Uses of Blockchain in Supply Chain Traceability

Marek Laskowski and Henry Kim
Schulich School of Business, York University
http://blockchain.lab.yorku.ca
Agenda

• Cryptographic Foundations
• Blockchain (what is, notable use cases)
• An Abstract Traceability Use case
• Ontologies for Blockchain Application design
• Traceable Resource Units (TRU)
• Prototype Traceability Smart Contract
• Standardization
• Some key questions
Cryptographic Principles

• Cryptographic encryption and signature
  – Each Actor has their own set of Keys
  – Public (others can create an encrypted message only the Actor can read, and verify signed messages)
  – Private (used by Actor to sign messages, and decrypt or read messages encrypted with the public key)

• Hashing functions (message digest)
  – Hashing operations produce a much shorter digest (hash) of data or a document.
  – original data cannot be reconstructed from the hash
  – probability of different data producing same hash $\approx 0$
Blockchain

• A blockchain is a decentralized shared ledger, where a network of peers—rather than a centralized intermediary—maintain copies of one truthful ledger.
• New ledger entries are “chained” to the end of the blockchain using the hash-digest of the previous block within the current block.
• Previous entries cannot be readily modified nor deleted.
• Security ≠ Privacy
  – Many Blockchain implementations consider data to be public (e.g. Bitcoin)
• Potential Niche: in regulatory environment, the cost (trust) of maintaining a central database can instead be spread across a network of stakeholders
Blockchain

• Blockchain is a useful buzzword referring to a family of technologies like “the cloud”
• True value could be as part of a Digital Transformation story.
• Federated Technologies include:
  – low-cost ubiquitous networked sensors (Internet of Things, IoT)
  – Business & Data analytics – allows us to make sense of all this, big picture
  – Content addressable storage
• “Smart Contract” has come to mean a program which is executed on a blockchain and it’s state is secured by the blockchain. Can be used to encode business logic and carry out transactions (hence contract) → decentralized applications
• Multiple decentralized applications can be run on the same blockchain
A Hypothetical “Pipeline”

- Deliberately abstract
- Could correspond to:
  - supply chain activities
  - import/export documentation
  - Shipping
  - bills of lading
  - various certificates (quality etc.)
Blockchain “1.0” (ex. Bitcoin)

Stage 1

Stage 2

Stage 3

Hash / digest of document / data

Digital signature (prevent falsification of Actor’s Identity)

Actor 1

Blockchain
Blockchain “1.0”

Stage 1

Stage 2

Stage 3

Actor 2 + hash / digest of document / data

χ_{11001111} digital signature

Reference to previous transaction
Blockchain “1.0”

Stage 1

Stage 2

Stage 3

Actor 3

\[\chi_{11001111}\]
Blockchain “1.0”

*Blocks are time-stamped

Later, at $T_N$ we can prove a document was the original one used at $T_0$ by comparing the hash of the supposed original with what was recorded on the blockchain.

→ Prevents falsification of records
Blockchain “1.5” ex. Bitcoin + IPFS

Each Stage

Encrypted original data stored in so-called content addressable storage

Actor 1

+ Hash of Encrypted document also stored on-chain

Auditor can decrypt and view original data

$T_N$
Blockchain “2.0” ex. Smart Contracts (Ethereum) + IPFS

Interaction with the blockchain is mediated through a Smart Contract that encodes business logic; can be used to *drive* the process.

*Encrypted original data stored in so-called content addressable storage*
An example ontology: for Enterprise Modelling

Ontology ≈ Domain Specific Data Model + Business Rules + Formalism + Philosophy
**Definition:** A Traceable Resource Unit (TRU) is a collection of one or more Objects (goods) that cannot be individually traced further.

**Smart Contract**

```solidity
contract Trace{
    struct Tru{
        bool consumed;
        bool used;
        bool created;
        uint id;
        uint producedBy;
        uint consumedBy;
    }
}
```

**Trace Axiom: Cons-1. A tru is produced only once.**

\[
\forall A \forall St_1 \forall Rt \forall s \left[ holds(produce(St_1,A),s) \land holds(produces(St_1,Rt),s) \Rightarrow \exists St_2 \left\{ holds(produce(St_2,A),s) \land holds(produces(St_2,Rt),s) \land St_1 \neq St_2 \right\} \right].
\]

- \( A \): an activity which produces \( Rt \)
- \( St_1, St_2 \): the same state describing the production of \( Rt \)
- \( s \): an extant situation
An example primitive trace

* In the case of multiple source activities for each TRU, each branch would have to be searched
Regarding Standardization

- Networks become more valuable with more users → interoperability
- Numerous efforts are underway to standardize blockchain and distributed ledger
  - Interoperability at a *protocol* level
  - Interoperability at a *semantic* level
- Both must be addressed.
- *Now is the time!*
Semantic Interoperability

- Blockchain Lab currently trialing Smart Contract “meta standard”
- Permit inspection of a Smart Contract’s underlying Data Model
- It can be reasoned whether two Data Models are compatible
- Would become necessary if new versions of a Data Model are introduced or modified over time.
Some Questions

• How to implement Key Management?
• How to manage Identification on the blockchain?
• How to scale blockchain applications?
• Can blockchain be used to implement Single Window?
Recent Headlines

• ISO starts Blockchain standardization process
• UN World Food Programme using blockchain for tracking food aid
• Alibaba building blockchain solution for food traceability and provenance to fight "fake food"
• IBM launches commercial blockchain effort for identity with 6 Canadian Banks; Carbon Credits in China & more…
• CreditEase / Yixin launches blockchain solution for supply chain
Recent Headlines

- Enterprise Ethereum Alliance Releases Goals for 2017:
  - Develop a sufficiently modular Ethereum implementation to separate and define clear interfaces between networking and storage layers - that is a prototype for pluggable consensus that minimizes the code changes required to switch consensus algorithms.
  - Experiment with potential consensus algorithms, along with data privacy and permissioning frameworks.
Recent Headlines

• **Enterprise Ethereum Alliance Releases Goals for 2017** (continued):

• Develop a clear set of capabilities:
  – 100 transactions per second, across a 10 party network
  – High volume and value use cases
  – High availability/reliability
  – Parallelization and horizontal scaling

• Produce a reference implementation.

• Leverage a robust governance process to ensure alignment and agreement on approaches
Prototype: Ontologies and Blockchain for Supply Chain Traceability
UML Model Used to develop traceability smart contract