



Blockchain: Overview, Applications, and Meaning for Identity, Verification and Trust

John Leslie King

jlking@umich.edu

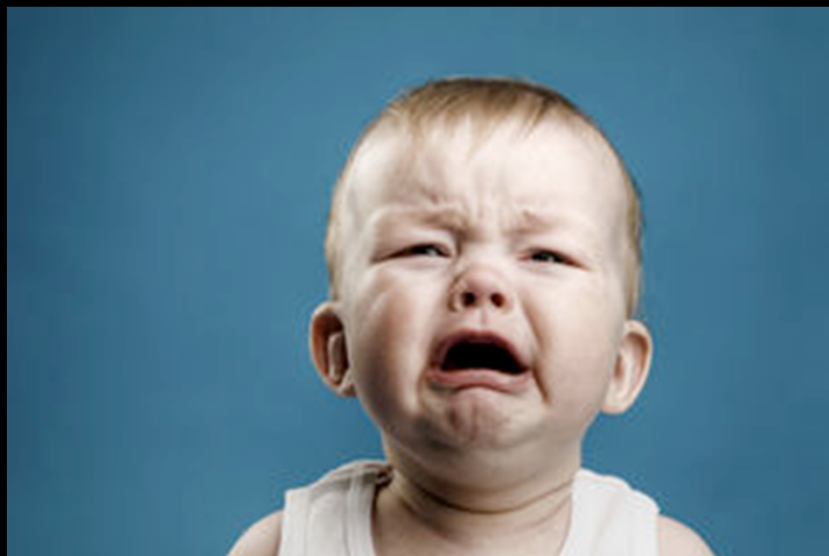


Standard disclaimer: Nothing in the visuals for this presentation has been cleared for copyright and is presented as classroom presentation under fair use provisions of US copyright law.

