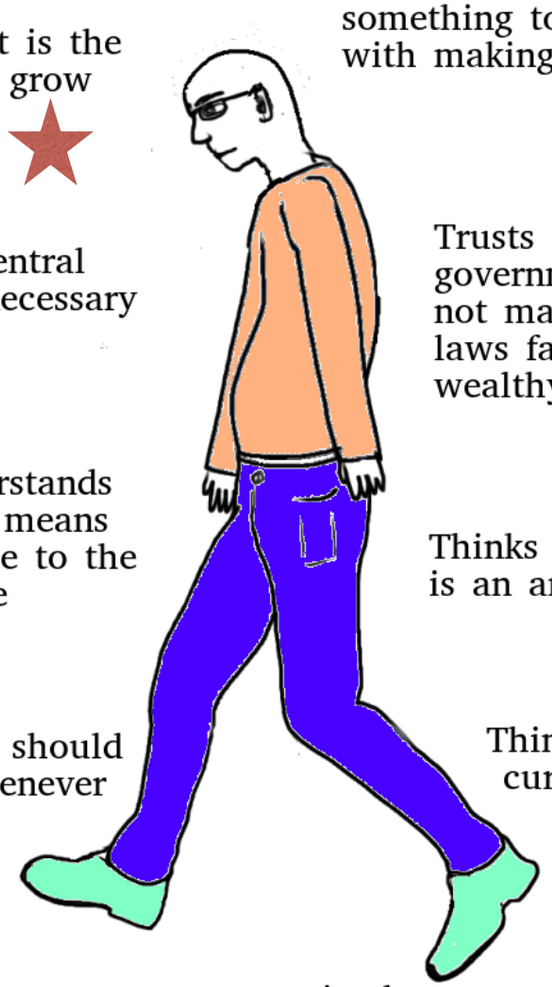
- United Wholesale Mortgage announced plans this week to accept cryptocurrency for home loans, in an apparent first for the national mortgage industry.
- The company hopes to start accepting bitcoin in Q3, and it is currently weighing other digital currencies like ether.

In this article UWMC +0.02 (+0.28%)

RELATED

Second-largest U.S. mortgage lender will accept payment in bitcoin

Virgin No-Coiner



Believes debt is the only way to grow an economy

Thinks hashing has something to do with making weed

Feels that central banking is necessary

Trusts that the government will not make financial laws favoring the wealthy

Only understands what 'fiat' means in reference to the automobile

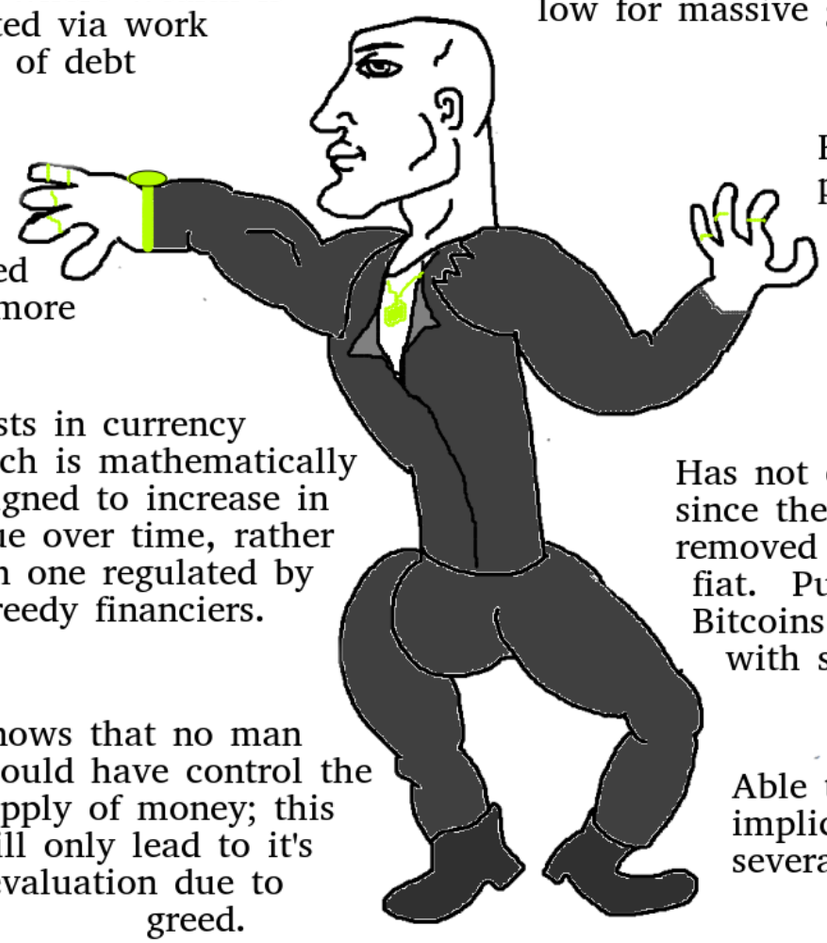
Thinks Satoshi Nakamoto is an anime

Thinks money should be printed whenever it is needed

Thinks an inflationary currency is a good thing

Thinks cryptos are a ponzi scheme while ignorring the fact that there will always be more debt owed to the Federal Reserve than there is USD in existence, and to pay off debt would require more loans from the Federal Reserve.

Chad Bitcoiner



Believes in a monetary system where wealth is generated via work instead of debt

Enjoys market instability; sells off on every high and buys in on every low for massive gains

Understands that there is no need for centralized banking anymore

Knows Satoshi Nakamoto personally and regularly has drinks with the fellow at bars which accept cryptos.

Trusts in currency which is mathematically designed to increase in value over time, rather than one regulated by greedy financiers.

Has not owned a single USD since the gold standard was removed and the USD declared fiat. Purchased all of his Bitcoins and mining equipment with saved up gold bullion.

Knows that no man should have control the supply of money; this will only lead to it's devaluation due to greed.

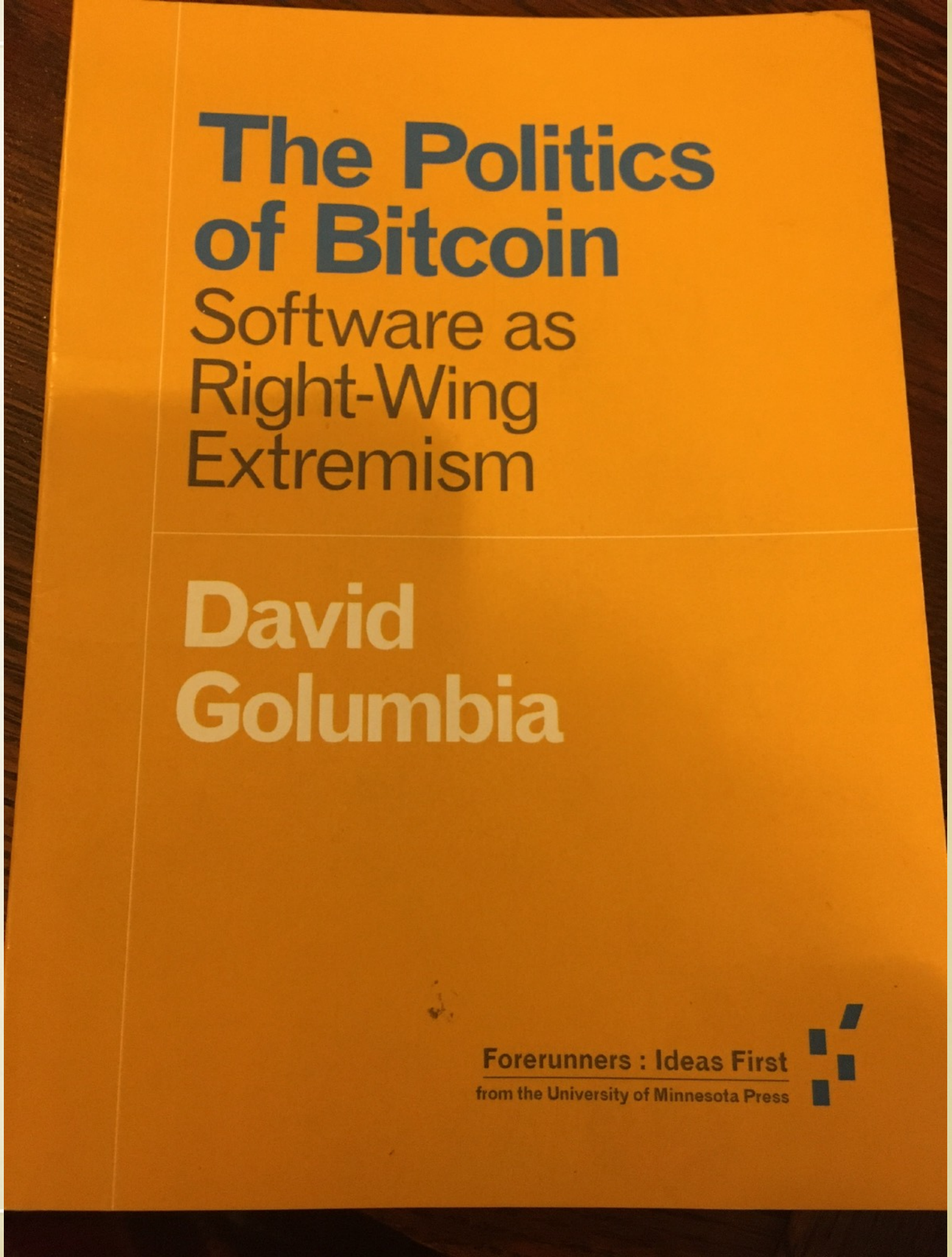
Able to mentally calculate implicit trade values accross several markets simultaneously

Knows that every time someone says Bitcoin is crashing it is a Virgin No-Coiner speaking.

