PROJECT DESCRIPTION

MANUFACTURING SUPPLY CHAIN TRACEABILITY WITH BLOCKCHAIN RELATED TECHNOLOGY

Reference Implementation

Michael Pease
Keith Stouffer
Smart Connected Systems
Communications Technology Laboratory

Evan Wallace
Systems Integration Division
Engineering Laboratory

Harvey Reed
Steve Granata
The MITRE Corporation
McLean VA

DRAFT

April 2023

blockchain_nccoe@nist.gov

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov/.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a Community of Interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

Abstract

Manufacturing supply chains are increasingly critical to maintaining the health, security, and the economic strength of the United States. As supply chains supporting Critical Infrastructure become more complex and the origins of products become harder to discern, efforts are emerging that improve traceability of goods by exchanging traceability data records using blockchain related technologies. Recent events and current economic conditions exposed the impact of disruptions in the security and continuity of the U.S. national manufacturing supply chain. This in turn, drew critical attention to the need to illuminate and secure the supply chain from numerous hazards and risks. Further, the U.S. manufacturing supply chain is susceptible to logistical disruptions, in addition to the effects of nefarious actors seeking fraudulent gain or attempting to sabotage or corrupt manufactured products. Improving the traceability of goods and materials that flow through the manufacturing supply chain may help mitigate these risks. This project will continue building on ongoing NCCoE efforts to demonstrate the role that blockchain related technologies may play to improve manufacturing supply chain traceability and integrity by exploring several use cases and the issues surrounding implementing supply chain traceability and will result in a freely available NIST Cybersecurity publication.

Keywords

anticounterfeiting; antitampering; blockchain, distributed permissioned ledger; ecosystem; identity, pedigree; provenance; supply chain traceability

Disclaimer

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Comments on NCCoE Documents

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov/.

Comments on this publication may be submitted to blockchain_nccoe@nist.gov

Public comment period: April 14, 2023 to May 16, 2023

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 Executive Summary

Purpose

Manufacturing supply chains are increasingly critical to maintaining the health, security, and the economic strength of the United States. As supply chains supporting critical Infrastructure become more complex and the origins of products become harder to discern, efforts are emerging that improve traceability of goods by exchanging traceability data records using ecosystems enabled by blockchain related technologies that provide provenance and integrity.

This document describes a Minimum Viable Product (MVP) Reference Implementation (RI) of manufacturing supply chain ecosystems, to illustrate product traceability across microelectronic and ICT (Industrial Control Technologies) supply chains to critical infrastructure operators. The MVP RI is a follow-on effort from NISTIR 8419 "Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability" [1]. In addition, the project seeks technical exchange and discussion with related groups (e.g., industry and standards groups [2][3][4]) to discover and refine relevant MVP use cases regarding data sharing of traceability information; data, pedigree and provenance integrity; and manufacturing supply chain wide traceability queries.

The choice of microelectronics and industrial controls emphasizes the importance of manufacturing supply chain traceability, although the MVP RI should be understandable in other contexts and serve as an architectural approach for other supply chain domains and critical infrastructure sectors.

The choice of critical infrastructure as the consumer emphasizes the importance of manufactured products, and constituent products and assemblies therein, which are used for purposes that are critical to civil society. These MVP approaches may also be adapted to national security and other contexts.

This project has a goal to demonstrate traceability across manufacturing domain stakeholder "blockchain related technologies"[1] enabled ecosystems [1] to determine authenticity of products for use in critical infrastructures. The project will continue building on NCCoE ongoing efforts to demonstrate the role that blockchain related technologies may play to improve manufacturing supply chain traceability. This project will result in a freely available NIST Cybersecurity Practice Guide. For the specific architecture used in this MVP, blockchain will be used as the as example of blockchain related technologies; however, other implementations such as confidential distributed ledgers is also within the scope of possibilities for this work.

Scope

This project addresses key challenges in manufacturing supply chain:

- Improve visibility, integrity and permanence of manufacturing supply chain product pedigree. The initial claim of product authenticity by a manufacturer needs to survive the lifetime of the manufacturer through mergers, acquisitions, and dissolution.

[1] "Blockchain related technologies" refers to the family of technologies around blockchain, permissioned ledgers, and confidential distributed ledgers that provide integrity, traceability, and identity information about items and who added them using byzantine fault tolerance consensus mechanisms.

- Improve visibility and integrity of provenance across tiers of manufacturers. The existing process of tracking provenance via bi-lateral exchange of traceability information between buyer and seller is: (a) complicated, and (b) non-permanent, where information may be lost or further obscured during mergers, acquisitions, and dissolution.

This project describes and delivers a reference implementation of a potential manufacturing supply chain traceability mechanism that demonstrates:

- Manufacturers' ability to post traceability records to their respective industry ecosystem blockchains. Each traceability record written to the blockchain related technology links to the prior traceability record(s), going back to the original traceability record(s) (e.g., 'making' the product) where the traceability record links to the originating manufacturer.
- Establishing traceability record links and form an immutable[2] traceability chain. Traceability records can link to multiple prior traceability records in the case of combining components in higher-order assemblies and products.
- Associating traceability records link to relevant context. In addition to linking to previous traceability records, traceability records point to relevant context such as the author (e.g., who wrote the record) and additional data in external repositories as needed.
- Establishing traceability record links to external data as required. In addition to the minimal data in the traceability record, the traceability can link to external data as needed (with appropriate access controls) for larger data sets, images, audio, video, etc.

This project delivers an MVP RI that:

- Demonstrates manufacturers joining their respective blockchain related technology enabled ecosystems.
- Demonstrates manufacturers writing and linking traceability records.
- Demonstrates critical infrastructure operators reading the traceability chain to inform their assessment whether to employ the manufactured product.
- Uses microelectronics, industrial controls, and critical infrastructure as example domains.
- Positions the MVP RI as a starting point for future research and refinement.

Assumptions/Challenges

The key project challenge is to explain and illustrate the traceability chain method with sufficient fidelity to indicate potential suitability for traceability of complex manufacturing supply chains, while avoiding detail which may be better suited for future refinement. The key assumption is that the MVP project, once complete, is a starting point for further research and refinement. Beyond the scope of the MVP, further topics such as ecosystem governance, identity proofing, and cyber-physical identification can be explored.

[2] The term 'immutable' is used in this document in a practical sense. Please see NISTIR 8202 Sect. 7.1 for further technical discussion, and the alternative phrase 'tamper evident.'

Background

Supply chain participants are motivated to increase traceability in complex manufacturing supply chains to mitigate risk of supply chain vulnerabilities [5]. Vulnerabilities can arise in any manufacturing supply chain, and are exemplified by the industrial control technology (ICT) domains. ICT includes hardware, software, and managed services, where consequences of ICT supply chain vulnerabilities can impact the daily operation of U.S. critical infrastructure [6]. Today, organizations lack the ability to readily distinguish between trustworthy and untrustworthy products. Having a repeatable, quick, and provable means to determine if a product is trustworthy is a critical foundation of cybersecurity supply chain risk management [7].

An ecosystem perspective of the manufacturing supply chain serves to define provable traceability for a subset (an ecosystem) of the manufacturing supply chain stakeholders (e.g., suppliers, critical infrastructure), and to share and store applicable product traceability data records (e.g., pedigree, provenance). Traceability requirements and their means of implementation will be unique for each ecosystem (e.g., microelectronics, industrial controls, critical infrastructure).

Traceability data includes information about product provenance, pedigree, and other data as needed. Early industry ecosystem efforts indicate that the ecosystem perspective is useful and perhaps necessary to enable trusted and symmetric supply chain information sharing and migrate away from existing linear and bi-lateral information exchange. The existing status quo of bi-lateral information sharing is susceptible to incomplete coverages, differing implementations, corruption and alteration of data, and potential semantic gaps in data elements. A semantic gap may occur when a stakeholder multiple tiers away writes or conveys a traceability record that may not be fully understood or recognized downstream. Ecosystem-wide agreement on traceability information requirements, mitigates semantic gaps in understanding traceability data records within a manufacturing domain. This ecosystem perspective is layered atop, and does not replace, the existing and prevalent “per acquirer” perspective of supply chain management and security.