Two years old

Bubble memory

Nuclear weapons



Learning

Technical articles_____

**Megabit bubble-memory chip
gets support from LSI family**

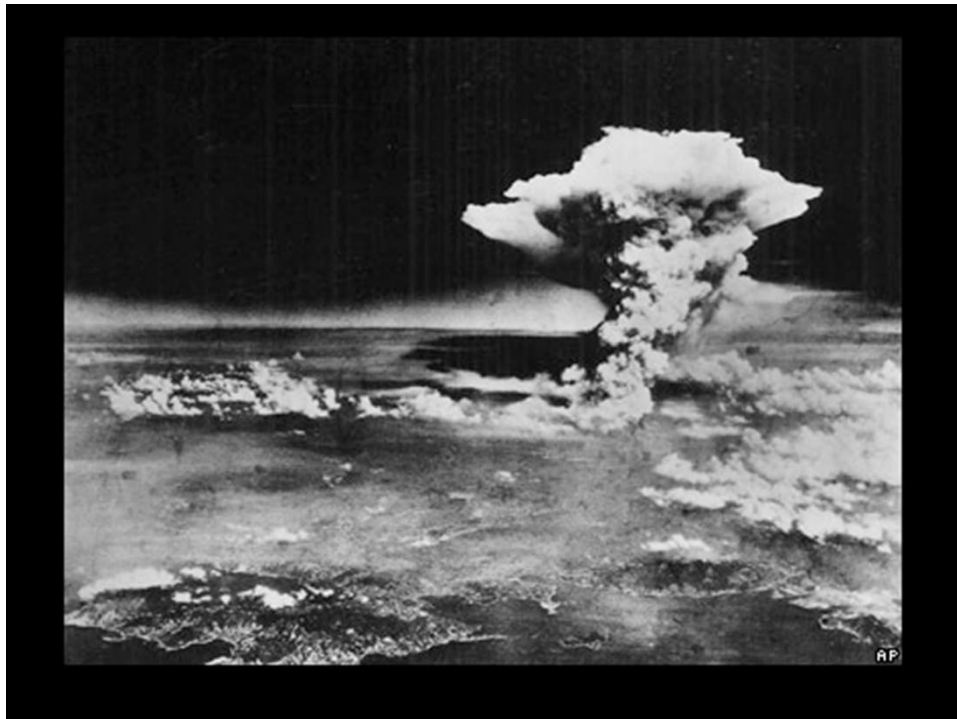
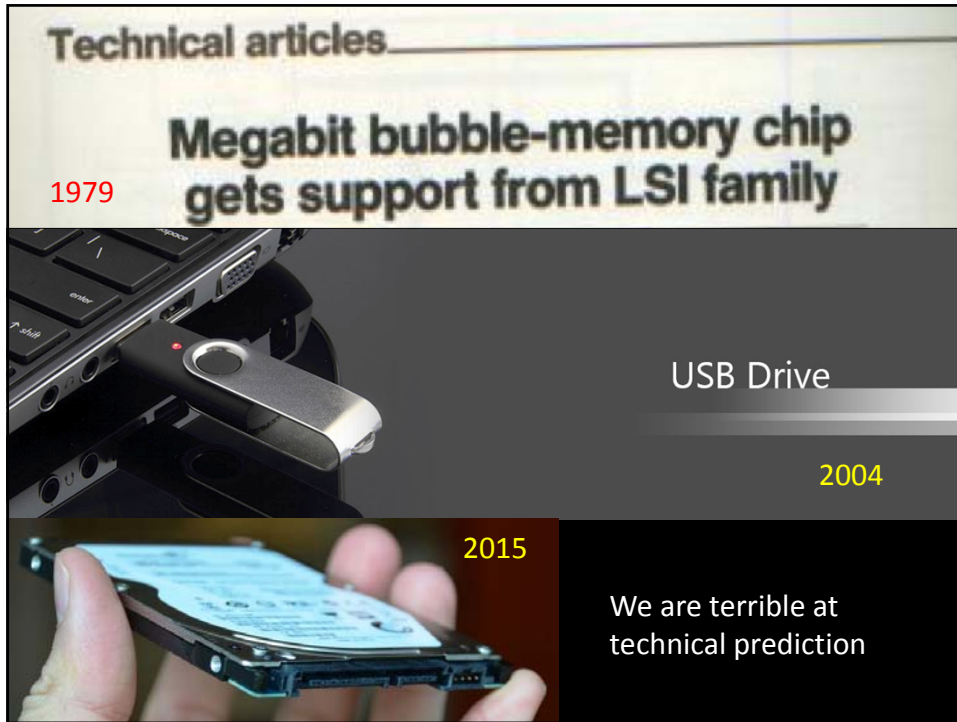
1979

