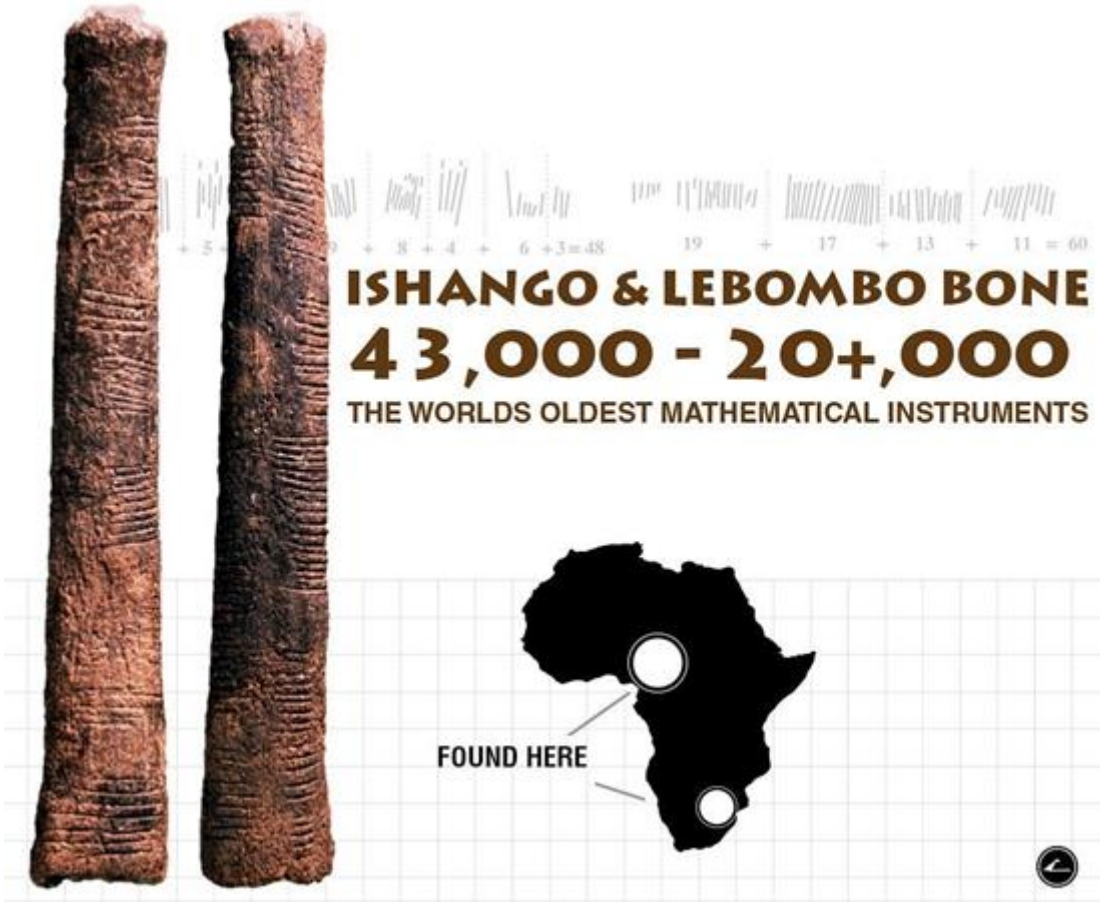
Blockchain

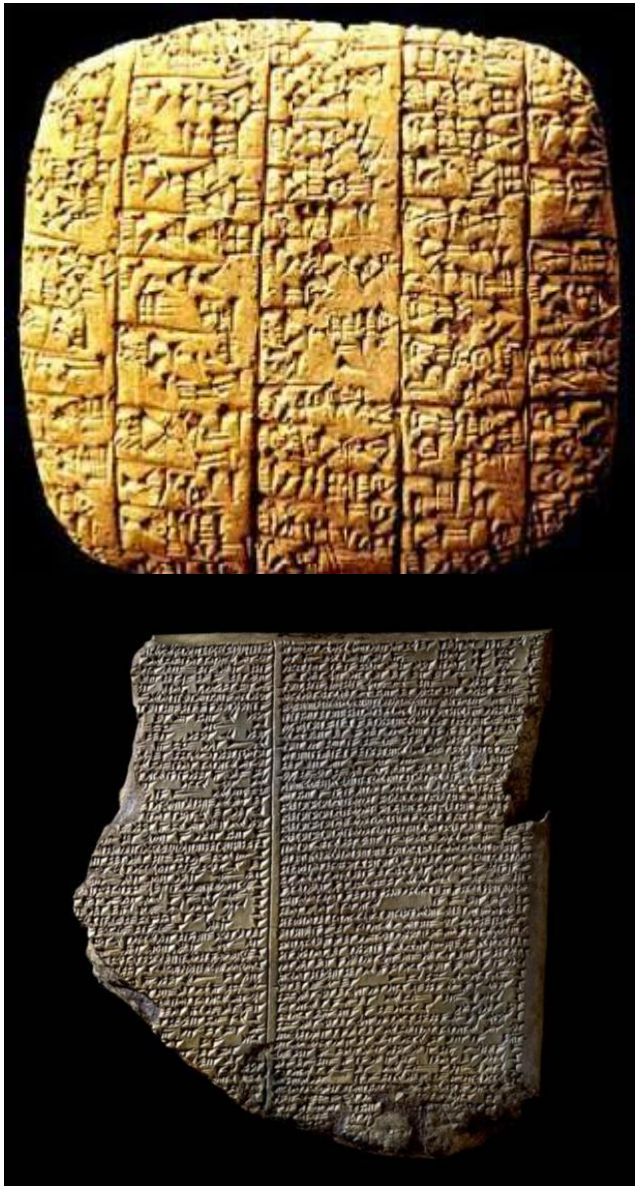
A suitable technology in a Research Information context?

technology
financial
cryptography
network
digital
currency
litecoin
finance
transaction
cryptocurrency
internet
Blockchain
data
bitcoin
coin
contract
crypto
smart
protocol
payments
money
exchange
market
business
electronic
virtual
node
concept
ledger
