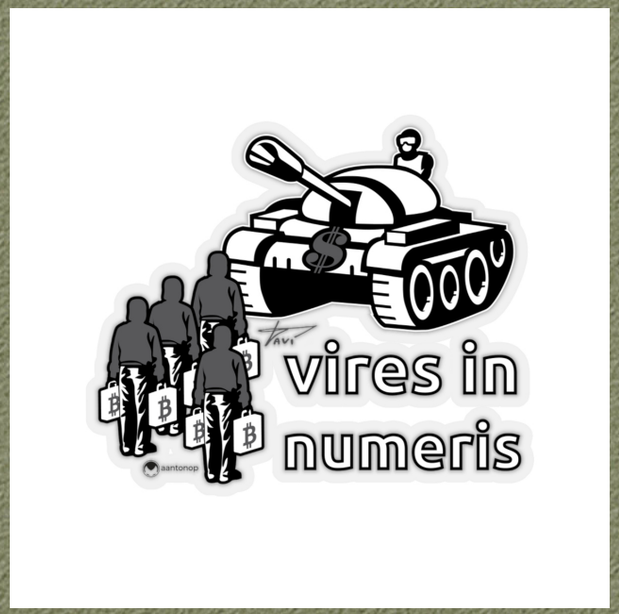
Cryptocurrency, Blockchain, and a new economic world

olli

late summer 2021

lecture 1

Bebo White - bebo.white@gmail.com



CLASSES | SPEAKER SERIES | INTEREST GROUPS | **ALL PRESENTED via ZOOM CONFERENCE**

OLLI
San Francisco State University

Late Summer 2021

August 9 – September 20

Registration open through Thursday, August 5.
Monday classes skip September 6.

For more information and to register:
https://olli.sfsu.edu/courses

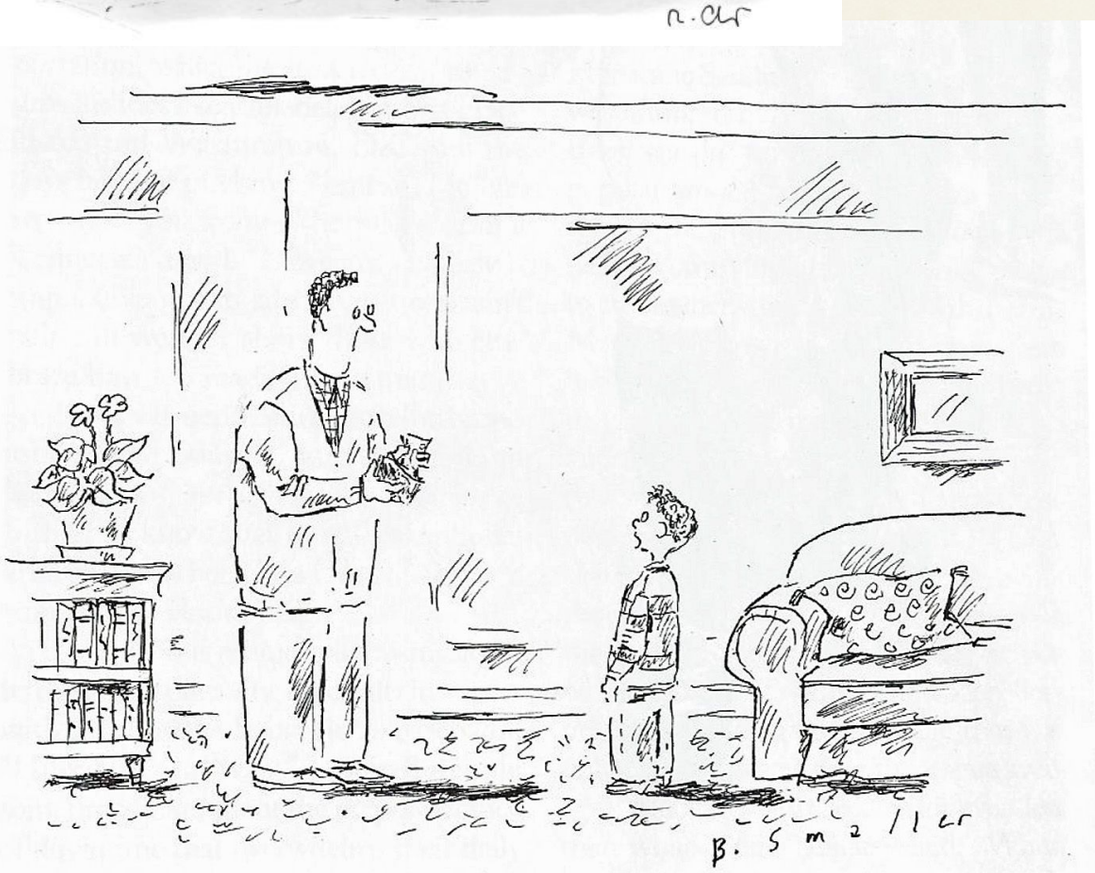
Day	Time	Course	Instructor	Meeting Dates	Schedule
M	10:00 am - 12:00 pm	**Oral Histories: A Personal Narrative Writing Workshop**	Sara Broderick	8/9 - 9/20	6 Meetings
M	12:30 pm - 2:30 pm	**Vincent van Gogh: His Life, His Letters, and His Art**	Maureen O'Brien DeGeller	8/9 - 9/20	6 Meetings
M	3:00 pm - 5:00 pm	**A Collage a Day Keeps the Blues Away**	Lola Fraknoi	8/9 - 9/20	6 Meetings
T	10:00 am - 12:00 pm	**Art of Directing Theater**	Carey Perloff	8/10 - 9/14	6 Meetings
T	12:30 pm - 2:30 pm	**Languages of the World**	Asya Pereltsvaig	8/10 - 9/14	6 Meetings
T	3:00 pm - 5:00 pm	**South Asians in America**	Falu Bakrania	8/10 - 9/14	6 Meetings
W	10:00 am - 12:00 pm	**From Farm to Facebook: The Family in Global and Historical Perspective**	Elaine Leeder	8/11 - 9/15	6 Meetings
W	3:00 pm - 5:00 pm	**Fighting Slavery in the Civil War Era**	Richard Bell	8/11 - 9/15	6 Meetings
Th	10:00 am - 12:00 pm	**Viva Verdi! Opera and the Birth of Modern Italy**	Clifford "Kip" Cranna	8/12 - 9/16	6 Meetings
Th	12:30 pm - 2:00 pm	**Hollywood in the Thirties: Window on America**	Elliot Lavine	8/12 - 9/16	6 Meetings
Th	3:00 pm - 5:00 pm	**Introduction to Ecology**	Tania Pollak	8/12 - 9/16	6 Meetings
F	10:00 am - 12:00 pm	**Turning Prose into Drama, the Alchemy of Adaptation**	Denize Springer	8/13 - 9/17	6 Meetings
F	12:30 pm - 2:30 pm	**Cryptocurrency, Blockchain, and a New Economic World**	Bebo White	8/13 - 9/17	6 Meetings

ADMINISTRIVIA

- all slides will be available online after each class (https://bit.ly/3CHqpKC); all have Creative Commons license (i.e., can be freely shared) - don't try to write down materials on slides - that's why they are dense - focus on listening, understanding and questions
- if I get too technical or going too fast, please let me know
- topics are a "moving target" - I'll try to keep up with current news stories, developments and issues
- please submit stories that you come across
- I'll provide a reference list/bibliography if there is interest

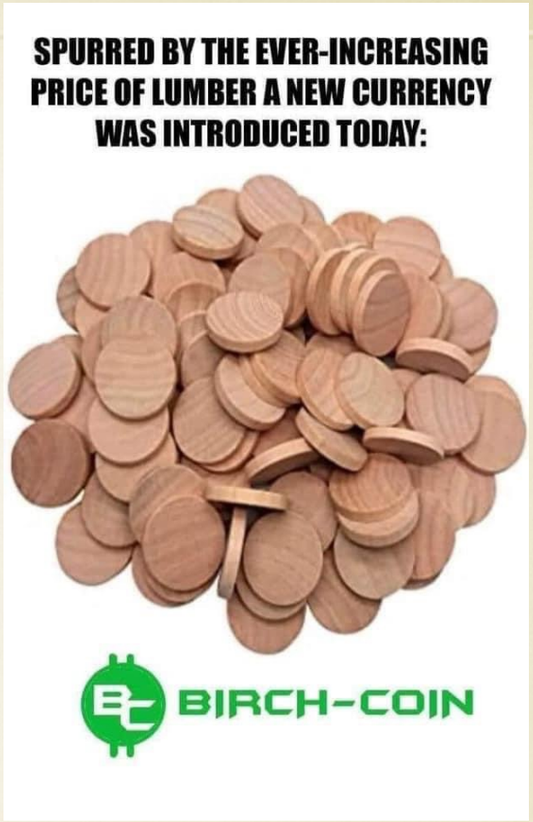
PROLOGUE

- **1** don't compare cryptocurrency/Bitcoin to the Dutch tulip mania - ***bubbles don't burst*** three times in a decade and come back stronger each resurgence
- it's clear that right now cryptocurrency is experiencing unprecedented volatility - that makes news - but it should not be unexpected or surprising - something new every day!
- in such times such as these, predictions and prognostications often run the spectrum from positive to negative - is it the ***death of cryptocurrency (has the bubble burst?)*** or an ***overdue adjustment?***
- in fact, nobody knows what's going to happen, but many have opinions
- don't be swayed by hype, speculation, financial planning, crime, etc.
- no matter your position - the whole phenomenon remains fascinating (IMHO) and is still worth learning about and discussing because it's not going away



"If it's all the same to you, I'd like my allowance in bitcoins."