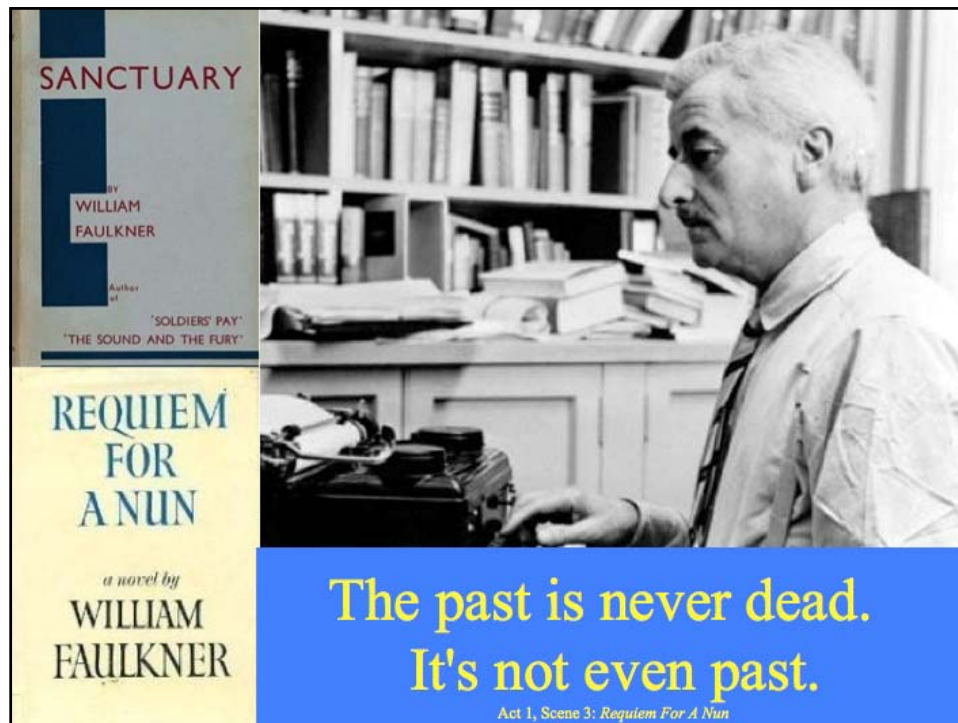
USB Drive

2004

2015

We are terrible at
technical prediction







The relationship between technical change and social change

Highly-institutionalized production sectors of the economy/society

Evolving the Social in the Socio-Technical System of Blockchain

John Leslie King, University of Michigan
Dagstuhl Seminar, March 26-29, 2017

Blockchain technology seems promising in its own right, and might be “disruptive.” We have a poor track record predicting what new technologies mean over the long run, and an even poorer record knowing in advance what is truly disruptive. However, there is considerable experience with social evolution. Blockchain is already a socio-technical system. Even if Blockchain technology enables changes in the social, prediction of technology is flawed. The evolution of some aspects of the socio-technical system is easier to predict. Often the social is more important than the technology in the evolution of the socio-technical system.

Blockchain – *qu'est-ce que c'est?*

- Distributed ledger system (DLS), log of transactions (the transfer of land title in a land registry, smart contracts, etc.)
- Hash-linked chains of valid data blocks,
- Linear or directed acyclic graph, not a tree
- Consensus mechanism
- Decentralization or hybrid
- Permanent, unchangeable record

Blockchain – Applications

- Payments (e.g. , Bitcoin) and credit registry
- Proof of ownership (e.g., land, cargo, entertainment, software)
- Smart contracts (e.g., Ethereum, pensions)
- Digital identity (LifeLog, certified CVs, access management, education certificates)
- Data Storage (e.g., Government Records)
- E-voting

Blockchain – Unresolved

- Governance (e.g., consistency vs. consensus)
- Serialisation (e.g., changing locks on property)
- Insuring security (e.g. access control)
- Network design (e.g., ideal topologies)
- Upper/lower bounds (e.g. P/NP, scalability, time to consensus, concrete complexity)
- Risk and cost to remedy
- Storage, linearization, and other options
- Managing conflict (back to governance)