cash

A short introductory historic overview of record keeping



Assyrian Clay Tablets



Egyptian alphabet for record keeping

glyph	translit.	phonetic
	ꜣ	[ʔ]
	i	[i]
	y	[y]
	ꜥ	[ʕ]
	w	[w]
	b	[b]
	p	[p]
	f	[f]
	m	[m]
	n	[n]
	r	[r]
	h	[h]

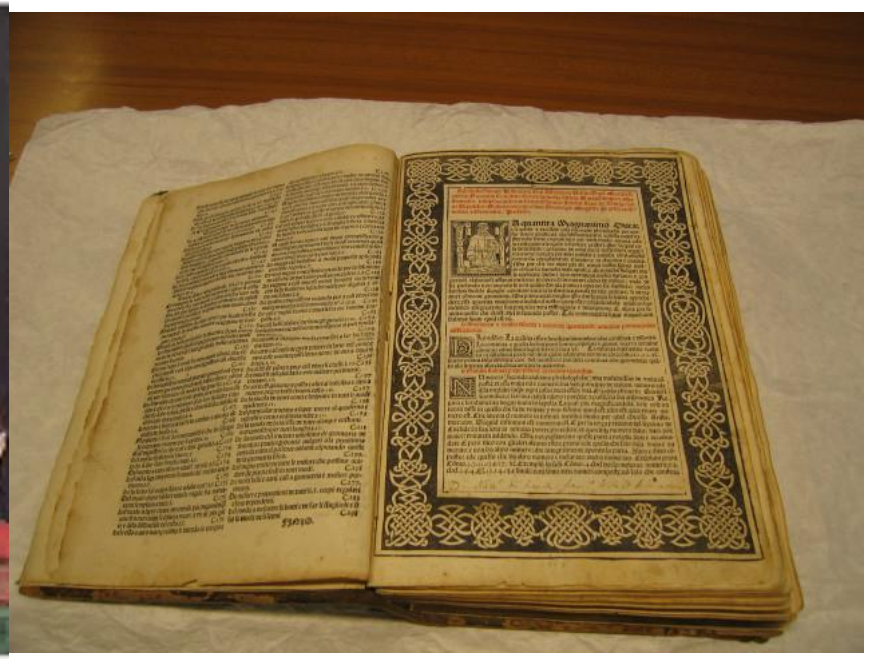
glyph	translit.	phonetic
	ḥ	[ħ]
	ḫ	[x]
	ḫ	[ç]
	s	[s]
	ś	[ʃ]
	ḳ	[q]
	k	[k]
	g	[g]
	t	[t]
	ṯ	[tʲ], [c]
	d	[d]
	ḏ	[dʲ], [ɟ]

