Week 1

What is money? What is a Decentralized Web? Principles of cryptocurrency.

Goals for this Club

- Dispel the myths.
- Focus on the technology.
- Understand how crypto and blockchain technology will impact you.
- Help you find an area in crypto that excites you.

1. Money

What is money?

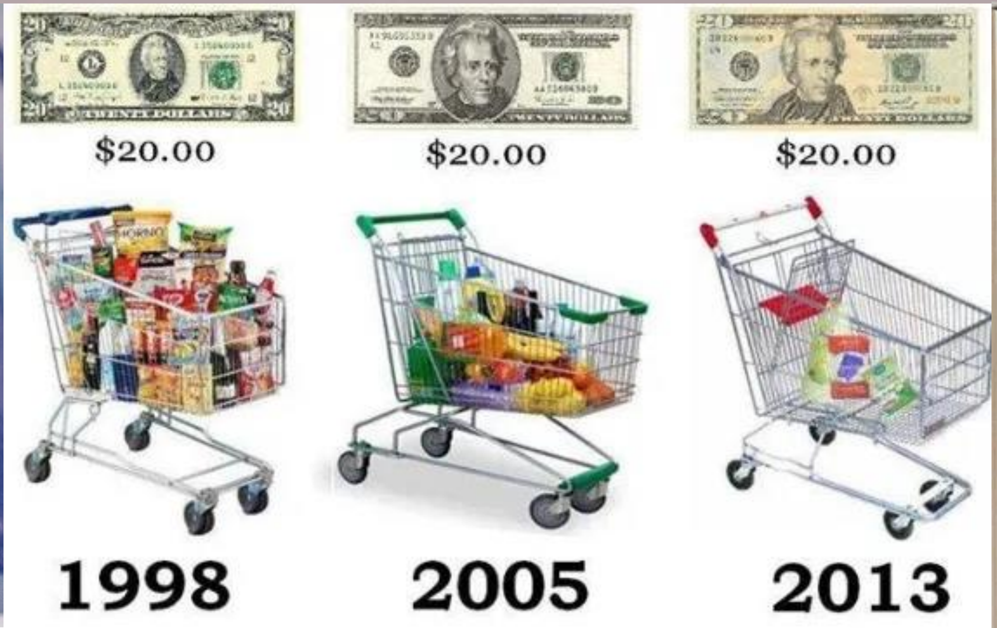
- Money can be defined in three basic sects; it must fulfill all of these.

- Medium of exchange- "I will give you money(the medium) for XYZ."
- Store of value- Gold is valuable because its relatively scarce. Bitcoin is absolutely scarce.
- Unit of account- ”This ice cream is $5.”

Why the quality of that money matters.

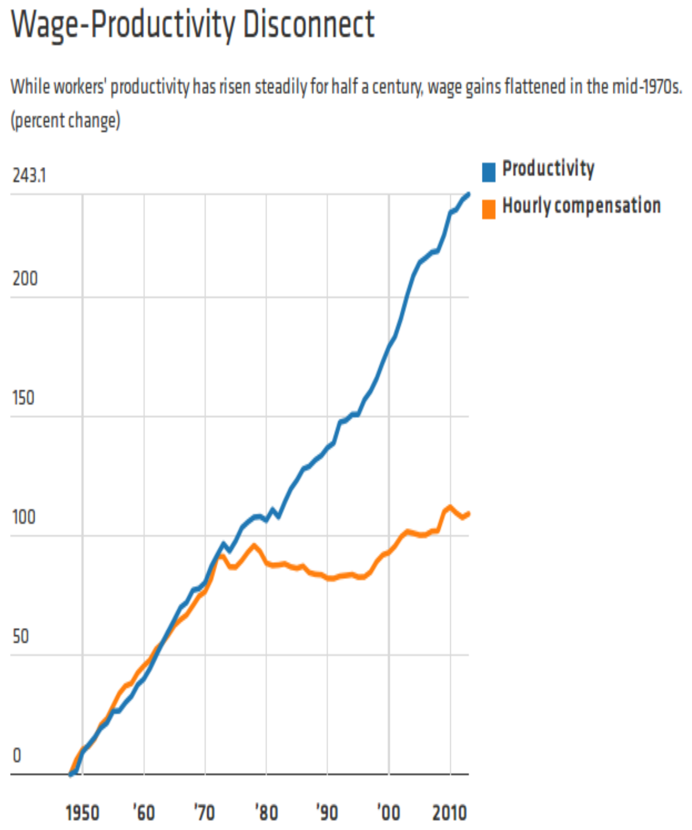
- It is vital that you work for GOOD money.
- Imagine you go to school every day for 18 years, then go to work every single day for this thing called money.
- But do you know what is really is? Where did it come from? Why is it valuable in the first place?