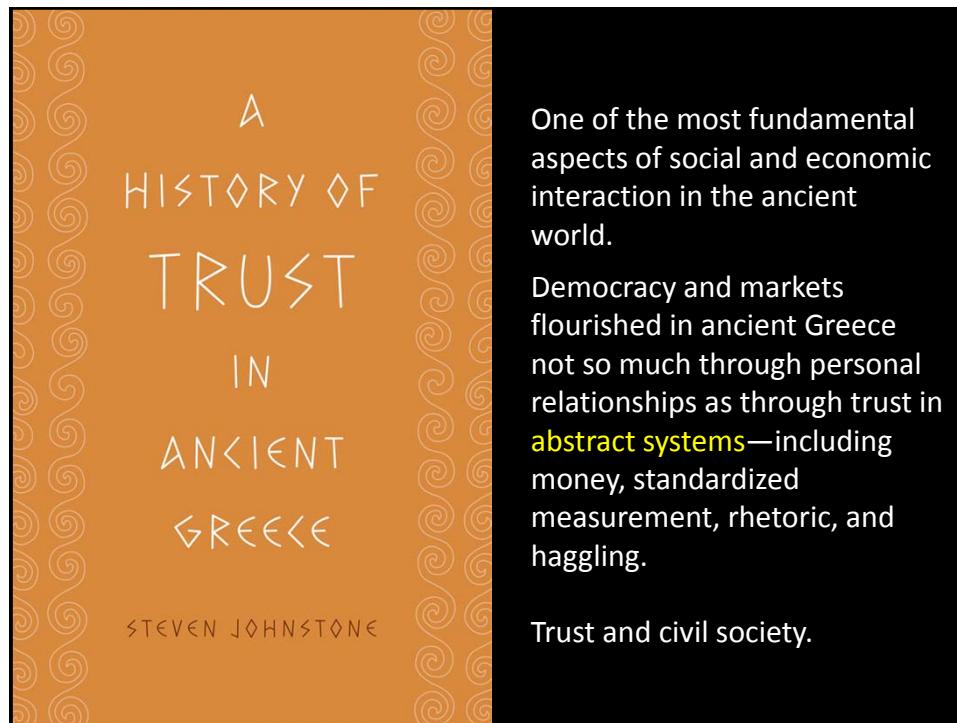
Blockchain and Trust

- Institutions carry trust
- Disintermediation of institutions
- Elimination of trust

I don't *think* so

This talk is about why...

Trust is ancient



1

Managing Distance over Time: The Evolution of Technologies of Dis/Ambiguation

John Leslie King and Robert L. Frost

The management of distance is as old as work itself. Successful management of distance requires a careful balancing of disambiguation and ambiguation in the construction of meaning among disparate parties in collaboration. We argue that current efforts to develop technology for improved management of distance concentrate almost exclusively on improving means of disambiguation. This strategy overlooks the subtle but crucial role of ambiguation in maintaining shared understanding while allowing local discretion. We explore four successful technologies of dis/ambiguation that have evolved over centuries: writing and money as examples of disambiguating technologies, the doctrinal traditions of the Roman Catholic Church, and the creation of constitutional government as examples of ambiguitating technologies.