Why are these funny? (assuming that you think they are) - let's find out

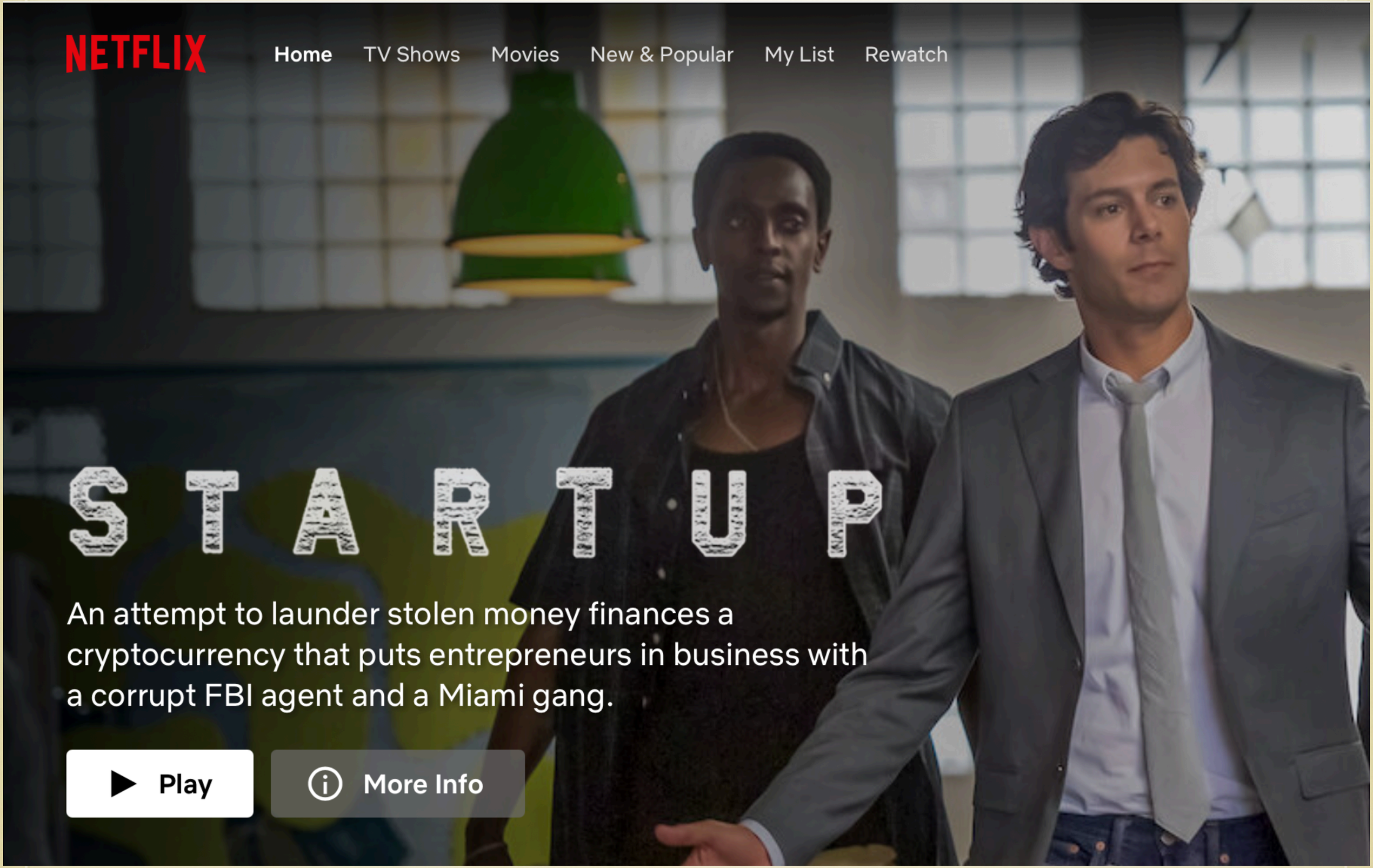


- when I tell people that I research/teach/discuss/advocate(?) cryptocurrency/bitcoin and blockchain, the typical reaction is that I'm
  - a techie/computer nerd/idealist academic, etc.
  - a hacker, criminal or anarchist
  - unaware (or willing to overlook) the social and/or environmental issues associated with the technology
- why this reaction?

BECAUSE THEY THINK OF THIS...

Bitcoin is imploding — here's where bitcoin bulls and bears see it headed from here

Published: Nov 20, 2018 3:38 p.m. ET


NETFLIX
Home
TV Shows
Movies
New & Popular
My List
Rewatch
STARTUP
An attempt to launder stolen money finances a cryptocurrency that puts entrepreneurs in business with a corrupt FBI agent and a Miami gang.
Play
More Info

MY GOALS FOR THIS COURSE

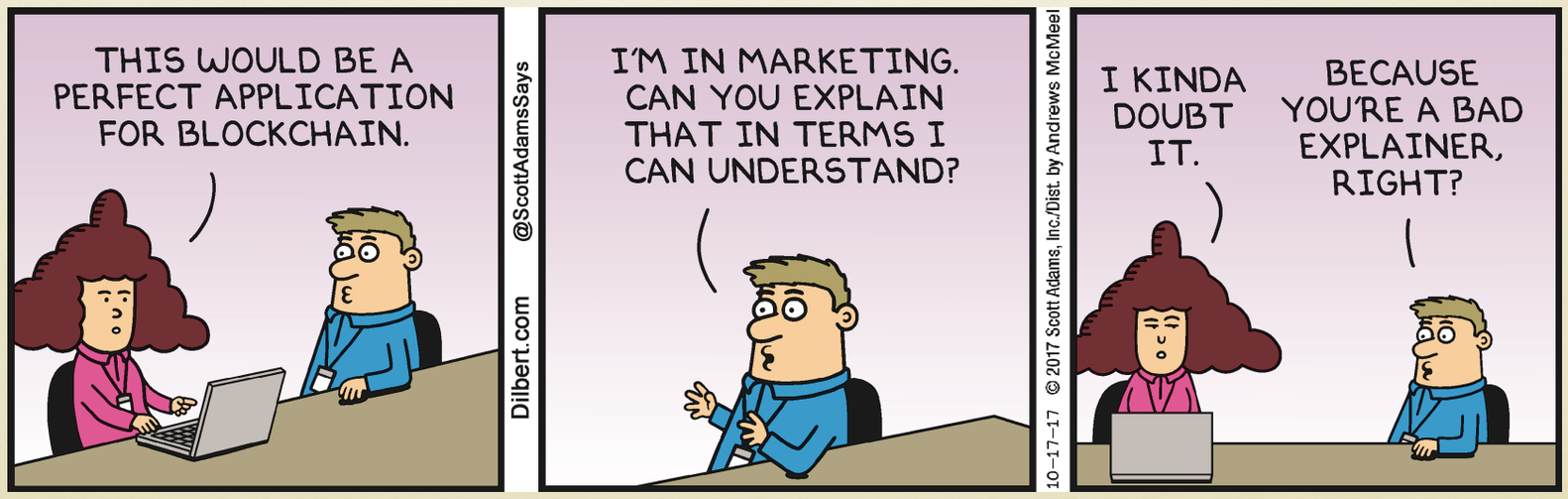
- to <u>help</u> you
  - appreciate why this technology is special, unique, revolutionary and disruptive
  - understand what all the cryptocurrency/blockchain conversation is about - both positively and negatively
  - have the vocabulary to analyze stories/commentary etc. that you read/hear
  - do some good mental exercises
- **<u>not to convince</u> you to buy or invest in cryptocurrency**
- <u>to have fun and be challenged</u>

"Insomnia eh? Have you tried listening to a guy try to explain Bitcoin?"

WRITER ALEXIS NOVAK
ARTIST JASON CHATFIELD

MADMAG.COM

Please ask questions - don't let me drone on

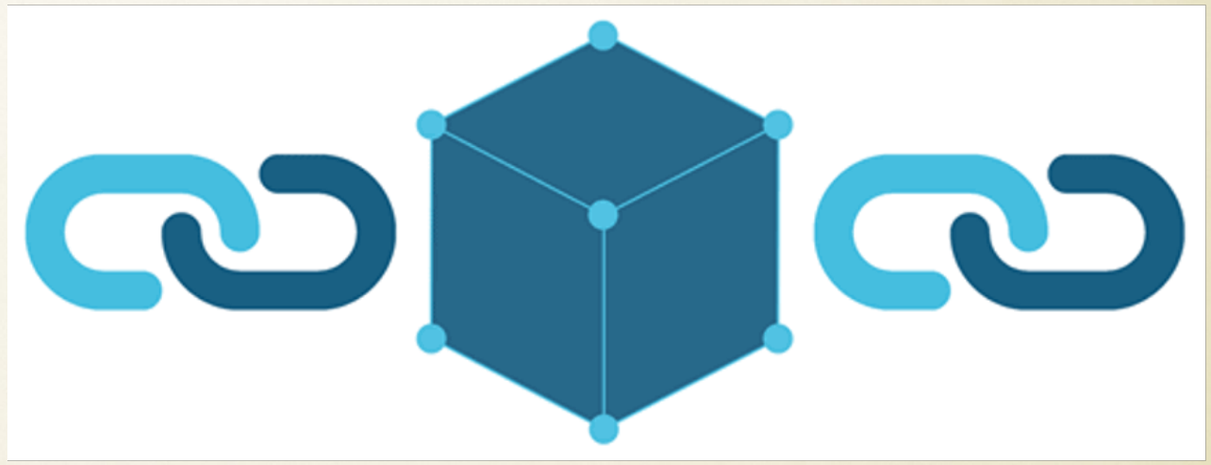


THERE ARE SO MANY ANGLES TO COVER (1/2)

- brief history of money and how it lead to cryptocurrency
- roots of cryptocurrency and early attempts at digital currency
- what's blockchain all about?
- what's "the crypto in cryptocurrency?"
- how do cryptocurrency and blockchain really work?
- getting involved with cryptocurrency
- the different flavors of cryptocurrency
- crypto-economics and Fintech
- ICOs and all that hype
- cryptocurrency for social benefit
- what is the future of cryptocurrency?

THERE ARE SO MANY ANGLES TO COVER (2/2)

- blockchain is a totally independent topic
- different flavors of blockchain
- blockchain: from cryptocurrency to contracts to Web 3.0
- blockchain applications beyond cryptocurrency
- NFT-madness
- blockchain and the future



are you out of the bus,
in the bus,
or under the bus?

WHY SHOULD ANYONE CARE ABOUT CRYPTOCURRENCY IF YOU'RE NOT FINANCIALLY INVOLVED?

Because it's everywhere! - news, finance and culture

Colonial Pipeline paid 75 Bitcoin, or roughly $5 million, to hackers.

The shutdown of the Colonial Pipeline triggered a cascading crisis that led to a jump in gas prices and panic buying at gas pumps. Erik S Lesser/EPA, via Shutterstock

By Nicole Perlroth

May 13, 2021

Colonial Pipeline paid its extortionists roughly 75 Bitcoin, or nearly $5 million, to recover its stolen data, according to five people briefed on the transaction.

Form **1040** Department of the Treasury—Internal Revenue Service (99) **U.S. Individual Income Tax Return** **2020** OMB No. 1545-0074 IRS Use Only—Do not write or staple in this space.

Filing Status Check only one box. ☐ Single ☐ Married filing jointly ☐ Married filing separately (MFS) ☐ Head of household (HOH) ☐ Qualifying widow(er) (QW)

If you checked the MFS box, enter the name of your spouse. If you checked the HOH or QW box, enter the child's name if the qualifying person is a child but not your dependent ►

Your first name and middle initial	Last name	**Your social security number**
If joint return, spouse's first name and middle initial	Last name	**Spouse's social security number**
Home address (number and street). If you have a P.O. box, see instructions.	Apt. no.	**Presidential Election Campaign** Check here if you, or your spouse if filing jointly, want $3 to go to this fund. Checking a box below will not change your tax or refund. ☐ You ☐ Spouse
City, town, or post office. If you have a foreign address, also complete spaces below.	State / ZIP code	
Foreign country name / Foreign province/state/county / Foreign postal code		

At any time during 2020, did you receive, sell, send, exchange, or otherwise acquire any financial interest in any virtual currency? ☑ Yes ☐ No

AMC theaters will start accepting Bitcoin this year

The chain hopes meme stock buyers will turn into loyal customers.