Across complex manufacturing supply chains, multiple ecosystems will arise and must themselves link traceability information across the ecosystems in order to establish trusted and symmetric traceability data, from commodities to final assemblies used in critical infrastructure, where products include hardware, software, and services [1]. The resulting traceability chain across industry ecosystems provides a path (links) to follow traceability records across ecosystems. The linking of traceability records can be performed with a small number of data fields. Further, traceability records can be specialized to meet the needs of various industry sectors as needed. The traceability links allow for multiple source components to be combined in an assembly, where the traceability record for the assembly can contain a list of constituent links back to the sourced components. This enables a tree structure of links, with a critical infrastructure acquirer ultimately receiving the root traceability record . The root traceability record can then be followed backwards, or upstream in the product supply chain, as necessary through ecosystems and across the chain of product traceability records.

2 Scenarios

Scenario Stakeholders and Ecosystems

The following ecosystems and manufacturing stakeholders are used in the MVP scenarios to illustrate the MVP traceability chain mechanism:

- Three (3) distinct blockchain related technology enabled ecosystems:
  1. Microelectronic manufacturing domain
  2. Industrial Control Technology manufacturing domain
  3. Critical Infrastructure domain
- Three (3) distinct manufacturing stakeholders:
  1. MEP-001 – microelectronic manufacturer
  2. ICT-001 – industrial control technology manufacturer
  3. CI-001 – critical infrastructure operator

The manufacturing stakeholders participate in an economic value chain, where value chain activities result in manufacture, making, and employing products. When products are made, included in assemblies, and ultimately used by the end operating environment, **traceability records** are written to the ecosystem blockchain related technologies. This provides both permanence for the traceability chain, surviving company mergers, acquisitions, and dissolutions, and a simplification of navigating traceability chains. The manufacturing domain ecosystems evolve slower than the constituent manufacturing stakeholders, and once established persist over time, providing permanence to the traceability records.

The manufactured products used in the scenarios are assumed to be represented in data records, but not manifested physically or in software code. The relationships between the stakeholders and ecosystems used in the MVP are illustrated below.

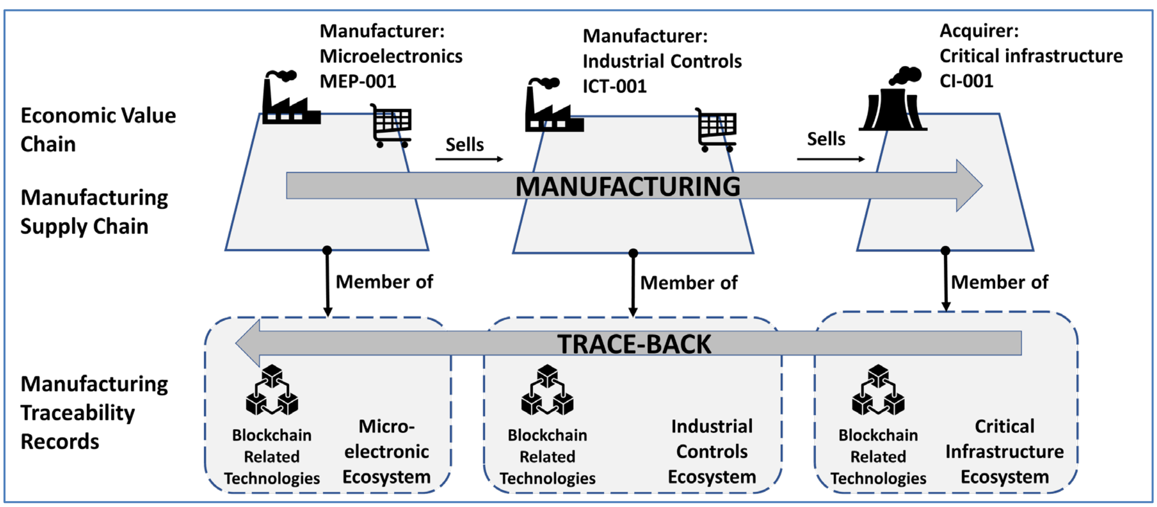


Figure 1: Manufacturers Participate in Blockchain Related Technologies Enabled Ecosystems to Record Traceability Records

Scenario 1: Supply chain manufactures industrial control assembly

MVP Scenario 1 exercises the set of manufacturing domain ecosystems to produce and sell manufactured goods for procurement by critical infrastructure, recording traceability data to establish pedigree and provenance:

1. MEP-001 produces a chip and sells the chip to ICT-001:
   a. Marks the chip with a unique ID

   b. MEP-001 creates a traceability record and writes it to the microelectronic traceability ecosystem. The traceability record has with a URI pointer to internal private manufacturing data, the ID of the chip, and a digest of traceability manufacturing data including hashes as needed, and the identity of MEP-001 and purchaser ICT-001.
   c. MEP-001 virtually delivers the chip to the purchaser, an industrial controls manufacturer ICT-001.
2. ICT-001 records receipt of the virtual chip and applicable chip traceability data and writes a traceability record, in the industrial controls ecosystem blockchain related technology, acknowledging receipt which contains the ID of MEP-001, ICT-001, and the ID of the chip:
   a. ICT-001 adds their software to the chip, where the software development steps are assumed to be traceable themselves, but (similar to the chip manufacturing above) doesn't have to be demonstrated just referenced via URI.
   b. ICT-001 adds the chip and software to an industrial control assembly and virtually delivers the industrial control assembly to critical infrastructure operator CI-001.
3. CI-001 records receipt of the industrial control assembly and writes a traceability record, in the critical infrastructure ecosystem blockchain related technology, acknowledging receipt which contains the ID of ICT-001, and the ID of the industrial control assembly.
   a. CI-001 starts a process to verify authenticity of the industrial control assembly.
4. Include additional chip and software deliveries which are invalid.
   a. Emulate fraudulent parts to test whether authenticity queries (see Scenario 2) can detect the fraudulent manufactured goods.

Scenario #1 (sub parts 1-3) is notionally illustrated below.

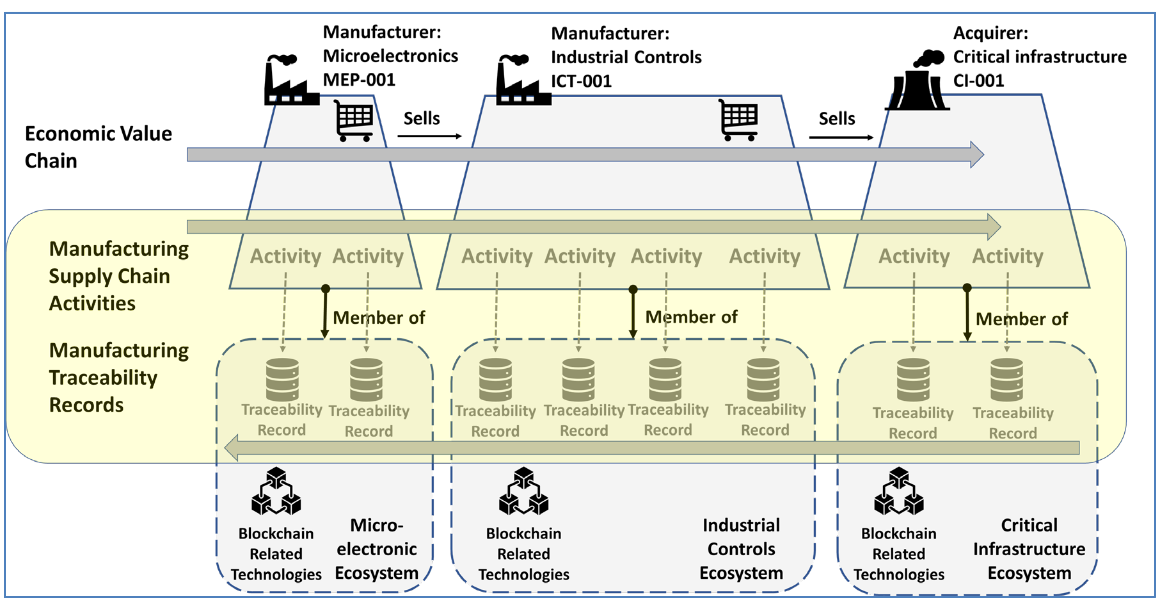


Figure 2: Traceability Chain Mirrors the Manufacturing Supply Chain in Reverse

Scenario 2: CI-001 uses the traceability chain to query the industrial control ecosystem and validate the authenticity of the industrial control assembly

MVP Scenario 2 exercises the query facility of each ecosystem to determine if a received manufactured good is authentic, by querying traceability records written to ecosystem blockchains during manufacturing, for example:

1. ICT-001 queries the microelectronic ecosystem blockchain using the chip ID as a primary query parameter.
2. CI-001 queries the industrial control ecosystem blockchain using the industrial control assembly ID as a primary query parameter.