100000000000000 RESERVE BANK OF ZIMBABWE
I promise to pay the bearer on demand
ONE HUNDRED TRILLION DOLLARS
for the Reserve Bank of Zimbabwe
HARARE 2008



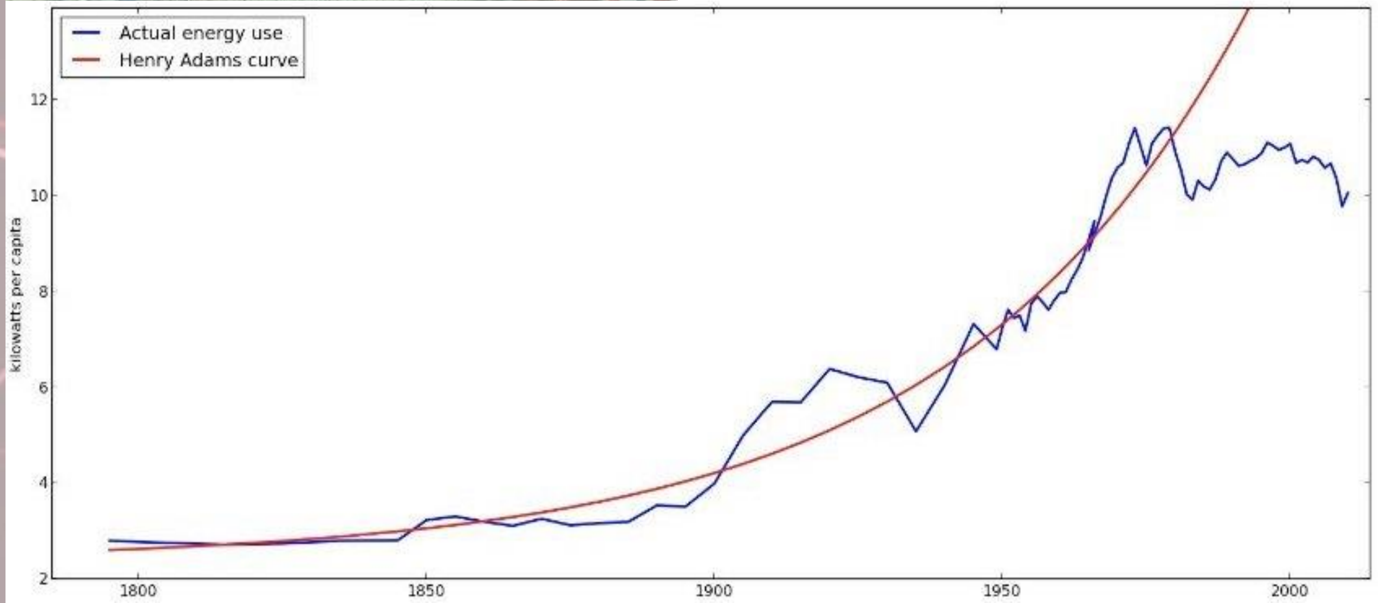
Why the quality of money matters. (continued)

- Inflation robs people in more ways than the ones visible on the surface.
- wtfhappenedin1971.com
- Pictures: **Top Left**- Glass soda bottles (taken 1980); **Bottom**- Adams Energy Curve, slowed technological advancement; **Top Right**- productivity vs compensation



