

Currency and Digital Cash: History & New Trends

Behrooz Parhami

University of California, Santa Barbara

About This Presentation

This slide show was first developed in July 2021 for presentation at a meeting of the 1968 Graduates of the College of Engineering, Tehran University. ©2021 Behrooz Parhami

In loving memory of my late Fanni classmate
Hamid Khan-Afshar



Edition	Released	Revised	Revised	Revised
First	July 2021			

File: http://www.ece.ucsb.edu/~parhami/pres_folder/parh21-general-talk-currency-digital-cash.pdf

Currency and Digital Cash: History & New Trends

The discussion of money and its underpinnings is a lot deeper than most people realize. In this talk, I will review the history of this made-up thing that makes the world go around, from its earliest forms in human pre-history up to and including cryptocurrencies that are poised to dominate the 21st century.

In the beginning, humans bartered, exchanging a chicken for some wheat, say. Bartering is feasible only if the needs of the two parties engaged in it coincide in time and space. Money is a collection of agreed-upon valuable tokens that everyone recognizes and honors as an intermediary between exchanged goods.

A fundamental requirement for money to work is trust: Assurance that the gold coins of yore were actually worth the advertised amount or that today's physically worthless paper or digital money will actually buy you something when needed. Most often, trust is provided by guarantees from a powerful authority.

In late 20th century, use of paper money was gradually replaced by electronic transactions via debit cards, credit cards, electronic fund transfers, and so on, even though some groups, including criminals, still preferred paper money.

Digital currency does away with paper money altogether. The money you own is represented by digital codes stored on computers. In this new realm, assuring trust becomes even more challenging, leading to solutions such as blockchain.

Bartering: Pros and Cons

Direct, less prone to manipulation
No special arrangements needed
No trusted authority needed
Flexible “pricing” based on needs
Immune from hyper-inflation



Needs must coincide in time & space
Some goods are indivisible
Disease transmission: Solutions in Africa
Vastly different values: car v. apples
Does not allow one to store wealth

From Cattle to Leather Money (BCE)

PBS Nova:
History of Money

9000-6000 BCE:
Cattle

1200 BCE:
Cowrie shells

1000 BCE:
First coins

500 BCE:
Modern coins

118 BCE:
Leather money



From Nose to Paper Bills (CE)

PBS Nova: History of Money

800-900 CE:

The nose

806 CE:

Paper money

1535 CE:

Wampums

1816 CE:

Gold Standard

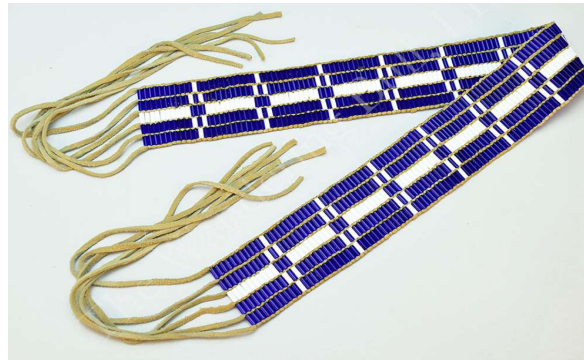
~1930 CE:

End of Gold Std.



“Paying
through
the nose”

Kublai
Khan



The Gold Standard: Direct & Indirect

A system that allows money to be freely convertible to gold

1789: US Constitution gives Congress authority to issue money

1792: Bimetallic Std., ratio 15:1 Gold/Silver

1821: England adopts Gold Std.

1871: Int'l Gold Standard; countries accumulated gold when they had trade surplus; lost gold with deficit
US holds 8000 tons of gold;
Current gold price: ~ \$1800/oz

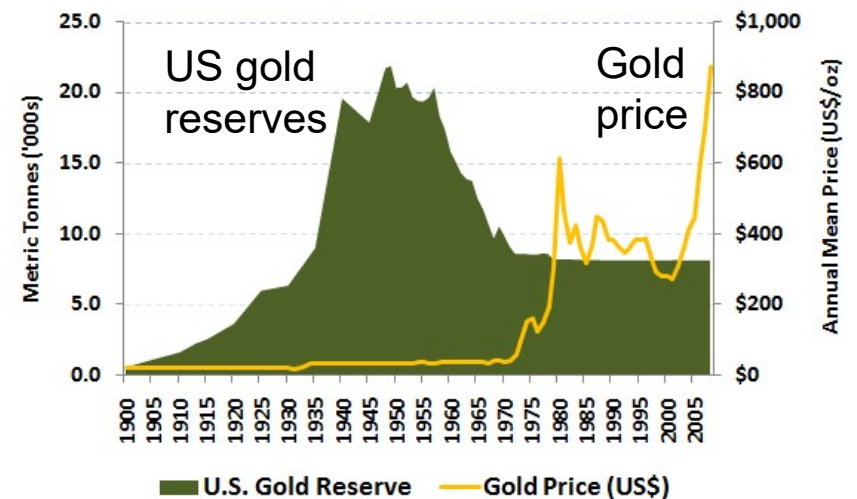
1931: Gold Std. was abolished

1933: US raises price \$20.67 → \$35

1971: US ends \$35/oz guarantee



Official U.S. Gold Reserves and Gold Price (1900 to 2008)