Note: The scenario can include generated faults (counterfeit data records) to simulate general supply chain issues and identify how supply chain trackability can assist with detection. Generated faults may include:

- Swapping the genuine manufactured good (altering product ID), at point of sale, with a counterfeit part.
- Generate faults for chips, and the industrial control assembly which represent counterfeiting between manufacturer and acquirer.
- Generate faults for software which represent subversion of the software development process internal to ICT-001.

Scenario 3: After installation, CI-001 performs statistical quality check to re-verify authenticity of the industrial control assembly

MVP Scenario 3 also exercises traceability query facilities of each ecosystem as in Scenario 2. However, with a difference that the goods being verified are parts that are already in use in the critical infrastructure. This scenario demonstrates how the traceability ecosystems can continue to protect critical infrastructure after manufactured goods are in use. The MVP scenario will include generated faults to simulate a malicious actor swapping a valid manufactured good for a counterfeit and potentially malicious manufactured good.

All Scenarios: Traceability Chain

A traceability chain is a chain of linked traceability records. A traceability record is a blockchain related technology transaction, which is tamper evident and difficult to destroy. The manufacturing traceability records are of the sub-types: make, assemble, transport, receive, employ. The data fields in the sub-types are developed further in section 3 below. The traceability record sub-types link to each other, providing an immutable traceability chain.

The diagram below illustrates the traceability record sub-types, and how they can be linked to form a traceability chain.

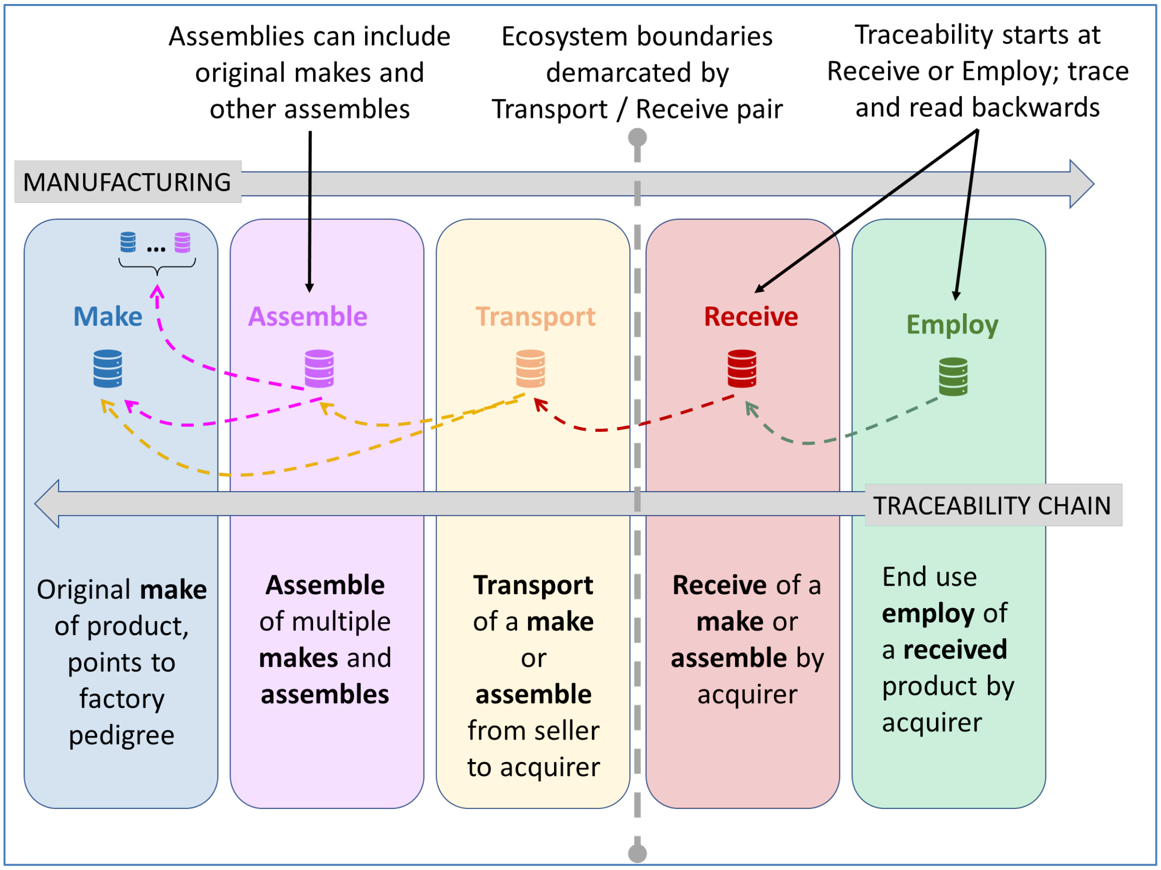


Figure 3: Traceability Records Form a Traceability Chain

The three scenarios above describe manufacturing actors making chips, software, and assembling them into industrial controls, then selling the resulting assembly to a critical infrastructure.

Scenario #1 Revisited: Illustrated with Traceability Data Types

The primary purpose of the MVP is to illustrate traceability records linked in traceability chains, across the chip, industrial control, and critical infrastructure ecosystems, performing activities as outlined in the above scenarios.

Figure 4: Traceability Chain Mirrors the Manufacturing Supply Chain in Reverse is an illustrated lifecycle of Scenario #1 which creates and uses a manufacturing supply chain traceability chain across ecosystems. The lifecycle steps are denoted by circular numbered markers 1-8:

1. Chip manufacturer MEP-001 makes a chip and writes a **make-chip traceability record** with a statement of authentic product pedigree (summation of factory internal process, provenance, certification, testing, etc.) and links to the factory.
2. Chip manufacturer MEP-001 transports (ships, uploads, etc.) the chip to a buyer Industrial control manufacturer ICT-001, in a different ecosystem, and writes a **transport traceability record** which links to the **make-chip traceability** record, which in turn links to the factory.
3. ICT-001 receives (loading dock, downloads, etc.) the chip, and writes a **receive traceability record** which links to the prior **transport traceability record**.

4. ICT-001 makes software for the chip for use in an ICT assembly, and writes a **make-software traceability record** with a statement of authentic product pedigree (summation of software development internal process, SBOM, etc.).
5. ICT-001 makes an ICT assembly with the chip, software, (could also include sensors, actuators, etc.), and writes an **assemble traceability record**, which includes the ICT assembly pedigree, and links to the **chip receive traceability record** and the **make software traceability records**.
6. ICT-001 transmits (ships, uploads, etc.) the ICT assembly to a critical infrastructure CI-001 buyer, in a different ecosystem, and writes a **transport traceability record** which links to the **assembly traceability record**.
7. CI-001 receives ICT assembly and writes a **receive traceability record** which links to the prior **transport traceability record**. The security officer for CI-001 uses the **receives traceability record** to trace-back through the traceability chain backward for pedigree and provenance information which informs the decision as to whether the ICT assembly should be employed in the infrastructure.
8. The critical infrastructure acquirer CI-001 decides whether to employ the ICT assembly, and writes an **employ traceability record** that links back to the **receive traceability record**. The **employ traceability record** includes a link to the acquirer's decision documentation whether to employ the product, as well as documentation of where the product is employed, if the decision is to employ the product. Thus, this **employ traceability record** explains both the rationale of the employment decision and the capacity in which the employed product will be used. This **employ traceability record** enables periodic future inspection to determine whether the product may have been substituted inappropriately, thereby serving as a means to discover security risk vectors described in Scenario #3.

