2019

Applying Blockchain for Dual Use Technologies Supply Chain Security

Babita Gupta
California State University, Monterey Bay, bgupta@csumb.edu

Seema Gahlaut
The Stimson Center, Washington, DC, sgahlaut@stimson.org

Shwadhin Sharma
California State University, Monterey Bay, ssharma@csumb.edu

Applying Blockchain for Dual Use Technologies Supply Chain Security

Extended Abstract

Babita Gupta, California State University, Monterey Bay, U.S.A., bgupta@csumb.edu
Seema Gahlaut, The Stimson Center, Washington, DC, U.S.A., sgahlaut@stimson.org
Shwadhin Sharma, California State University, Monterey Bay, U.S.A., ssharma@csumb.edu

Background

Blockchain technology is gaining momentum with potential applications in businesses, government, and social context with some impressive applications for storing information, eliminating intermediaries, and enabling greater coordination between entities in issues such as in maintaining data standards (Higginson, Nadeau, and Rajgopal, 2019). While there are aspects of this technology that are still not settled such as the question of whether it is a disruptor or foundational technology, there is an agreement that it has the capability to increase security and transparency of transactions to all parties. Smart contracts using blockchain are theorized to be manifested using machine-to-machine coordination within IoT or with decentralized digital marketplaces (Beck, Müller-Bloch, and King, 2018). However, even though the blockchain technology has the potential towards decentralization of authority decision-making, current research indicates that so far that has not transpired and blockchain applications mostly operate in the environment of centralization mimicking notion of "benevolent dictatorship" (Beck, Müller-Bloch, and King, 2018).

The main purpose of this work is to understand the gaps in application of blockchain technology in supply chain with domain focus on the supply chains involving dual use products.

Background on Dual Use Technology Supply Chain

U.S. National Research Council defines dual use technologies as "technologies intended for civilian application that can also be used for military purposes." (National Research Council, 2004, p. 18). For example, the technology used to make aerosol of particles with microns of a particular bacteria to control gypsy moths in agriculture, a benign use, is the same technology that can produce an aerosol of anthrax (Forge, 2010). Similarly, everyday products such as cell phones, ball bearings, and batteries transported across continents could be used in making weapons. Supply chain security, thus, is a critical concerns for state actors to ensure that the transportation of these technology artifacts is conducted in such a way to avoid resulting in use of these artifacts to produce unintended outcomes (Forge, 2010; Rychnovská, 2016).

The Problem

There is need for a supply chain system that eliminates, or at least, reduces the risks at various touch points involving many state actors, regulators, government regulations and policies, customs, transportation and shipping manifests, material, equipment, and people. Blockchain can be applied for this purpose (Gahlaut, 2018; Vestergaard, 2018) using smart contracts for:

- **Item authentication**: blockchain can help establish the physical point of origin and in tagging the specification and controls in combination with RFID
- **Licenses authentication and security**: Ensuring that the paperwork on safety, security, end-use conditions accessible to all those persons and institutions selected as relevant; any changes in location, control, ownership recorded through the supply chain

- **People identity authentication**: Establishing identity of *bonafide* actors and entities with right, verified, authorized persons having access to items and licenses. This is a high-risk concern with authentication required at various points in the supply chain as item moves with changes in location and/or ownership across regional and national boundaries.

We reviewed the current literature on blockchain application in supply chain management with applications in manufacturing, smart grid energy trading, B2B supply chain integration, decentralized smart contract system HAWK, and healthcare (Abeyratne and Monfared, 2016; Aitzhan & Svetinovic, 2018; Korpela, Hallikas, & Dahlberg, 2017; Kosba, Miller, Shi, Wen & Papamanthou, 2016; Yue, Wang, Jin, Li, & Jiang, 2016). Most applications are proposal or an early stage proof of concepts with several elements missing (Loebbecke, Lueneborg, & Niederle, 2018). There are several unanswered questions that are relevant to most supply chains and are especially relevant to blockchain enabled dual-use technology supply chains. In this paper, we plan to explore the following:

1. Record creation: Since blockchain ensures that once a record is created, it is immutable, it becomes vital that record creation process creates only the authentic records.
    a. This becomes complex with the mix of state actors, different government legislations, and policies, custom policies, people, and national cultures.
    b. It create the problem of "everyone's responsibility is no one's responsibility" because if an error is made initially in establishing an identity, then it may keep getting propagated unless blockchain enabled system have a mechanism to make corrections.
    c. For authentication of people or products in the supply chain, does the majority nodes verification rule apply or do all nodes have to agree for verification? If the former rule is applied, what if the minority was right in refusing the identity verification?

2. Trust Mechanisms: In order to ensure that blockchain does indeed carry "true" information, requirements of a trust mechanism to verify all items, licenses, and people in the supply chain are even more critical. It may require third party processes, perhaps similar to Department of Motor Vehicles in the U.S., which is used to authenticate a person's identity for a driving license. These could be a consortium of entities such international license issuing and trade control enforcement agencies, and trade associations. Trust mechanism would need to ensure:
    a. Item verification: If person X in company X says that item X is not a "controlled" item and is packed in a box ready for shipment, then trust mechanism needs to be able to verify that person, company and item are indeed authenticated before the record is appended to the blockchain.
    b. Destination and people verification: If item X is destined to be shipped to entity Y in country Y, then it indeed reaches that destination and is verified as such without any foul play with RFID tags or paperwork.
    c. Articulation of Domain-specific languages (DSLs): In order for blockchain and associated digital technologies to work seamlessly in this complex ecosystem, there is a need for clearly defined syntax and semantics that can aid in specifying valid contracts and their proper execution.

Proposed Research Approach:
We plan to use the grounded theory approach (Corbin & Strauss, 1990) to qualitative and quantitative data from companies and agencies that we have identified who are involved in dual-use technology supply chain and are beginning to either contemplate using blockchain or already implement blockchain technologies to secure the supply chain. This approach may allow us to tease out the technical, regulatory, financial, and cultural challenges associated with dual use domain and develop guiding framework for blockchain applications.

During the workshop, we hope to get robust feedback as well as engage in discussions with other researchers about the research directions available in addressing trust mechanism issues in blockchain applications.

References are available upon request.