"…nothing epitomizes the hubris of the techno-utopianists more than the idea of reinventing money…the cryptocurrency bubble will also blow up at some point…as time goes on, cryptocurrencies get more enmeshed in our economic system and the risk of financial contagion grows"

-Moshe Vardi, Rice University

“the decision to limit the supply of Bitcoins comes right out of the John Birch Society and its founder Robert Welch’s belief that inflation is itself ‘an insidious tax’”



"Millennials are too stupid to realize that bitcoin is a bubble they should avoid like the plague."

-Scott Nations, CNBC analyst

Doesn't the stock market rely on bubbles?

"DotCom" <u>was</u> a bubble

Is cryptocurrency a Ponzi scheme?

"nearly half of millennial millionaires have at least 25% of their wealth in cryptocurrencies" (CNBC Millionaire Survey)

ELIZABETH WARREN

"As the demand for cryptocurrencies continues to grow and these assets become more embedded in our financial system, consumers, the environment, and our financial system are under growing threats," she added.

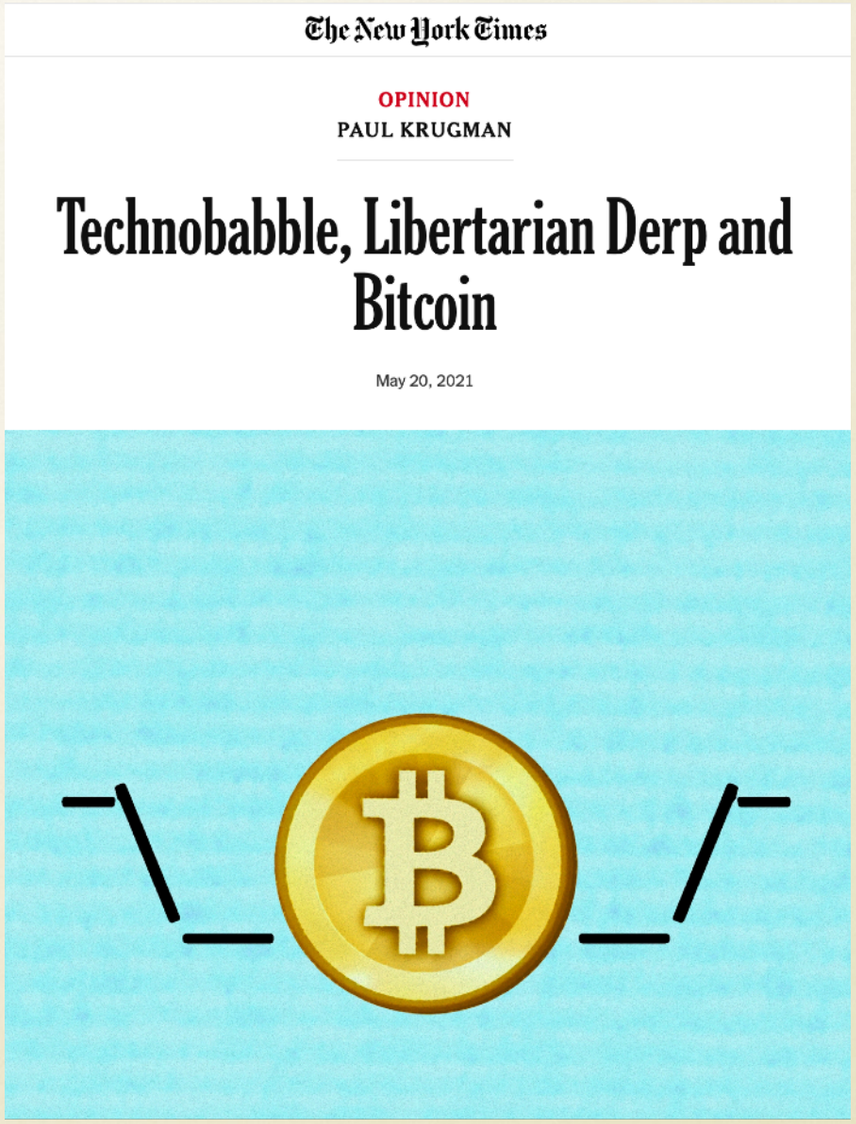
Warren cited five risks posed by an underregulated crypto market. In her words, they are:

- Exposure to hedge funds and other investment vehicles that lack transparency
- Risks to banks ?
- Unique threats posed by stablecoins
- Use in cyberattacks that can disrupt the financial system ✗
- Risks from decentralized finance

The cypherpunks might say that these are excellent talking points but regulation may not be the solution

SEVERAL OF YOU POINTED OUT THIS PAUL KRUGMAN OP-ED...

"But I've been in numerous meetings with enthusiasts for cryptocurrency and/or blockchain, the concept that underlies it. In such meetings I and others always ask, as politely as we can: "*What problem does this technology solve? What does it do that other, much cheaper and easier-to-use technologies can't do just as well or better?*" I still haven't heard a clear answer."



The New York Times

OPINION

PAUL KRUGMAN

Technobabble, Libertarian Derp and Bitcoin

May 20, 2021

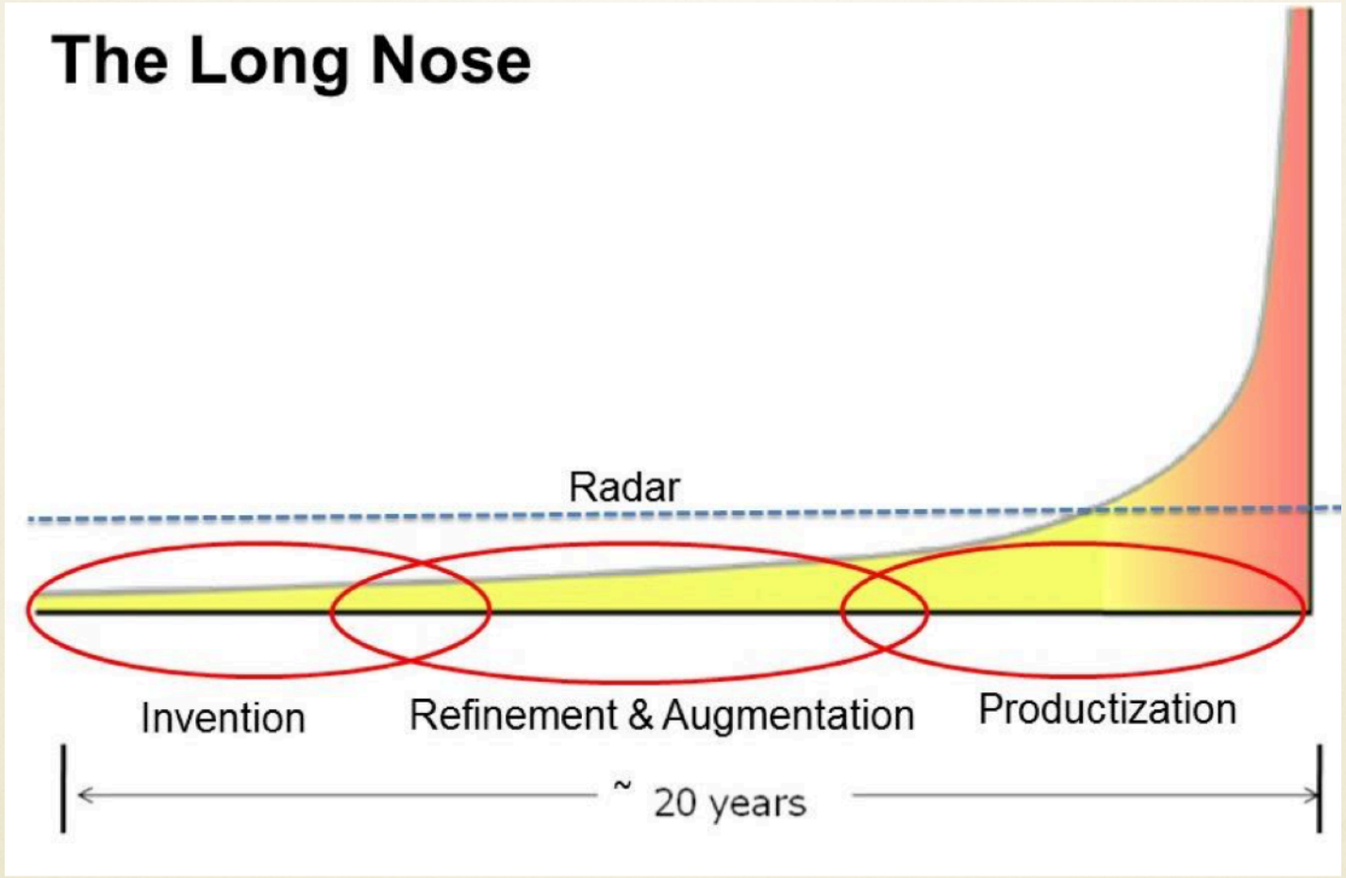
“Twelve years on, cryptocurrencies play almost no role in normal economic activity. Almost the only time we hear about them being used as a means of payment — as opposed to speculative trading — is in association with illegal activity, like money laundering or the Bitcoin ransom Colonial Pipeline paid to hackers who shut it down…Twelve years is an eon in information technology time…By the time a technology gets as old as cryptocurrency, we expect it either to have become part of the fabric of everyday life or to have been given up as a nonstarter.” (Paul Krugman)

