Distributed Ledger Technologies (DLT) for Nonproliferation and Safeguards

Presented at: Just Trust Me Workshop
Organized by: Institute of Nuclear Materials Management (INMM), Southwest Chapter
Location: Albuquerque, NM
Date: Tuesday, March 12th, 2019

Presented by

Michael P. Frank (Center for Computing Research)
Abstract

It has been approximately two years since we proposed applications of distributed ledger technology (DLT) in the high stakes domains of nonproliferation and international safeguards [1].

Around the same time, a number of high profile industry ventures jumped headlong into implementations and deployments of conceptually similar systems, such as food safety supply chain provenance [2] and international shipping chain of custody [3]. Some of these industry efforts are starting to communicate lessons learned [4,5].

In this talk, we will reconcile these lessons learned against our original proposal, and present a revised and contemporary vision for valid roles of DLT in nuclear nonproliferation and international safeguards.

Outline of Talk

Review of our earlier work:
- Original motivation for this effort
- Specific application areas within the nonproliferation context
- Original proposed concept for DLT-based tools for nonproliferation & safeguards
  - Overall approach
  - Applications (in nonproliferation-related domains)
  - Methodology
  - Future work (as envisioned at the time)

Implementation barriers encountered by others
Lessons learned
Implications for nonproliferation application
Conclusion—Recommendations going forwards
Original Motivation & Research Question

Context: Treaty arrangements are increasingly multilateral
- How to build trust among distributed parties?

Distributed Ledger Based Accounting Systems (DLBAS), which include blockchain-based systems, offer potentially useful features for nonproliferation applications:
- Immutability/non-repudiability of data (leverages digital signatures and secure timestamps)
  - Ensures integrity of transactions, prevents a large class of possible fraudulent uses of system
- Availability of data (distributed across all parties to the distributed ledger system)
  - Any subset of parties can transact without depending on any other party to host the system

Blockchain technology has had some notable successes in the financial sector
- Total market cap of all cryptocurrencies attained $835B in Jan. 2018 ($133B currently)

Research question: How can DBLAS support nonproliferation efforts?
- E.g. w.r.t. accountability of nuclear materials & assets under multilateral agreements?
Specific Application Areas

Five classes of problems that we identified for further research into DLBAS for multilateral, nonproliferation-related agreements: (and see* re: bulleted details)

1. Availability and non-repudiability of compliance data (e.g. CTBTO data sharing)
2. Chain of custody and provenance tracking, including:
   - Automating process flows for e.g. complex book transfers, such as flag swaps
   - More readily assuring supply chain integrity w.r.t. multilateral export control regimes
3. Material balances
   - More streamlined matching of ICRs (inventory change reports)
4. Traceability/auditability of data
5. Trusted computing systems

Approach

Distributed ledgers allow parties to perform transactions without any specific third party in control—making the process less reliant on trust in (or subject to the influence of) any single organization or party. Distributed ledgers have challenged traditional designs because of these intrinsic features they offer. Bitcoin, for example, has challenged the financial industry design by giving participants the same ability to do what we trust banks to do.

Traditional ‘central bank’ approach => trust from the fact that banks have ledgers & know how much each entity has, therefore can approve or deny transactions.
Distributed ledger design (e.g., blockchain) => trust built by all parties having a copy of the ledger, so all parties know whether an entity has sufficient funds

Here, blockchain simultaneously demonstrates the two key attributes of DLBAS:

- Non-repudiation – all transactions are added to the blockchain (ledger) for all to review. Because of this, immutability is guaranteed and authenticity cannot be disputed
- Availability – any participant can verify the transaction; no single point of failure or data existence
Methodology

Consider a notional, highly transparent nonproliferation-related agreement in which declarations, and perhaps some unattended monitoring data, are reported to a centralized monitoring agency (CMA). The CMA then compares this incoming data to its current ‘ledger’ of related information, verifies the incoming data and then shares back to the other states party to the agreement.

Traditional, centralized architecture. This scheme forces all data to be validated at a common source. The reliance on this CMA, however, is problematic because it could (a) be down, (b) be incorrect or (c) be compromised.

Note: This architecture could apply at a national, regional, or international scale (as with reporting to IAEA), or at several levels simultaneously.
One possible more-distributed architecture for validation:

In our new model, data is sent to multiple parties randomly selected from the agreement signatories. Each party has a copy of the data store (distributed ledger) that they can then verify against.

Independently, these parties validate the data against their copy of the ledger and vote on the acceptance of the data. Validation of the data is signed and sent back to the originator.

Continued on next slide...
The originator takes these signed validations and creates a block for the ledger as a receipt of compliance. This new block is published and sent to all agreement signatories across the network for them to add to the ledger, including the central monitoring agency.

Some architecture considerations in this new paradigm include:

- Flow of Data (through CMA to others vs. directly to others)
- Source of Trust (CMA as mutually agreed upon sovereign vs. ‘crowdsourcing’)
- Points of Failure (CMA being compromised vs. random agreement signatories compromised)
- Enhanced Resilience (dynamic attack surface vs. single attack path in CMA)
Our earlier vision of...

