SAND2017-9213C

Sandia National Laboratories

Exceptional service in the national interest

Investigating Distributed Ledger-Based Accounting Systems for Nonproliferation

Authors: James Baker, Nick Pattengale, Adam D. Williams, Russell Graves, Sharon Deland

Abstract

As treaty arrangements move from bilateral to multilateral relationships, new challenges emerge regarding building trust among distributed parties. Distributed Ledger-Based Accounting Systems (DLBAS), like blockchain in the finance sector, offer two attributes that can support a variety of nonproliferation applications:

- Non-repudiation of data (e.g., integrity for each transaction between parties, crucial for applications where trust cannot be guaranteed)
- Availability of data (e.g., offers all parties access to the ledger, so transactions can be done without depending on a third party)

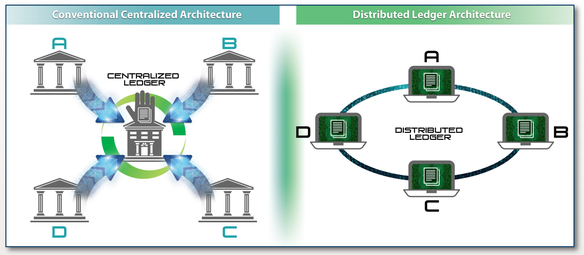
Blockchain's success in the financial sector has spurred the interest of many other industries. While still in its infancy, this research considers the application of a DLBAS solution to support verification in the nonproliferation regime and is highlighted with a theoretical DLBAS design for the accountability of nuclear materials or assets under multilateral agreement(s). We explore how establishing an immutable chain-of-custody provides confidence for multiple parties that the nuclear materials and assets is authentic and accurate—to potentially reshape how multilateral agreements are designed and implemented.

Research Question

How can Distributed Ledger-Based Accounting Systems (DLBAS) support Nonproliferation Efforts?

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:

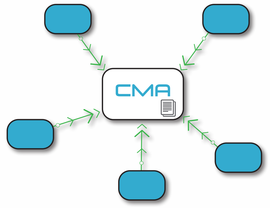
- Non-repudiation – all transactions are added to the blockchain (ledger) for all to review. Because of this, immutability is guaranteed and authenticity cannot be disputed
- Availability – any participant can verify the transaction; no single point of failure or data existence

Five classes of problems that we have identified for further research into DLBAS for multilateral, nonproliferation-related agreements:

- Availability and Non-Repudiation of Compliance Data (example: CTBTO data sharing)
- Chain of Custody and Provenance Tracking
- Material Balances
- Traceability of Data
- Trusted Computing Systems

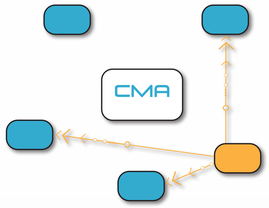
Methodology

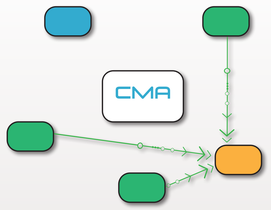
Consider a notional, highly transparent nonproliferation-related agreement in which declarations, and perhaps some unattended monitoring data, are reported to a centralized monitoring agency (CMA). The CMA then compares this incoming data to its current 'ledger' of related information, verifies the incoming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

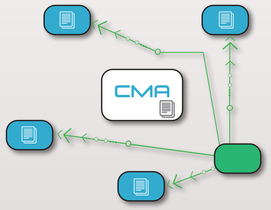
In our new model, data is sent to multiple parties randomly selected from the agreement signatories. Each party has a copy of the data store (distributed ledger) that they can then verify against.





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.

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.

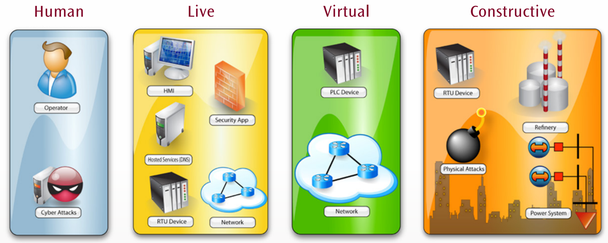


Some architecture considerations in this new paradigm include:

- 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)

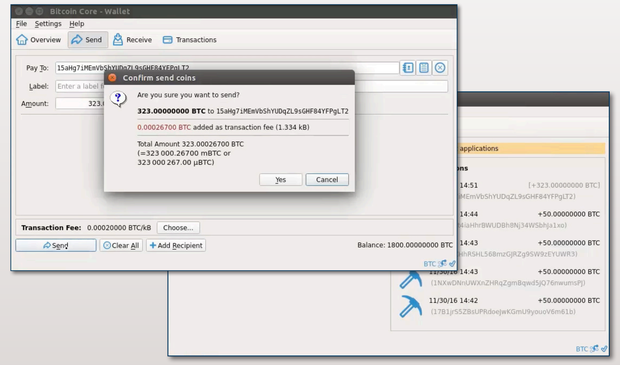
Future Work and Key Questions

- 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



Sandia has strong capabilities within modeling and simulating complex systems and environments across various industry sectors. These services can be extended in partnership with other capabilities to support DLBAS experimentation and development.

- Leverage Sandia's bitplayer – a closed loop bitcoin network environment.



Bitplayer is an environment for running closed-loop bitcoin networks that produce specific blockchains. This novel capability provides a validatable and repeatable environment to, for example, realistically test proposed bitcoin extensions, rapidly prototype scalable overlay protocols, or easily produce blockchain variants for sensitivity analysis of current bitcoin analytics.

U.S. DEPARTMENT OF ENERGY NNSA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXX C

Sandia National Laboratories

CGSC Center for Global Security and Cooperation

www.sandia.gov