“Maybe or maybe not. (=; ” (Bebo White)

<*slight digression*>

"The growth of the Internet will slow drastically…by 2005 or so, it will become clear that the Internet's impact on the economy has been no great than the fax machine's" (Paul Krugman, 1998)

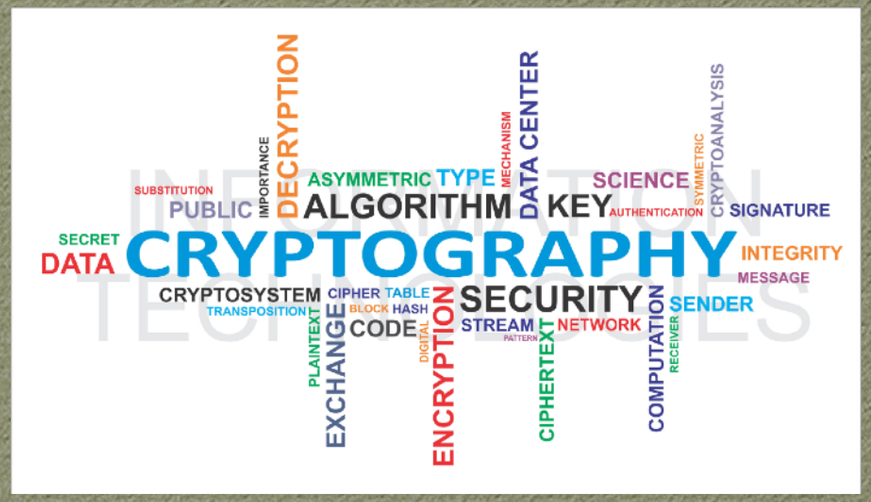
THE LONG NOSE OF INNOVATION (BILL BUXTON)



The bulk of innovation behind the latest “wow” moment is low-amplitude and takes place over a long period - well before the “new” idea has become generally known, fully refined, much less reached the tipping point where it becomes widely adopted.

"What the Long Nose tells us is that any technology that is going to have significant impact in the next 10 years is already at least 10 years old. Any technology that is going to have significant impact in the next 5 years is already at least 15 years old, and likely still below the radar. Hence, beware of anyone arguing for some "new" idea that is "going to" take off in the next 5 years, unless they can trace its history back for 15.[6] If they cannot do so, most likely they are either wrong, or have not done their homework." (Bill Buxton, Microsoft)

</end of slight digression>



WHAT'S THE CRYPTO IN CRYPTOCURRENCY?

A soft INTRODUCTION TO CRYPTOGRAPHY

HOW DOES ALL THIS CRYPTOCURRENCY AND BLOCKCHAIN STUFF WORK?

- the short answer is mathematics ("Vires in Numeris")
- but more precisely the mathematics behind cryptography
- computer algorithms
- think of all those things in our lives that we are not expected to understand but we are expected to trust
- please be patient - it's more the logic than the mathematics

WHAT IS CRYPTOGRAPHY?

- "crypto" from Greek "kruptos" - hidden
  - cryptocurrency means "hidden money?" 😄
- means "writing that is hidden"
- defines how to send data/messages "in the presence of adversaries"
- involves transforming data (***encryption***) in a manner such that it cannot be meaningfully interpreted because it is garbled (***ciphertext*** or ***cyphertext***)
- ***decryption*** means transforming encrypted (garbled) data back into interpretable form (***cleartext*** or ***plaintext***)

CRYPTOGRAPHY VOCABULARY

- cryptoanalysis - the art of breaking encrypted data
- cryptosystem - a system for encrypting and decrypting
- cryptographers - people who do cryptography
- cryptanalysts - practitioners of cryptanalysis
- cryptology - the branch of mathematics that studies the foundations of cryptographic methods
- cipher - the encoder, i.e., the encryption/decryption scheme
- substitution - exchanging one character for another
- transposition - rearranging the order of characters

WHY USE CRYPTOGRAPHY?

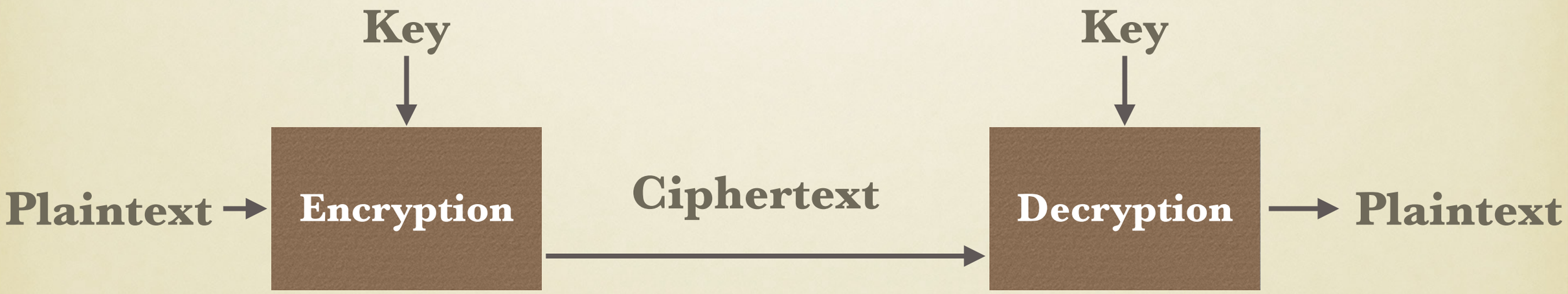
- confidentiality
- integrity
- authentication
- authenticity
- fault tolerance
- secure protocols

use examples

- online payments
- military secrets
- stock prices
- secure email
- IP protection
- secure transactions
- etc., etc.

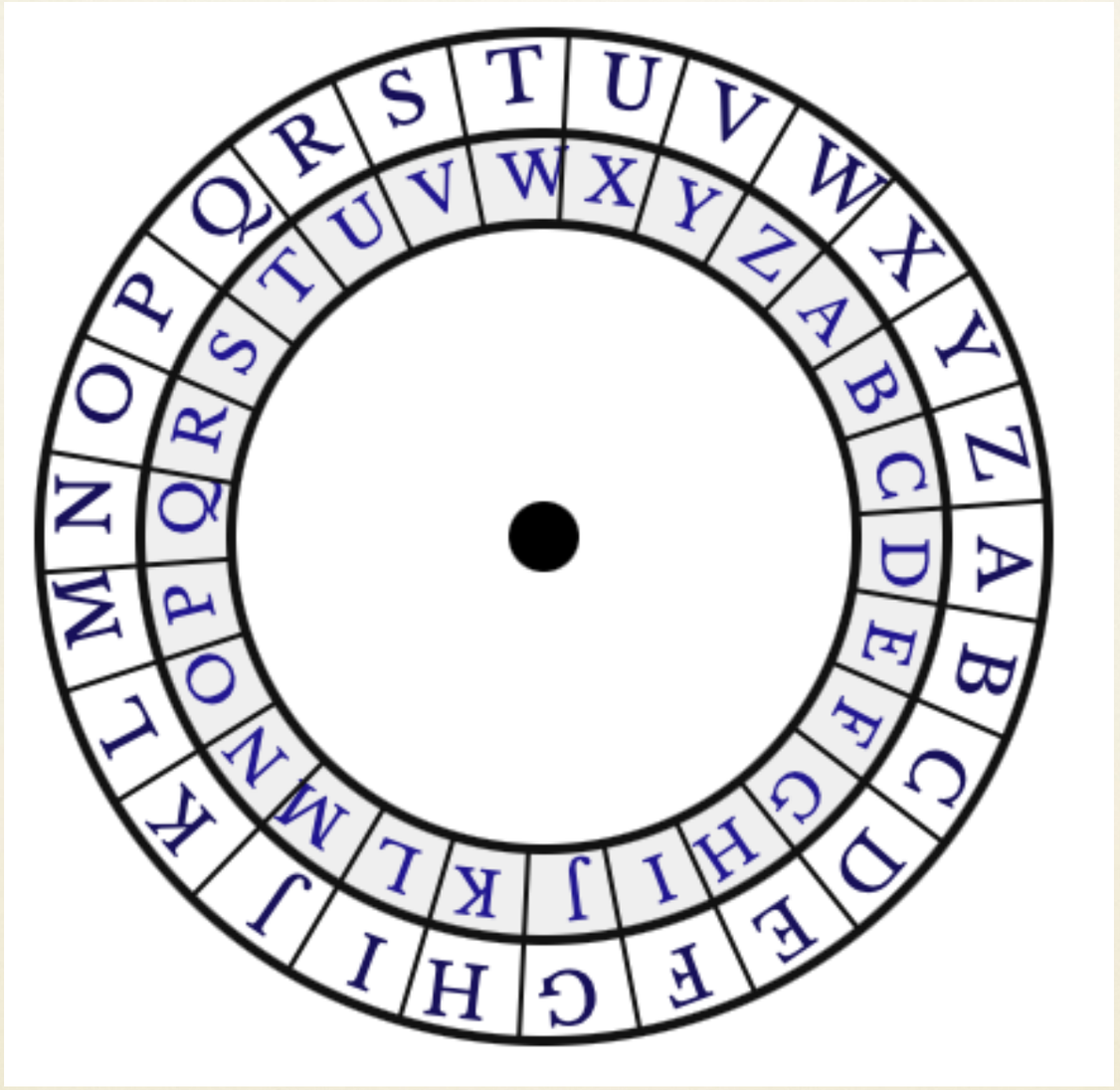
KEYS

- a variable value used by cryptographic algorithms to produce encrypted content or to decrypt encrypted content
- the "length" of the key indicates the difficulty to decrypt from the decrypted content
- ***symmetric encryption*** means that *same* key is used for encryption and decryption
- sender shares key with recipient (if they can…)