DEPARTMENT OF
ECONOMY, SCIENCE & INNOVATION

Flanders
State of the Art

Double Entry Book Keeping

Luca Patioli



Summa de arithmetica, geometria, proportione et proportionalita, 1494

The central ledger AKA the database

- **Assets are booked in a propriety ledger**
- **Transactions between two party at remote location require a trusted 3rd party or intermediary**

  → E.g. financial transaction across the border
- **Double spending is possible**
- **The central authority of the ledger is also a single point of failure**

The Database

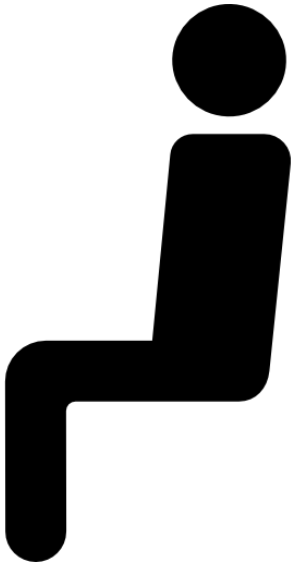
- **Digitalisation by the implementation of classical database inherited the fundamental weaknesses of the central ledger**
  - E.g. Security : a layer on top of the database core

Blockchain

Bitcoin: A Peer-to-Peer Electronic Cash System

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

- Posted on the The Cryptography Mailing list
- First one to solve the double spending problem



Bitcoin ≠ Blockchain

- **Bitcoin charaterisctics**
  - → Digital Currency Minting system
  - → Digital Currency Payment system

