An Infrastructure for Truth
Entrusting Digital Facts to Archival Theory

Luciana Duranti, Director, The InterPARES Trust Project

ICA –ALA Conference

Mexico City, 27 November 2017

Today Issues

- **Post-Truth**: "relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief" (Oxford English Dictionary, 2016)
- **Alternative Facts**: a version of facts different from the one provided by the official sources
- **Disinformation:** information that is incorrect by design and used by those who wish to spread confusion and deceit by using emotions as well as alternative version of the facts
- **Misinformation**: Information that is incorrect by mistake

InterPARES Trust

What is New?

- The 'always on' **connectivity**, that lets falsehoods as well as erroneous information circulate at rates unimaginable only a few decades ago
- The **pervasiveness** of distribution channels through social media
- Technical infrastructures are increasingly **complex**, often invisible, and **hidden**
- The **lack of trust** in traditional institutions in favor of a populism where reputation as a trusted source no longer carries much, if any, weight

The Case in Point

Truth vs. **Trust**

- The **historical truth** is not directly accessible: facts and acts slide into the past as they happen
- There are two ways of indirectly accessing the past: witness testimony and the **documentary truth** represented by the written accounts of the facts and the material instruments of the acts, the **records**
- In both cases, what we will regard as truth will entirely depend on our trust in its source

InterPARES Trust

What is Trust?

- Some view it as a four-level progression: from **individual**, as a personality trait, to **interpersonal**, as a tie directed from one person to another (son to father); to **relational**, as a property of a mutual relationship (people doing business); and **societal**, as a feature of a community as a whole.
- InterPARES Trust defines it as confidence of one party in another, **based on alignment of value systems with respect to specific actions or benefits**, and involving a relationship of voluntary vulnerability, dependence, and reliance, based on risk assessment
- Substantially, trust involves acting without the knowledge needed to act, by **substituting the information that one does not have with other information**, e.g. the testimony of witnesses, oral tradition, documentary truth

Documentary Truth

Archives are the whole of the documents which are made or received in the course of activity (i.e. **records**), and which are kept for further action or for reference by their creator or its legitimate successor (including a heritage institution).

Records are instruments for and by-products of action. They are the primary sources of evidence for any kind of research because they were not produced to answer the questions we ask of them today but as a means to act.

InterPARES Trust

Records, Archives and Truth

In the context of **written cultures** (and I use the term written in the diplomatic sense of information affixed to any medium in any form to transmit it across space and/or through time, including for example Peruvian quipu)

- records and archives form the infrastructure through which beliefs and values are upheld and understood;
- they provide **evidence** of facts and acts, where evidence is the relationship between a fact to be proven and the fact that proves it.

This has been the case since antiquity.

InterPARES Trust

Archival Concepts in Antiquity

- Records preserve **perpetual memory of the facts and acts** from which they result (as opposed to "about which they talk")
- Records authentication is based on the **procedure** in records' creation and use
- Deposit of records in a **public place** (the place of an authority considered sovereign by a given social group) guarantees their reliability as witnesses of facts and acts
- **Antiquity** provides records with the highest authority with respect to the interests for which they are used today
- The trustworthiness of records can to be verified using **scientific methods** looking at the process of records creation, records form and structure, and transmission through time and space.

Trustworthiness in Archival Science

Reliability

The trustworthiness of a document as a **statement of fact**,

based on:

- the competence of its author
- the controls on its creation

Accuracy

The **correctness and precision** of a document's content

based on:

- the competence of its author
- the controls on content recording and transmission

Authenticity

The trustworthiness of a document that **is what it purports to be**, untampered with and uncorrupted

based on:

- identity
- integrity

InterPARES Trust

Archival authentication

A declaration of authenticity based on either on material proof, inference, or deduction

Let's move from theory to practice: what are the means for authenticating digital facts?