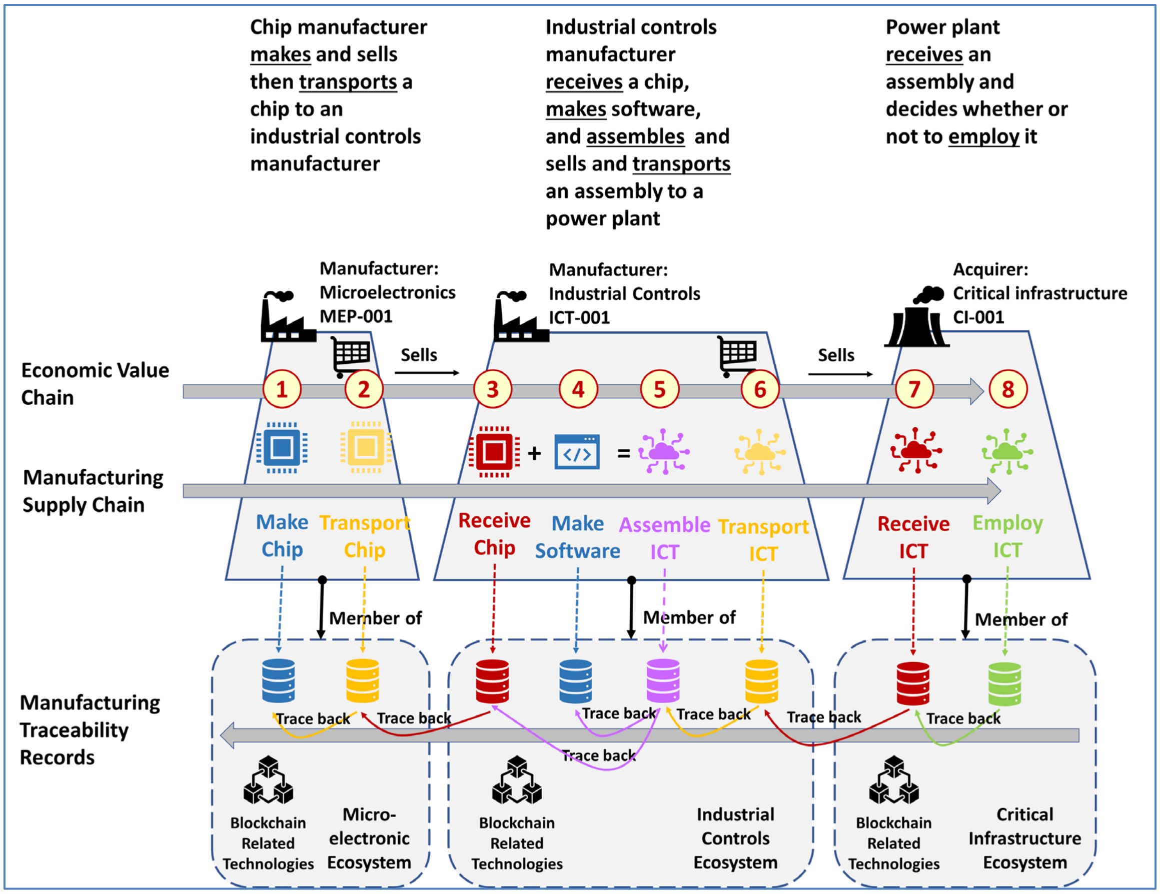


Figure 4: Traceability Chain Mirrors the Manufacturing Supply Chain in Reverse

Each new traceability record written to an ecosystem blockchain points back to the preceding applicable traceability record also written to an ecosystem blockchain (hash-links) thus forming an immutable manufacturing traceability chain which can later be 'crawled' backward through applicable ecosystem blockchains to read the whole traceability chain for full pedigree and provenance information, as described in Scenario #2. The hash-linked manufacturing traceability records link to provable manufacturer claims of authentic product pedigree, and provable provenance as the product moves through the supply chain.

Fully expanded, the shape of the manufacturing supply chain is a tree, and the shape of the corresponding manufacturing traceability chain is the same tree in reverse. **The primary objective of the MVP is to construct the traceability chain (linked traceability records) described above.**

Note: While this MVP will not require smart contracts, the MVP does not preclude the addition of smart contracts to illustrate additional financial and other transactional activities in the context of specific manufacturing traceability record ecosystem blockchain transactions.

3 High-Level Architecture

Overview

The high-level architecture below, develops the structure of the MVP components, expressed in a server/host architecture context. The high-level architecture description then continues to develop the data structure of traceability records and the resulting traceability chain, by stepping through the lifecycle of using traceability records to create a traceability chain.

Components and Server Architecture

Figure 5: Component and Server Architecture, depicts the MVP components. The architecture separates the ecosystem hosts to emphasize that ecosystems (and blockchain instances within) operate, evolve, and innovate independently. The single MVP identity provider provides the ecosystems with a consistent identity scheme. The scenarios are driven by, and results recorded in, a Scenario Dashboard as a separate component.

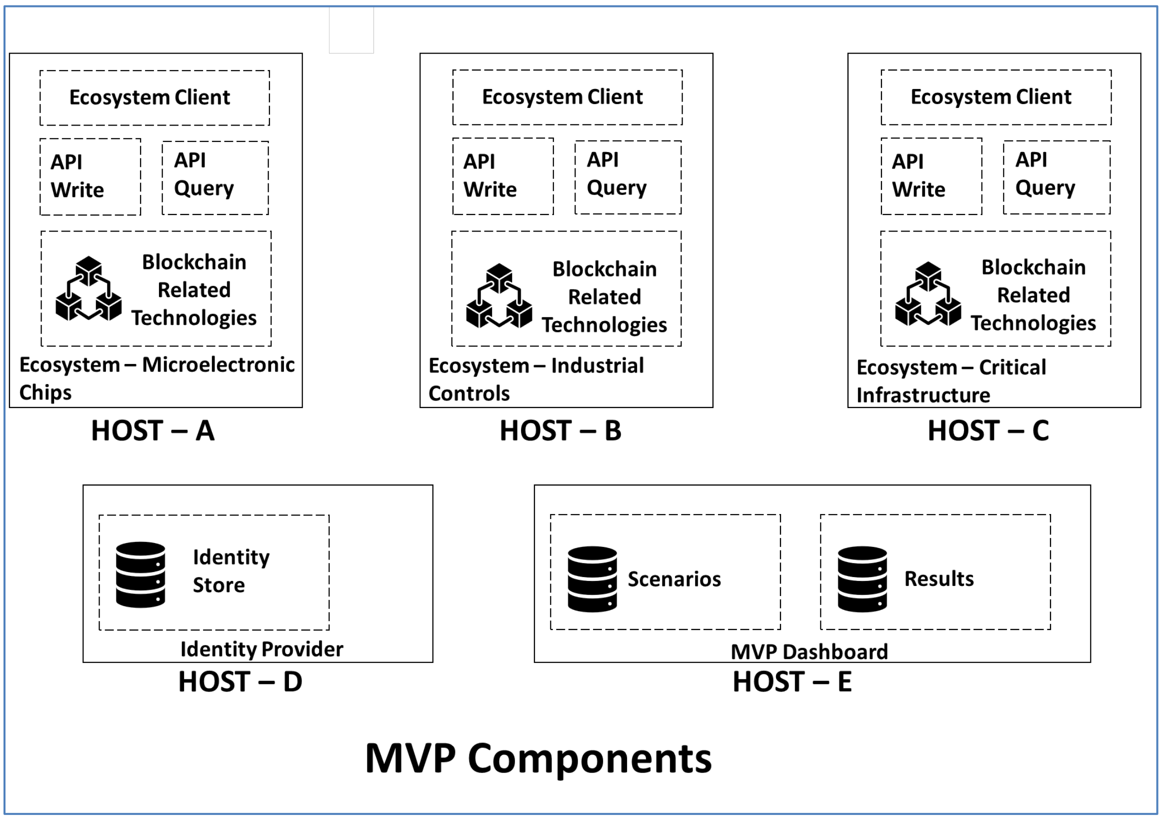


Figure 5: Component and Server Architecture

Identity (role-based)

The MVP assumes one identity provider and a single flat identity space across ecosystems. Identifiers can be simple labels, although in production, identities may be based on Credentials Community Group Decentralized Identifiers (W3C DID) emerging standards. Further, in production each ecosystem governance will independently generate their own identities. Identities for the MVP are role-based, and related to activities of make, assemble, transport, receive, and employ.

