#### CSE446: Blockchain & Cryptocurrencies

Lecture - 6: History and Properties of Money



# Agenda

- The history of money
- Properties of money
- Bitcoin

### Let's talk about money....



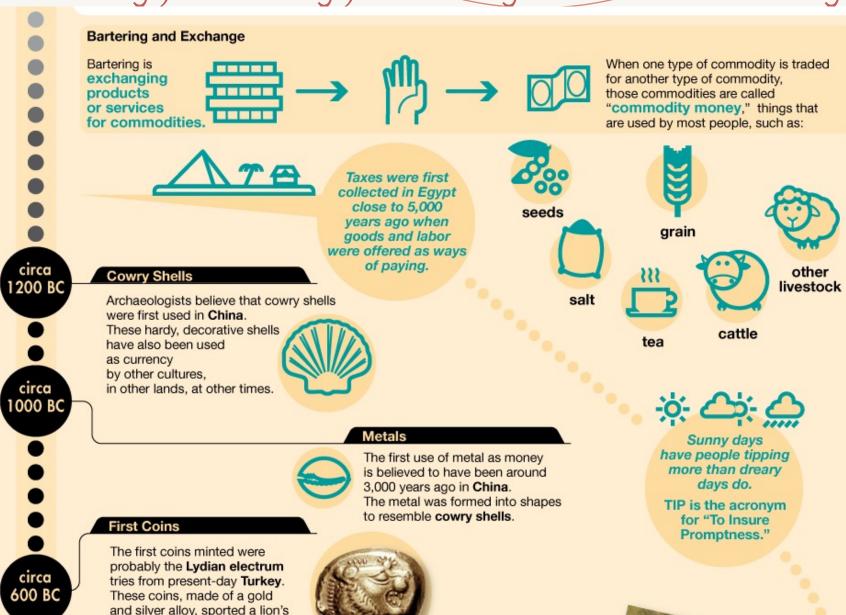
https://media.tenor.com/Wkb4VlC1BHoAAAAC/money-money-rain.gif



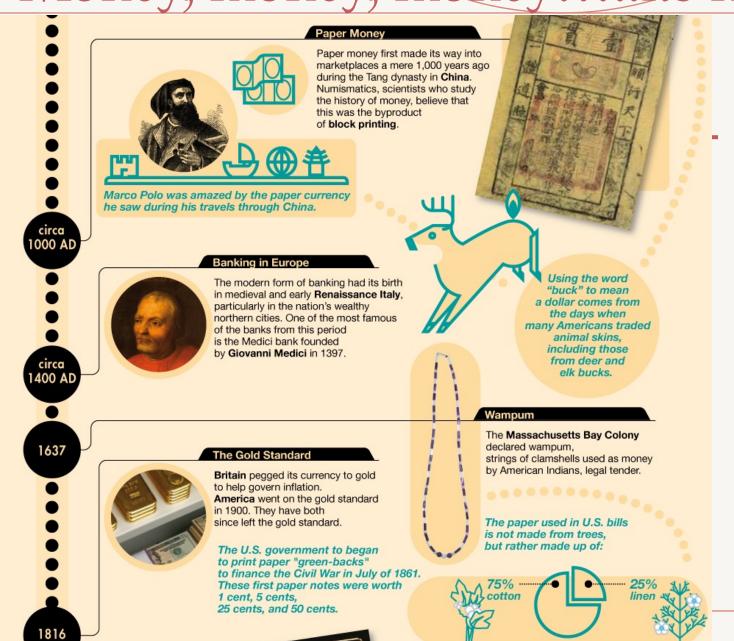
https://media3.giphy.com/media/JpG2A9P3dPHXaTYrwu/giphy.gif?cid=ecf05e4785vmquns0oo0f7x59qjgnyjx467oxq37irfv5z7d&rid=giphy.gif&ct=g

- Money is a medium of exchange
- Stands in for an arbitrarily long chain of barter
  - exchanging goods or services for other goods or services without using a monetary unit
- Widely accepted





head on one side.



#### Properties of money

- Money is a unit of account
  - a nominal monetary unit of measure used to represent the real value (or cost) of any economic item; i.e. goods, services, assets, liabilities, income, expenses.
- Money is a store of value
- Recognisable
- Fungible (mutually interchangeable)



https://upload.wikimedia.org/wikipedia/commons/e/e3/Gold-295936.jpg

### Properties of money

- Divisible
- Transportable
- Transferable
- Hard to counterfeit
- Stable supply



https://upload.wikimedia.org/wikipedia/commons/e/e3/Gold-295936.jpg

• With the evolution SSL / TLS – 1996 of the Internet, the need for digital currency became clear

HTTP- 1990

TCP/IP - 1974

Ethernet - 1974









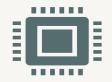


DigiCash - the first ever digital currency invented by David Chaum in 1983, commercialised in 1990, went bankruptcy in 1998 with the paper:

"Blind signatures for untraceable payments"

\$

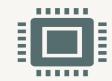
b-money, an anonymous, distributed electronic cash system by Wei Dai in 1998



Bit Gold a proposal by
Nick Szabo in 1998
where he
conceptualised the
idea of utilising
cryptographic puzzles
for unforgeable proof
of work chains: a direct
pre-cursor of Bitcoin
idea







sal by

998

the

All these ventures or ideas failed because they utilised mostly centralised components. And the puzzle to move money online between two entities seems like an elusive idea...until??

in 1998 with the paper:

"Blind signatures for untraceable payments"

cryptographic puzzles for unforgeable proof of work chains: a direct pre-cursor of Bitcoin idea

#### Crypto-currency

- Based on cryptography
- Derives trust from mathematical properties/algorithms/systems
- Based on established, trusted cryptographic primitives NOT from chemical/physical properties
- NOT from coercive (imposed) Legal Tender statutes
  - Legal tender is a medium of payment recognised by a legal system to be valid for meeting a financial obligation