Sources: World Gold Council

www.DollarDaze.org

Money Is a Made-up Thing

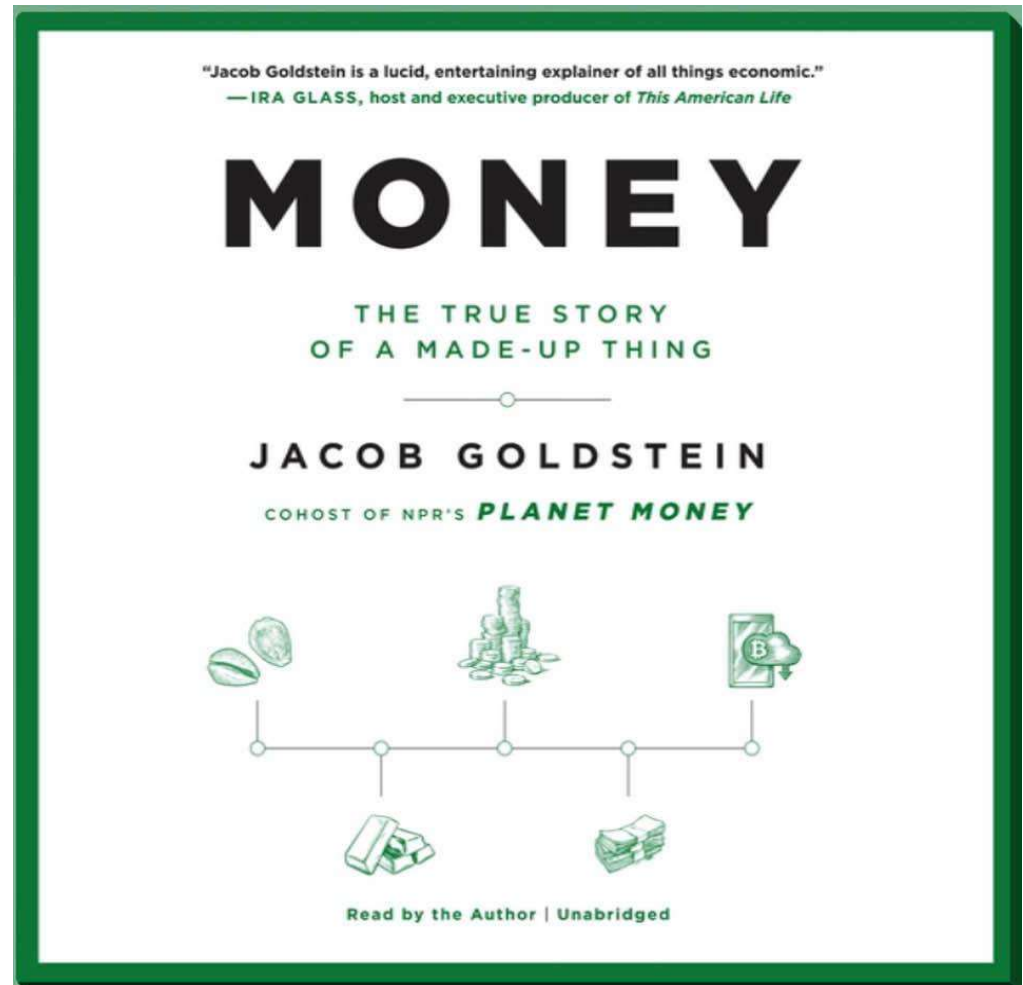
Anything that's accepted as a medium of exchange (e.g., Kent cigarettes in communist Romania)

Unit of account that allows comparing costs/values

Store of value

Commodity vs. fiat money (gold has intrinsic value, a piece of paper doesn't)

Money supply



Money Ultimately Results from Work

Direct work: Cultivating wheat, raising cattle, fishing, mining, teaching, treasure-hunting

Work of your ancestors: Inheritance

Work of those from whom you or your ancestors stole



Money Is Related to Ownership

Rules of ownership can be quite complicated

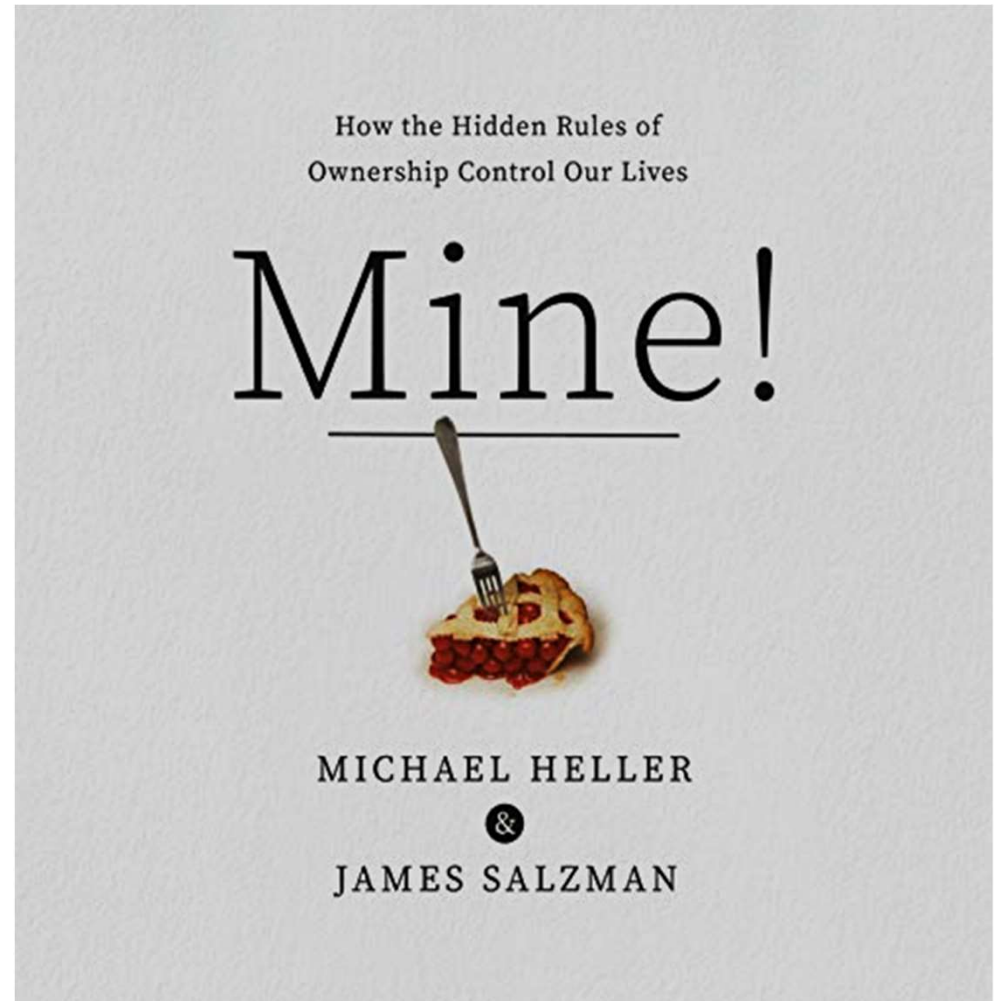
Some cases are easy:
You own a cow, you own the milk and the calves

