

A splash around in **Cryptocurrencies**

Mark Twells
June 2024





What is this session?

I am not making recommendations or definitive statements

A dry look at how cryptocurrency works



What is a currency

A currency is **a standardization of money in any form, in use or circulation as a medium of exchange**, for example banknotes and coins. A more general definition is that a currency is a system of money in common use within a specific environment over time, especially for people in a nation state. (Wikipedia)

noun

, plural *cur-ren-cies*.

1. something that is used as a medium of exchange; money.
2. general acceptance; prevalence; vogue.
3. a time or period during which something is widely accepted and circulated.
4. the fact or quality of being widely accepted and circulated from person to person.
5. circulation, as of coin.



What is money

Money is any item or verifiable record that is generally accepted as payment for goods and services and repayment of debts, such as taxes, in a particular country or socio-economic context. The primary functions which distinguish money are: medium of exchange, a unit of account, a store of value and sometimes, a standard of deferred payment.



Standard

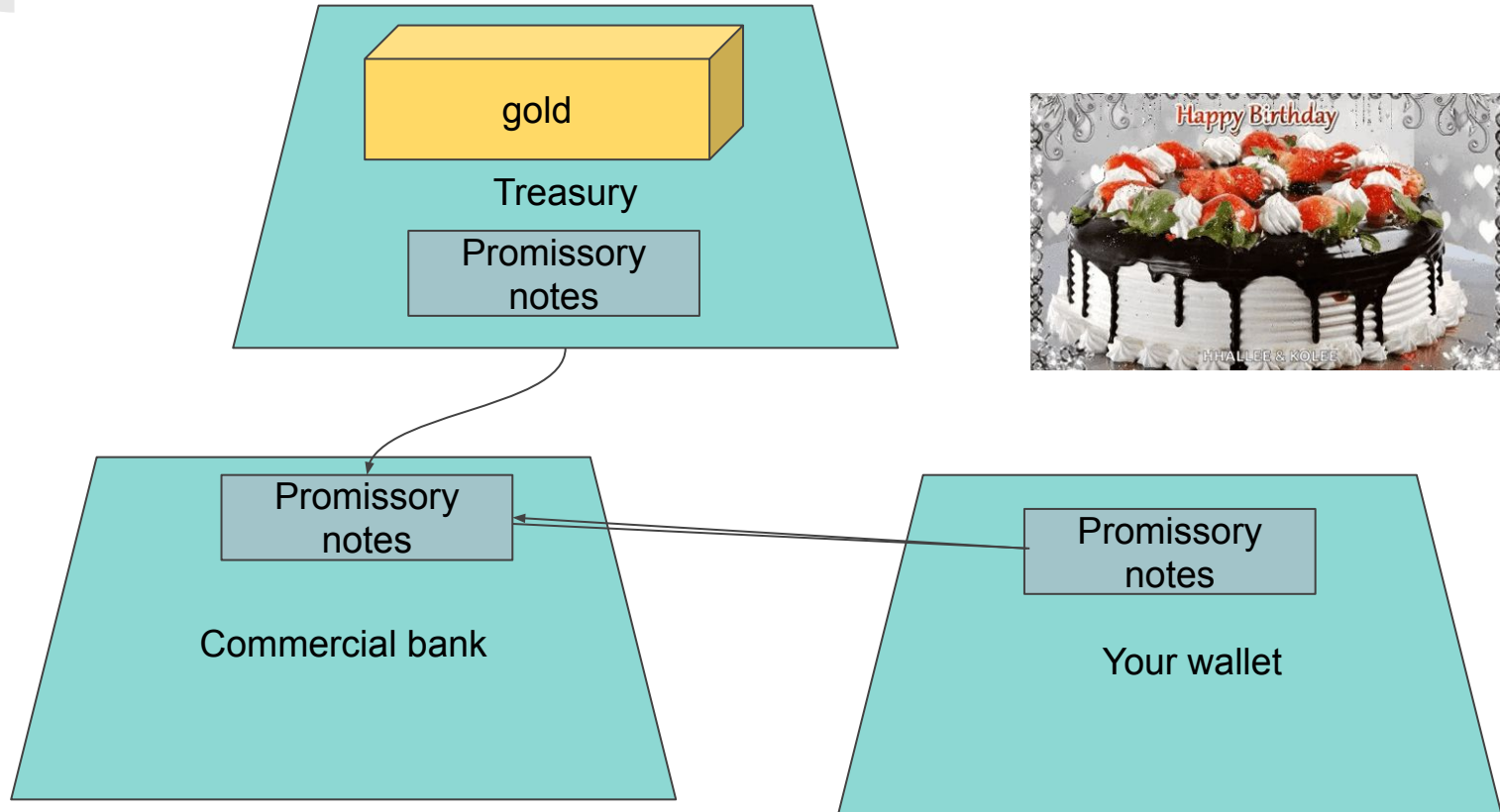
Salt - Salary - salarium

GOLD standard

*I promise to pay the bearer on demand...*promissory notes

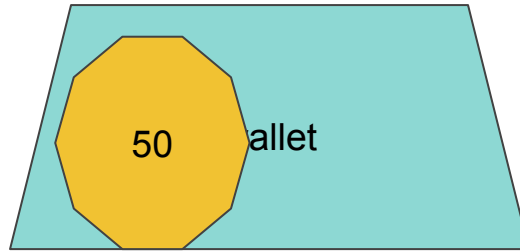
What is £1 ?

The gold standard: a traditional model



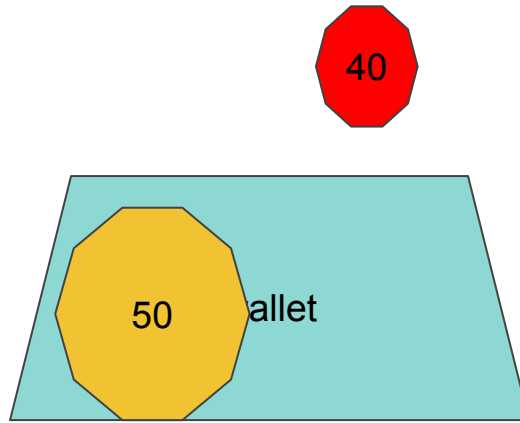


Digital currency ?



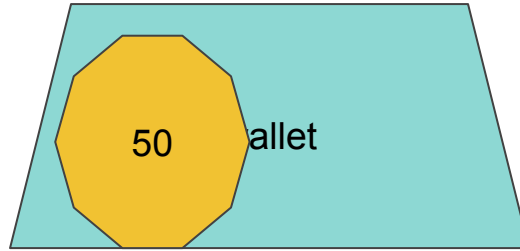
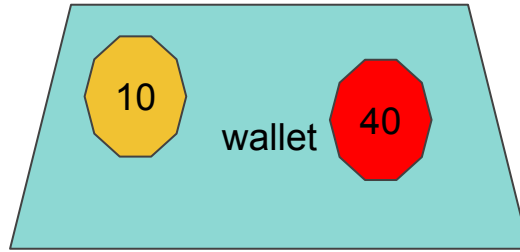


Digital currency ?





Digital currency ?





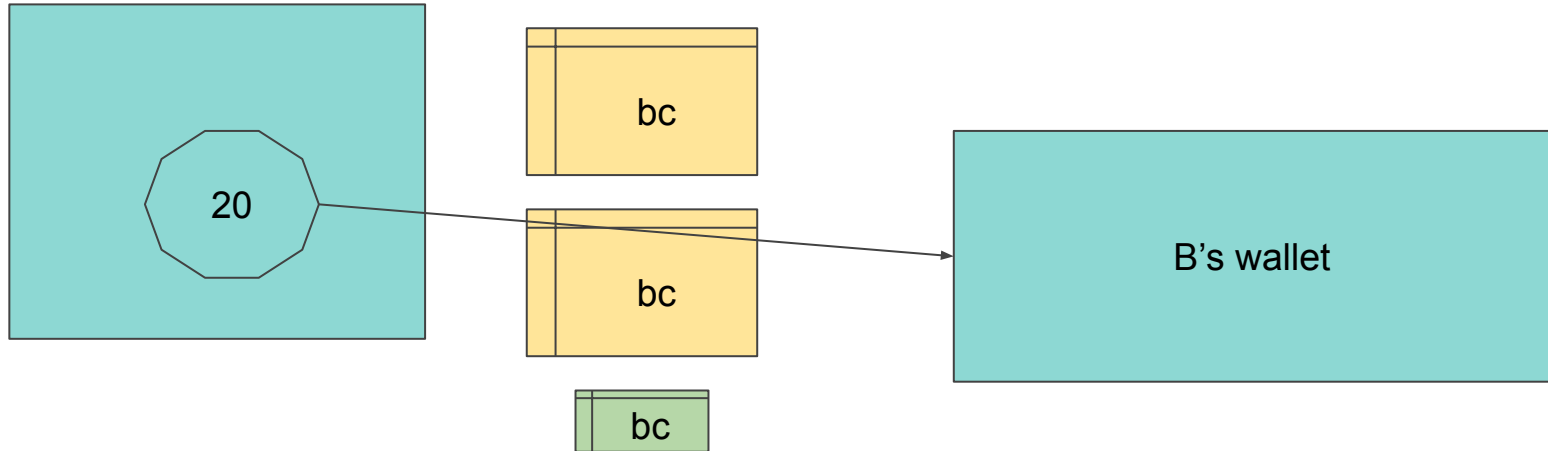
crypto...