Ecosystems (blockchain, query component)

When a traceability chain is crawled, each link to the preceding traceability record can be followed, even to a different ecosystem, to the preceding traceability record. This link includes a hash of the preceding traceability record. For the MVP, the hash of the preceding traceability record can serve as simple authorization to access the preceding traceability record. The hash linking of traceability records is conceptually similar to linking blocks in a blockchain, except a traceability chain is an inverted tree not a linear chain, and spans multiple blockchain instances. Thus, the traceability chain is a higher order data construct above blockchain, retaining the property of tamper evident data.

Note that critical infrastructures may adopt traceability ecosystems at a slower rate than the relevant manufacturing supply chains. Alternately, in the early phases of adoption, the critical infrastructure operating environments can store the traceability records (e.g., receive, employ) in their enterprise asset management and vulnerability analysis systems. If ecosystems are adopted by critical infrastructure operating environments, the traceability records can be stored there.

Blockchain Related Technologies

Each ecosystem will have an independent instance of the blockchain related technologies. The blockchain related technology selected can be the same or differing types across the ecosystems.

Traceability Chain Lifecycle

The sequence of diagrams below illustrates the notional lifecycle of manufacturing traceability records written to industry ecosystem blockchains, and the resultant persistent and immutable traceability chain. The notional lifecycle informs the explication of traceability data types. The diagrams are accompanied by a high-level description of data associated by traceability records. Following the diagrams is a table of traceability records with a summary of applicable data fields.

NOTE: The number of ecosystems and where products are made below, is different from the MVP scenarios above. This difference highlights the flexibility of the traceability chain approach which is intended to accommodate an arbitrary number of stakeholders in an arbitrary number of ecosystems. Nonetheless, the data field requirements for each of the make, assemble, transport, receive, and employ traceability records are the same in any situation.

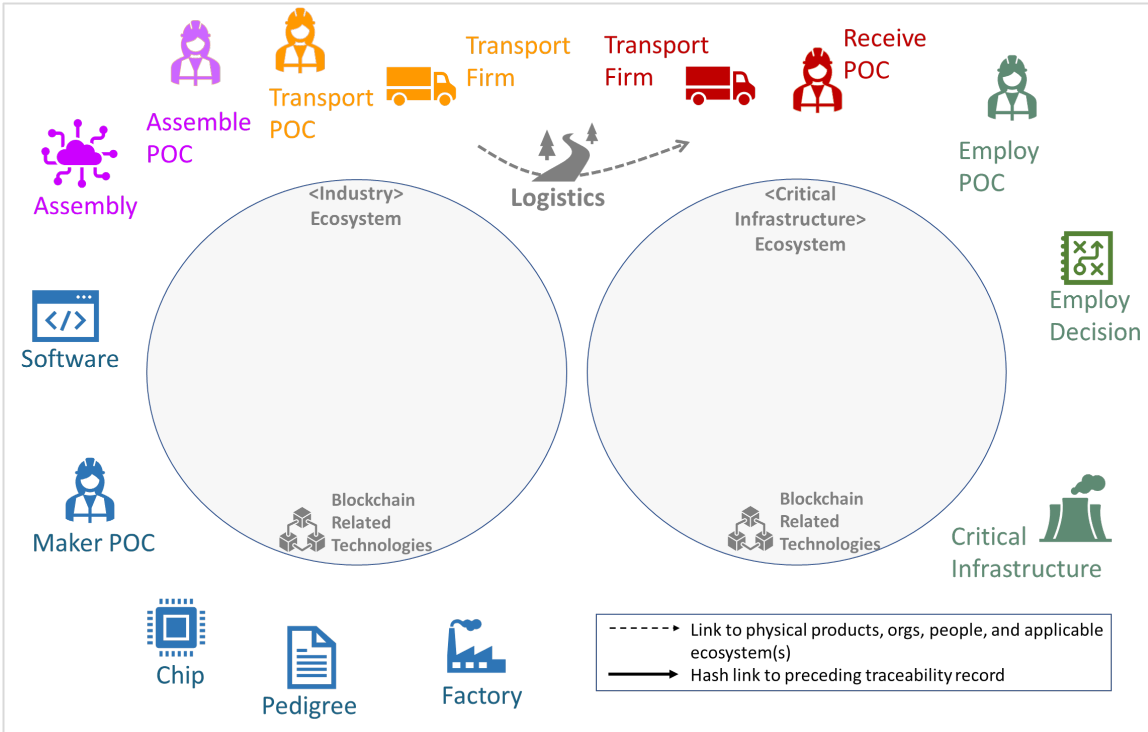
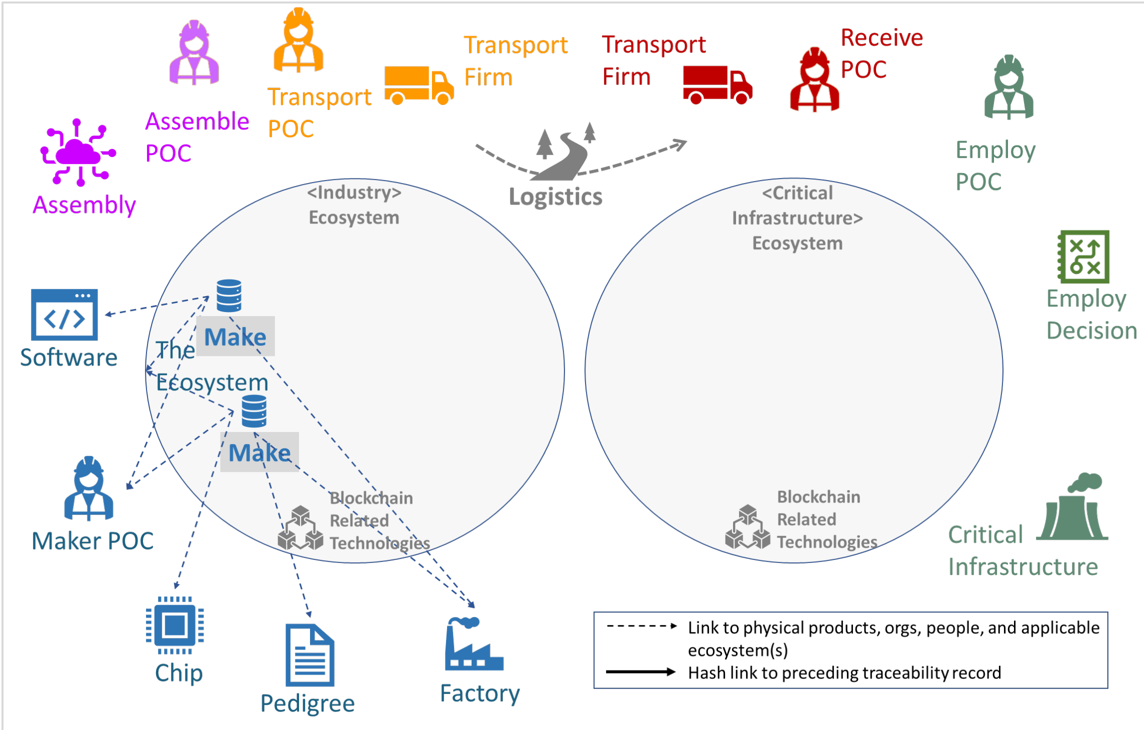