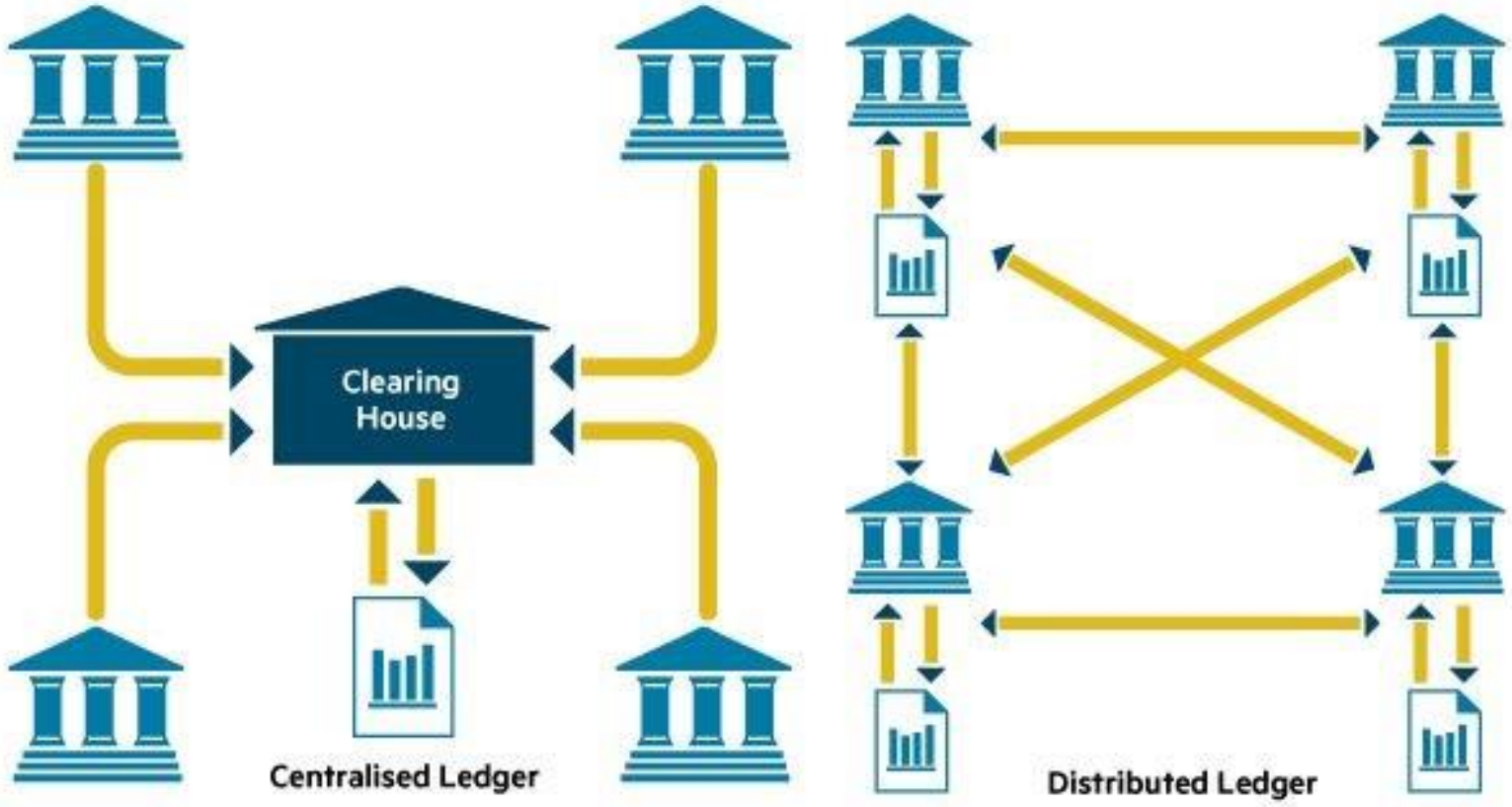
- **By design Bitcoin uses a Blockchain database**
  - → Peer to Peer network of databases recording ownership through time
  - → Transactions cryptographically concealed in blocks
  - → Block of transactions cryptographically connected in a chain

Blockchain explained in less than 3’

- https://vimeo.com/206253172

Embedding distributed ledger technology

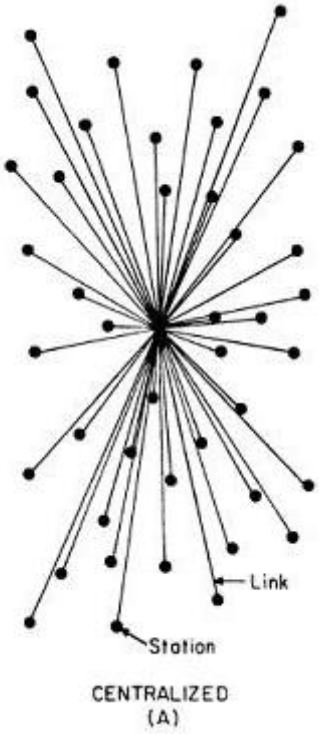
A distributed ledger is a network that records ownership through a shared registry



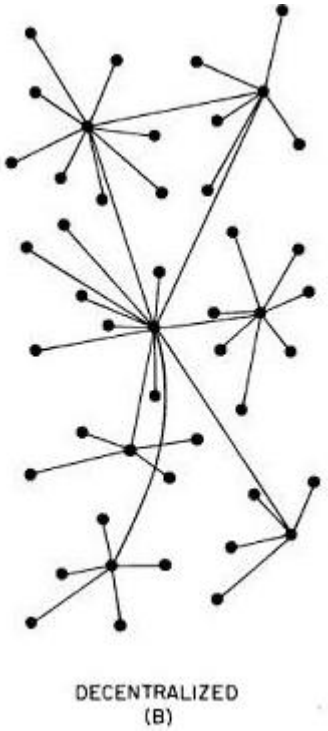
In contrast to today's networks, distributed ledgers eliminate the need for central authorities to certify ownership and clear transactions. They can be open, verifying anonymous actors in the network, or they can be closed and require actors in the network to be already identified. The best known existing use for the distributed ledger is the cryptocurrency Bitcoin