A **cryptocurrency**, **crypto-currency**, or **crypto**^[a] is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it.^[2]



Crypto: paying B \$20

The currency is linked not to a physical standard, but to a cryptographic one. The transactions are held encrypted in a ledger - the blockchain - . You can't forge it because you cannot decrypt the blockchain, copies of which are held everywhere



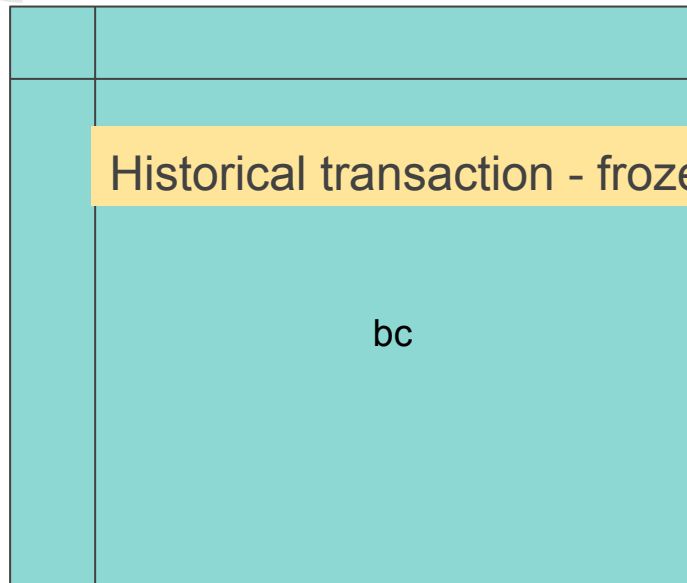


The blockchain

Satoshi Nakamoto?



TRANSACTIONS



A pays B **₿**2000 - forged

Current state signed
+ **A pays B ₿20**+cryptosignature



blockchain

A blockchain is “a distributed database that maintains a continuously growing list of ordered records, called blocks.” These blocks “are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.



Security and safety of currency?

Depends on cryptography.

Current web shopping and cryptocurrency depend on cryptography - factorising numbers which are the product of two prime numbers (public and secret keys)

How difficult is:

Factorise 21

Research on prime numbers suddenly a hot topic.



..what if the blockchains differ?

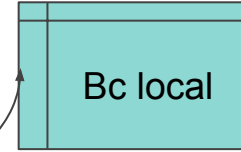
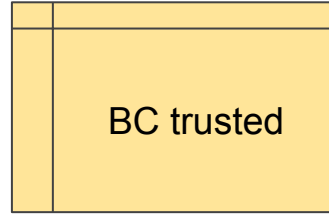
l.e. there is no consensus

forgery...

How are the transactions signed?

A pays B 20

A



A,B,20,202412250800,history,[cryptosigned by A]

Cannot be forged



A bicycle makes a blockchain

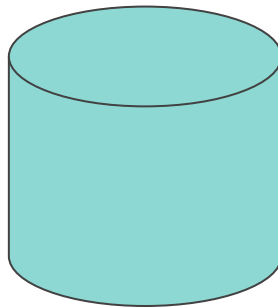
```
{'asset': {'data': {'bicycle': {'manufacturer': 'bkfab', 'serial_number':  
'abcd1234'}}}},  
  'id': 'bfe679e84f528410270fe67d309f19d03afe09970650140621daedfe6f546598',  
  'inputs': [{'fulfillment':  
'pGSAIGXrEQNtYgyzOBswGHnoWgbUFWFVE89Kez25zti91PTzgUDY8sy8E9FtHwO9-nab89wBsp  
emhBCshbbRRJqLlqilTQ7HbJZYMfr8_mawfTDre3lpJEgLSrqFU-clmJjkrwUO',  
    'fulfills': None,  
    'owners_before': ['7rr59L64LvwwMKr8dtieotdugk13oHkosFFoTuXCjzz6']}]},  
  'metadata': {'planet': 'earth'},  
  'operation': 'CREATE',  
  'outputs': [{'amount': '1',  
    'condition': {'details': {'public_key':  
'7rr59L64LvwwMKr8dtieotdugk13oHkosFFoTuXCjzz6',  
    'type': 'ed25519-sha-256'},  
    'uri':  
'ni:///sha-256;e2C00fzLhNG_nLwWVmZOyGbIQ6lqDCduYZy7HKPr23c?fpt=ed25519-sha-  
256&cost=131072'}},
```