SIMPLE EXAMPLE - THE CAESAR CIPHER

- supposedly used by Julius Caesar
  - replace each letter position λ with (λ+3) mod 26 (i.e., divide by 26 and just consider the remainder - new letter position)
    - "Osher Lifelong Learning" becomes "Rvkhu Olihorqj Ohduqlqj"
- two components
  - *algorithm*: shift characters by a fixed amount
  - *key*: the fixed amount (e.g., +3)



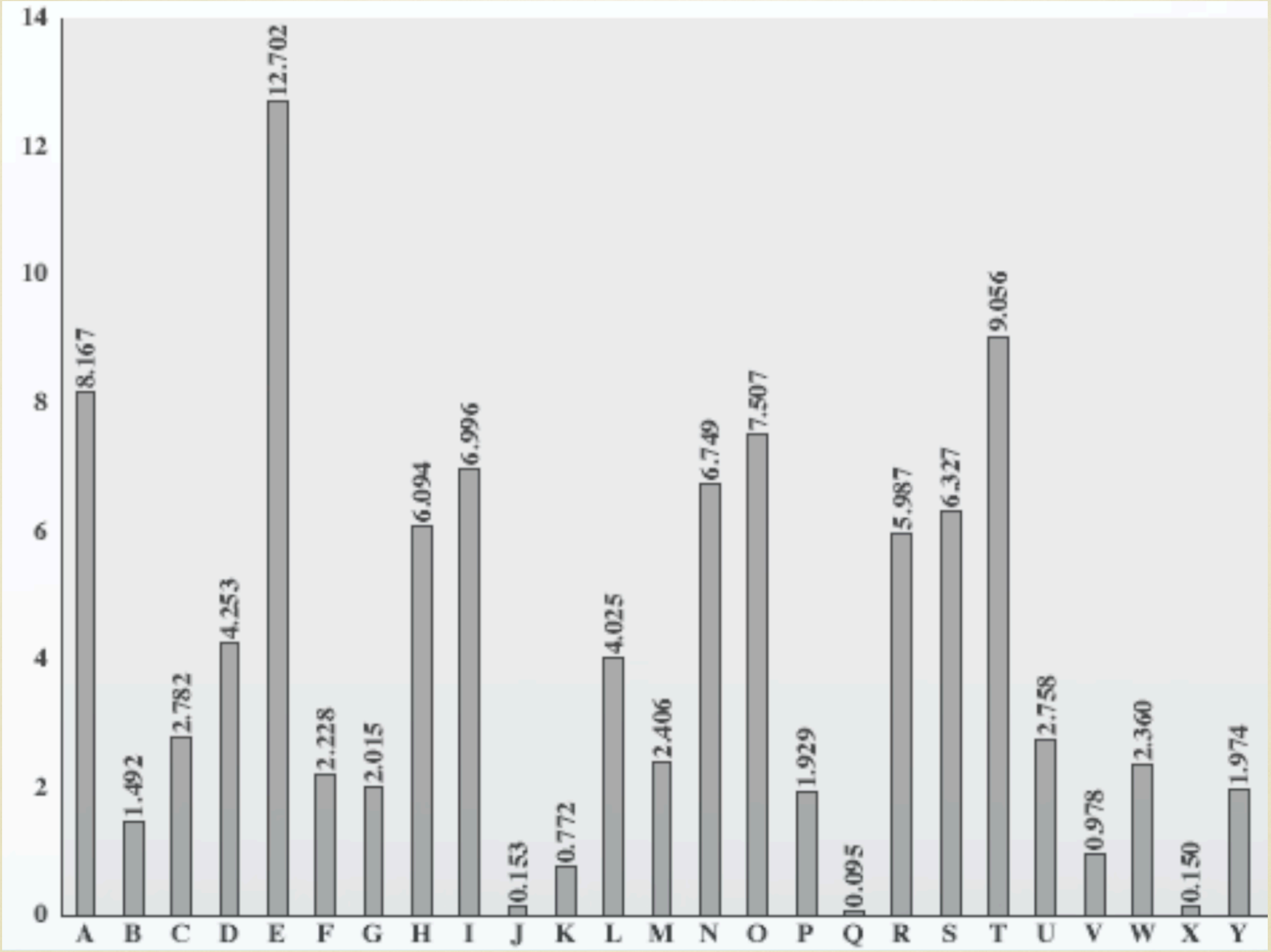
anybody have one of these?

KEYSPACE

- the ***keyspace*** is the set of all possible keys
  - Caesar Cipher: keyspace = {0,1,2,…25}
- size of the keyspace helps to estimate security
  - assumption: exhaustive search (brute force) is the only way to find a key

ISSUES WITH THE CAESAR CIPHER

- how do you share the algorithm and key (the shift) with desired recipient?
- pretty easy to "break" by an adversary - small keyspace
  - maintains the same word structure/capitalization
  - suppose you broke code into equal length blocks (if possible) with no capitalization? - "rv kh uo li ho rq jo hd uq lq j" - would that make it more difficult?
- letter frequency statistics
  - e,t,a,o most common English letters
  - using a single key preserves frequency


14
12
10
8
6
4
2
0
A 8.167
B 1.492
C 2.782
D 4.253
E 12.702
F 2.228
G 2.015
H 6.094
I 6.996
J 0.153
K 0.772
L 4.025
M 2.406
N 6.749
O 7.507
P 1.929
Q 0.095
R 5.987
S 6.327
T 9.056
U 2.758
V 0.978
W 2.360
X 0.150
Y 1.974

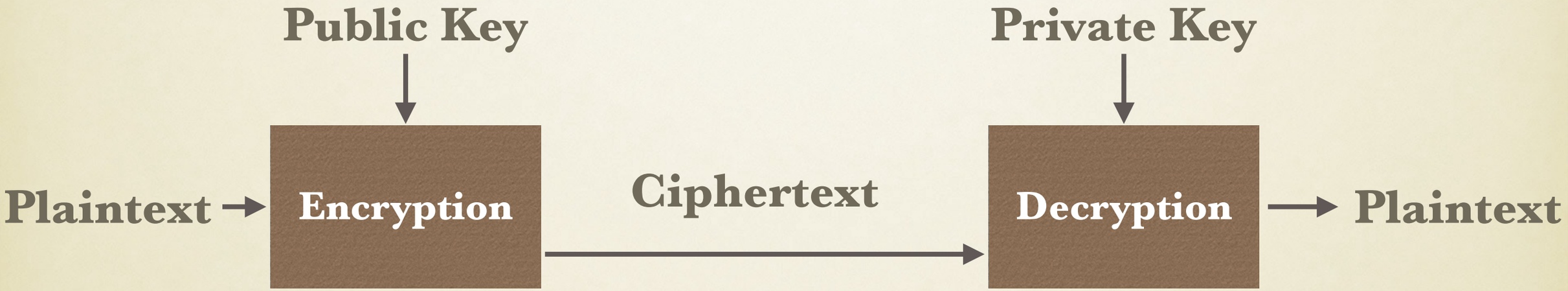
IS SYMMETRIC ENCRYPTION STILL RELEVANT?

- computationally easy to encrypt and decrypt
- in an Internet-connected world, how can you safely share keys?
- there are more sophisticated symmetric encryption methods and algorithms than the Caesar Cipher
- can use symmetric encryption in conjunction with other methods
- ***yes!*** we use it all the time (part of HTTPS includes symmetric encryption - "the session key" used one time)

PUBLIC-KEY/ASYMMETRIC ENCRYPTION (1 OF 2)

- involves 2 distinct keys - one public and one private
- the *private* key is kept secret and never divulged and is password protected (***passphrase***)
- the *public* key is not secret and can be freely distributed, shared with anyone
- both keys can be used for encryption and decryption
- someone encrypts something with your *public* key, sends it to you, and only you can decrypt it with your *private* key - sounds like magic!
- the *public* and *private* keys are generated at the same time and are mathematically related by complex mathematical functions
- asymmetric encryption is 100 to 1000 times slower than symmetric encryption
- it is computationally infeasible to derive the *private* key from the *public* key - note: that's why some people are worried about quantum computing

PUBLIC-KEY/ASYMMETRIC ENCRYPTION (2 OF 2)



Would not make much sense to encrypt with private key…effectively no encryption at all since anyone can see your public key

AN OVER-SIMPLISTIC EXAMPLE

- public key = 4; private key = 1/4; message = 5
- **encryption**:
  - ciphertext c = m * public key
  - 5 * 4 = 20
- **decryption**:
  - plaintext m = c * private key
  - 20 * 1/4 = 5
- clearly the relationship between these public and private keys is not too complex