J. Fingas
@jonfingas
August 10th, 2021

In this article: news, gear, currency, Apple Pay, internet, Google Pay, entertainment, theater, AMC, Bitcoin, movies, money, cryptocurrency

Noam Galai/Getty Images

Wondering what to do with your Bitcoin stash now that you can't buy a Tesla? It might be time to catch a big-screen flick. According to *CNN*, AMC has announced that it plans to accept Bitcoin as payment for tickets and snacks at

Forbes

EDITORS' PICK | Aug 11, 2021, 11:02am EDT | 2,158 views

10 Giant Crypto And Blockchain Rounds Single-Handedly Raised $3.9 Billion This Year

SEAHAWKS

Former Seattle Seahawk Russell Okung puts half of salary in Bitcoin, considered highest paid in the league now

FEB 22, 2021 / BY JONATHAN WARNER

Elon Musk
@elonmusk

Replying to @ChainLinkGod and @PeterMcCormack

Bitcoin is actually highly centralized, with supermajority controlled by handful of big mining (aka hashing) companies.

A single coal mine in Xinjiang flooded, almost killing miners, and Bitcoin hash rate dropped 35%. Sound "decentralized" to you?

fortune.com/2021/04/20/bit...

11:17 AM · May 16, 2021 · Twitter for iPhone

It’s real

Total cryptocurrency market capitalization, or the value of all cryptocurrencies in existence, peaked in May 2021 at about $2.4 trillion, up from around $200 billion in 2019. Even during the crypto bubble in 2018, the market only ever reached about $720 billion.

77 tokens are now worth at least $1 billion each, and 1,600 are worth at least $1 million.

Approximately twice the scale of Google, Apple and Amazon

“an issue that has been vexing us” (Sen. Pat Toomey)

MSNBC

The Senate's infrastructure cryptocurrency fight was just the beginning

The bipartisan infrastructure bill the Senate passed Tuesday will, among other things, help upgrade America’s water systems and highways. Oddly, though, in the days leading up to its passage, about the only provision in the bill people were arguing about didn’t involve roads or bridges. Instead, it had to do with, of all things, cryptocurrency.

The provision in question is supposed to help pay for the bill by raising $28 billion over 10 years from taxes on crypto transactions. But its more significant function will be to expand the government’s ability to trace and track crypto transactions and bring crypto more fully under the financial regulatory umbrella. In that sense, it’s a testament to cryptocurrency’s growing importance. But the fight over the bill shows something else, too: how tricky it’s going to be for the government to regulate a financial technology designed, in a lot of ways, to avoid regulation.

THE POINT WITH CHRIS CILLIZZA

It’s official: Cryptocurrency is infrastructure

Analysis by Lauren Dezenski, CNN
Published 6:30 PM EDT, Mon August 9, 2021

Shutterstock

(CNN) — Senate negotiators – not always known for their tech savvy – made a breakthrough Monday over regulations on online transactions known as cryptocurrency.

The breakthrough is significant for two reasons: 1) Negotiators were able to reach a bipartisan consensus. 2) It deals with a largely new industry, which uses blockchain technology for online transactions.

A lead negotiator, Sen. Pat Toomey, put it more bluntly on Monday, describing cryptocurrency as “an issue that has been vexing us.” Another lead negotiator, Sen. Cynthia Lummis, called it “such a new subject to so many people in the US Senate.”

The Senate’s average age is 64.3 years – older than the House’s 58.4 years, according to the Library of Congress. And among US investors over 50, 76% say they haven’t even heard of cryptocurrencies, according to a recent Gallup poll.

A last-minute cryptocurrency tax provision was tacked on to the $1.2 trillion bipartisan infrastructure bill last week, which complicated infrastructure negotiations as a bitter dispute emerged over proposed tax reporting requirements for cryptocurrency transactions. It also prompted a sharp public outcry over the item’s initial language. On Monday, Toomey and Lummis announced an amendment to the provision, negotiated with the Treasury Department, focused on regulating digital assets by requiring brokers to report their transactions.

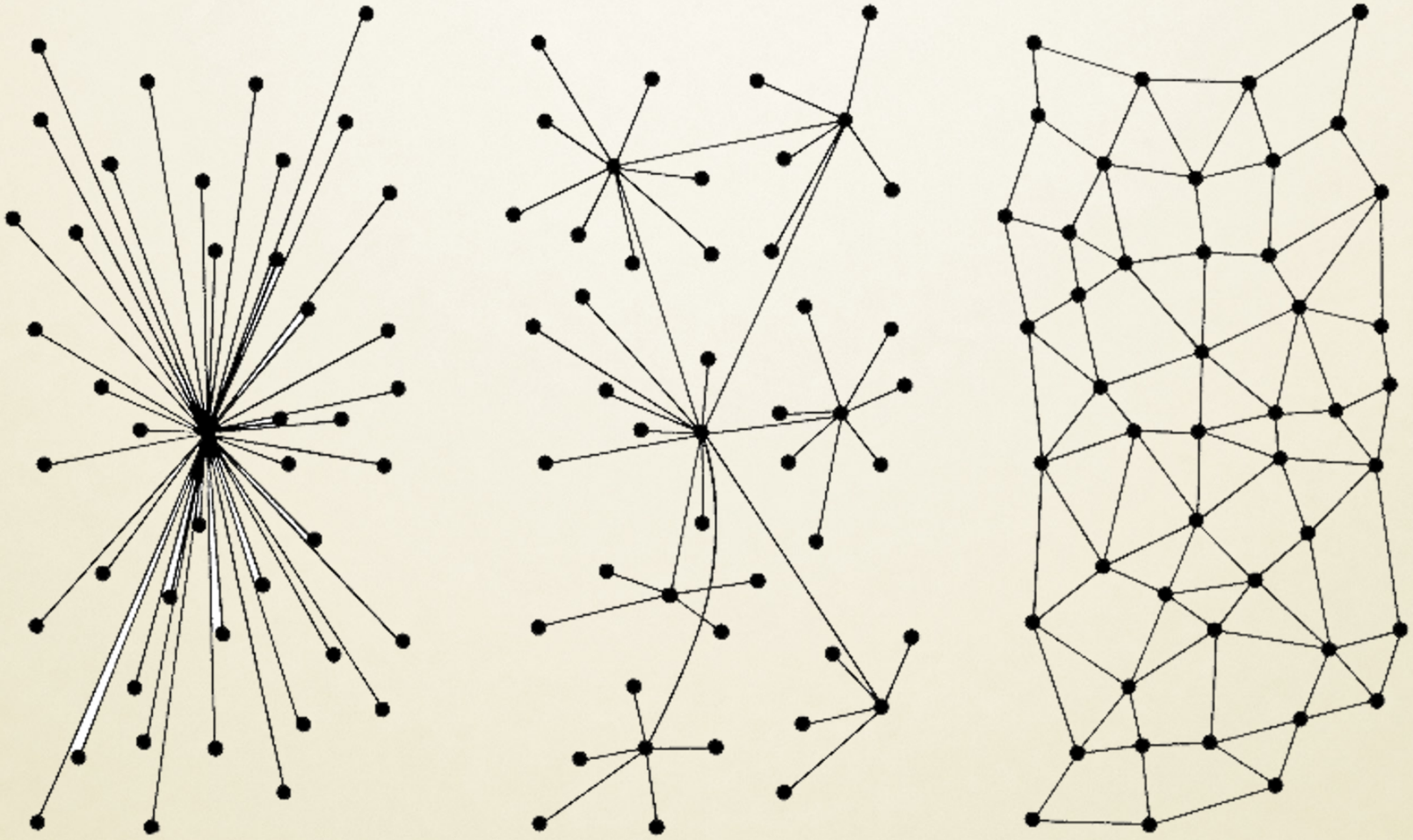
IT'S INTERESTING - CRYPTOCURRENCY IS A TALE OF MYSTERY, INTRIGUE, MONEY, MATH AND HOPE COMPLETE WITH

- unknown and mysterious characters
- the Internet (both visible and dark) and a networked society
- hackers, anarchists and cypherpunks
- wackjobs, conspiracy theorists, criminals, charlatans and gamblers
- extremist economists and libertarians
- "people who love money and trust mathematics and technology"
- idealistic academics and technologists
- venture capitalists and those with "start up dreams"
- the global financial system and its "wheelers and dealers"
- a media anxious for controversial/sensational headlines and stories
- a serious dream/attempt to create a new financial system with economic equality

FIRST - A FEW SIMPLE DEFINITIONS TO GET US STARTED (MORE DETAILS TO COME) (1/2)

- **cryptocurrency**
  - any form of currency (i.e., means of exchange or stored value) that exists only digitally (i.e., virtually - not based on gold, silver, etc.) and that typically has no central or regulating authority (e.g., a government, bank, etc.) but instead uses a **decentralized networked ledger** to record transactions and manage the issuance of new units and that relies upon **cryptography** to prevent counterfeiting and fraudulent transactions (e.g., lack of funds, nonrepudiation, double-spending, etc.)
  - cryptocurrency transactions should be **anonymous** - just like cash
  - limited **entries** in a shared, global ledger that no one can modify (except in extraordinary or impossible circumstances)
  - examples include bitcoin, litecoin, ether, dogecoin, ripple, etc., etc.

NETWORKS MAKE IT POSSIBLE

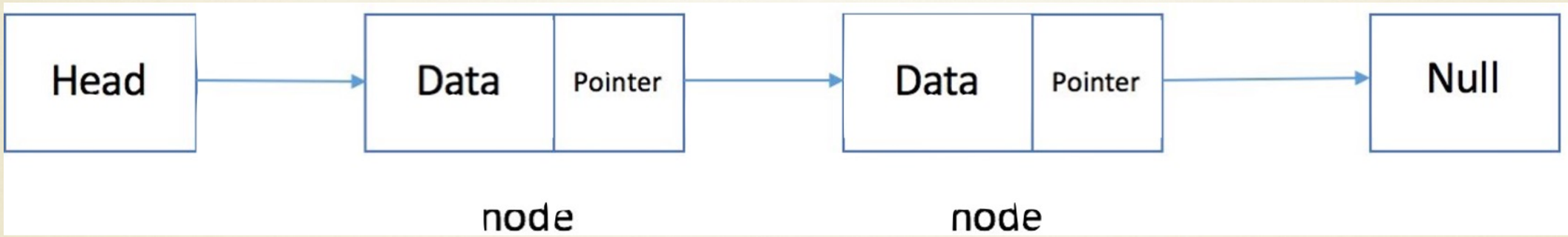


Examples (look for paths and points of possible failure)

FIRST - A FEW SIMPLE DEFINITIONS TO GET US STARTED (MORE DETAILS TO COME) (2/2)