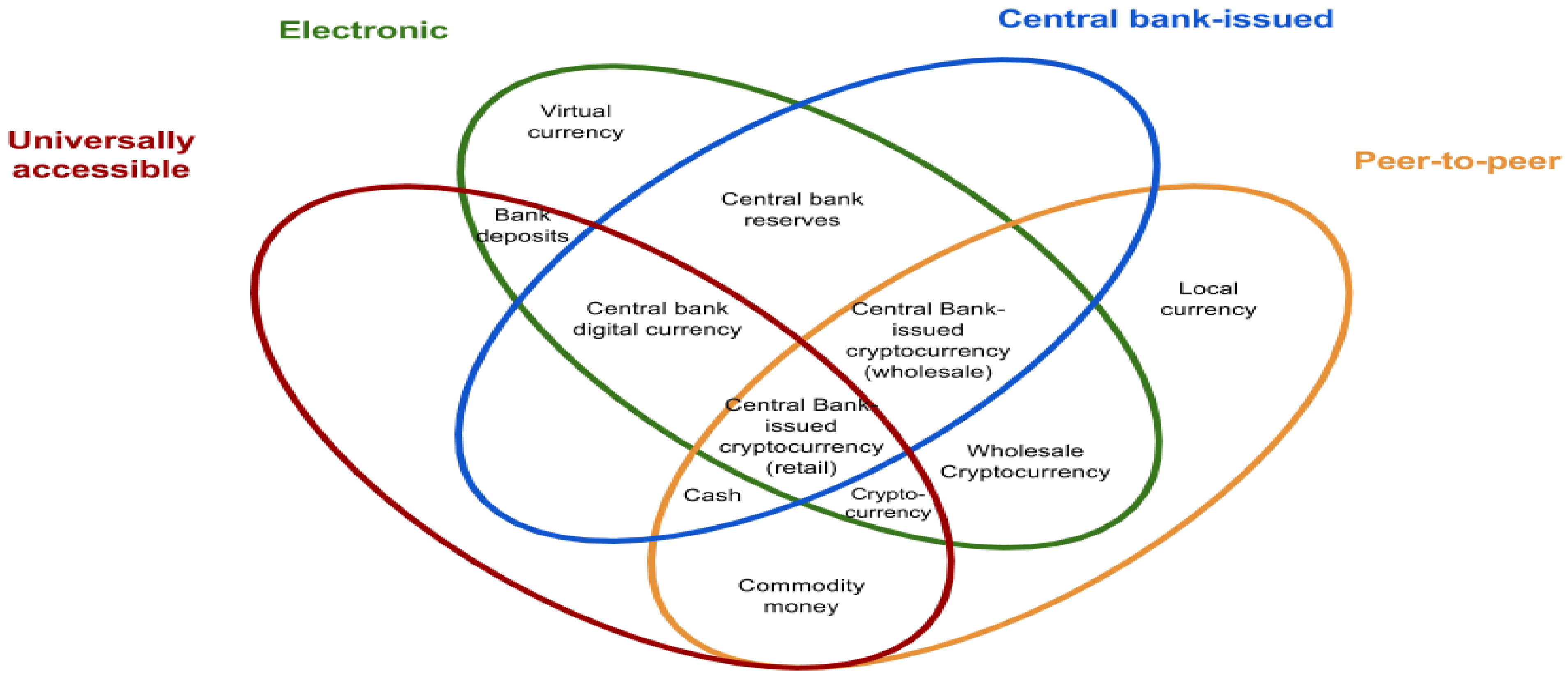
Wage-Productivity Disconnect

While workers' productivity has risen steadily for half a century, wage gains flattened in the mid-1970s. (percent change)



Centralized vs Decentralized money

The money flower: a taxonomy of money



Adaptation from Bank for International Settlements (2017)