Hinds and Kiesler (eds.), *Distributed Work*, MIT Press, 2002

Trust

It goes deeper

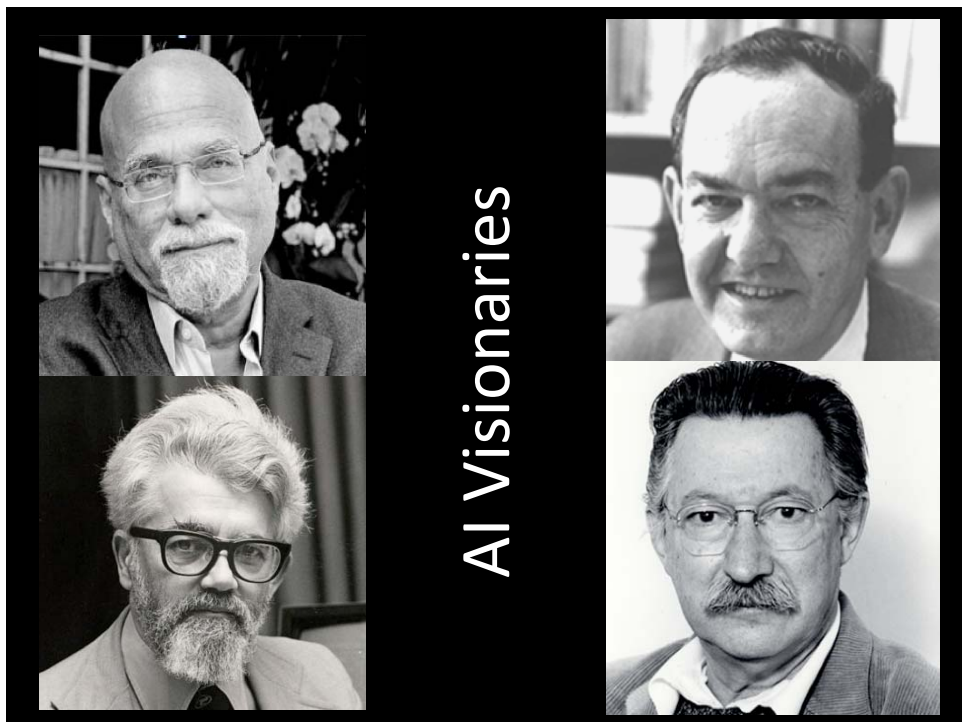
Is more amazing

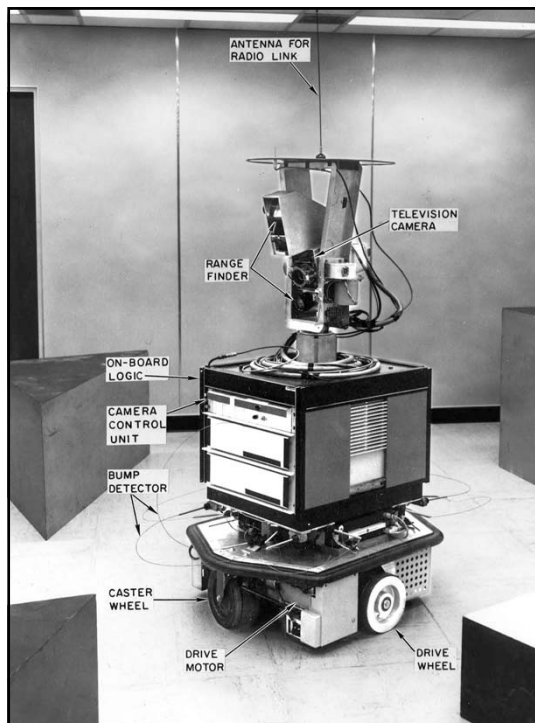
Is more human

Blockchain will teach us

An Historic Analog

- Natural language processing, 1950-1980
- Early days of computing
 - General purpose
 - Great power
- Unified theories of language
 - Chomsky's models





Shakey
the Robot at
SRI ~1968

“In from three to eight years we will have a machine with the general intelligence of an average human being... able to read Shakespeare, grease a car, play office politics, tell a joke, and have a fight. At that point, the machine will begin to educate itself with fantastic speed. In a few months, it will be at genius level and a few months after that its powers will be incalculable.”