Difficult cases are decided by negotiation or courts

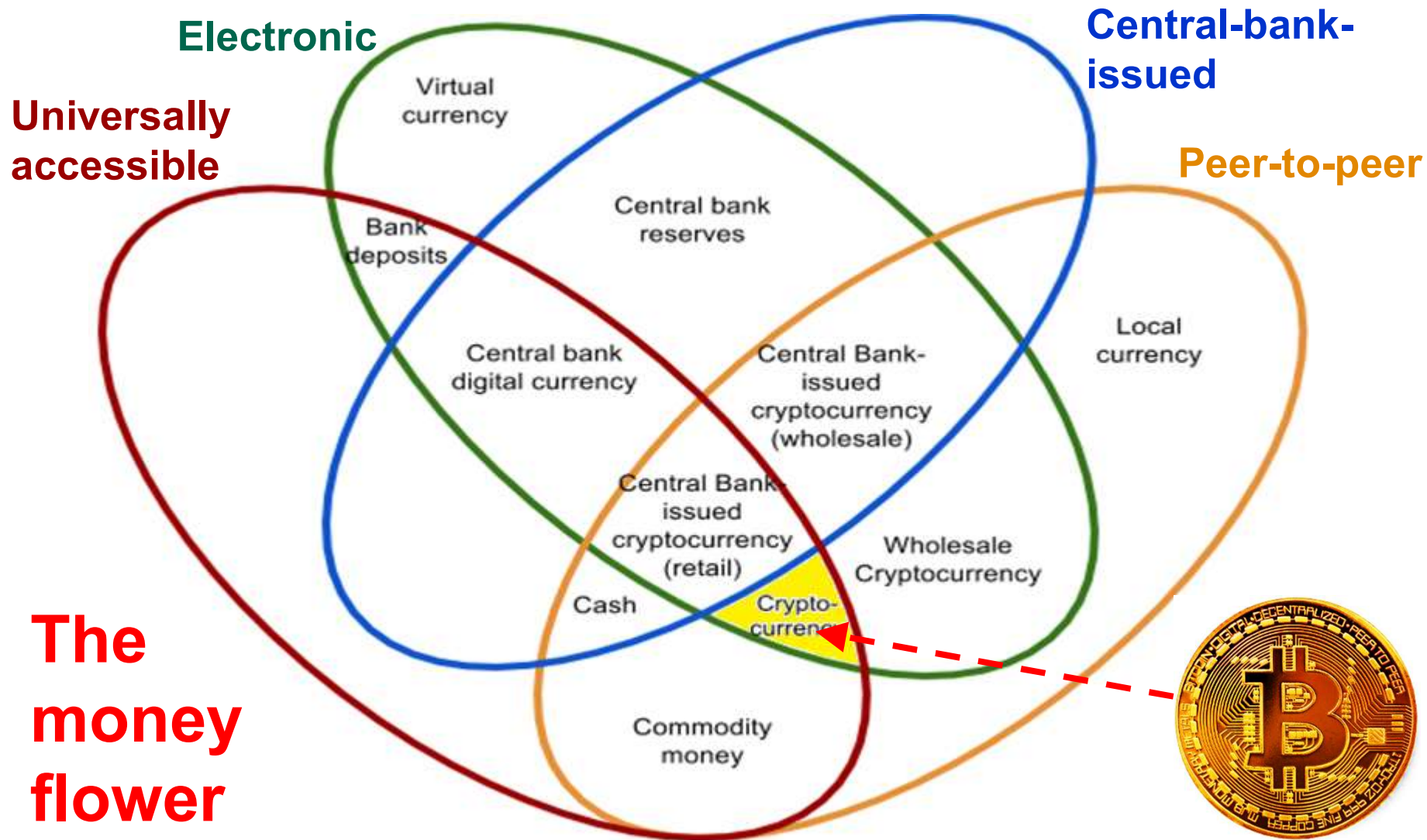
Ex.: Who owns the space wedge behind an airplane seat?



Or air above your house?



A Taxonomy of Money



The money flower



Early Forms of Digital Currency

Airline miles

Rewards points

Cash/Gift cards

Digital wallets



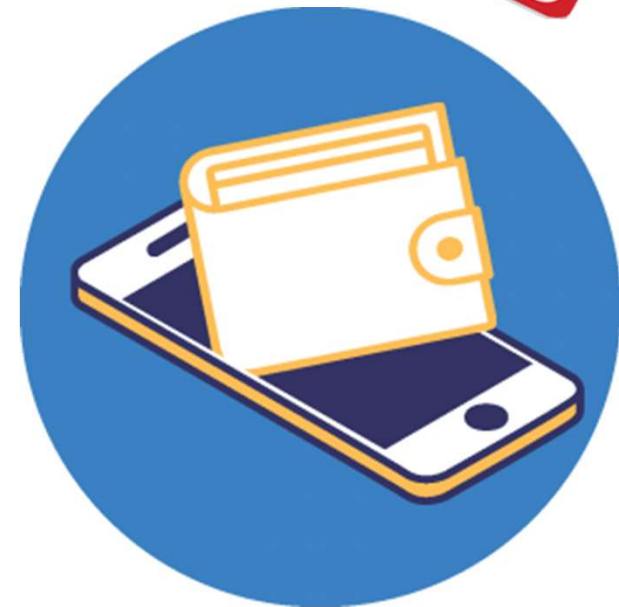
Digital currency vs. Virtual currency

Digital currency vs. Cryptocurrency

Securing digital currencies

Hiding digital currency transactions

Conversion of digital currency to
physical currency or goods



How Governments Manipulate Money

Increasing money supply to finance deficit spending

→ Inflation, which benefits the government

Inflation is a type of tax (like sales tax) paid by every citizen

Inflation is an evil tax that has asymmetric effects on people

Inflation creates temporary benefits (e.g., higher employment)

Inflation creates false economic signals → poor decisions

Inflation discourages saving/investment, favors hard assets

Some people insist that we must return to the Gold Standard

Bitcoin aimed to take this control away from the government

Bitcoin Mining

Mining for gold



Mining for bitcoin

Bitcoin miners aim to “solve a numeric problem”