- **blockchain**
  - a simple form of non-proprietary database: a loosely structured collection of information (e.g., a simple spreadsheet)
  - a digital ledger in which all actions are recorded chronologically/time-stamped, with lots of synchronized copies and publicly available to anyone
  - consider a typical ledger of credits and debits
  - a growing list of entries/nodes/**blocks** that are linked together
  - links between the blocks are cryptographically generated creating a persistent, tamper-proof path/list of relevant transactions
  - synonymous with the term distributed ledger technology (DLT) where synchronized copies of a ledger are shared across peer-to-peer (P2P) networks
  - independent of cryptocurrency

A VERY SIMPLE DATABASE (THOUGH NOT QUITE A BLOCKCHAIN)

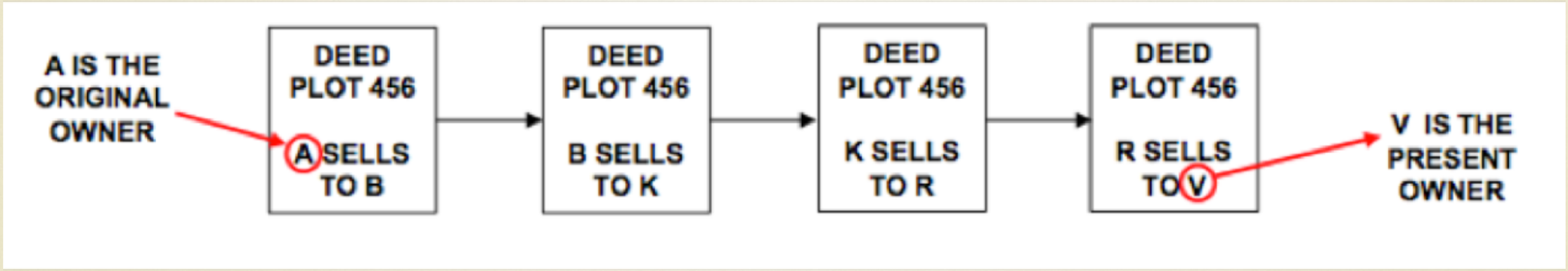


Many simple examples
e.g., your checkbook (links are dates),
probably little need to share
with others

SIMPLE ANALOGY: REAL ESTATE (1/3)

- real estate ownership is defined by a “chain of title” - a sequence of deeds leading from the original owner to the present owner
- deeds are recorded in a registry kept in some special place (e.g., the San Francisco City and County Office of the Assessor-Recorder)
- ownership is established by searching the registry
- ownership transfers (sales) are just entries at the end of the registry; the registry is a ledger
- if the registry is altered/destroyed (e.g., the 1906 earthquake) entries can be lost
- double-selling/ownership is prevented by timestamps

SIMPLE ANALOGY: REAL ESTATE (2/3)



SIMPLE ANALOGY: REAL ESTATE (3/3)

- suppose all deeds (and the ledger) were made available to thousands of nodes on a decentralized network?
- a cheater (or thief) would have to change all copies of a deed in order to make a false claim on the property
- **if** the deeds are genuine **and** the network members agree on the chain of title, **then** we can tell who owns a piece of property
- if there's a question, query the network and count the responses - if a majority says that someone is the owner, then they are - i.e., we can do operations on this ledger
- there must be enough honest members that false responses cannot dominate (or give them a reward for being honest)
- the registry is **not** (by definition) under a **centralized** control
- therefore, your deed should be **non-contestable** even if the assessor-recorder's office burns down or there is a revolution

THINK OF THIS DISTRIBUTED LEDGER/ BLOCKCHAIN AS A PLATFORM

- remember “query the network and count responses?”
- **platform** - a technology environment with protocols and rules upon which computer software applications operate
- the **Internet** is a platform; the Web, e-mail, mobile apps, etc. are applications that operate on that platform - that’s why the Internet and the Web are not the same thing
- example - **bitcoin** (small “b”) is the currency unit; **Bitcoin** (capital “B”) is the network protocol that makes it all work
- if blockchain is a platform, then cryptocurrencies are only specific applications that can “run” on it (much more later!)
- it is important to separate cryptocurrency from blockchain - don’t let your opinion on one affect your opinion on the other

"[cryptocurrency is] everything you don't understand about money combined with everything you don't understand about computers"

-John Oliver

"[We] can best interpret the different forms money takes - the money commodity, coins, convertible and inconvertible paper currencies, various credit moneys, etc. - as an outcome of the drive to <u>perfect</u> money as a <u>frictionless</u>, <u>costless</u> and instantaneously adjustable 'lubricant' of exchange while preserving the 'quality' of money as measure of value"

-David Harvey (CUNY) - **<u>anthropologist</u>**

IS CRYPTOCURRENCY/ BITCOIN REALLY MONEY?

Lloyd Blankfein
@lloydblankfein

Still thinking about #Bitcoin. No conclusion - not endorsing/rejecting. Know that folks also were skeptical when paper money displaced gold.

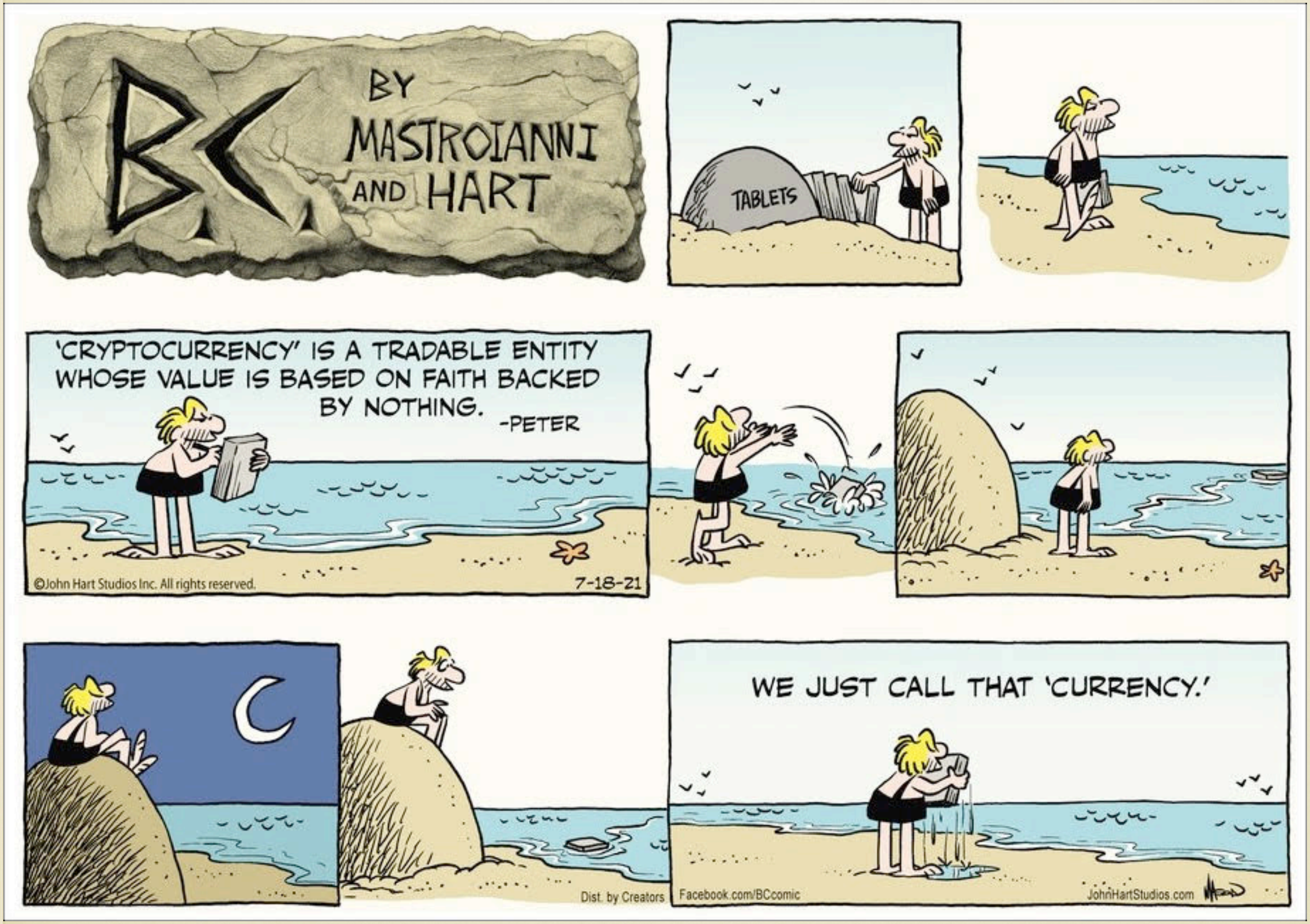
10:09 AM - Oct 3, 2017

6,656 4,226 people are talking about this

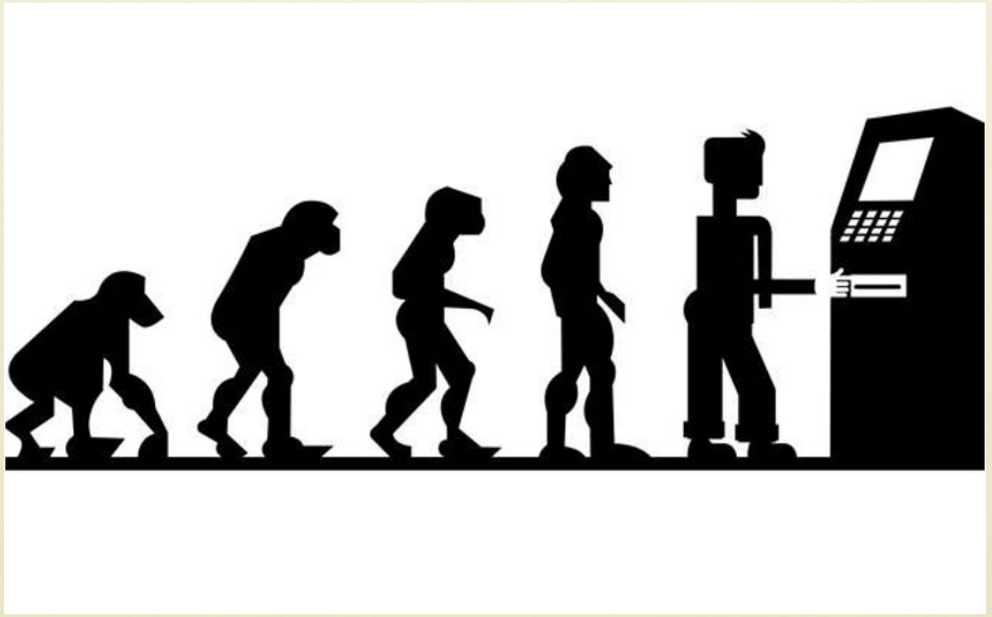
CEO
Goldman Sachs
2006-2018

Once the dollar was taken off the gold standard by the Nixon administration, the door was opened to allow all forms of electronic money. There is nothing physical backing up banknotes, so they are not needed any more. The banknote becomes an entry, a number, on a ledger or spreadsheet on a computer. So when money is wired or transferred anywhere in the world, the amount is simply deducted from one ledger and added to another ledger. Nothing changes hands, nothing physical is moved.