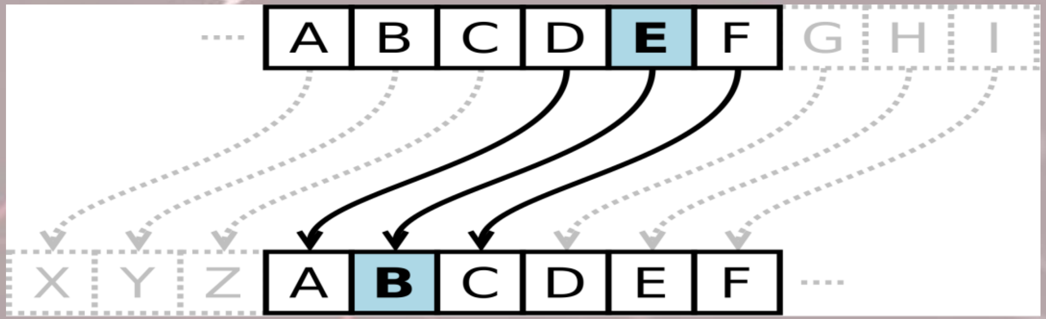
2. History of Cryptography and Cryptocurrency

Early predictions of cryptocurrency

- **Henry Ford (1921)**- Henry Ford stated in a news article that the gold standard model of world currencies always led to war and greatly extended their lengths. He said that replacing it with an *“energy currency”* would make money backed by *natural wealth* instead of gold loans which led to debt.
- **F.A. Hayek (1984)**- “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 it violently out of the hands of government, all we can do is by some sly *roundabout* way introduce something that *they can’t stop*.”
- **Milton Friedman (1999)**- During an interview, Milton Friedman explained that the internet could play a huge role in reducing the governments involvement in the economy and make a reliable *“e-cash”* where **A** can send money to **B** would either end knowing each other.

Early cryptography (1900 B.C.-1930s)

- For centuries, cryptography was mainly a hobby of mathematicians, spies, military leaders, and diplomats. This mainly consisted of making it harder to read letters in the event of capture.
- Methods included speaking other languages, switching letters for numbers (vice versa).
- Caesar Cipher is one of the earliest known methods, which shifted three letters previous of what was ever written (pictured).

