
The economics of (self-sovereign) identity

Alastair Berg

Blockchain Innovation Hub

RMIT Blockchain Innovation Hub

sites.rmit.edu.au/blockchain-innovation-hub/

What I'm going to do today

- Briefly introduce institutional cryptoeconomics
- Characterise identity as a peculiar co-produced economic good
- Characterise identity as an input into contracting
- Talk to the current state of identity, and how we got here
- Define self-sovereign identity
- Talk about why identity technologies and institutions are important

Institutional cryptoeconomics

An economy is made of ledgers

When ledger technology changes, so does the world

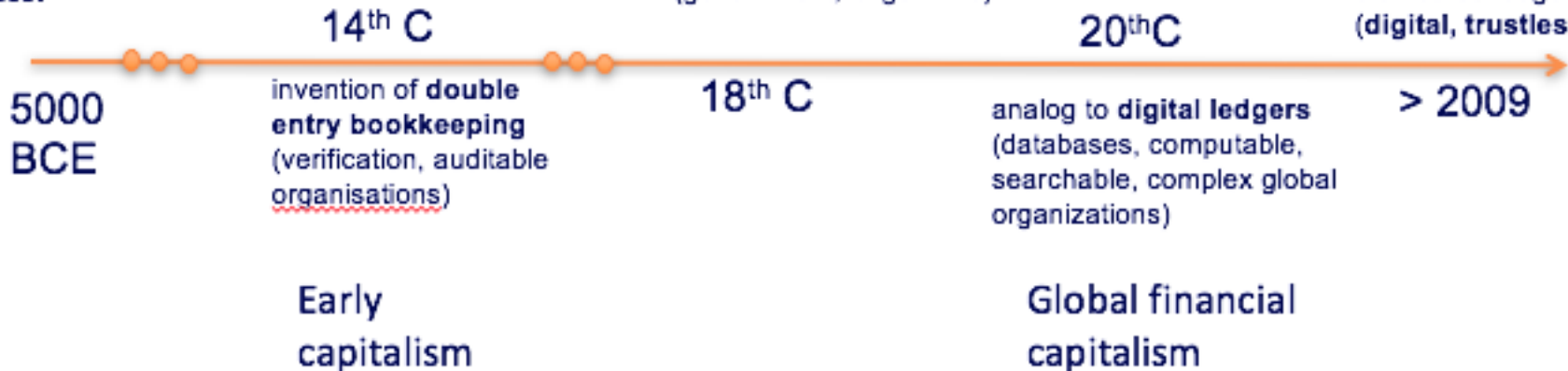
Market society

Empire capitalism

Ledgers & writing
simultaneously
emerged to record
production, trade,
debt

centralised distributed
ledgers – trust in
centralised institutions
(government, large firms)

decentralised (P2P)
distributed ledgers
(digital, trustless)



Institutional cryptoeconomics

- Blockchains are enormously successful proof of concept around distributed ledger technology
- A ledger is a tool for mapping and verifying agreed facts about relationships
- Ledgers are everywhere
 - Bitcoin has shown us that money is a ledger
 - Property rights are ledgers (see Hernando de Soto)
 - A firm is a ledger, structuring capital, labour and processes
 - The social security system is a ledger
 - Citizenship is ledger

Identity is a co-produced good

- Identity and identity verification is an economic coordination problem

A co-produced good

- **You produce** some identity information
- Others (people and things, firms and governments) produce information **for you**
- **Others validate** information you produce
- Yet others (you don't know who) add **information you don't see**

Identity is very peculiar

- It's an **information good**
- It's a **quasi-public** good
- It's **socially** produced
- It has a **network** production function
- It is (or often is) '**append-only**'
- It has an **asymmetric information** production process

Identity as input to contracting

Exchange

- Any (most) transactions involves **money**, **good/service**, and **identity**
- Money to carry **value**
- Identity to secure and validate counterparty in a world of **asymmetric information** and **opportunism**

Technology

- Limit of the market is determined by **identity costs**
- Identity technology as a **privately and publically produced good**
- **Bundling of identity attributes** as a result

Oversupply of a public good

Bundling

Minimal attributes based on context and preference



Self-sovereign identity

- Loffreto, Devon. 2012. What is "Sovereign Source Authority"? The Moxy Tongue.
- Allen, Christopher. 2016. The Path to Self-Sovereign Identity.

- Existence
- Control
- Access
- Transparency
- Persistence
- Portability
- Interoperability
- Consent
- Minimalisation
- Protection



CURRENT MODEL OF IDENTITY



SELF-SOVEREIGN IDENTITY

Hasso-Plattner-Institut

What does this mean?

- **Blockchains** to store and act as **(censor resistant)** infrastructure for sharing **decentralised identifiers (DID)**
- Stored **verified claims** reduce capacity for surveillance
- New ways of organising **relationships** and **contracting**
- Less **information asymmetry** with **more privacy**
- **Banking sector** (and other 'trust' institutions) becomes less and less necessary for contracting relationships

Questions?

Alastair Berg
Blockchain Innovation Hub