Public key

Made available anywhere and to anyone

Generated together

Protected and kept secret

Private key

BEBO WANTS TO SEND A SECURE MESSAGE TO NICK

Nick's public key

Bebo's message (plaintext)

Bebo's message (ciphertext)

Insecure channel

Bebo's message (ciphertext)

Bebo's message (plaintext)

Nick's private key

REALITY CHECK

- in case you're wondering where we're going…
- <u>suppose, for example</u>:
  - instead of sending a message/text, it is value/money or some representation of such
    - Bebo is the *payer*
    - Nick is the *payee*
    - the communication is occurring via a computer/mobile telephone and the "insecure channel" is the Internet/telephone network
- is the value/money cryptocurrency?
- is this model sufficient? **- *no!* -** Nick could still say that he never got paid

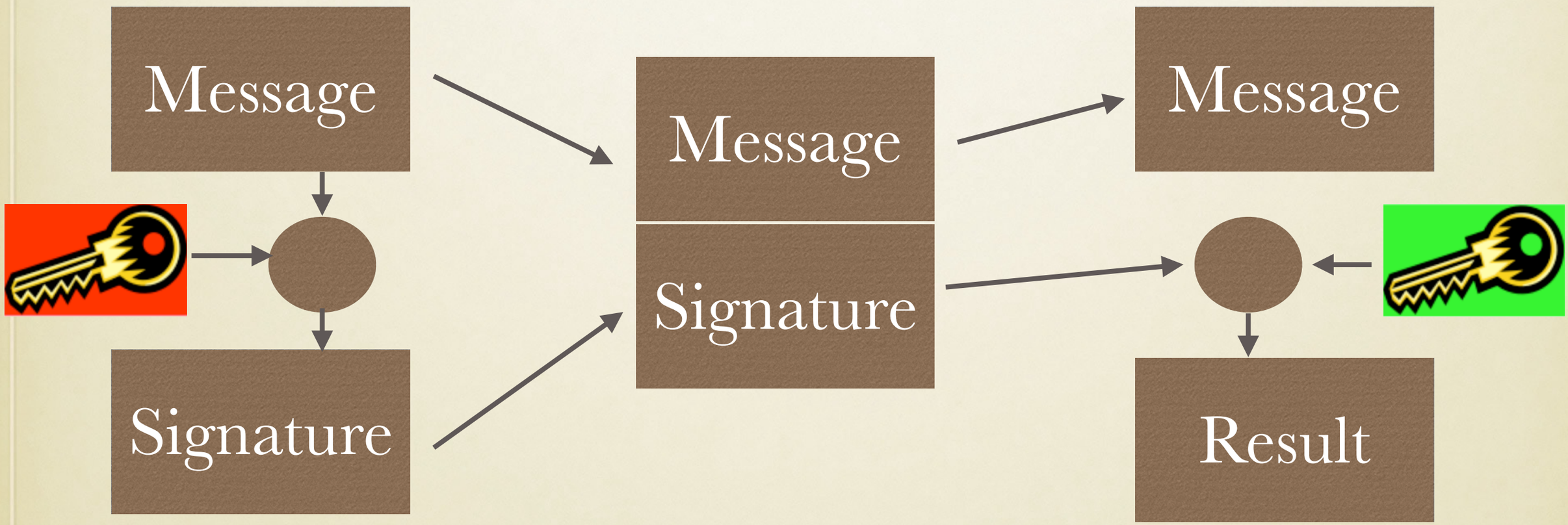
DIGITAL SIGNATURES (1/3)

- mechanism used to cryptographically bind entities to objects
- fundamental idea:
  - digital signature computed and attached to an object, e.g., file, photo, etc.
  - if anyone tries to alter that object, the digital signature will not verify

DIGITAL SIGNATURES (2/3)

- encrypt with private key
- therefore can only decrypt with public key
- anyone can verify that you "signed" the entity since only you could have encrypted it with your private key
- signed and encrypted messages
  - encrypt with your private key
  - encrypt with recipient's public key
  - so, recipient reverses the process- decrypts with their private key and then decrypts the result with the sender's public key

DIGITAL SIGNATURES (3/3)



If the result is not identical to the message then the message was altered in transmission

KEY MANAGEMENT - PUBLIC KEY INFRASTRUCTURE (PKI)

- consider, when you go to www.amazon.com, how do you know that you're going to the real Amazon?
- how do you know that the keys being used by this questionable Amazon are legitimate?

- PKI is a system that uses asymmetric encryption and **digital certificates** to achieve secure Internet services
- have you ever seen messages about certificates or "certificate expired" when visiting a web site?
- since cryptocurrency is largely anonymous, PKI is not always an issue
- we will talk further about PKI when we cover blockchains and FinTech

MESSAGE-DIGEST/HASH FUNCTIONS

- if you think that asymmetric encryption is magic, there are hash functions
- they map a variable-length input message to a fixed-length output character string
- not encryption - it is not feasible to determine the original input based on the hash value (non-reversible)
- it is impossible (?) to find an arbitrary message that has a desired hash value - remember this…
- it is infeasible to find two messages that have the same hash value (the hash function would be broken)
- no secret keys are involved - hash functions are public information
- examples- MDx {x=2,4,5,6} SHAx {x=0,1,3,224,256,384,384,512}

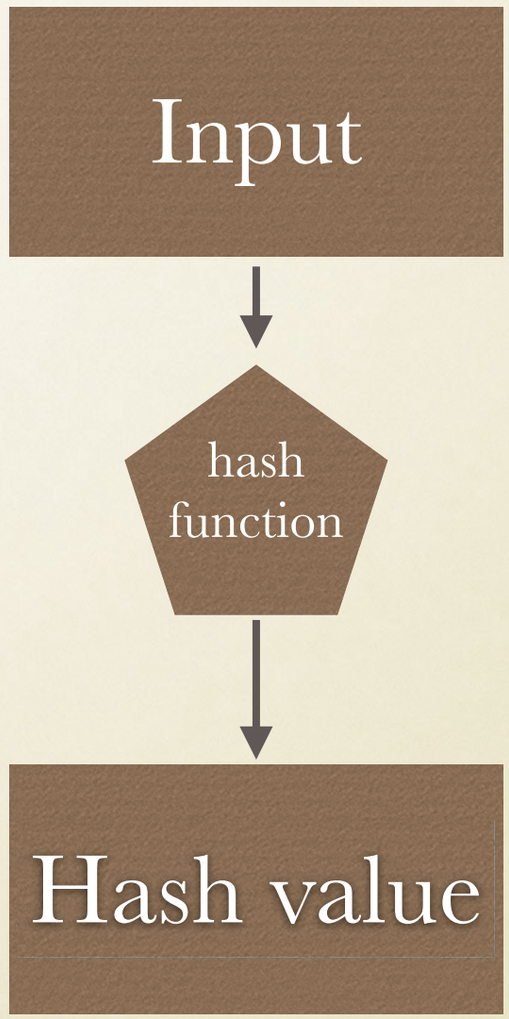
MESSAGE DIGEST/HASH FUNCTIONS

- a ***hash function*** is a mathematical equation that outputs a hash value from the input

- a ***hash value*** is used to create a unique digital signature from a particular input

- any changes in the input value (no matter how minor) results in a totally new hash value

- used to determine if the input value has been changed



This online tool allows you to generate the SHA256 hash of any string. SHA256 is designed by NSA, it's more reliable than SHA1.

Enter your text below:

OLLI
Olli
0LLI

Generate | Clear All | MD5 | SHA1 | SHA512 | Password Generator

☑ Treat each line as a separate string

SHA256 Hash of your string:

```
EE0255B7B15FB9145998D8003B8C06A594053CFAA928FDFDD3497261EF51E3CD
26640DB311F579617D7FCC12827F62D6321C6005367ADDABF770D457FC54EFC3
8D5D56A5218767310BA6EE01E7C830651AFFB0FB903CA34F2836439C24B5E52D
```