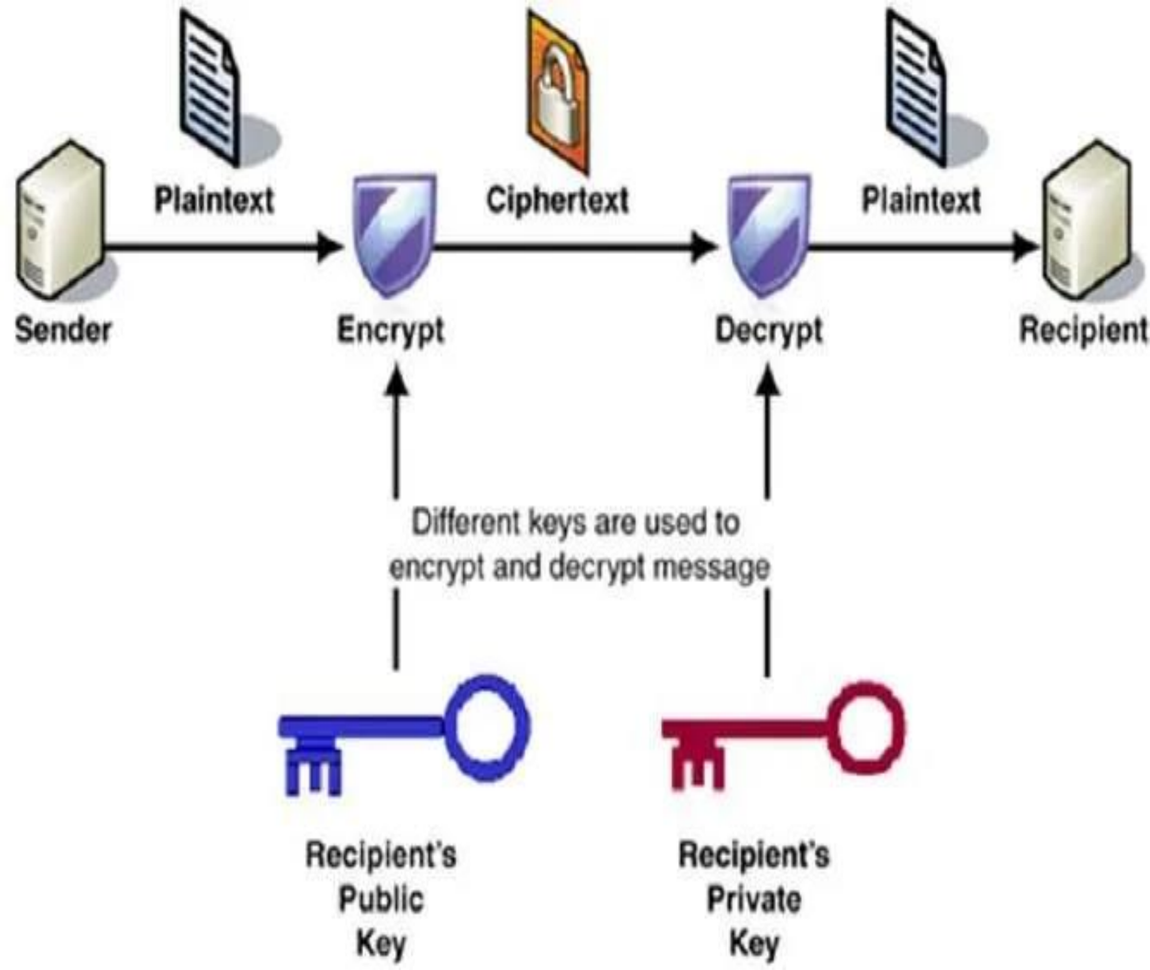


Emergence of modern cryptography

- Before the 20th century, cryptography mainly was focused on linguistics and symbolism.
- Since then, much more mathematical disciplines like information theory, statistics, and combinatorics, have been applied.
- Modern cryptography emerged from initially during WWI, but ramped up massively during WWII, when information was transmitted over radio.
- Digital computers make the creation of complex ciphers much easier. But the growing raw computing power also made it easier to crack these ciphers.

1970s and 1980s

- **Data Encryption Standard**- The US Government releases the Data Encryption Standard in 1975, making cryptography public information.
- ***New Directions in Cryptography***- Dr. Whitfield Diffie and Dr. Martin Hellman write the first publicly available work on public-key cryptography.
- **Dr. David Chaum**- Dr. Chaum writes extensively on anonymous digital cash in Security without Identification: Transaction Systems to Make Big Brother Obsolete. First know proposal of a blockchain.



Crackdown & the rise of the Cypherpunks

- In the early 90s the US government and its allies attempted to limit the public's access to cryptography tools.
- In 1992, **Eric Hughes, Tim May and John Gilmore** founded the Cypherpunks mailing list.
- They knew that the internet would be a battleground for human freedom, and they created a network to defense the space.
- Launched the "First Crypto War" in the 90s when the NSA developed the "Clipper Chip" to be put in all cell phones, equipped with a backdoor for law enforcement to listen in.

Notable Cypherpunks

Eric Hughes: A Cypherpunks Manifesto

- "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."