In today's world, with the ease and low cost of transfers, there is simply no legitimate reason for a person to have large amounts of cash. That's why the fed did away with large bills, there were only going to be used for illegal transactions. The Fed is more likely to do away with $50's and $100''s, than to bring back the $500 or $1000 bill. Big bills, or really all banknotes have become obsolete.


BC
BY MASTROIANNI AND HART
TABLETS
'CRYPTOCURRENCY' IS A TRADABLE ENTITY WHOSE VALUE IS BASED ON FAITH BACKED BY NOTHING.
-PETER
©John Hart Studios Inc. All rights reserved.
7-18-21
WE JUST CALL THAT 'CURRENCY.'
Dist. by Creators
Facebook.com/BCcomic
JohnHartStudios.com

A SIMPLE HISTORY OF MONEY - WHY AND HOW



WHAT IS MONEY? (1/3)

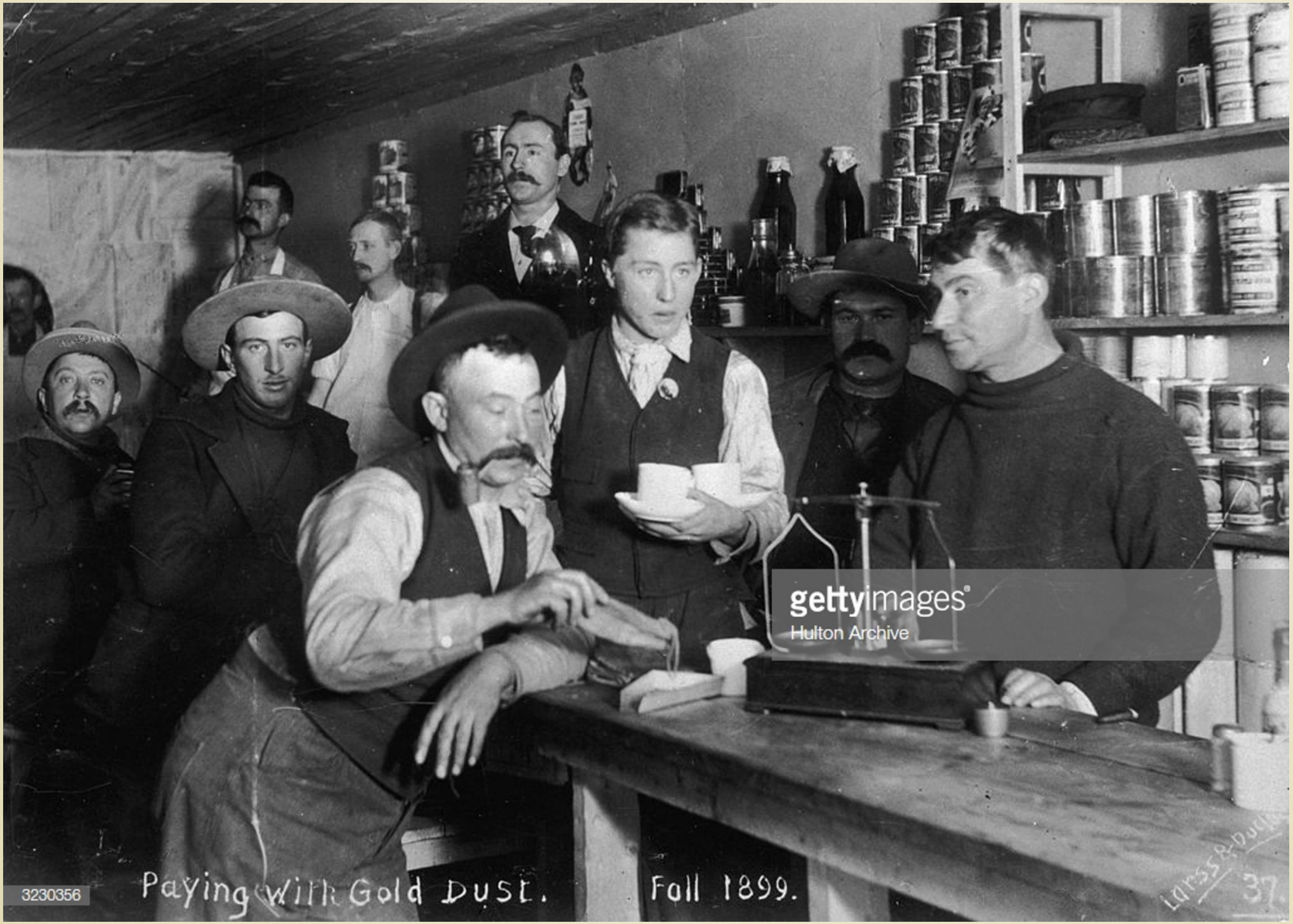
- a system of value so that people could compare items they wanted to exchange or services they wanted to negotiate
- a set of shared rules within a community for exchanging value
- as long as all parties in a community share and abide by the agreed rules, money can take on a rich and diverse range of characteristics
- rules are subject to change due to historical and social phenomena
- can also be a means of storing and accumulating wealth

WHAT IS MONEY? (2/3)

- allows strangers to transact without the need to trust each other - they trust currency (or whatever) instead (remember this one!)

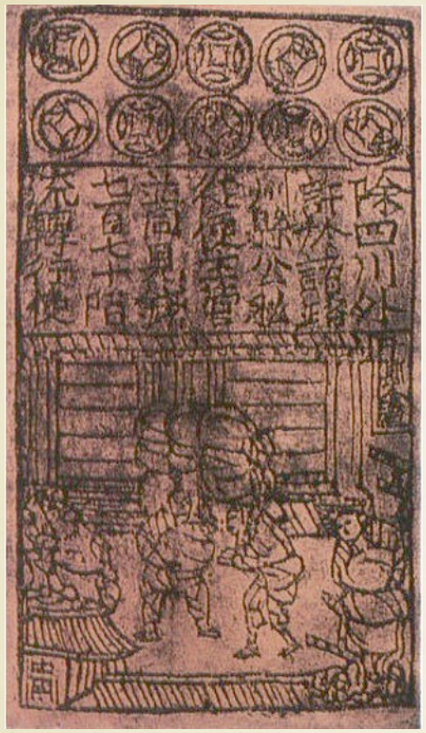
- this trust was easy when the currency had instrinsic value recognized by all communities (e.g., gold, silver) and/or value by scarcity (e.g., salt, food, shells) and could provide the basis for bartering: commodity money

- works well at the borders or fringes of these communities (or societies)

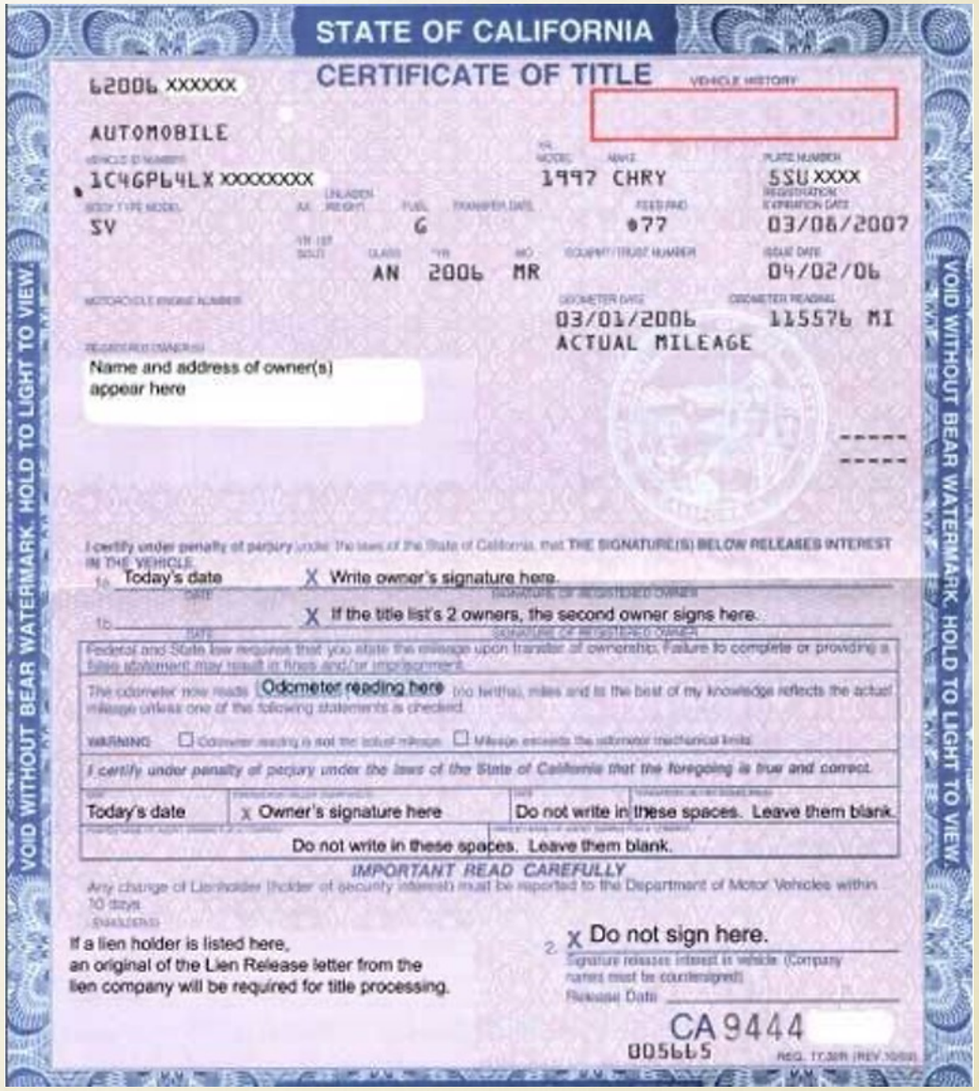

Paying With Gold Dust.
Fall 1899.
3230356
gettyimages
Hulton Archive

REPRESENTATIVE MONEY

- represents something of value, but has no intrinsic value of its own (e.g., paper)
- not necessarily paper money…yet
- a claim on a commodity ("commodity-backed value")
- has a face value greater than its value as a material substance




PITTSBURG


STATE OF CALIFORNIA
CERTIFICATE OF TITLE
VEHICLE HISTORY
62006 XXXXXX
AUTOMOBILE
1C4GP64LX XXXXXXX
1997 CHRY
5SU XXXX
SV
G
077
03/08/2007
AN 2006 MR
04/02/06
03/01/2006
ACTUAL MILEAGE
115576 MI
Name and address of owner(s) appear here
I certify under penalty of perjury under the laws of the State of California, that THE SIGNATURE(S) BELOW RELEASES INTEREST IN THE VEHICLE.
1a. Today's date
X Write owner's signature here.
1b.
X If the title list's 2 owners, the second owner signs here.
Federal and State law requires that you state the mileage upon transfer of ownership. Failure to complete or providing a false statement may result in fines and/or imprisonment.
The odometer now reads Odometer reading here (no tenths) miles and to the best of my knowledge reflects the actual mileage unless one of the following statements is checked.
WARNING
I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.
Today's date
X Owner's signature here
Do not write in these spaces. Leave them blank.
Do not write in these spaces. Leave them blank.
IMPORTANT READ CAREFULLY
Any change of Lienholder (holder of security interest) must be reported to the Department of Motor Vehicles within 10 days
If a lien holder is listed here, an original of the Lien Release letter from the lien company will be required for title processing.
2. X Do not sign here.
Signature releases interest in vehicle (Company names must be countersigned)
Release Date
CA 9444
005665
VOID WITHOUT BEAR WATERMARK. HOLD TO LIGHT TO VIEW.