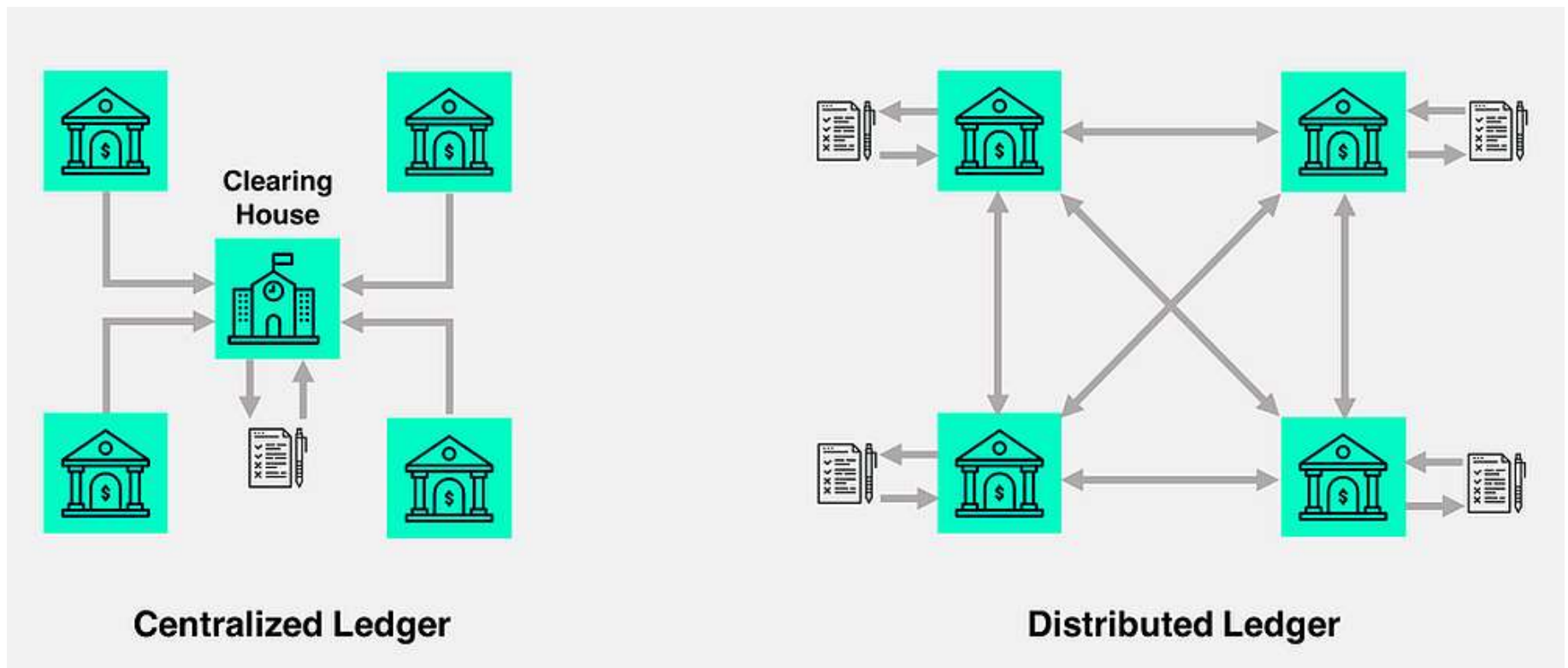


It’s a lot of hard “computational” work

You have to finish first to be rewarded with a bitcoin

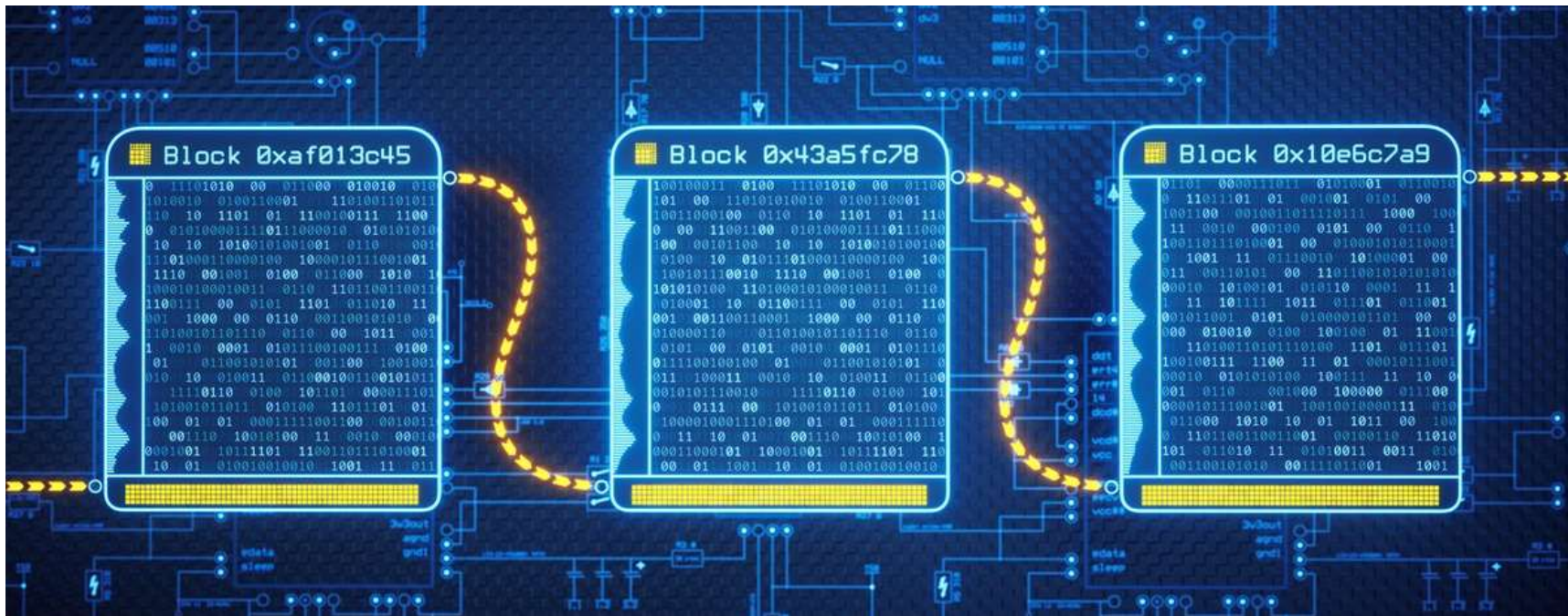
Centralized vs. Distributed Ledgers

Copies of the ledger are kept on a large number of nodes
Each node can process a transaction and update its ledger
Ledger copies are kept consistent by a consensus protocol



Bitcoin's Blockchain Protocol

Blockchain records transactions in a chain of blocks
Blocks are created one at a time, verified, and closed
Hash of the previous block is included in the next block
It's impossible to modify a closed block w/o being detected