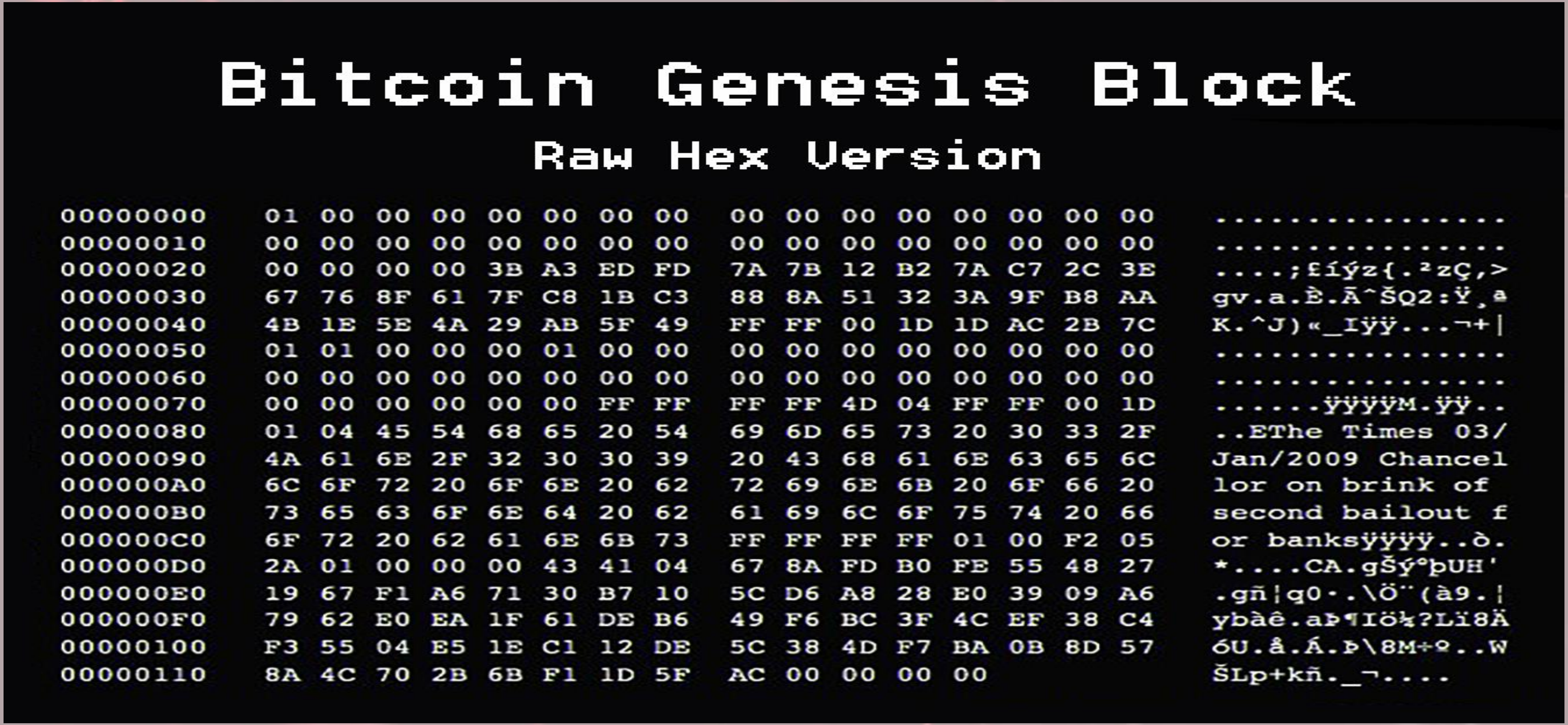
Attempts at Digital Money

- DigiCash-
- E-gold-
- BitGold-

2008: Bitcoin

- Created by the anonymous creator or group under the name Satoshi Nakamoto.
- First working decentralized blockchain, a digital ledger to record data points.

January 3, 2009: Genesis Block is Mined.



Bitcoin Genesis Block

Raw Hex Version

```
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._¬....
```

