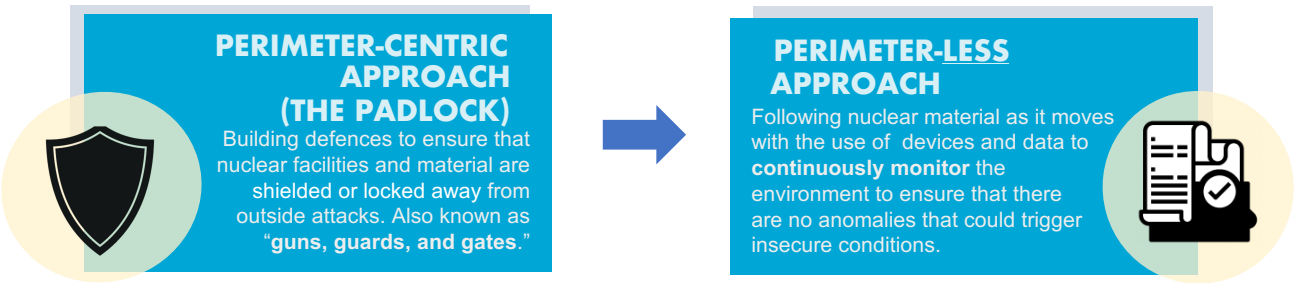
COMPLEMENTING THE PADLOCK

Distributed Ledger Technology (Blockchain) for Nuclear Security – A Summary

Read full policy paper : https://www.stimson.org/2020/complementing-the-padlock-the-prospect-of-blockchain-for-strengthening-nuclear-security/

Distributed ledger technology* (DLT)** — more commonly known as ***blockchain — establishes a digital shared ledger in which data is cryptographically verified upon a single "block" and replicated across a participating network, thereby enhancing transparency while providing data privacy among all parties involved. An alternative to centralized systems that are susceptible to a single point of failure (e.g., when hacked, the entire system would be left exposed), DLT platforms combine computing concepts of cryptographic hashing, peer-to-peer protocols, and distributed consensus algorithms to allow a network of participants to share and validate data across a blocked ledger. Private DLT platforms allow different levels of access controls for various users, and most importantly, provides improved source authentication, which builds confidence among untrusting stakeholders.

DLT offers a novel way to embed protective properties into data collection by tracking and validating the integrity of the transactions. **Thus, it could enhance existing best practices for nuclear security, adding a layer of data provenance and authentication that complements the traditional, "perimeter-centric" approach to protecting nuclear material (securing with a "padlock").**



Potential Use–Cases:

Nuclear Material Accounting & Control (NMAC)

DLT could **streamline and secure accounting information as nuclear material move through material-balancing areas** and facilitate better knowledge-sharing across appropriate stakeholders. If an insider threat attempts to manipulate records, the adversary would also have to simultaneously change every copy of data across the chain, risking detection.

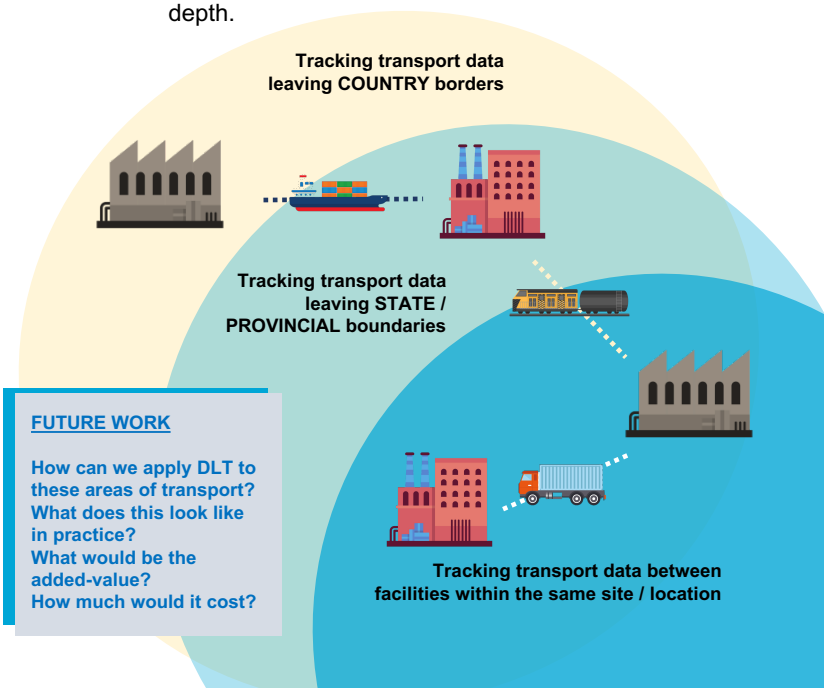
Transport Security (Most Promising)

A DLT platform could offer an **added layer of assurance on the flows of sensitive data related to transport by logging information onto the chain as nuclear material travels from origin to destination**. Transport data (e.g., personnel credentials or authentication of necessary documents) could be monitored and accessed by specific personnel depending on their need-to-know requirements proportionate to the risk. Data would be automatically logged onto the chain, certifying its source (it has not been tampered).

This platform would not only provide an immutable record of checkpoints for a given shipment in real time, but also monitor the activities of individuals handling the material directly (detection of any activities that could indicate insider threat).

Insider Threat Mitigation

Create digital identities for personnel to authenticate credentials and track the data they share with whom, when, and for how long. Personnel activity would be logged onto the chain, not the actual sensitive information itself. In this case, DLT would serve as an add-on to existing information security measures, which follows the principles of defence-in-depth.



FUTURE WORK

How can we apply DLT to these areas of transport?
What does this look like in practice?
What would be the added-value?
How much would it cost?

STIMSON

With support from U.S. Department of Energy – NNSA
Illustrations from VectorStock, Alamy, and FreePik