Bitcoin's Hash Function

Input

Hash output

Hello world

A948904f2f0f479b8f8197694b30184b0d2ed1c1cd2a1ec0fb85d299a192a447

Hello worle

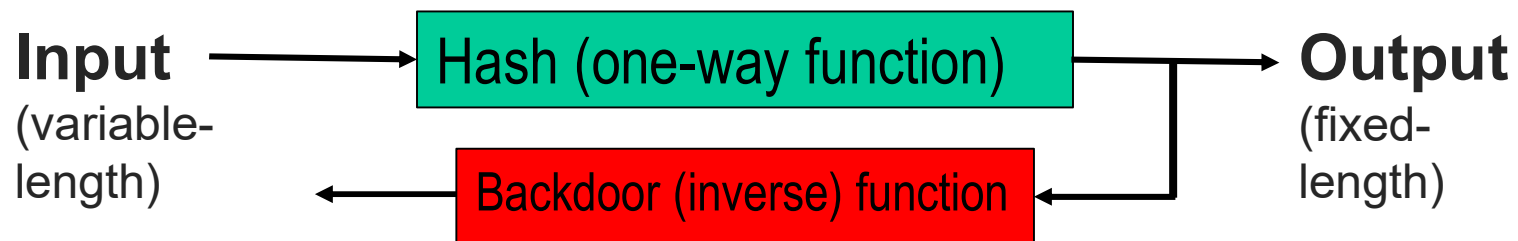
30e731839774de9ea08ff1adb8aa6b638e05f64900d005f84aea563cab0092b5

Change the last letter of the input so that the hash begins with 0
(there is no shortcut; have to try all possibilities)

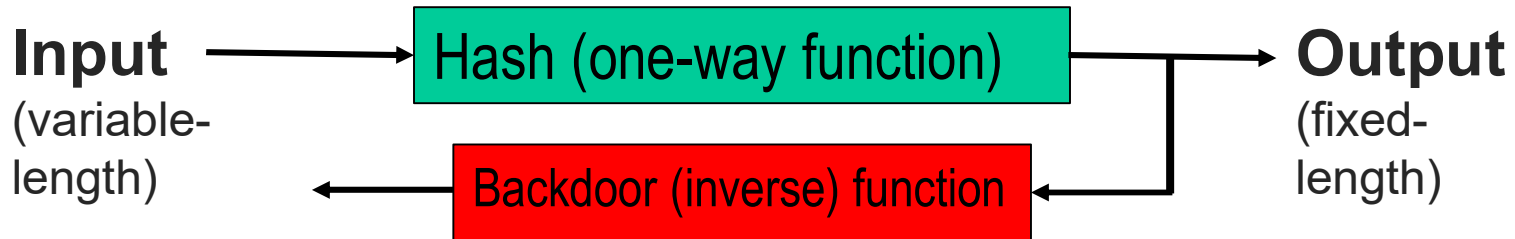
Hello worlC

0d7eae0f646102a05716b3ab0309c2ccc2952c0b3420b4aabb24ff969a320f8c

Find an input whose hash begins with 0000 0000 0000 0000 xxxx ...



Simple Example of a One-Way Function

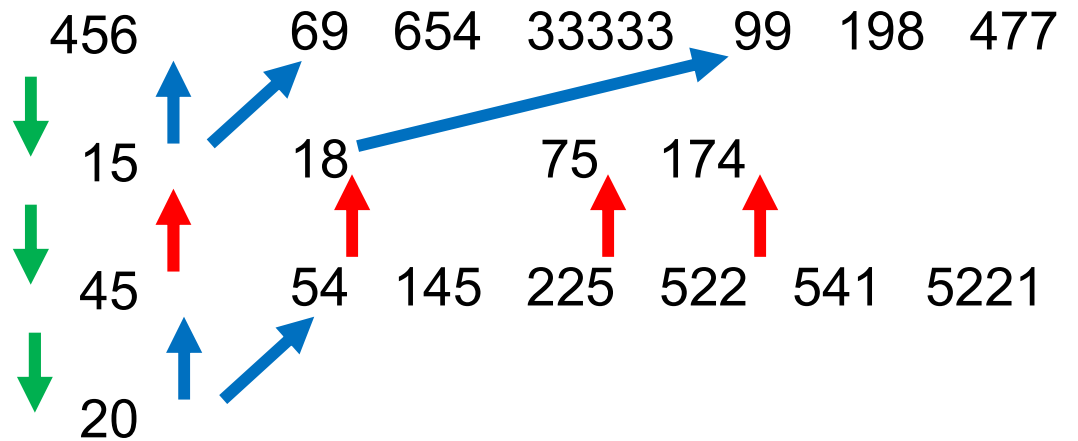


Magicians play a trick of guessing your number: Reversible function

Think of a 3-digit number
Add up the digits

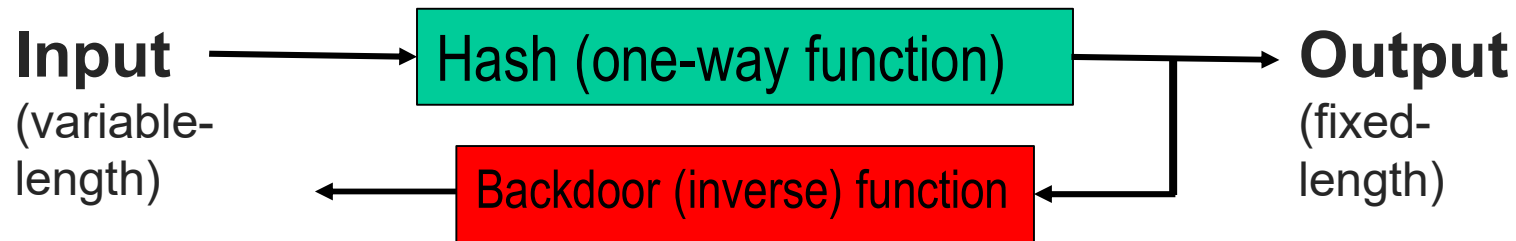
Triple the resulting number

Multiply the digits



$f(456) = 20$ $f^{-1}(20) = ?$

Computing the Hash Function



SHA256 Computation

Pre-processing phase: Convert input to a fixed-length binary string

Derivation of initial hash values $int((\sqrt{p} \bmod 1) * 16^8)$

Initial Hash Values ($p = 2, 3, 5, 7, 11, 13, 17, 19$)