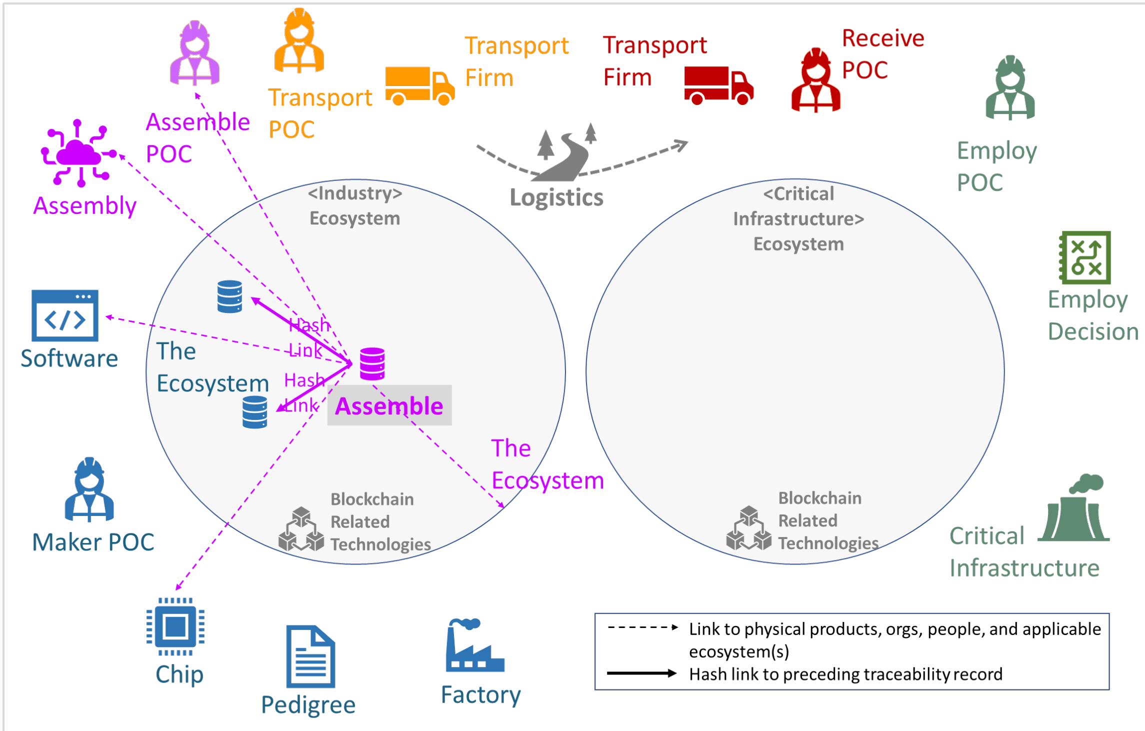
Figure 6: Traceability Chain Lifecycle - Actors

The actors include people and organizations (e.g., factories, critical infrastructure, transport firms), the ecosystems which group actors and enable actors to write blockchain transactions (e.g., traceability records), and the object of traceability (e.g., chip). The people actors are grouped into Make, Assemble, Transport, Receive, and Employ, responsible for those respective activities and are the Author of the respective traceability records.



420 **Figure 7: Notional Traceability Chain Lifecycle - Make**

421 The Make POC writes a Make traceability record to the <industry> ecosystem. The make
422 traceability record includes the Maker POC ID, the Product ID (e.g., chip), link to the Pedigree
423 summary, and link to the Factory (if needed and agreed can query for more detailed pedigree).
424 Another make traceability record is similarly written for software.



425 **Figure 8: Notional Traceability Chain Lifecycle – Assemble**

426 The assemble POC writes an assemble traceability record to the <industry> ecosystem. The
427 assemble traceability record includes a list (in this case two) of included products.

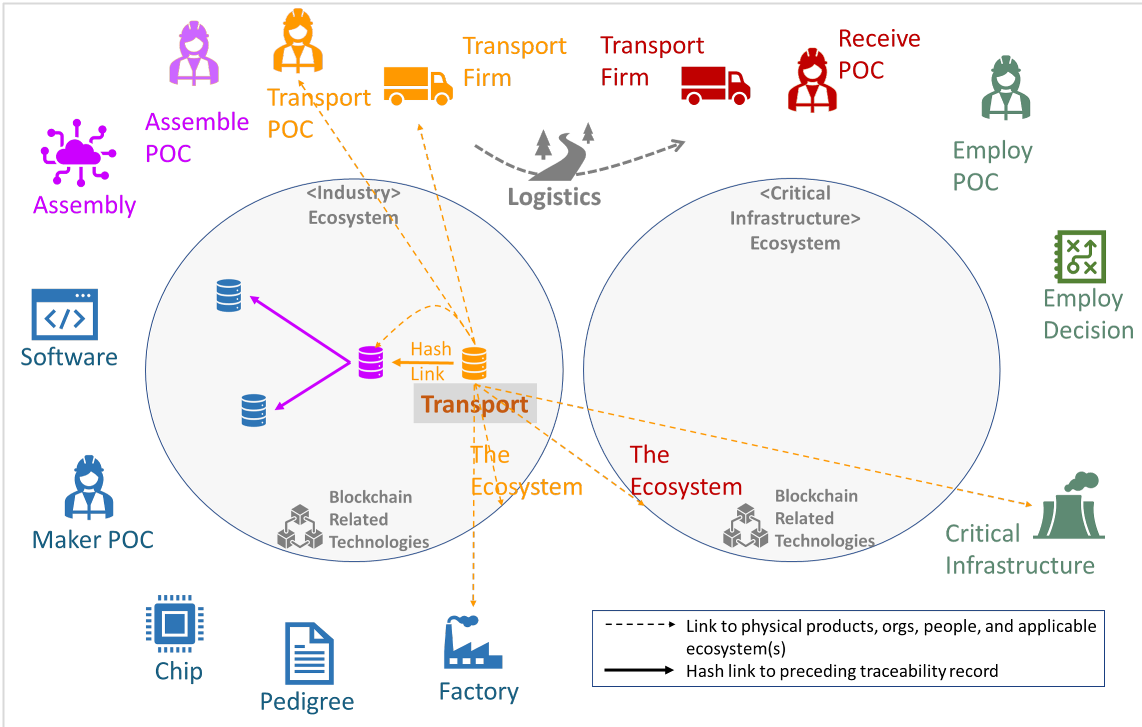
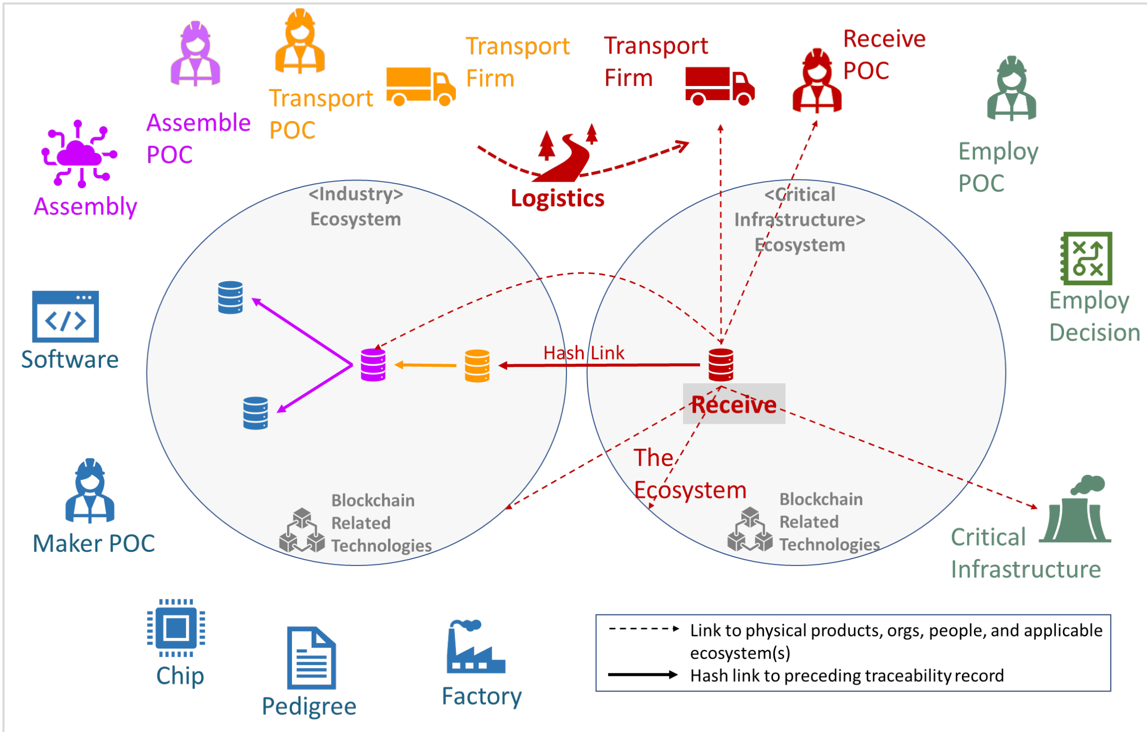


Figure 9: Notional Traceability Chain Lifecycle – Transport

The Transport POC writes a Transport traceability record to the <industry> ecosystem. The Transport traceability record includes the Transport POC ID, the Product ID (e.g., chip), the Factory ID, the original Make traceability record, the destination ecosystem, the destination org ID (e.g., critical infrastructure).