Recorder's File No.
H 10824
GRANT DEED
Fee $
PAGES

GOVERNMENTS GET INVOLVED

- perhaps the easiest commodity to deal with is precious metals (scarcity)
- consistency required for receiving taxes, tributes, etc. - you can't easily pay taxes with pigs…
- government identity (vanity, nationalism…)

- portability
- control over population, trade, accumulation of wealth
- regulation of supply, value, banks, exchange rates, etc. (centralization)
- definition of units of commodity
- dealing with problems (e.g., counterfeiting)

"Coins appear to have originated as government 'pay tokens' as nothing more than evidence of debt"

-L.Randall Wray

"It appears that many early Lydian coins were minted by merchants as tokens to be used in trade transactions. The Lydian state also minted coins""

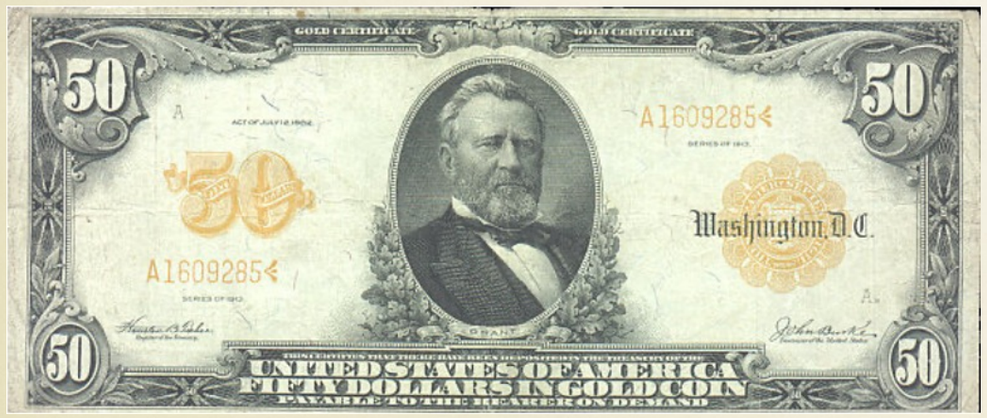
-Ancient History Encyclopedia

"...coinage seems to be invented or at least widely popularized to pay soldiers - more or less simultaneously in China, India, and the Mediterranean, where governments find the easiest way to provision the troops is to issue them standard issue bits of gold and silver and then demand everyone else in the kingdom give them one of those coins back again"

-David Graeber, "Debt: The First 5000 Years"

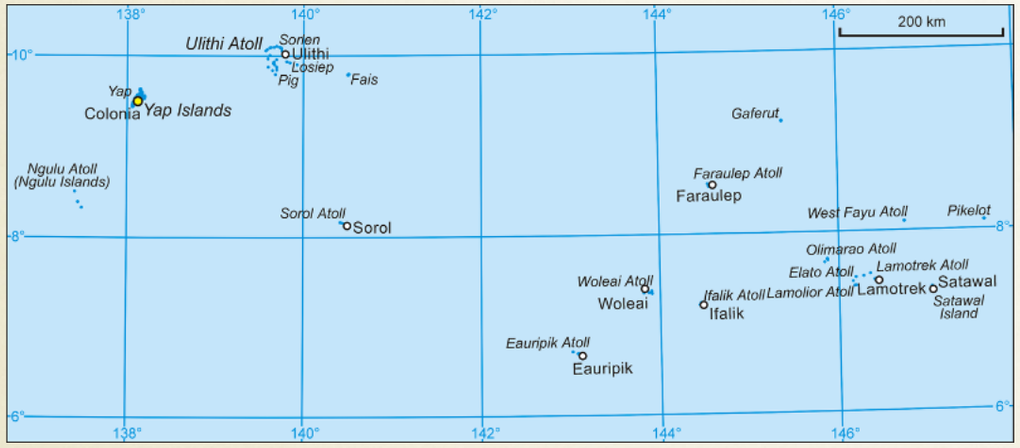
THERE ARE ISSUES

- loss of control over precious metal supply
- portability
- is the money valuable because of its material value or because the government says that it is?
- fraud (e.g., "coin shaving")
- inflation? (fluctuations in precious metal value?)
- maybe time to re-consider representative money?
- how about a piece of paper that could be redeemed/converted for commodity-based money on demand?



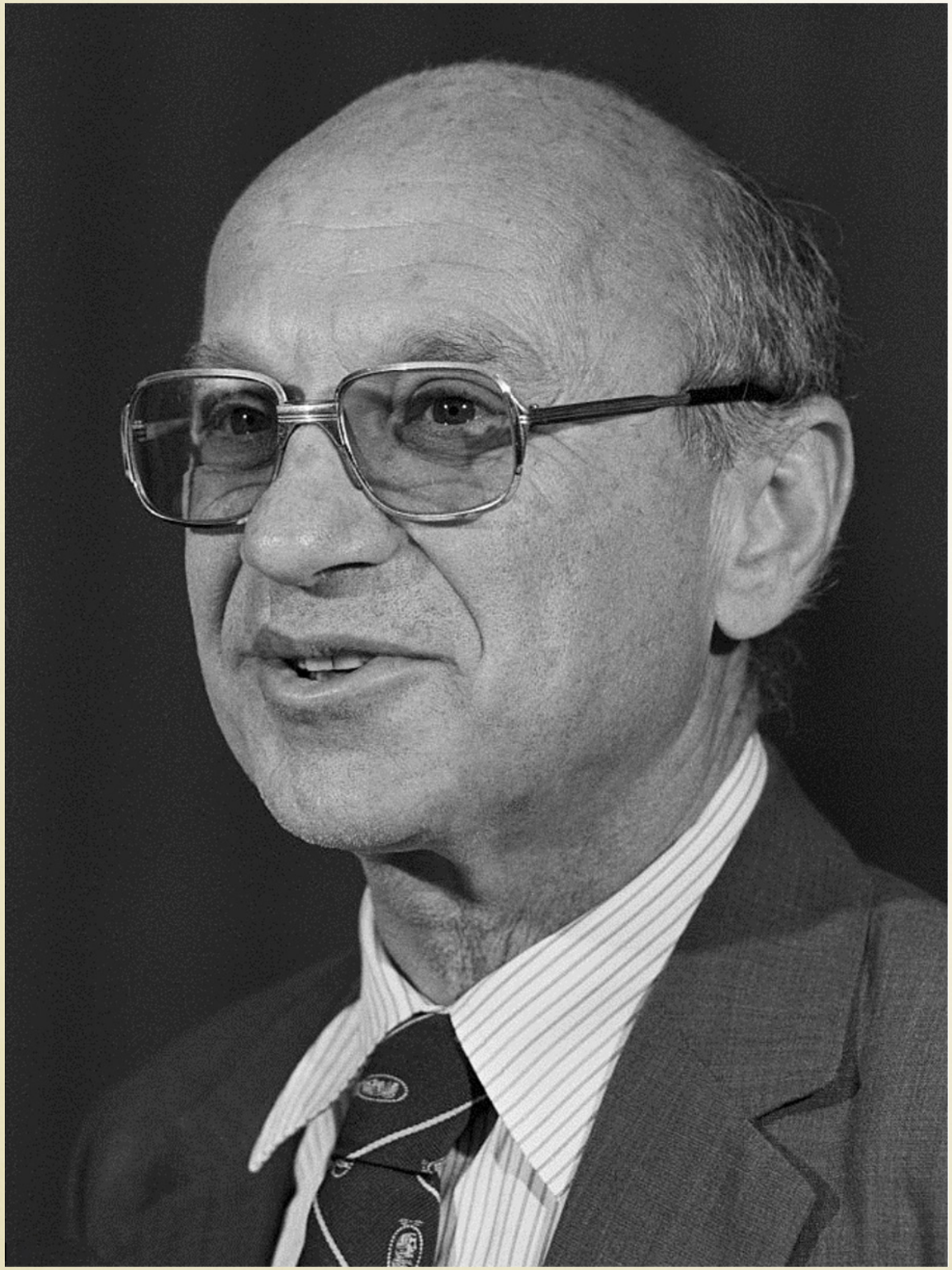
Representative/paper money that is issued by a government and is commodity-based is conceptually the same as bartering but has been made simpler and more convenient; no one doubts its legitimacy as money

LET'S TAKE AN UNEXPECTED EXCURSION TO THE ISLAND OF YAP



THE ISLAND OF STONE MONEY

- the largest (by size) currency in the world (the rai)
- Yap has no reserves of metals to serve as a commodity
- has fascinated economists since it demonstrates how the Yap society took money from the tangible to the abstract
- perception of ownership is more important that physical ownership (which for the rai is impractical)
- bookkeeping and management comes from "the crowd" (i.e., is decentralized)



From The Collected Works of Milton Friedman, compiled and edited by Robert Leeson and Charles G. Palm.

"The Island Of Stone Money"
by Milton Friedman
Working Papers in Economics, no. E-91-3. Stanford, California: Hoover Institution, 1991.

Abstract

Large stones quarried and shaped on a distant island were used as, money on the Island of Yap. After Germany acquired the island at the turn of the century, its officials had difficulty inducing the residents to repair the footpaths until they resorted to the desperate expedient of taking possession of many of the stones by marking them with a cross in black paint, to be removed when the paths were repaired. The apparently meaningless measure had real results. That was equally true of an eerily similar event that occurred in 1932 when the New York Federal Reserve Bank transferred gold to the Bank of France by earmarking gold in its vaults.

The Island Of Stone Money

From 1899 to 1919 the Caroline Islands, in Micronesia, were a German colony. The most westerly of the group is the Island of Uap or Yap, which at the time had a population of five to six thousand.

THE RAI-BASED ECONOMY

- acquisition: Yap residents traveled to nearby islands where limestone was mined and carved; at home they described each rai's history so all could establish its worth
- storage: by displaying rai in public places the community could verify its quality and features
- exchange: after verification and placement in a public space, rai could be exchanged for various (major) goods and services
- auditability: oral transaction histories for each rai were available to all community members over generations (e.g., "the sunken rai")

Are rai money? What kind of money? Could this model be used elsewhere?