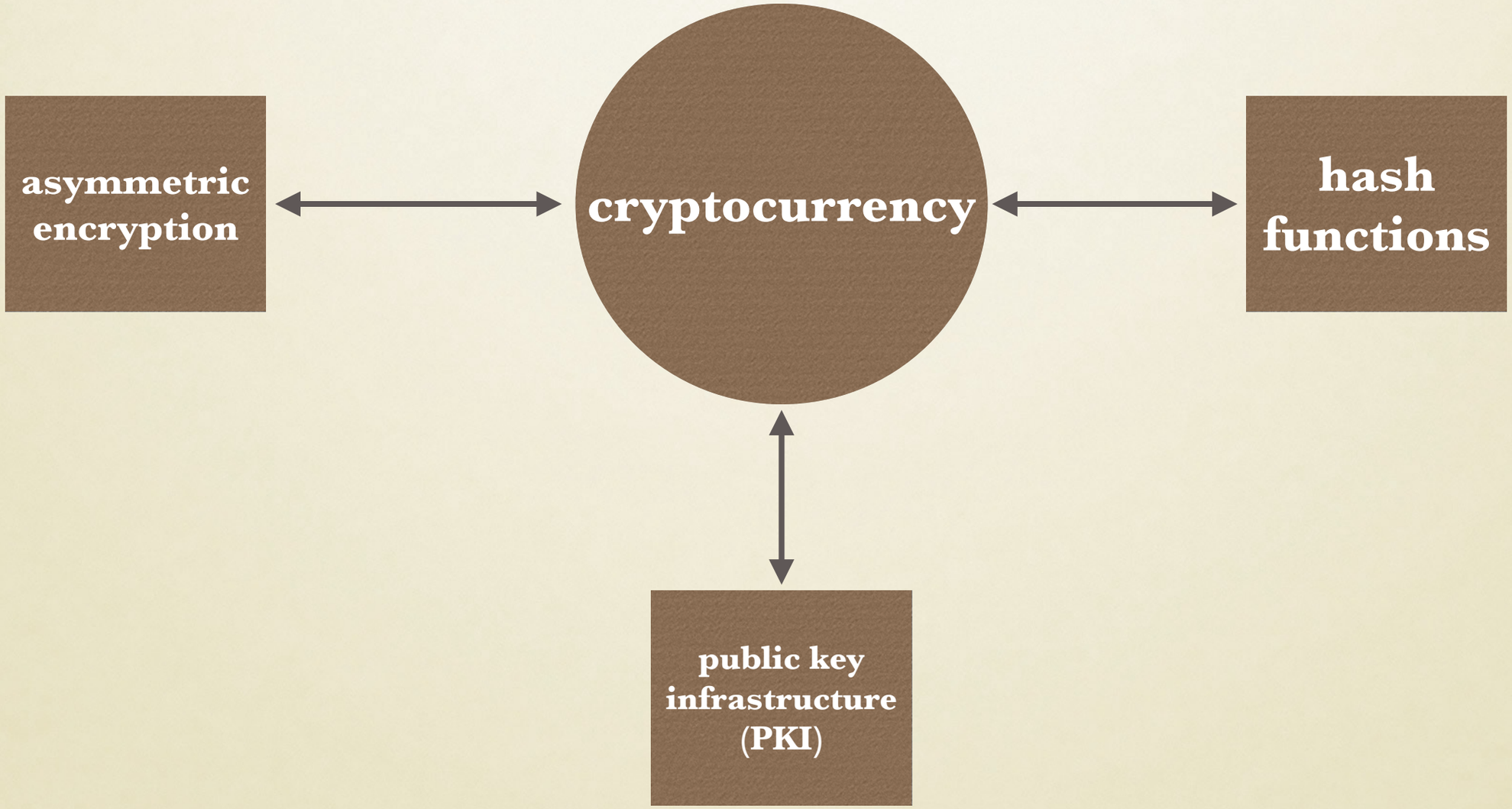
The complete text of "War and Peace" would create a unique 256 bit string

256 bits = 64 hexadecimal characters

TO PUT HASH VALUE POSSIBILITIES INTO CONTEXT

- SHA256 outputs a 256 bit (1's and 0's) string
- $2^{256} = 10^{77}$
  - 3 x 10^{23} = number of *stars* in observable universe
  - 10^{78} to 10^{82} = number of *atoms* in observable universe
- if the hash function (e.g., SHA256) is mathematically robust, then the hash strings it generates should be trusted

WE NOW HAVE ALL THE PIECES!



WHAT EXACTLY IS BITCOIN (AND IN GENERAL OTHER CRYPTOCURRENCIES)?

- no physical entity - not even a character string
- "a chain of digitally signed transaction records leading from the original owner to the current owner"
- permanent - can't be lost, but can be inaccessible
- the transaction records contain
  - hashes that are difficult to find AND
  - virtual/anonymous owner IDs (addresses)
- no bitcoin registry; no centralization
- bitcoin blockchains are broadcast globally; anyone can verify them; they encompass all the past and present transactions

HOW BITCOIN REALLY WORKS (ADDRESSES/KEYS)

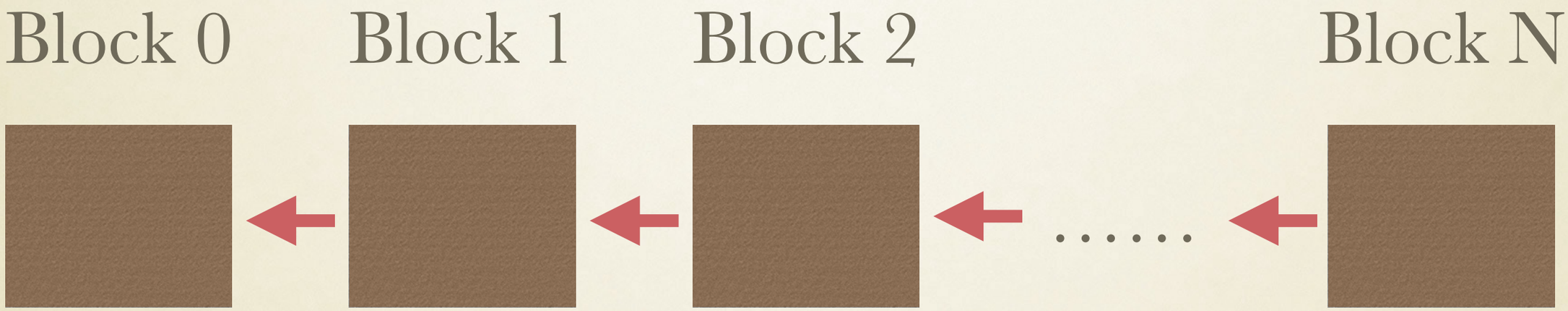
- software generates bitcoin addresses of 25-44 characters for users - a public and private key pair
- sample public key: 1BBsbEq8Q29JpQr4jygjPof7F7uphqyUCQ
- to send/spend bitcoins, user specifies a receiving public key and amount - like digital signatures
- to receive bitcoin, provide your public key and amount
- keys are not registered to users to insure anonymity; a user can use a different key for every transaction

YOU DON'T REALLY HAVE TO REMEMBER THAT LONG ADDRESS...

- just your public key, not your private key
- is stored in your cryptocurrency wallet
- usually stored as a QR code that you can display
- used when you receive bitcoin, e.g., get paid, at an ATM
- need to know the recipient's public key in order to make a payment
- usually read the recipient's QR code with your mobile telephone camera

- that's the role of cryptography in transactions - to make them safe, secure and anonymous
- next the transaction has to get added to the blockchain/ledger - that's what cryptocurrency mining is all about - the subject of a future lecture
- what's the role of cryptography in the blockchain/ledger that allows it to be public and immutable?

REMEMBER WHAT THE BLOCKCHAIN LOOKS LIKE? (1/2)



Block = Data + pointer to next block
a so-called “linked list”
Blocks are added at the end (newest)

REMEMBER WHAT THE BLOCKCHAIN LOOKS LIKE? (2/2)

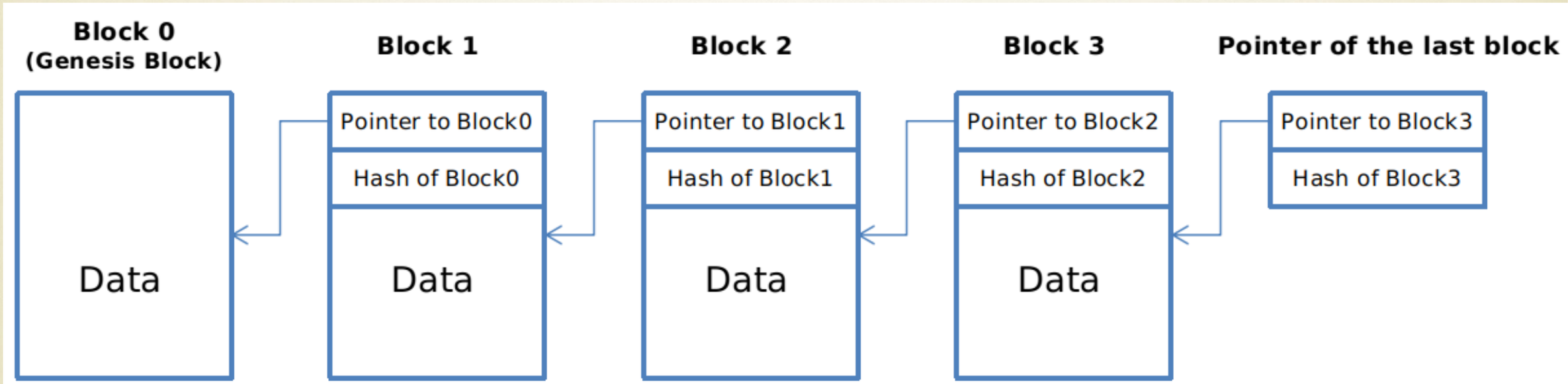
- if this were on a single computer, the pointer/link would be to a memory address/location (e.g., in computer memory, on an attached hard drive, etc.) - that's how your computer finds data - someone couldn't change it unless they had access to your computer

- how can multiple networked computers use a distributed ledger safely and securely as the blockchain concept suggests?