FT graphic. Source: Santander InnoVentures, Oliver Wyman & Anthemis Partners

All organisations



Internet & Bitcoin



Problems	Solutions
Central Point of failure	Decentralized network
High security cost	Security costs shared
Need of Trusted party	Trust = fixed set of rules

Characterizing components of Blockchain

Replicated ledger

- History of all transactions
- Append-only with immutable past
- Distributed and replicated

Cryptography

- Integrity of ledger
- Authenticity of transactions
- Privacy of transactions
- Identity of participants

Consensus

- Decentralized protocol
- Shared control tolerating disruption
- Transactions validated

Business logic

- Logic embedded in the ledger
- Executed together with transactions
- From simple "coins" to self-enforcing "smart contracts"

Characteristics of open Blockchains

- **Censorship resistance**
- **Decentralization**
  - Anyone can own a copy of the open blockchain
- **Security is by design**
  - Shared by people and companies
    - The Network will see and reject fraud
- **Immutability by design**
  - Consensus mechanism
    - Proof of Work
    - Proof of Stake
- **Open Access**
  - Open to anyone without identification or authentication
- **Open Innovation**
  - New application development is open

Open Blockchain

- **Trade off**
  - Inefficient Database
    - Limitations on the number of transactions
  - Consensus mechanism
    - Proof of Work
      - Power intensive
- **Use**
  - Currency Mining with mathematical consensus mechanism

Private Blockchain

- **Characteristics**
  - → Interoperability
  - → Permissioned access
  - → Editability
  - → Centralization
  - → Business Innovation

- **Use**
  - → When social consensus models are preferred
    - Proof of Stake
  - → Not for currency or Mining
  - → Within organisations
    - Intranet >< internet
    - Financial institutions, Corporate, Governments, Cross-Industry

The Blockchain disruption

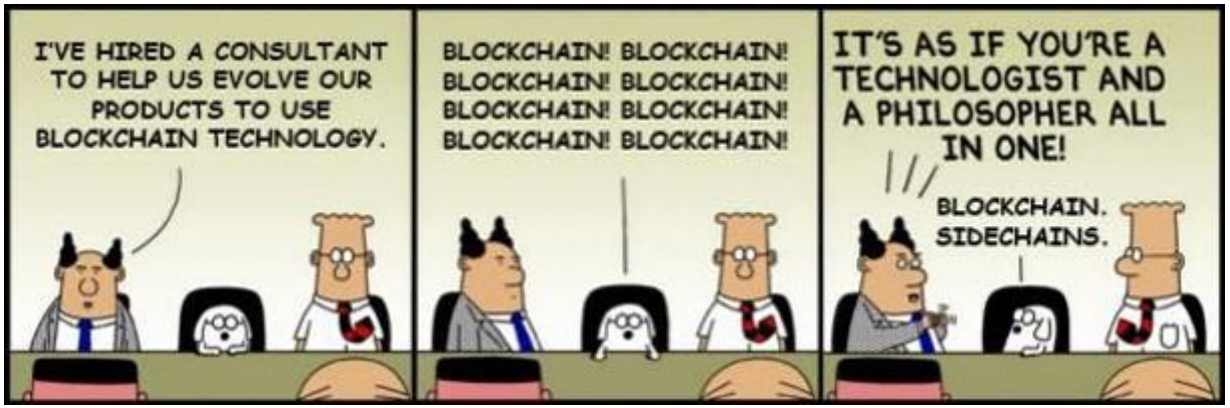
- **Substantial decrease in intermediaries**
  - → Elimination of
    - single points of failure
    - Undesirable monopolies
  - → Transparent and decentralized nature
  - → Records of data
    - Non-refutable
    - Unbreakable
- **Fraud resistance by design**
- **Real-time open access to all information**