Future Work and Key Questions

- Focus in on specific application areas ✔
- Demonstrate inherent weaknesses ✔
- Define design requirements and constraints
- Distributed, Private, Permissioned ✔
  - Leveraging modern advances in threshold cryptography
  - Offer varying levels of privacy of the originator and data
  - Countries cannot sign (validate) a block of data without verifying members
- Partner with Global Security stakeholders
  - Theoretical Approach
  - System Analysis of DLBAS
- Exercise identified weaknesses against DLBAS design
  - Overall system impact analysis
  - Develop resilience metrics
- Develop DLBAS System with Sandia’s simulation capabilities
  - Leverage Emulytics™ Capabilities – High Fidelity Simulation Environments
Some Existing Related Efforts in the Commercial Sector

Mid 2017 – IBM/Mersk TradeLens
  ◦ Platform for global shipment tracking based on IBM’s Hyperledger Fabric

Late 2017 – Blockchain Food Safety Alliance (IBM, Walmart, etc.)
  ◦ Provenance tracking for produce from farm to retail outlet (store/restaurant)
  ◦ Followed up by IBM Food Trust, launched in Nov. 2018
    ◦ Commercial product rollout
    ◦ Applications include:
      ◦ Food safety/freshness, supply chain efficiency/waste reduction, sustainability, brand trust/prev. fraud

Some other entrants (relatively little adoption to date):
  ◦ Waltonchain (WTC) – Focused on RFID tracking; partnerships in China
  ◦ VeChain (VET) – Also NFC/QR. Asia-based partnerships
  ◦ SophiaTX (SPXTX) – SAP integration.

Some other popular DLT platforms:*
  ◦ Ethereum Quorum and Burrow – Permissioned versions of this popular smart-contract blockchain
  ◦ MultiChain with “Smart Filters” – Open platform for building custom blockchains
  ◦ R3 Corda – “Open-source blockchain for business”

Implementation Barriers Encountered by Others

Common barriers to blockchain adoption (cf. *Information Week*)

- **Understanding blockchain** – Advantages/limits of applicability often misunderstood
- **Identifying a business outcome** – What is the bottom line for the business’s operations?
- **Teamwork** – Requires collaboration between team members of disparate backgrounds
- **Culture** – Traditional ways of doing business may not mesh well with DLT platform
- **Regulation** – Varies by jurisdiction; makes global SCM problem very complex
- **Throughput and scale** – Traditional DLT platforms have low capacity & don’t scale well
- **Development tools** – Existing tools tend to be immature, poorly documented
- **Costs** – Long, complex road from concept to fully-functioning distributed system
- **Talent** – Difficult to find developers with DLT experience as it’s a novel technology

Notable case study: IBM/Maersk Tradelens

- Had difficulty signing partners due to concerns over IP ownership [5]

Other possible issues and problems:

- **Denial-of-Service attacks** – E.g. network flooding attacks on Bitcoin blockchain
  - This type of problem is inherent to any permissionless blockchain
Some of the top/most important lessons learned recently, in our assessment, are:

- Permissioned ledgers may be preferable to permissionless for many applications
  - Can help reduce spam attacks from unauthorized network users
  - Additional layer of OPSEC preventing accidental public release of private data
- Make sure the use case identified truly requires a blockchain-based solution
  - As opposed to, say, a traditional distributed (or centralized) database
    - Simply using unforgeable digitally-signed chains of transactions does not itself actually require a DLT-based solution.
- To encourage buy-in, make sure deployment/operation is perceived as fair!
  - Partners shouldn’t feel like using the system gives its originators an unfair advantage
Implications for Nonproliferation Applications

Permissioned ledgers *may* be viable in the reasonably near term for nonproliferation

- Specifically in treaty/safeguards verification

A DLT-based solution will *not* by itself adequately address *all* nonproliferation issues, of course...

- Trusted international organizations such as IAEA most likely still play an essential role
  - At minimum, to control access to a permissioned ledger, or in cases where manual verification is needed
- Where trust in nonproliferation can be increased via consensus, blockchains *may* be useful

Methods to encourage buy-in for nonproliferation could include:

- “Pilot” applications in regional contexts
- Partnering with “trusted” international bodies like the IAEA or WINS
Conclusion

Some of our recommendations in regards to this enterprise going forwards are:

◦ Engage stakeholders at all levels of the global nonproliferation ecosystem in ongoing discussions about the design and deployment of DLT-based solutions for these applications
  ◦ This will ensure buy-in from the get-go
  ◦ Don’t try to “push” a preconceived (and perhaps mis-conceived) solution on users

◦ Carefully consider the benefits and costs of pursuing a DLT-based approach for each application…
  ◦ Don’t use a DLT just because it is “trendy” in situations where a more centralized approach would be satisfactory
  ◦ Consider: What steps need to be taken to convince users of the increased trustability benefits of a DLT-based solution?

◦ Carefully select a DLT technology platform to build upon:
  ◦ There are a wide variety competing contenders already in play
  ◦ Pros/cons of the different options need to be carefully weighed
  ◦ Some questions: How stable / well-supported / well-documented / open is the platform?

◦ Consider developing the system’s codebase in an open-source fashion!
  ◦ This allows the maximum number of parties to vet the system design, looking for security holes
  ◦ It’s probably the only way to ensure that users of the system will trust that the code is correct and not compromised