- how to make pointer/link general/unambiguous for shared data or on shared computers all over the world? - the pointers and data have to be in one big file

- how to make pointers and data in that one big shared file secure, unique and non-corruptible? i.e., how to keep someone from just editing that file? - make it impossible(?) to change without detection

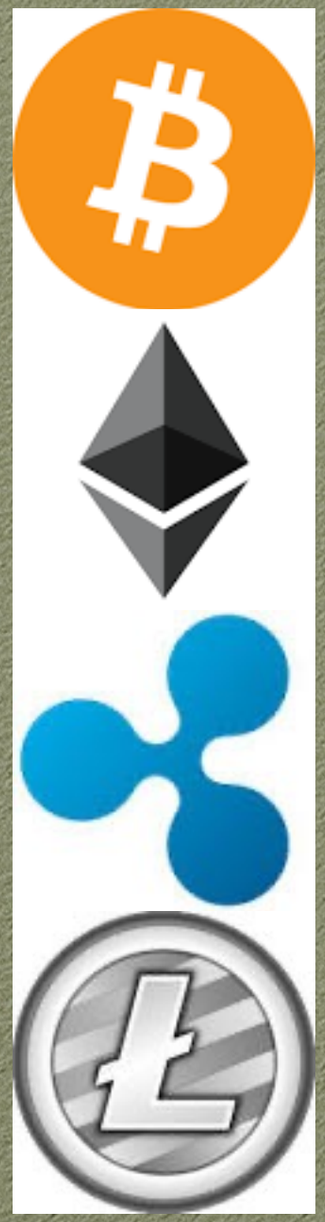
SATOSHI USED HASH POINTERS



the hash stored in the hash pointer is the hash of the whole data of the previous block, which also includes the hash pointer to the block previous to it

This makes it impossible to tamper with a block in the blockchain without letting everyone know since if you change data in "Block 2" that you'll have to change all blocks that come after it…


If you don't believe it or don't get it, I don't have the time to try to convince you, sorry.
Satoshi Nakamoto
quotefancy



STICKING YOUR TOE INTO CRYPTO

ACCOUNTS, WALLETS, USAGE

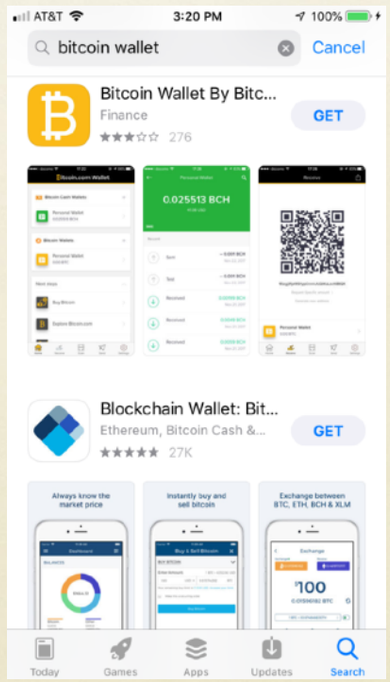
HOW TO GET CRYPTOCURRENCY

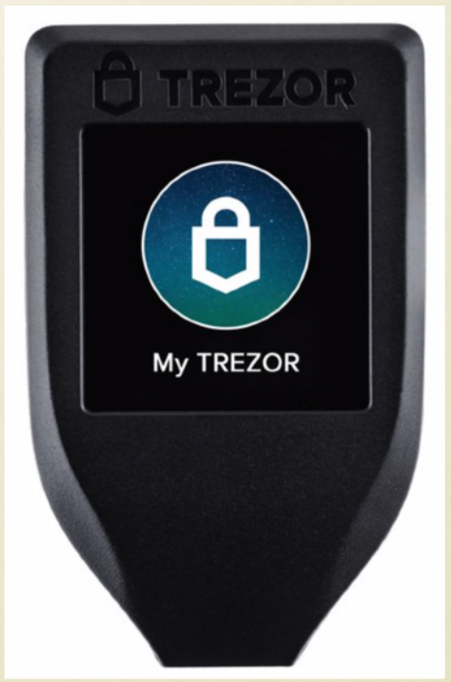
- receive a gift or donation
- receive as payment
- receive salary in it (legal ramifications?)
- use an ATM
- use a coin exchange (like an online bank)
- from games, rewards, gambling, etc.
- participate in an ICO (more about that later)
- become a "miner" (more about that later)
- steal it (I'm not serious)

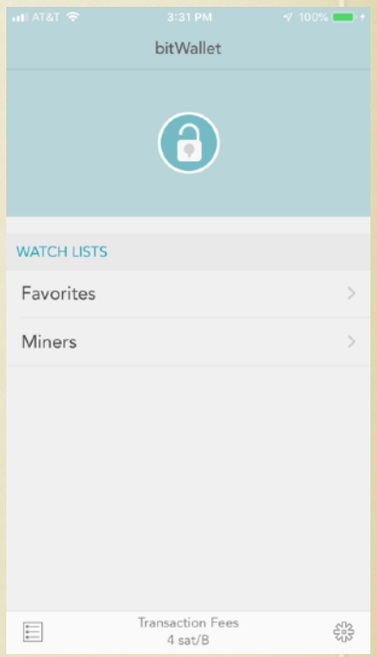
ALL IT REALLY TAKES

FIRST YOU NEED A WALLET

- a software application, not a physical wallet
- on a computing device - typically desktop computer, laptop computer, or mobile telephone
- dedicated hardware
- a means to backup your wallet
- a memorable passphrase (not always required)
- as many wallets (and keys) as you want







WALLETS

- all wallets are variations on the same theme:
  - establish an identity - some of this information is used in public-private key generation
  - link to financial institution - only necessary for buying/selling to/from fiat currency
  - maintain wallet(s) - multiple accounts, multiple types of cryptocurrency
    - generating keys - as strings and/or QR codes
    - tools for sending/receiving cryptocurrency
- some wallets offer key management
- differences in computer interface capabilities, usability
- often provide new keys for each transaction
- ***most important thing is to backup your wallet! - why?***

"HOT WALLETS" AND "COLD STORAGE"

- *hot wallet* is online and connected in some way to the Internet
  - security issues similar to storing content "in the cloud"
- *cold storage* is offline
  - only as secure as the storage device
- most coin exchanges use a combination

The New York Times

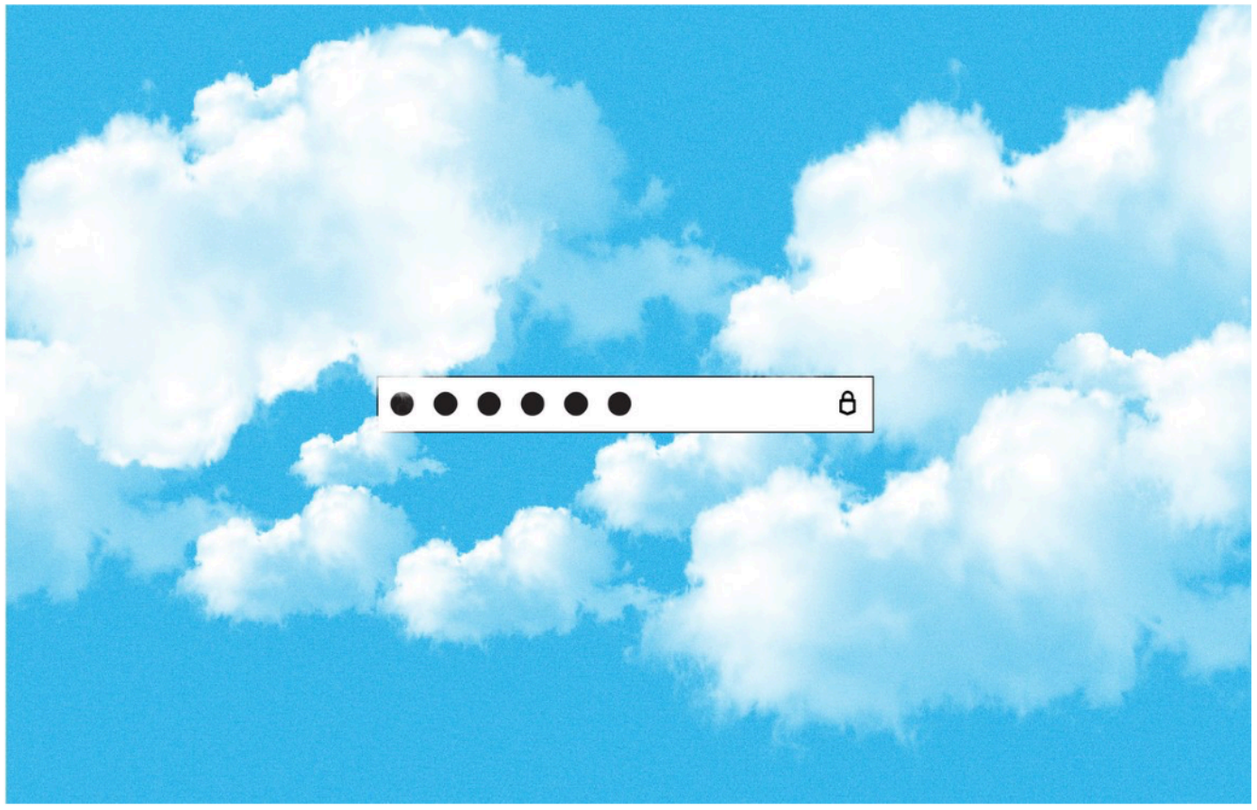
Account

Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes

Bitcoin owners are getting rich because the cryptocurrency has soared. But what happens when you can't tap that wealth because you forgot the password to your digital wallet?