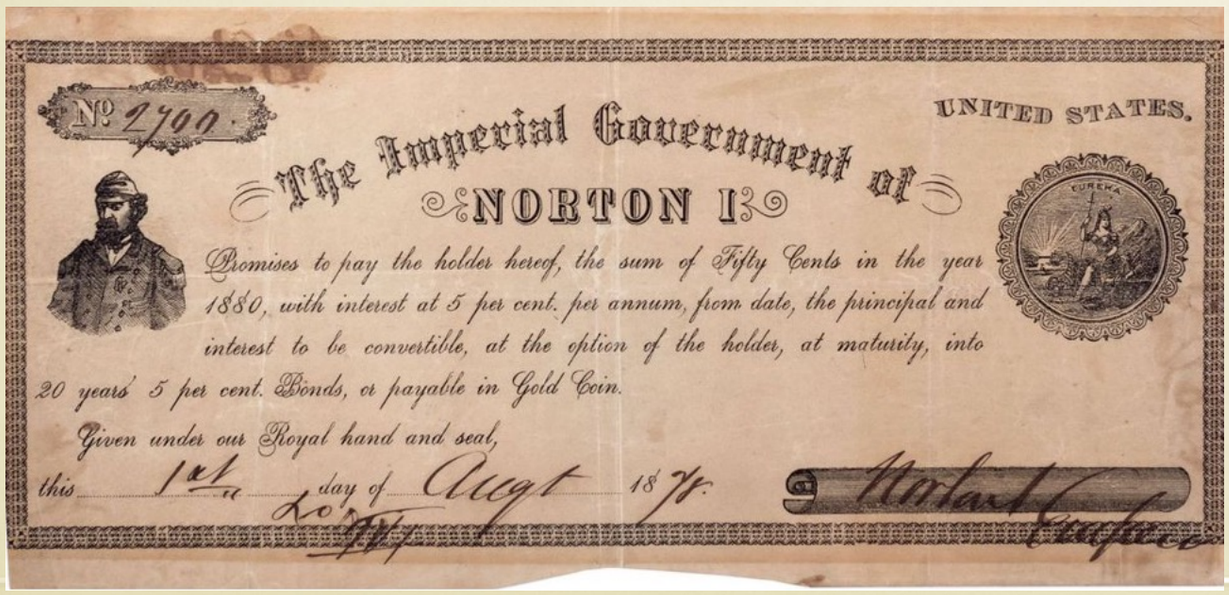
BACK TO HISTORY - FIAT CURRENCY

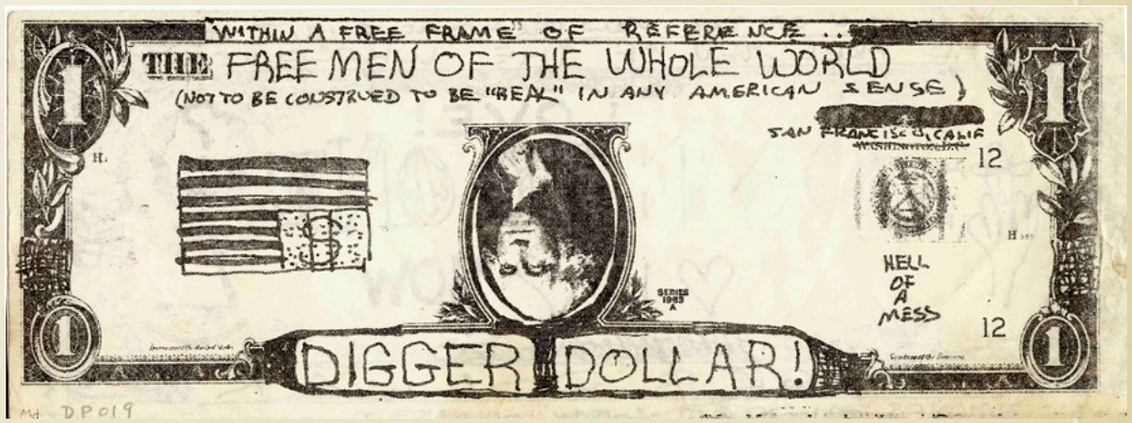
- fiat: "let it be done"
- currency without intrinsic value (except maybe the paper)
- has value only because a government or bank decrees so; maintains its value because parties engaging in exchange agree on a value
- requires user trust in government or issuer e.g., when the U.S. went off the gold standard in 1971
- the global economy appears to have converged on fiat currency systems (especially the $US)


FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
C 38028901 B
WASHINGTON, D.C.
SERIES 2009
ONE DOLLAR
C 38028901 B
CollecTons
STOCK PHOTO


20
The Hongkong and Shanghai Banking Corporation Limited
香港上海滙豐銀行有限公司
Promises to pay the bearer on demand
at its office here
港幣貳拾元
TWENTY
HONG KONG DOLLARS
20
HSBC
ND221436
ND 221436
Chief Executive
Hong Kong 1 January 2014


100000000000000000000 RESERVE BANK OF ZIMBABWEE 100000000000000000000
I promise to pay
the bearer on demand
ONE HUNDRED
QUINTILLION
DOLLARS
for the Reserve Bank of Zimbabwee
Dr G. Gono
100000000000000000000 HARARE 2008
AZ0000113


№ 2700
UNITED STATES.
The Imperial Gouvernment of
NORTON I
Promises to pay the holder hereof, the sum of Fifty Cents in the year 1880, with interest at 5 per cent. per annum, from date, the principal and interest to be convertible, at the option of the holder, at maturity, into 20 years' 5 per cent. Bonds, or payable in Gold Coin.
Given under our Royal hand and seal,
this 1st day of Augt 18 77.


WITHIN A FREE FRAME OF REFERENCE ..
THE FREE MEN OF THE WHOLE WORLD
(NOT TO BE CONSTRUED TO BE "REAL" IN ANY AMERICAN SENSE)
SAN FRANCISCO, CALIF.
HELL OF A MESS
DIGGER DOLLAR!
MH DP019

MICROPAYMENTS

- what happens when a payment amount is less han the minimum unit of fiat currency?
- why is this even a relevant question? aren't units arbitrary?
- "almost free" concept (e.g., online intellectual property, marketing ploys)

1 mill = "lowest money of account, of which 1000 shall be equal to the federal dollar"
- Continental Congress, 1786

WHAT IS MONEY? (3/3)

- summary of characteristics (according to multiple economists)
  - a market-born institution
  - tool of exchange and saving
  - material commodity
  - divisible into units
  - imperishable (?) - what about your old francs from the France trip?
  - rare/scarce
  - homogeneous
  - easily stored
  - not subject to wide fluctuations in value (?)
  - always in demand among those you trade with (?) (only if usable)
- why do we say things like “time is money” or “data is the new currency?”

"I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something they can't stop"

-Friedrich Hayek, Nobel Prize Economics, 1974

SO, IS CRYPTOCURRENCY/ BITCOIN MONEY?

- if so, what kind?
- what characteristics of money apply?
- who is its community?
- what is its connection with fiat? or is it fiat since its community "decrees" it?
- how did it evolve?
- is it truly a <u>new form</u> of money?

Traits of Money	Gold	Fiat (US Dollar)	Crypto (Bitcoin)
Fungible *(Interchangeable)*	High	High	High
Non-Consumable	High	High	High
Portability	Moderate	High	High
Durable	High	Moderate	High
Highly Divisible	Moderate	Moderate	High
Secure *(Cannot be counterfeited)*	Moderate	Moderate	High
Easily Transactable	Low	High	High
Scarce *(Predictable Supply)*	Moderate	Low	High
Sovereign *(Government Issued)*	Low	High	Low
Decentralized	Low	Low	High
Smart *(Programmable)*	Low	Low	High

Investopedia

ELON MUSK - JANUARY 2020

"This sort of gets the crypto people angry, but there are transactions that are not within the balance of the law. And there are, obviously, many laws in different countries. And, normally, cash is used for these transactions. But, in order for illegal transactions to occur, cash must also be used for legal transactions. You need an illegal to legal bridge. That's where crypto comes in."

"Cash, these days, is used much rarer. It's increasingly difficult to use cash. Some places, you can't use cash at all. So, there's a forcing function for transactions that are illegal, quasi-legal, and in some cases legal. But it's got to have both legal and illegal...

So where I see crypto as, respectively, is a replacement for cash. But I do not see crypto being the primary database."