Hash computation phase $W_t = ROTL(\sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16})$

$$\sigma_0(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$$

$$\sigma_1(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$$

Total arithmetic/logic ops per hash: 10^9 (giga-ops)

The Mathematics of Bitcoin – SHA256

<https://medium.com/swlh/the-mathematics-of-bitcoin-74ebf6cefbb0>

Cryptocurrency Hash Computation

Find an input with a hash that is smaller than a target value (that is, the hash begins with a bunch of 0s)

This may take many millions or even billions of attempts ($\sim 10^9$)

Bitcoin hash is called “double SHA-256”

Start with a binary string of any length representing the input





Augment and modify the input according to a recipe to get:
sixty-four 32-bit words ($\sim 10^2$ words)

Subject each word to millions of arithmetic/logic ops ($\sim 10^7$ ops)

Total arithmetic ops = $10^9 \times 10^2 \times 10^7 = 10^{18}$ ops (Exa-ops)

(Tera = 10^{12} Peta = 10^{15} Exa = 10^{18} Zetta = 10^{21} Yotta = 10^{24})

Four Ways to Secure Blockchains

			
<h3>Proof of Work</h3>	<h3>Proof of Stake</h3>	<h3>Proof of Burn</h3>	<h3>Proof of Capacity</h3>
<p>Miners following this protocol compete to crack a cryptographic puzzle using sheer computing power. The first miner to solve it gets to create the next block. Other users then validate the block, including the transaction data inside it. If the block passes muster, it's added to the blockchain. The successful miner then gets a reward, in the form of cryptocurrency.</p>	<p>PoW's main rival is used by the Cardano platform's Ada cryptocurrency and by Peercoin. Ethereum is also in the process of switching to this mechanism. With PoS, it's not the amount of work that determines who makes the next block; it's how much of their crypto holdings users are willing to lock up as a stake. Normally an element of chance is built in so that the richest user doesn't win every time.</p>	<p>Rather than investing computing resources or putting up a stake to win the right to create new blocks, users "burn" some of their cryptocurrency by sending coins to a one-way address from which they can't be retrieved or spent. The more coins users burn, the better their chances of winning. Burned coins devalue with age, though, so users must continually invest in the network.</p>	<p>In contrast with PoW's real-time competition to solve cryptographic puzzles, users compute thousands or millions of potential answers and store them on their hard drives. The more memory the users have, the more potential answers they can store. Each time a new block needs to be made, users search for an answer to the puzzle. Whoever is fastest gets to mine that block.</p>

(Should say "Four of the Many Ways")

Illustration by Anders Wenngren

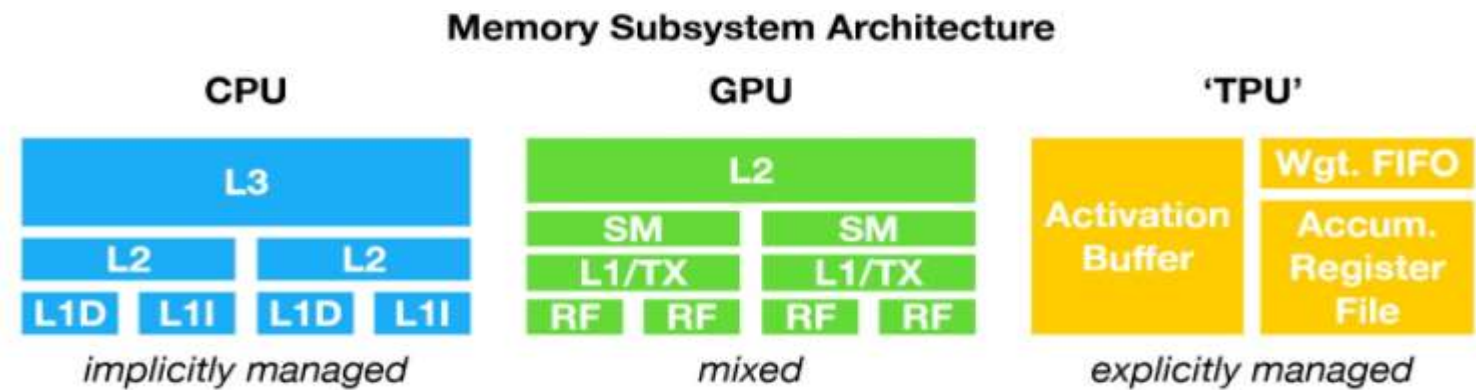
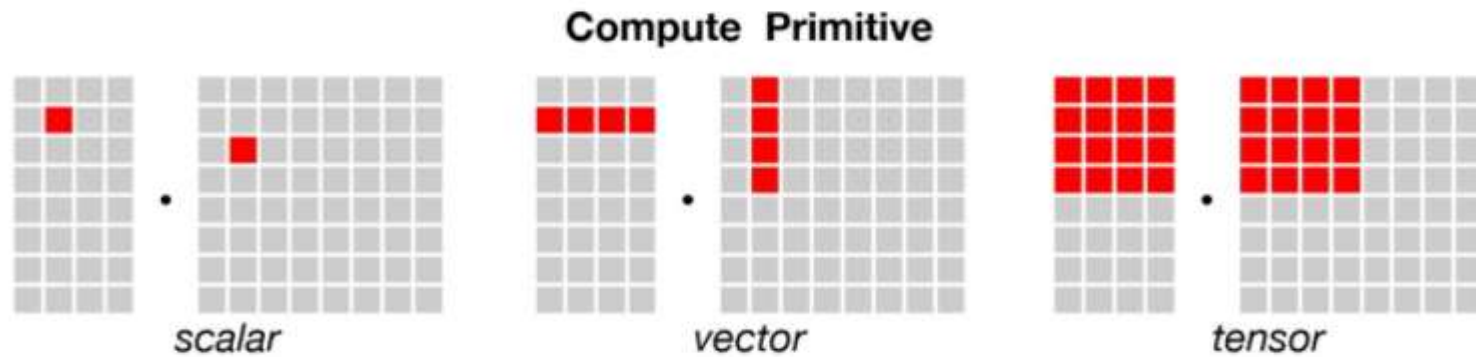
JULY 2021 SPECTRUM.IEEE.ORG 11

CPU, GPU, TPU, FPGA, Custom-VLSI

CPU = Central Processing Unit (processor or μ processor)

GPU = Graphic Processing Unit (numeric accelerator)

TPU = Tensor Processing Unit (AI / ML accelerator)