433 **Figure 10: Notional Traceability Chain Lifecycle – Receive**

434 The Receive POC writes a Receive traceability record to the <critical infrastructure> ecosystem.
435 The Receive traceability record includes the Receive POC ID, the Product ID (e.g., chip), the
436 Transport traceability record, the destination ecosystem, the destination org ID (e.g., critical
437 infrastructure).

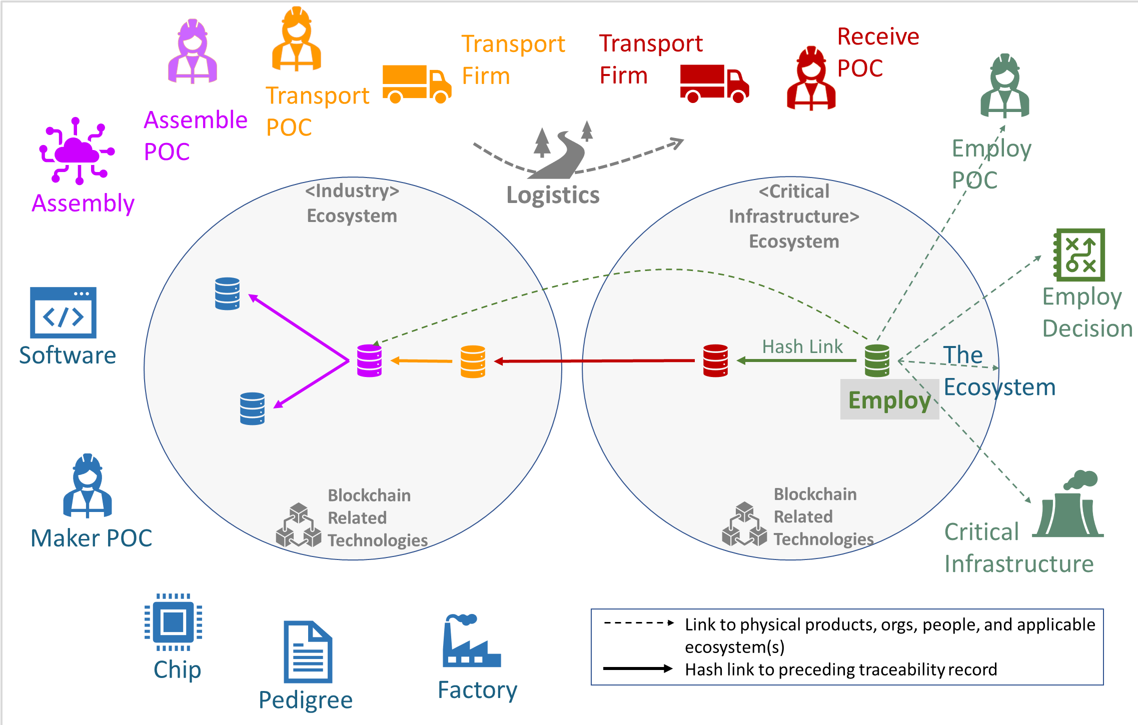


Figure 11: Notional Traceability Lifecycle – Employ

The Employ POC writes a Employ traceability record to the <critical infrastructure> ecosystem. The Employ traceability record includes the Employ POC ID, the Product ID (e.g., chip), the Receive traceability record, the destination ecosystem, the destination org ID (e.g., critical infrastructure).

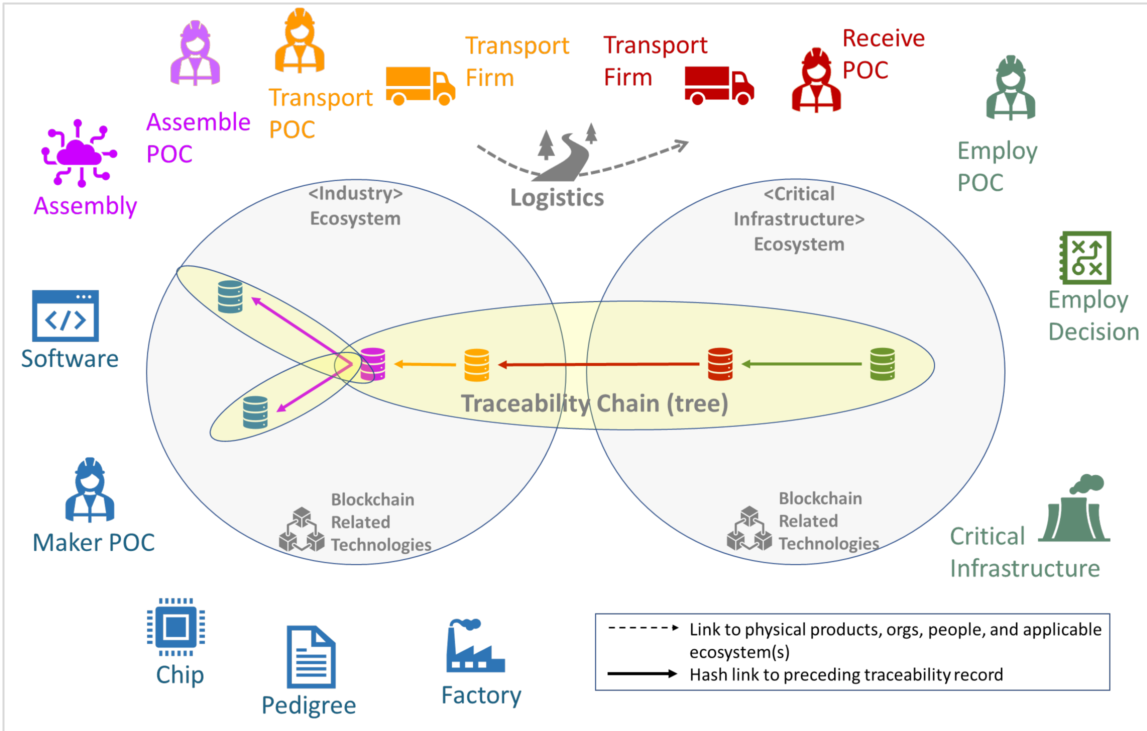


Figure 12: Notional Traceability Chain – Full Chain

The resulting traceability chain is depicted as a singular object, composed of constituent traceability records, which can be read starting at the final receive (or employ) traceability record, and tracing back to the original make records.

Traceability Record Data Types

Traceability records are written as blockchain transactions, of which the data types for the blockchain transaction data payload are specialized and sub-typed according to use. The traceability blockchain transactions are written to the relevant ecosystem blockchain where the activity occurred, and back linked (hash link) to the preceding traceability record as described below.