Marvin Minsky
1970

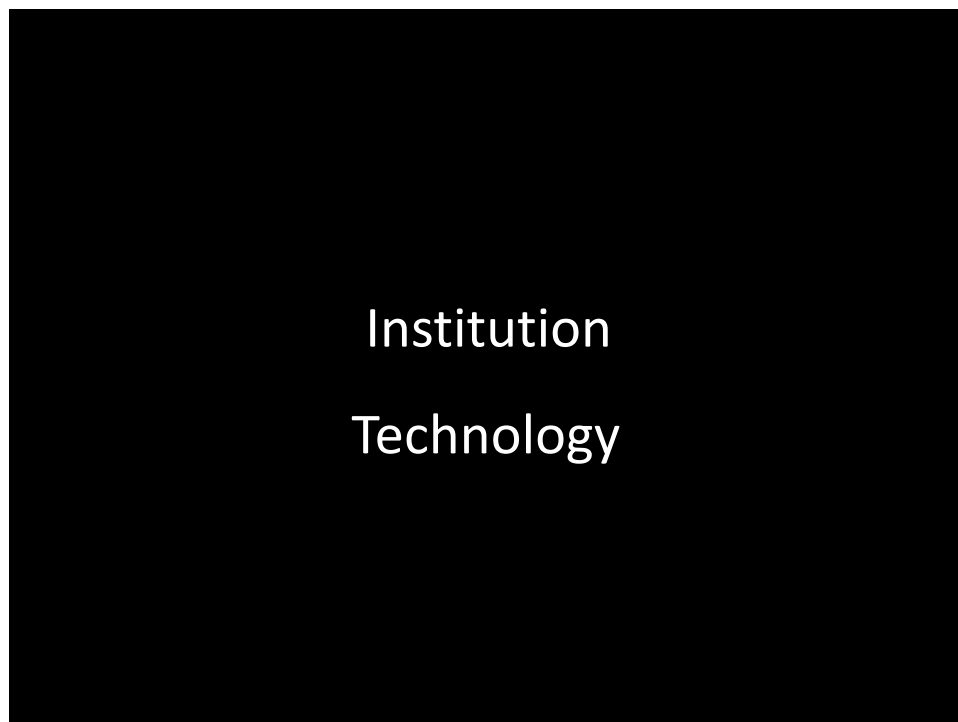
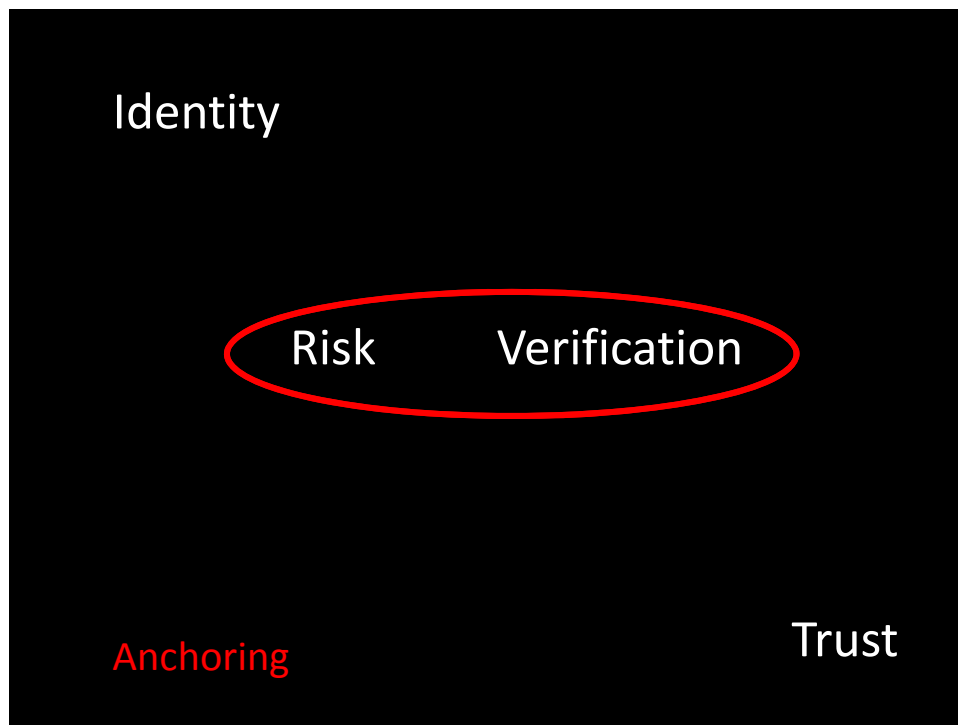
John visited his mother in hospital
and took her flowers.

Context

Research Start Ups

Reduced-Form Argument

- Trust is hard to understand
- Perturbing it will teach us more
- Knowing more will help design



Highly-institutionalized production

Constitutional	Order and Redress Legislation Law
Procedural	Law enforcement procedure Legal procedure Review and regulatory process Standardization process
Epistemological	Peer review Adjudication of Truth Warrants Honorifics

Institutions

- No way to avoid
- Getting ready
- Look at analogs
- Look at genuine differences
- Institutions will not handle all issues
- Mitigating harm

35

Questions

- Who decides what is stored in ledger?
- Who is granted or grants identifiers?
- Who has identifier information and
Who matches individual identifiers?
- A single truth?
- Security and risk behavior?
- System vs. actor relationships?
- Transparency, privacy, etc.?
- Disruption of incumbents?

36