Time & Energy: CPU, GPU, TPU

Total arithmetic ops = $10^9 \times 10^2 \times 10^7 = 10^{18}$ ops (Exa-ops)

Time goal $\sim 10^5$ s (~ 30 hours or ~ 1 day; assumption)

One CPU offers $\sim 10^9$ ops/s (need 10^4 CPUs)

One CPU consumes ~ 100 watts of power

Electric energy: $30 \times 10^4 \times 10^2 = 3 \times 10^7$ watt-hr = 30 MW-hr

GPU is ~ 15 x more powerful and ~ 2 x more energy-efficient,
thus reducing energy costs of bitcoin mining by ~ 30

TPU is ~ 100 x more powerful and ~ 30 x more energy-efficient,
thus reducing energy costs of bitcoin mining by ~ 3000

Custom VLSI can be ~ 1000 times more powerful and ~ 100 x
more energy efficient, reducing the energy costs by $\sim 10^5$ x

Time & Energy: Supercomputers

Total arithmetic ops = $10^9 \times 10^2 \times 10^7 = 10^{18}$ ops (Exa-ops)

Most powerful supercomputer: ~ 100 petaops/s = $\sim 10^{17}$ ops/s

Most energy-efficient supercomputer: 10^{15} ops/kW-hr

<https://www.top500.org/>



<https://www.top500.org/lists/green500/>



Cryptocurrency Energy Challenges

Assume 10 MW-hr of energy for bitcoin mining

Energy cost ~ \$1000

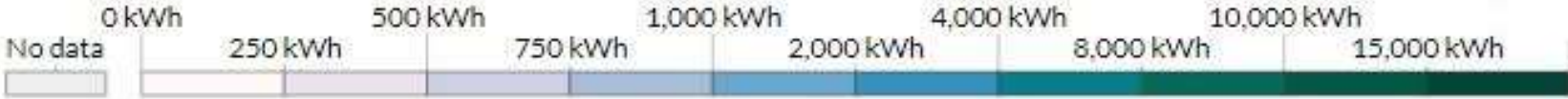
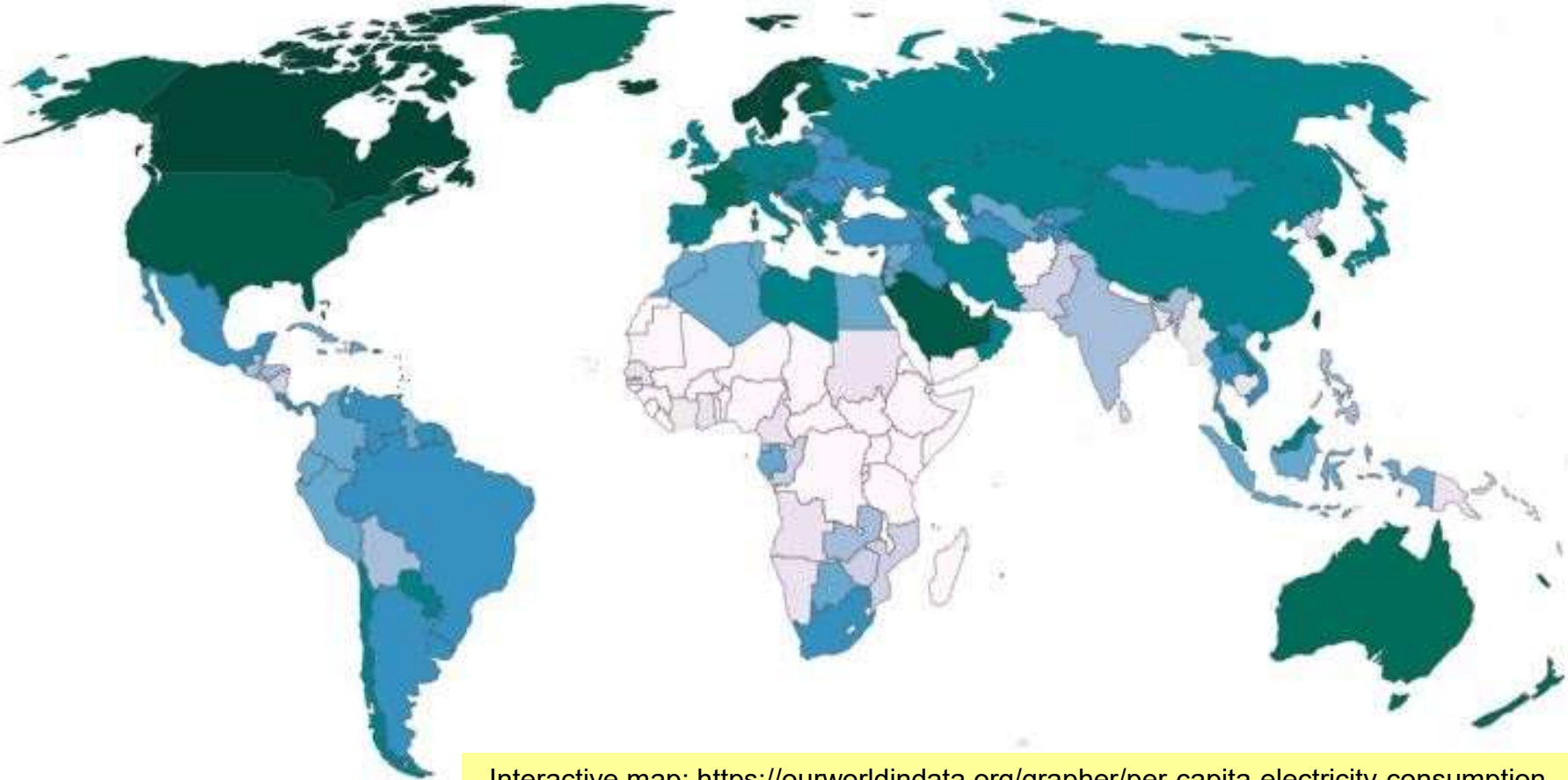
Average US home uses 10 MW-hr of electricity per year

Bitcoin mining energy per day = Home energy use per year

A bitcoin mining farm uses as much power at ~500 homes



Per-Capita Electricity Consumption



After All Glaciers Have Melted



The Ethics of Blockchain



Blocks and scales of justice

MS. TECH; SCALES: CHRIS POTTER; FLICKR

[Blockchain / Smart contracts](#)

Why it's time to start talking about blockchain ethics

Blockchain technology is changing the nature of money and organizations. We should probably start pondering the potential consequences.

by **Mike Orcutt**

October 10, 2019

Just like biotech, AI, & nukes, blockchain need its own ethics

With governments, investors, FB, & stock exchanges showing interest in cryptocurrency, its niche status may change

When money's nature changes, social rules & politics follow

In a leaderless organization, who's responsible for mishaps?