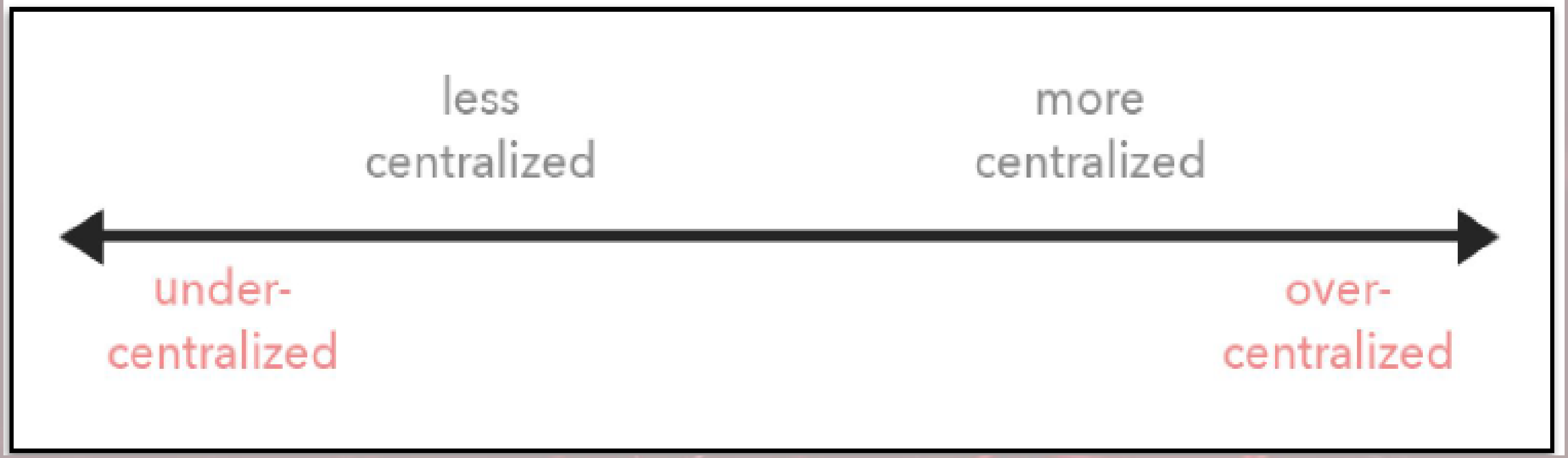
3. Decentralization

What is decentralization?

- The term came into being as an opposite to the term “centralization”, which became common in the 1800s.
- Term originated from Revolutionary France.

What is decentralization? (continued)

- Centralization and Decentralization can be seen as directions on a spectrum.



What is decentralization? (continued)

- The oscillating pattern is seen at a social scale throughout history
    - Revolutionary France
    - The United States
    - Government and Business

Failures of centralization

- Robinhood halts trading
- Google/ICAAN shut down internet
- Banks freezing accounts
- Financial crisis
- Communism

Challenges of decentralization

- Individuals may not hold enough of a stake
- Ill-defined responsibilities
- Growth ceases
    - Fall of Rome

Decentralization in finance

Decentralization on the internet (distributed networks)

- Can be utilized in many ways, not just cryptographic hashing.
- Think torrenting (Pirate Bay), telephone networks, or the World Wide Web itself
- Centralized platforms follow a similar life-cycle
  - Recruit users heavily
  - User relationship changes from positive-sum to zero-sum
  - “For 3rd parties, this transition from cooperation to competition feels like a bait-and-switch.” - Chris Dixon

Key words

- Trustless
- Permissionless
- Transparent
- Open-access

4. Blockchains

Blockchains overview

- A type of ledger that records data using “blocks”
  - The previous blocks are “read only” and therefore immutable
- Bitcoin is a decentralized and public blockchain hence the term distributed ledger
- Blockchains can be private
  - Think of them as a type of database

Transactions

- Each person has a “wallet address” that is unique to their wallet
  - ○ 3FZbgi29cpjq2GjdwV8eyHuJJnkLtktZc5
- I submit a transaction to this address into the public “queue” of transactions
- “Miner” takes your transaction and puts it onto the next block, which they then attach to the chain
- Everyone’s ledger is updated, and the money is moved

Double spend problem

Consensus mechanisms

Proof of Work

- Used in various other computational situations such as protecting an inbox from spam emails or protecting a website from a DDOS attack
- Requires the computer that is trying to do a task, to solve a complex math problem which slows it down.

Proof of stake

- Cryptocurrency-specific solution to problems imposed by Proof of Work (mostly environmental).
- Requires a user to put up all their coin as collateral before they validate the next block.