- **A chain of legitimate custody** remains ground for inferring authenticity and authenticate a record.
- **Digital chain of custody:** the information preserved about the record and its changes that shows specific data was in a particular state at a given date and time.
- A **declaration** made by an expert who bases it on the trustworthiness of the system hosting the record and procedures and processes controlling its preservation and use

InterPARES Trust

Technology Dependent Authentication

Digital signature:

- protects **bitwise integrity** (small change in a bit means a very different value presented on the screen or action taken in a program or database)
- verifies a record's origin (**identity**), makes record indisputable and incontestable (**non-repudiation**)
- has been given legal value by legislative acts (e.g., European Directive on electronic signatures) or regulatory bodies (Security Exchange Commission and hash functions)
- is enabled through complex and costly public-key infrastructures (PKI)
- ensures authenticity of information **across space,** not **time**!
- is subject to **obsolescence**, and compounds the problem of preservation

InterPARES Trust

Technology Dependent Authentication

Blockchain technology

- is the underlying technology enabling Bitcoin and many other applications
- is a ledger, i.e. an information store which keeps a final and definitive record of (business) transactions.
- relies upon a **distributed network** and **decentralized consensus**
  - Distributed: all nodes (servers) are equal – no centre(s); no single point of control or attack

Blockchain is a type of distributed ledger technology in which confirmed and validated sets of transactions are held in blocks, which are linked (chained) in a tamper-resistant, append-only chain which starts with a genesis block and where each block contains a hash of the prior block in the chain.

InterPARES Trust

Advantage of a distributed network

Enables **decentralized consensus**

- every participant (node/server) includes every event (transaction, record) in its ledger ("main book"/database)
- consensus is used in order to
  - ensure that all ledgers are exact copies (i.e. are synchronised)
  - **to determine documentary truth**
- An event is valid only if a qualified majority (50%+1 node) agrees upon it

IBM is pushing the British Columbia government to use it for all legal marijuana transactions to ensure shielding from illegal ones.

InterPARES Trust

How Can We Use Blockchain?

Blockchain can be used to confirm

- the **integrity** of a record
- that a record **existed** or **was created** at a certain point in time (i.e. not after being timestamped and registered in the blockchain)
- the **sequence** of records

Is it a **recordkeeping system**? No. It holds the hash of records. The records must still be stored and managed off chain.

InterPARES Trust

Some of the Legal Problems With Blockchain Records

- Proving **reliability** (and therefore enforceability)
- Preserving the **archival bond** (and thus contextual evidence)
- Handling the **decentralized** (and thus trans-jurisdictional) nature of the blockchain
- When the records result from **smart contracts**, dealing with code