Is it ethical to hack blockchain?
More serious than hacking FB?

July 2021



Currency and Digital Cash: History & New Trends



Slide 28

The Ethics of Risky Investments



Bitcoin does not provide any stability guarantees, so it must be ruled unethical as a currency

<https://www.business.rutgers.edu/business-insights/bitcoin-ethical-currency-not-according-professors-new-research>

Prof. Tobey Scharding (Rutgers):
[Using Johann Gottlieb Fichte's ideas, 1762-1814]

The purpose of currency is to underwrite a shared means of life for a population of people

A crucial property of this shared means is that it be stable/secure

Typically, the issuer of currency provides stability guarantees

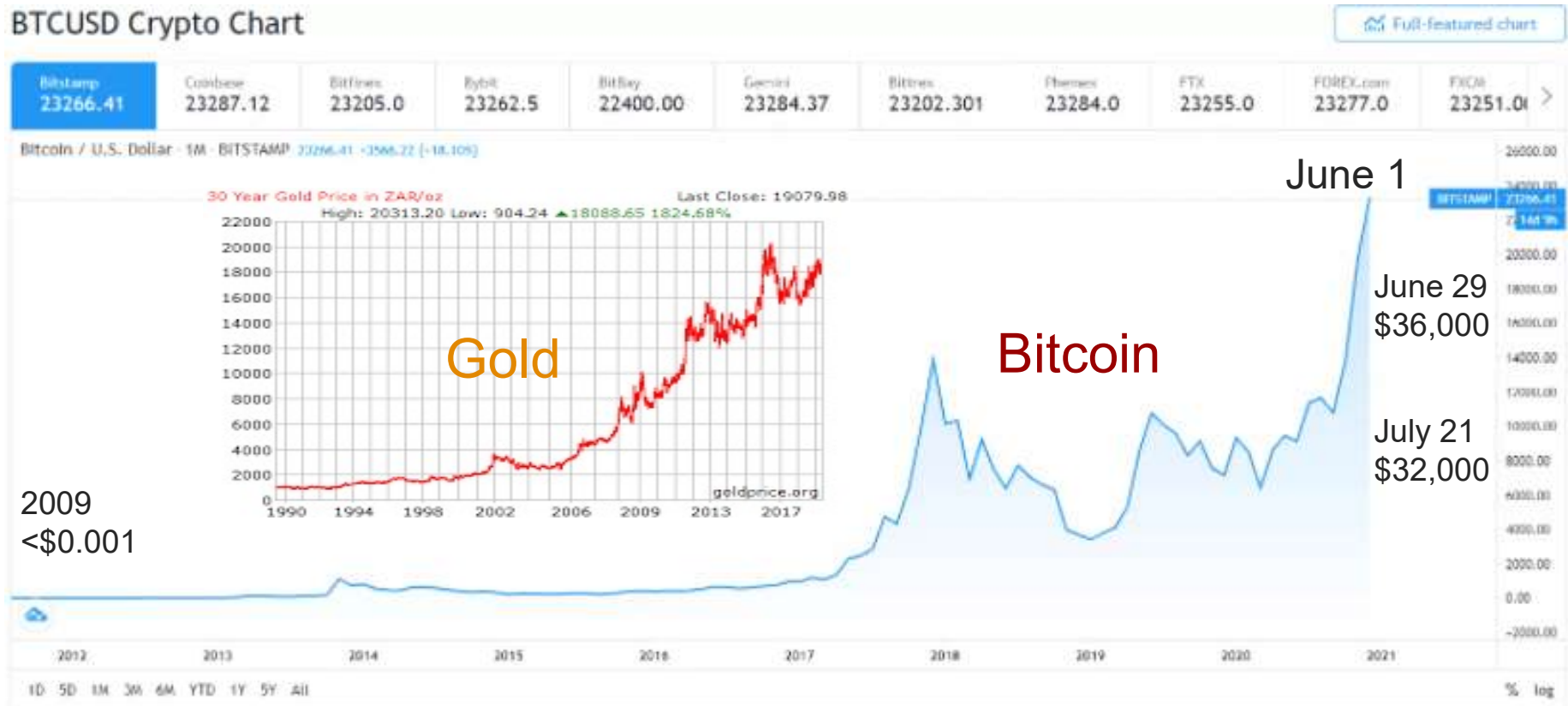
Bitcoin cannot provide stability and value guarantees

Fichte's ethics:
Living a good life, requires that you be able to plan with peace and security



Bitcoin's Price Volatility

Starting at < \$0.001 and hovering ~ \$1000 in mid-2010s, bitcoin's price entered a highly-volatile period in 2018



The Ethics of Covert Payments

Do cryptocurrencies such as bitcoin encourage / facilitate criminal activities?

How is bitcoin different from using \$100 bills by criminals?

- Bills have serial numbers
- Bills can be traced by surveillance
- Bills can be forged
- Dodging taxes (tax shelters)
- Money laundering



My Assessment:

Cryptocurrency does not seem to make things worse in terms of criminality

Is Bitcoin Truly Untraceable?

Not if you exchange your bitcoins for goods/services

Not if some government knows a backdoor

US government claimed that it had recovered ransom paid in bitcoins

Systems deemed ultra-secure have been hacked

Biggest hack ever: Shamoon (Iran)

China's hack of Microsoft network

Credit agencies, healthcare, ... hacks

Computer forensics

Methods/technologies to fight crime



Conclusions and Future Work

The Bottom Line:

Digital currencies are here to stay. We might as well work to solve the challenges they pose, instead of resisting them

Some Problems Being Worked on:

- Imposing international standards (regulation)
- Moderating price fluctuations
- Making computations more scalable and energy-efficient
- Safeguards against hacking and other digital attacks
- Other issues: Inheritance; Fairness; Regulating supply

Going Forward:

- More realistic reward system
- Acceptance from financial markets and businesses

Questions or Comments?

parhami@ece.ucsb.edu

<http://www.ece.ucsb.edu/~parhami/>