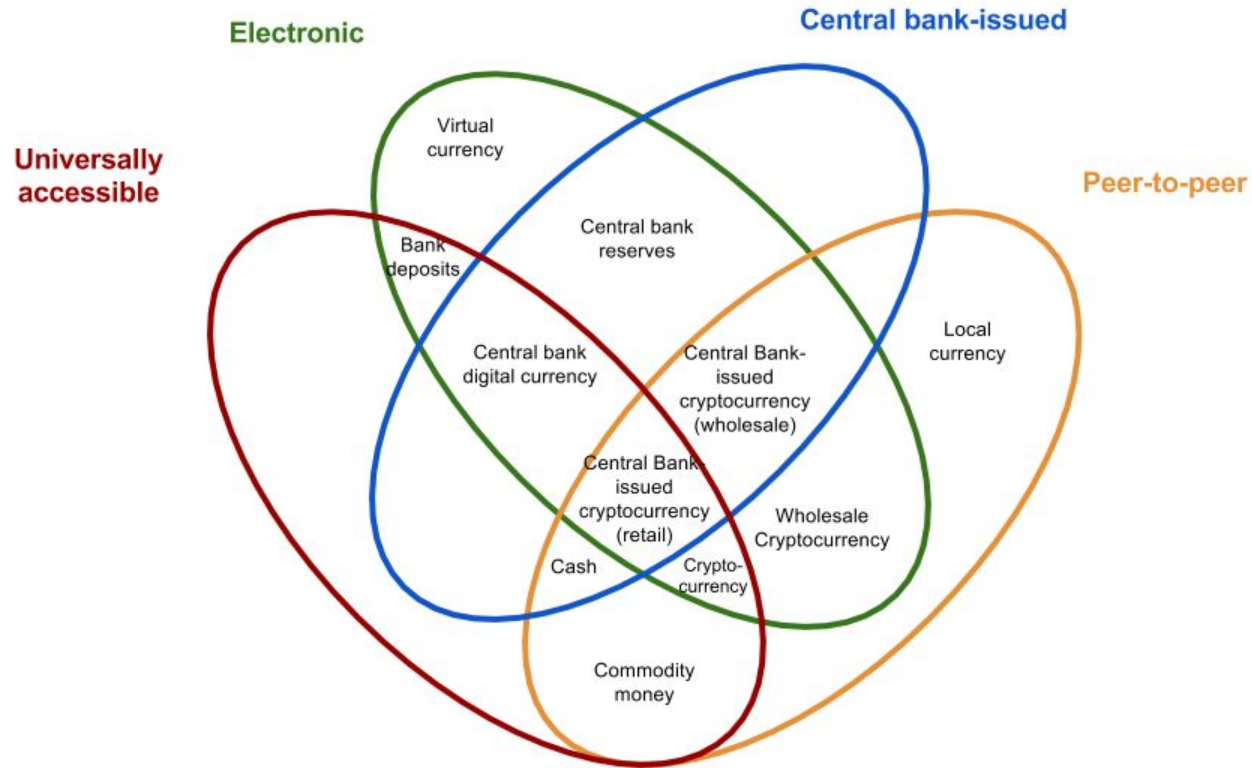
What is a blockchain

A blockchain consists of several key components:

- **distributed Ledger**
- **Blocks**
- **A Cryptographic Hash**
- **A Consensus Mechanism**
- **Mining**



The money flower: a taxonomy of money





Digital currencies

Bitcoin

Ethereum

Ripple

Litecoin



Crypto problems

- Accounting standards
- Lack of state support- e.g. CGT?
- Volatility
- Complexity esp. Mining



Bitcoin mining

- Software
- 21 million bitcoin to be made
- Mining is competitive
- When mining ceases - dealers



Exchange rates bitcoin to USD





Bitcoin dealers and storage

Search

Discover > Crypto > Coins > BTC



BTC • Bitcoin

65065.26 -712.04 (-1.08%)

Market Open • IN USD



Trade

 Overview

 Chart

 Analysis

 News

 Financials

Bitcoin price

▼ -5.44% Past Week



Never Trade Crypto Alone

Join millions who've already discovered smarter investing.



Storage



Google Play

Games

Apps

Movies & TV

Books

Bitcoin Wallet

Bitcoin Wallet developers

3.6★

33.6K reviews

5M+

Downloads

3

PEGI 3 ⓘ

Install



Share



Add to wishlist



This app is available for your device



TAX

CGT

Income Tax

...complicated...