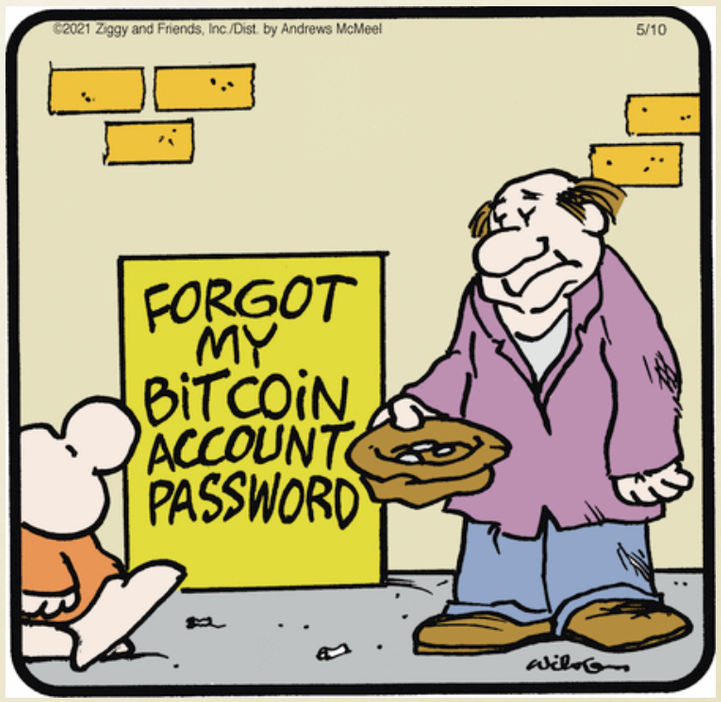
MARK FRAUENFELDER SECURITY 10.29.17 05:00 PM

‘I FORGOT MY PIN’: AN EPIC TALE OF LOSING $30,000 IN BITCOIN



NICK ORTEGA

Satoshigallery
son of a bit since 2008



The Trezor: January 4, 2016: 7.4 BTC = $3,000

In January 2016, I spent $3,000 to buy 7.4 bitcoins. At the time, it seemed an entirely worthwhile thing to do. I had recently started working as a research director at the Institute for the Future’s Blockchain Futures Lab, and I wanted firsthand experience with bitcoin, a cryptocurrency

Best Bitcoin Wallets

Ultra-secure Trezor and software wallet Exodus are top choices

By LUKE CONWAY | Reviewed by MARISA FIGAT | Updated Jul 22, 2021

Bitcoin has gained widespread acceptance and continues to grow in popularity. Unlike stocks at a stock brokerage, you can withdraw your cryptocurrencies from a crypto exchange and store them in an outside wallet. The best Bitcoin wallets make it easy (and maybe a little fun) to securely store and manage your crypto portfolio.

If you're looking to buy and store Bitcoin or other cryptocurrencies, you may be on the hunt for the best Bitcoin wallet. We looked at a long list of Bitcoin wallets with a focus on cost, user experience, supported cryptocurrencies, and other features. Keep reading for a look at some of the best Bitcoin wallets available today.

The Best Bitcoin Wallets of 2021

- **Best for Beginners:** Exodus
- **Best For Advanced Bitcoin Users:** Electrum
- **Best for Mobile Users:** Mycelium
- **Best Hardware Wallet:** Ledger Nano X
- **Best For Security:** Trezor Model T
- **Best Bang For Your Buck:** Ledger Nano S

2:53

Search

bitWallet™ — Bitcoin Wallet

Sollico Software

OPEN

105 RATINGS	AGE	CATEGORY	DE
3.4 ★★★☆☆	4+ Years Old	Finance	Sollic

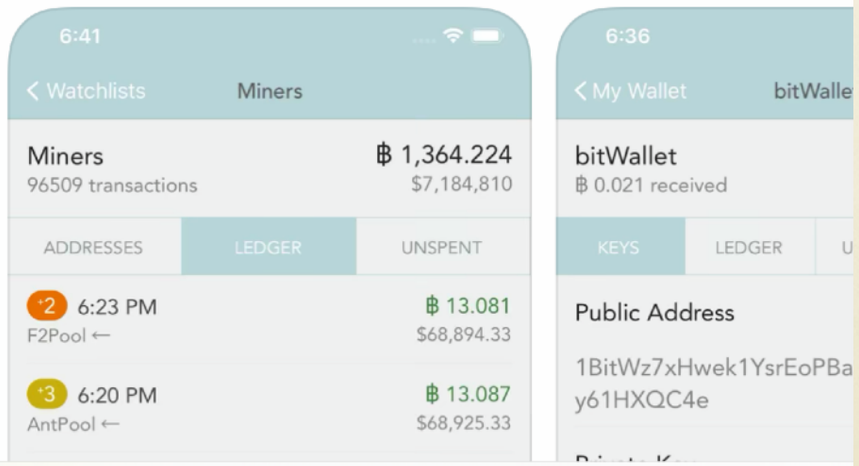
What's New

Version History

Version 2.6.8 — 1y ago

Unspent outputs with 0 confirmations can now be included in payments.

Preview



Today | Games | Apps | Arcade | Search

2:51

My Wallet — Howard White — Pay

Howard White

฿ [redacted] received

฿ [redacted]

KEYS | LEDGER | UNSPENT | VERIFY

Public Address

1HDAQozS8z2FY999Kjouu
yBFXhPXuhPQ5f

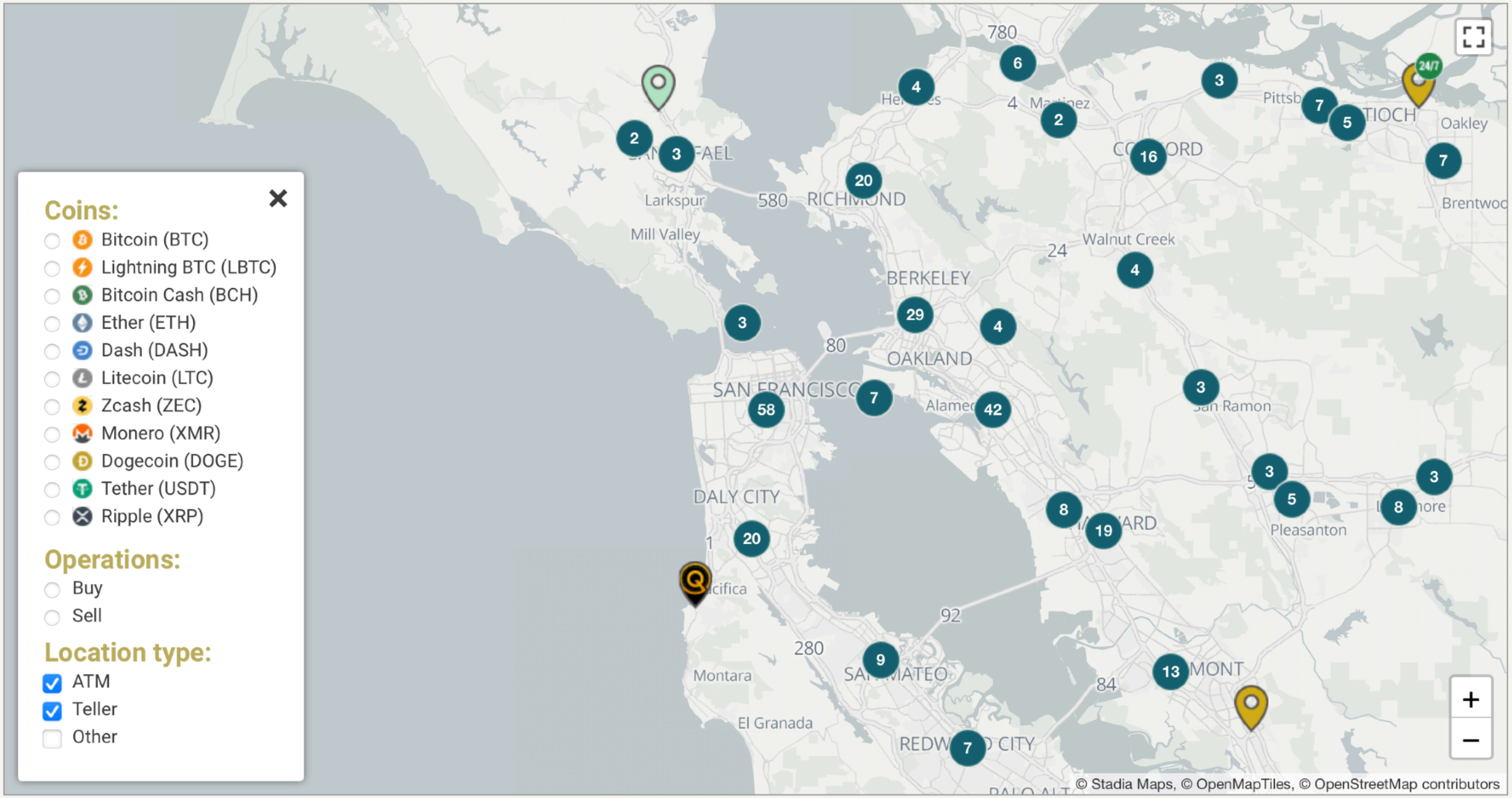
Private Key

[redacted]

Exchange Rate
$44,916

Bitcoin ATMs in San Francisco, United States.

Total number of Bitcoin ATMs / Tellers in and around San Francisco: 405



https://coinatmradar.com/city/142/bitcoin-atm-san-francisco/


How to Use
a Bitcoin ATM
BTM
BITCOIN TELLER MACHINE
1 BTC
609.91 CHF
START

Questions?
Comments?

bebo.white@gmail.com