InterPARES Trust

Records/Archives in a Blockchain-based system

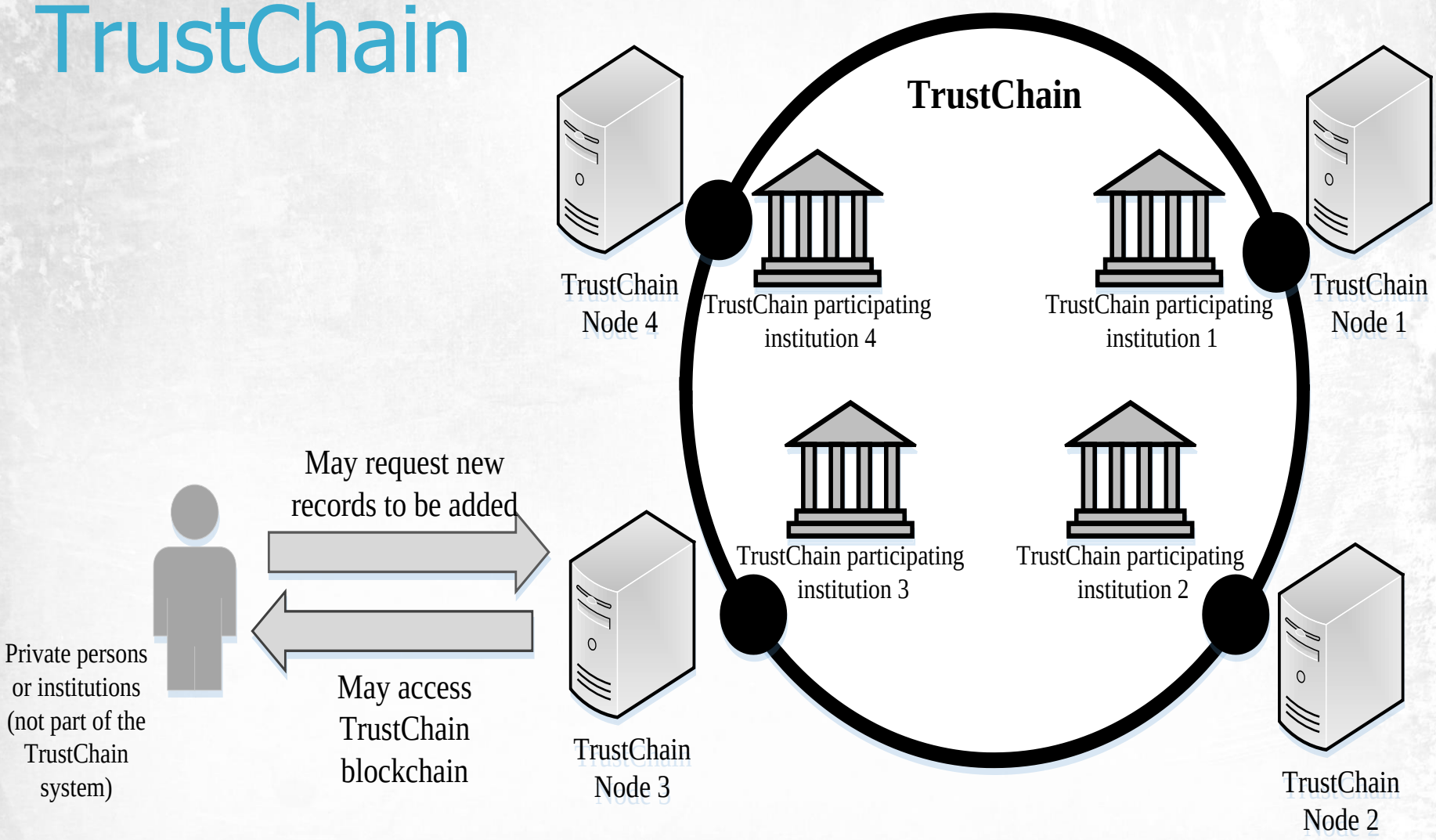
- InterPARES TRUSTER Preservation Model
  - Blockchain-based system called "**TrustChain**"
  - **VIP** (**V**alidity of **I**nformation **P**reservation) **solution**
  - Applies the concepts of
    - hash algorythms
    - Merkle tree
    - blockchain
    - distributed consensus
  - Presumptions:
    - private blockchain
    - only approved nodes can write
    - everyone can read

InterPARES Trust

TrustChain

- The proposed **TrustChain** system
  - relies on the involvement of a **group of trusted archival institutions**
  - would work **in concert with the recordkeeping and archival preservation systems** along the lifecycle of the records
  - would provide confirmation of **integrity**, time of **creation/existence**, **sequence of records**, **non-repudiation**, **validity of e-signatures** whose certificate has not expired
- We are also working on
  - development of a blockchain terminology database
  - ISO/TC 307 Blockchain and distributed ledger technologies standard

TrustChain



InterPARES Trust

Bill Maher, University of Illinois, stated:

"past practices and canons should not be automatically or peremptorily discarded. The fact that those practices no longer seem to apply or do not seem to cover present circumstances should be the start of conversation, not the end. They should not be simply considered as old school detritus but instead noted as lessons in how transient may be the dogmas we embrace today."

Getting to the Truth

One of the means to access the historical truth is the **documentary truth,** but understanding **whose truth** we are dealing with requires to

- use traditional archival principles, concepts and methods
- collaborate with technology experts while cultivating our disciplinary and professional knowledge
- produce functional requirements, tools, methods, and guidelines to ensure people's ability to access complete factual information based on authentic, accurate and reliable contextualised records and archives, and

If we build it, will they come?

I do not think so! We must develop

- **tools** to "nudge" people towards our infrastructure for documentary truth (e.g. slicing and dicing it for targeted audiences), just like Facebook did
- a **blueprint** for characterizing our infrastructure to potential users, just like Google did
- capabilities enabling people to easily trace, access, and assess records in context click after click, **fast** and **easily**, just like Wikipedia did

Only then the people will know that, also in the digital world,

archives are the means to unveil and denounce misinformation and disinformation and get to the truth, even if only the documentary truth and a partial one.

InterPARES Trust

THANK YOU

luciana.duranti@ubc.ca
www.interparestrust.org