All admirable characteristics of a Science system

Is Blockhain the new Nirwana

- **Blockchain is a database technology**
  - → With a radical different paradigm
  - → Quite young but moving form the proof of concept to the pilot project stage
  - → Developments are going fast

- **Not all use cases require blockchain as a solution**
  - → Care is needed



Use Cases

- Gideon Greenspan, Multichain

  Clear differences between blockchain and a centralized database

- Disintermediation. Blockchains enable multiple parties who do not fully trust each other to safely and directly share a single database without requiring a trusted intermediary.

- Confidentiality: All participants in a Blockchain see all of the transactions taking place.

"Blockchains represent a trade-off in which disintermediation is gained at the cost of confidentiality"

A blockchain use case

Use Case: Scientific Communication

- Actual research output cycle is does suffer from undesirable effects of intermediaries
  - → High level of friction
    - Publication cost
  - → Goal misalignment
    - Profit vs advancement of knowledge
    - Research organisation vs researchers
  - → Monopoly creation and exploitation
    - Publications
    - Identifiers
    - Central repositories of all kinds
  - → Profound measurement skewing

CRIS Systems are unfortunately embedded in this logic

A prototype

THE "FLAWS" OF THE CURRENT PROCESS

As a researcher

- You have no idea who reviews your article
- Future evolutions in the same research field can't be linked a posteriori
- You loose your IP on the article as it is published
- Referrals to your own work sponsor the publisher

... and this, for subsidised research

PROPHETS

HOW CAN WE RE-INVENT THIS PROCESS?

Aiming for a system in which all parties are rewarded based on their contributions throughout the flow.

Challenges

1. Is blockchain the right technology
2. How to exploit the advantages of blockchain without compromising usability
3. How do we make sure our reviewers are who they say they are
4. How do we automate the impact measurement of an article after the review process
5. How do we market such a platform

PROPHETS

THE BIRTH OF nabu

Validating scientific research based on peer reviews.

nabu FACILITATES A 100% TRANSPARENT TRANSACTION BETWEEN 'STRANGERS'.

Prof X in expert field A

Transaction:

- reviews
- citations
- comments
- expertise
- upvotes

Prof Y in expert field A

PROPHETS

STRUCTURALLY DIFFERENT BASED ON 5 CRUCIAL PRINCIPLES

- The entire **peer review process is transparent**
- There is **no central authority** that influences reviews
- Articles are open for **permanent reviews**, as knowledge keeps evolving as well
- **IP sticks to the author(s)**, and is not passed on to the publisher
- Continuous, qualitative reviews leads to **more expertise, rewards and exposure for reviewers**

PROPHETS

How to exploit the advantages of blockchain without compromising usability

BY MAKING THE SIGN-UP EASY

- Making use of a standard sign-up procedure
- Ether wallets in the background
- Accessible for everybody, even people without a degree

PROPHETS

How do we make sure our reviewers are who they say they are…

BY ADDING AN AUTHENTICATION LAYER

Attribute expertise (points system) based on:

- Peer to peer accreditations from within a specific research domain
- Collaborations from previously published articles
- Multiple reviews within a single research domain

PROPHETS

How do we automate the impact measurement of an article after the review process

BY RANKING THE ARTICLE BASED ON THE PROFILES OF THE REVIEWERS

- As we know who is part of the review process
- We take the sum of their value
- We multiply it with the amount of upvotes of their review
- We dynamically keep rating each article

HOW DO WE VISUALIZE THE VALUE OF AN ARTICLE

- Reviewed by 300-500-1000-5000 expertise points
- Most read
- Most revisioned
- Stayed relevant over time
- Cited 1-3-5-10-20-50 times

PROPHETS

How do we market this

NOT BY SAYING IT'S A BLOCKCHAIN APP!

No thanks!
We are too busy