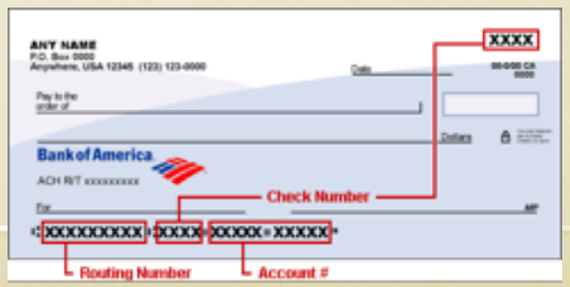

IRISH WHISKEY
TRIPLE DISTILLED
IRISH WHISKEY
I BELIEVE IN
HONEST MONEY
GOLD, SILVER, AND BITCOIN

PAYMENT SYSTEMS

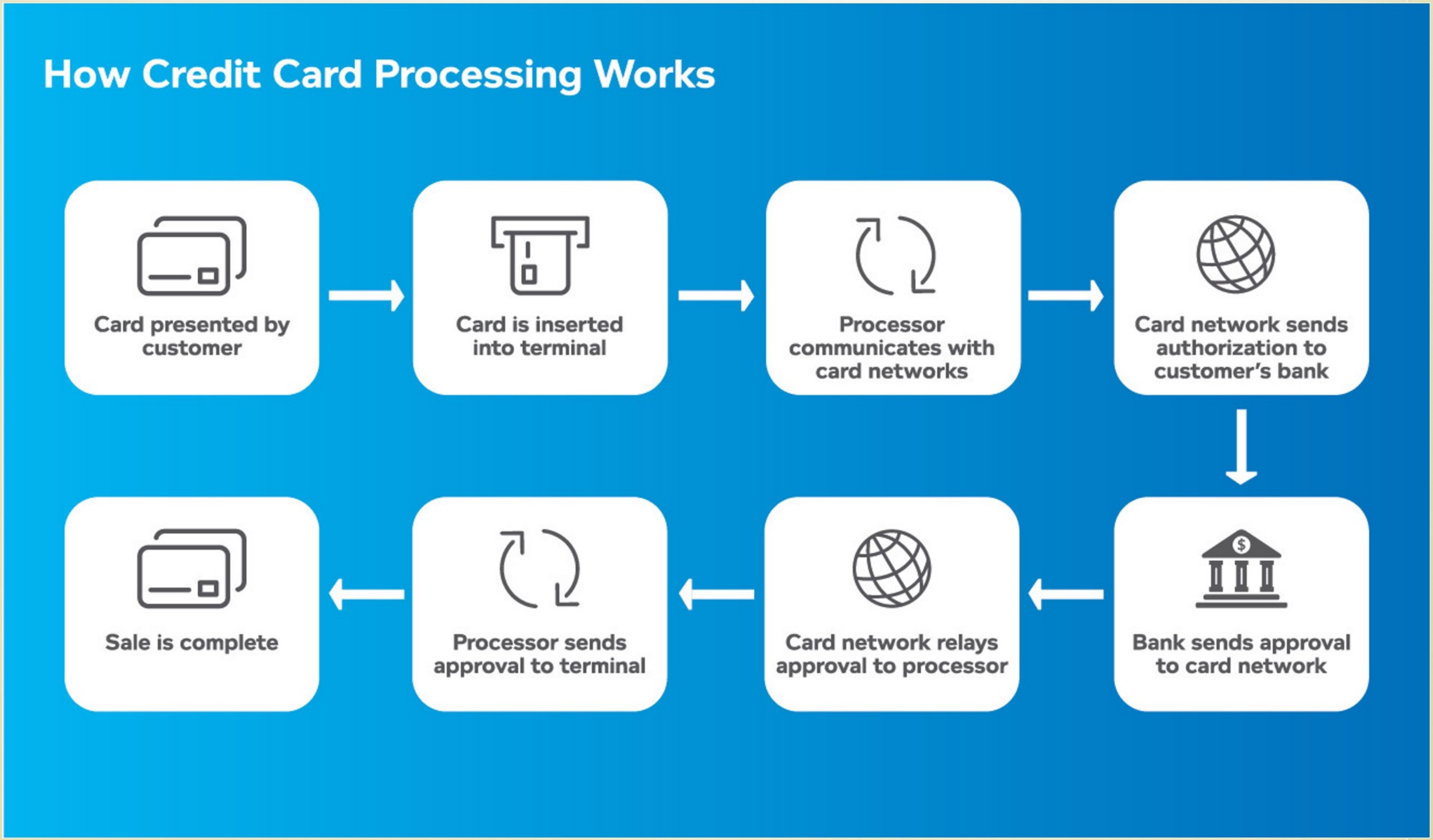
- follows from a description of money
- any system used to settle financial transactions through the transfer of monetary value and includes the institutions, instruments, people, rules, procedures, standards and technologies that make such an exchange possible
- systems that use fiat currencies but do not require in-person cash transactions

SOME FAMILIAR PAYMENT SYSTEMS

- stored value (smart) cards - e.g., Clipper, gift cards - operate like cash(?)
- debit cards, credit cards - require a path of validation
- checks - requires a path of validation - “notational money”
- money orders/wire transfers - path of validation, transaction fees
- online money transfers - e.g., PayPal, Venmo - requires path of validation



what “path of validation” means



PAYMENTS IN A DIGITAL/ NETWORKED WORLD

- one of the "killer apps" (IMHO) of WWW was e-commerce
- the community that wants to exchange value is the whole world
- exchange of value between parties who don't know one another, maybe don't trust one another and can't meet face-to-face - who sets the conditions?
- how does this align with fiat currencies and existing payment systems?
- the first "solution" was/is to "fit" existing currencies and payment systems to the digital/cyber community- e.g., credit cards
- later came systems like PayPal, but underneath they were just variations of the old payment systems…

TYPICAL CONCERNS ABOUT DIGITAL PAYMENTS

- security and privacy - e.g., credit card info protection, personal info protection, lack of anonymity, personal shopping history tracking, etc.
- what's this stuff about "https," digital certificates, SSL, etc.?
- consumer protection - "where's my stuff?" - non-repudiation
- fiat currency conversion, transaction fees
- etc., etc.

DEVELOPMENT OF A NATIVE DIGITAL PAYMENT SYSTEM BECAME A TECHNOLOGICAL "HOLY GRAIL"

"The one thing that's missing, but will soon be developed, is a reliable e-cash, a method whereby on the Internet, you can transfer funds from A to B, without A knowing B, or B knowing A"

—Milton Friedman, Nobel Prize Economics, 1976

THE CHALLENGES WERE/ARE

- trust
- anonymity
- de-centralization
- the “double spending” problem
- non-repudiation
- convertability to/from fiat currency
- adoption - not just a crazy computer science exercise

EARLY ATTEMPTS AT E-CASH

- eCash, DigiCash - 1982/1990 - David Chaum - required a third party
- Hashcash - 1997 - Adam Back - not really anonymous or de-centralized; difficult to set up
- Bit Gold - 1998 - Nick Szabo - difficulties with trust model; never implemented
- B-money - 1998 - Wei Dai - faced network constraints

THE CYPHERPUNK MOVEMENT

- consists of activists who advocate the use of strong cryptography and privacy-enhancing technologies as a route to social and political change - includes many of those individuals who investigated e-cash
- "privacy is necessary for an open society in the electronic age…we cannot expect governments, corporations, or other large, faceless organizations to grant us privacy…we must defend our own privacy if we expect to have any…cypherpunks write code. We know that someone has to write software to defend privacy, and…we're going to write it." - *A Cypherpunk's Manifesto*, Eric Hughes, 1993
- original communication mechanism was through the cypherpunk electronic mailing list (1992)

31 October 2008

- in the middle of one of the worst financial crises in history
- a paper was posted to the cypherpunk mailing list entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*
- the paper claimed to offer an alternative to the traditional banking system
- it was not posted through typical academic channels ★
- it laid out the fundamentals of Bitcoin, bitcoin, and blockchain
- the author was listed as ***Satoshi Nakamoto***
- Satoshi had communicated with some of the cypherpunks previously but no one knew who he/she/they were

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

https://bitcoin.org/bitcoin.pdf

"The root problem with conventional currency is all the <u>trust</u> that's required to make it work. The central bank must be trusted not to <u>debase</u> the currency, but the history of fiat currencies is full of <u>breaches</u> of that trust. Banks must be trusted to hold our money and transfer it <u>electronically</u>, but they lend it out in waves of credit bubbles with barely a fraction in reserve.

-Satoshi Nakamoto - **cypherpunk**

remember the Apple Computer promotion?

3 January 2009

- the first ever cryptocurrency was officially launched
- known as “the Genesis block” - the first transaction/block on the Bitcoin blockchain
- Satoshi makes a statement:

RAW HEX VERSION

BITCOIN GENESIS BLOCK

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

THE TIMES SUBSCRIBE

Chancellor Alistair Darling on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott, Deputy Political Editor, and Gary Duncan, Economics Editor

January 3 2009, 12:00am, The Times

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up “toxic assets”, *The Times* has learnt.

SATOSHI'S DREAM

- "The network is robust in its unstructured simplicity. Nodes work all at once with little coordination."
- a distributed, peer-to-peer network of payments ledgers (non-centralized)
  - impossible (?) to forge/modify - based on rigorous/proven mathematical and cryptographic technologies and techniques
  - doesn't allow double-spending and provides proof-of-payment (non-repudiation)
  - supported by "the power of the crowd"
- not based on dollars, euros, pounds, etc. (fiat currencies), but a currency "for the digital age" - bank-free, government-free, individual empowering

"Bitcoin adoption could multiply the more people become aware of how much of their wealth is controlled by governments and the big banks"

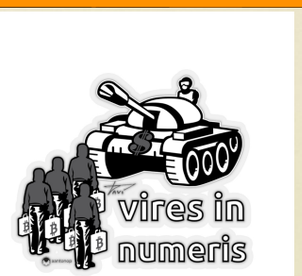
-Frank Holmes, CEO, US Global Investors

"Bitcoin for me is not an instrument for financial investment. Bitcoin for me is a declaration of our monetary independence."

-Nick Spanos, founder, NYC Bitcoin Center

WHY WERE THE CYPHERPUNKS ATTRACTED TO BITCOIN?

- loss of trust in banks and financial institutions as third parties?
- bad investment decisions by banks and financial institutions?
- techies had become a financial force and sought better solutions in technology?
- politics?
- anarchy and greed?
- how did it move beyond the cypherpunks?



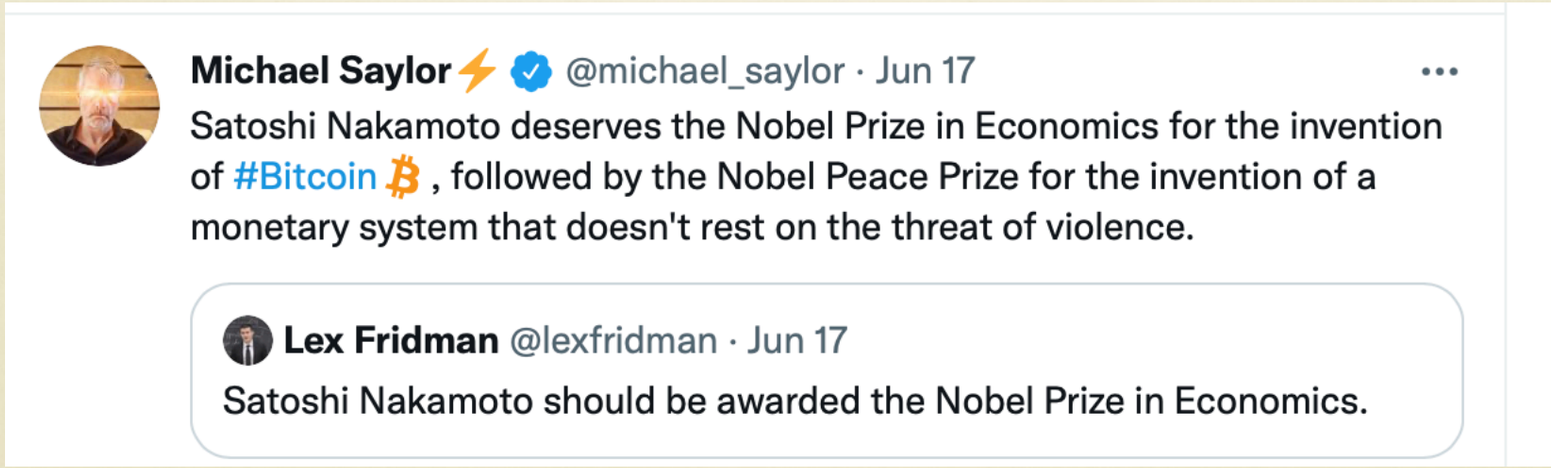
Satoshi Nakamoto should get the Nobel Prize in Economics: Charles Hoskinson

June 19, 2021 News

> **Charles Hoskinson believes that the founder of Bitcoin, Satoshi Nakamoto, deserves to get a Nobel Prize in Economics for transforming finance and data.**

> **In 2015, Nakamoto was proposed by an American senior academic but the Nobel team rejected the proposal simply because Nakamoto is anonymous.**

The cryptocurrency market is today worth $1.57 trillion, with the number of cryptocurrencies in its thousands and steadily growing. Blockchain technology has become an industry of its own as well, with every other sector applying it in one way or another. All this is down to one man – Satoshi Nakamoto, the man (or woman, or group of people, or even a robot from the future) who gave us Bitcoin. And according to Charles Hoskinson, Satoshi deserves a Nobel Prize in Economics for his contribution to humanity.



Questions? Comments?

bebo.white@gmail.com