Proof of Work

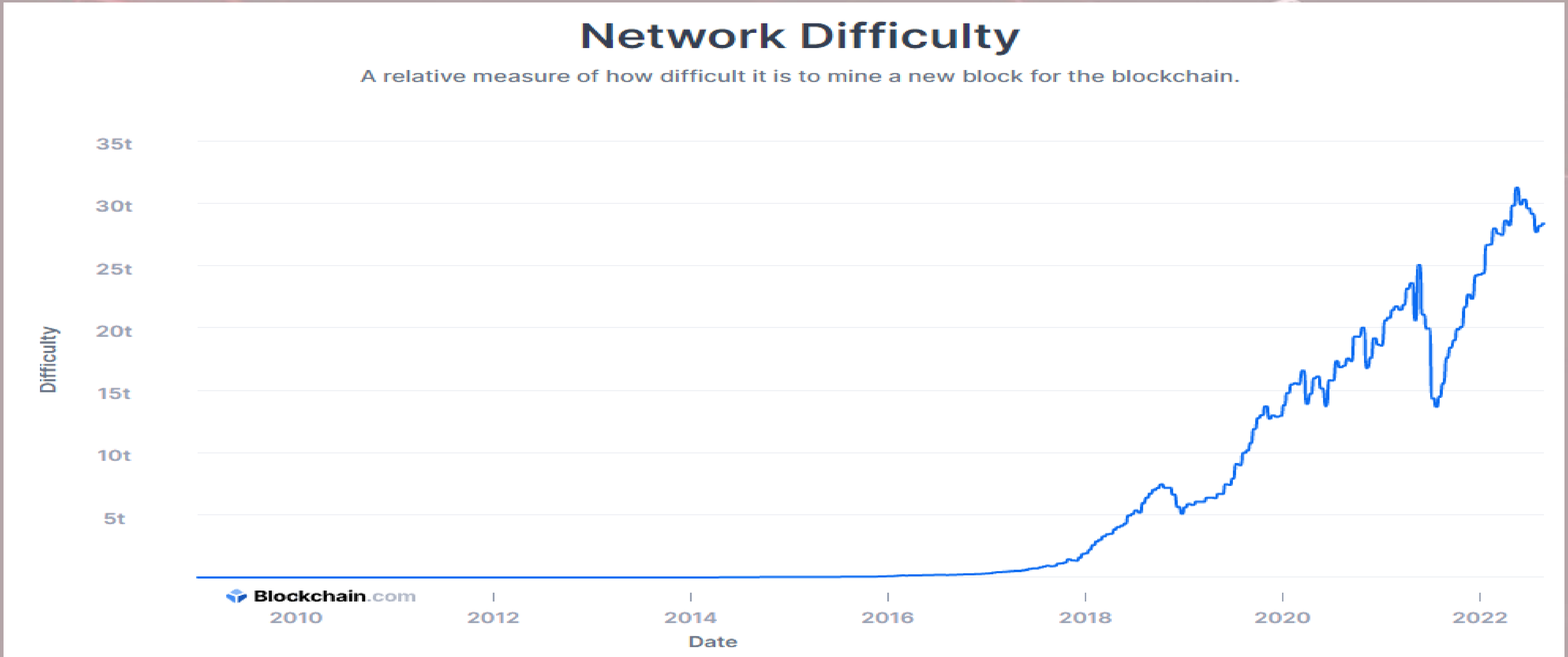
- SHA-256 Algorithm
- Outputs an alphanumeric string
- Seemingly random

“hello” ->

“2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e
73043362938b9824”

? -> “00000000asdjf23a423sdh23fads…”

Proof of work (continued)



Proof of stake

- Validators are selected at random depending on how
- much coin they have staked

Thanks!

Any questions?

Week 1 Resources

Websites & Articles

- Bitcoin Whitepaper https://bitcoin.org/bitcoin.pdf
- History of Bitcoin http://historyofbitcoin.org/
- Why Decentralization Matters https://onezero.medium.com/why-decentralization-matters-5e3f79f7638e
- Cambridge Mining Map https://ccaf.io/cbeci/mining_map

Videos-

- How Bitcoin Works (best explanation)- https://www.youtube.com/watch?v=bBC-nXj3Ng4
- How Bitcoin Works under the Hood- https://www.youtube.com/watch?v=Lx9zgZCMqXE
- How Secure is 256 bit? https://www.youtube.com/watch?v=S9JGmA5_unY

Favorite Apps, Websites, and Exchanges

Websites

- https://coinmarketcap.com/
- https://opensea.io/
- https://cryptoslate.com/

- **Apps**

Exchanges

- Coinbase
- Binance.US
- Kucoin
- Binance (only useable with foreign ID)

Next Week

- Bitcoin
- Blockchain Trilemma
- Ethereum and 2nd Gen Blockchains; Smart Contracts
- 3rd Gen Blockchains; Scalability