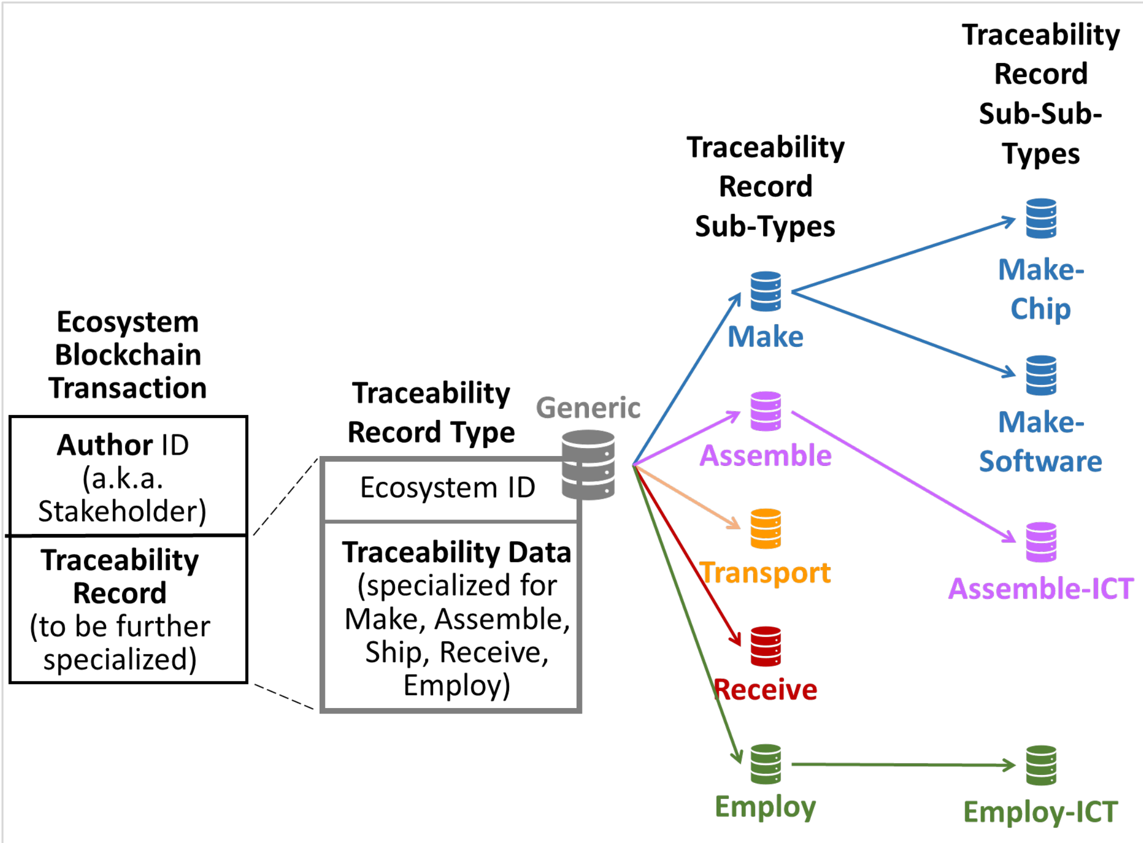


Figure 13: Traceability Data Types

Note that the blockchain address in the blockchain transaction is also called 'author.' The generic traceability record type is specialized to sub-types based on the activity category (Make, Assembly, Ship, Receive, Employ). Make and Employ sub-types, can be further specialized again to sub-sub-types for the specific industry type (e.g., make-chip, make-software). All concrete traceability records for Make and Employ are instances of a sub-sub-type (e.g., Make-Chip). The Transport and Receive traceability records serve as generic provenance links, and are not specialized to relevant industry for this MVP project. This structure of traceability types, sub-types, and sub-sub-types are initial considerations for standards development. The generic sub-types (Make, Assemble, Transport, Receive, Employ) are described in the table below.

Table 1: Traceability Record Sub-type Data Fields

Traceability Record Types	**Data Fields**	**Notes**
Top level (generic)	• Blockchain user address • Traceability Record (see below sub-types)	The blockchain user address is a public key, derived from the user private key; the user is the relevant stakeholder and an individual (not organization). Decentralized identity standards orgs are working the complex issues regarding organizational identity.
Make Sub-type	• Ecosystem ID (origination) • Factory ID (organization) • Product ID • Maker POC • Pedigree Statement	Factory is in (origination) ecosystem
Assemble Sub-type	• Ecosystem ID (origination) • Assembly ID • Assemble POC • For each product included in the assembly ○ Hash-link to Make traceability record ○ Product ID in Make traceability record	Assemble can refer to assemble / make records in the same ecosystem, and/or receive records from prior ecosystems Assemble traceability records are the branching nodes in the traceability chain/tree
Transport Sub-type	• Ecosystem ID (origination) • Factory ID (origination) • Transport POC • Transport Firm • Ecosystem ID (destination) • Consuming ID (destination organization) • Hash-link to Assemble or Make traceability record • Product ID (assemble or simple make)	Transport record is in origination ecosystem
Receive	• Ecosystem ID (origination) • Ecosystem ID (destination) • Transport Firm • Receive POC • Hash link to transport record • Product ID (assemble or simple make) • Consuming ID (destination organization)	Receive record is in destination ecosystem
Employ	• Ecosystem ID (final use in critical infrastructure, or equivalent) • Critical Infrastructure (or equivalent) ID • Employ POC • Hash link to receive record • Product ID (assemble or simple make) • Link to employ decision	The employ decision is the document which summarizes the decision to use the product, and where in the critical infrastructure (or equivalent) the product is used.

Cybersecurity Factors

The MVP is primarily concerned with the security and integrity of the overall traceability chain, which inherits properties of immutability from the blockchain associated with each individual traceability record. The MVP assumption is that each blockchain is secure, identities have been properly vetted, so the focus can be on each traceability record, and its data and links. In a production version, it is assumed that each ecosystem's blockchain will need to be risk-assessed and accredited for cybersecurity.

Architectural Notes

MVP Project

The MVP project includes many technical aspects of supply chain, data, and identity technology. Multiple industry contributors will be required to implement the MVP in blockchain related technologies. This project also assumes notional agreement around simplified traceability data types, which in a real industry sector adoption would be subject to negotiation and agreement, the same as any shared data standard.

Ecosystems

The MVP will implement specific manufacturing and critical infrastructure domains: (a) microelectronic chip manufacturers, (b) industrial control manufacturers, and (c) critical infrastructure. While the concepts are illustrated in the MVP using blockchain and a specific set of suppliers and infrastructure, the concepts can be applied to other blockchain related technologies for other manufacturing supply chain domains and critical infrastructures.

Ecosystem Stakeholders and Identity

MVP manufacturers and critical infrastructure operators are stakeholders of their respective manufacturing ecosystems. Each stakeholder has an identity which is unique across the MVP. For example, a critical infrastructure operator who has previously accessed a traceability record, can understand the identity of a microelectronic or industrial controls ecosystem, and the manufacturer stakeholder, who wrote the traceability record. Accessing a traceability record within an ecosystem is performed by providing the hash link to the traceability record to the query facility of the respective ecosystem, as simplified data access management for this MVP. For example, a power plant operator will accept the shipment of an ICT assembly, and in parallel accept the corresponding transport traceability record for the ICT assembly, writing a receive traceability record to acknowledge. This receive traceability record contains links to the preceding ecosystem and transport traceability record, which can be used to follow the traceability chain in reverse. This constraint simplifies the data access management aspect of the MVP implementation.

Identity Technology and Standards

Identity standards are currently being developed with important progress in the W3C suite of decentralized Identity specifications. There are open questions about what the manufacturing supply chain traceability ecosystem identity standards should be in the future. This MVP is intended to be a foundational starting point for refinement of future manufacturing supply chain traceability ecosystem identity standards. The section High Level Architecture above discusses a simple role-based identity scheme for use in this MVP project, intended to be supplanted by identity standards, both individual and organizational, as they become available.

Ecosystem Operations

The MVP illustrates select aspects of writing and reading manufacturing supply chain traceability records. A full implementation will include additional features, governance, and operational models that will leverage the specific blockchain related technologies being used. NIST IR 8419 [1] describes industry case studies which include an example where the ecosystem is operated by a consortium (e.g., Mediledger, pharma industry) where the consortium uses a third party company to build and operate the ecosystem blockchain and related code. Other operating models are possible, and beyond the scope of the MVP.

Blockchain Technology

Each MVP ecosystem (manufacturing and critical infrastructure) will include an instance of permissioned blockchain independent from the other ecosystem blockchains (no sharing of blockchain implementation across ecosystems). Beyond that, there is no requirement to employ a specific type of blockchain other than to use a type of permissioned blockchain technology which uses byzantine fault tolerance consensus mechanisms. Recommendation to keep the MVP simplified is to use the same type of byzantine fault tolerance consensus permission blockchain technology in each instance of ecosystem blockchain. Note that blockchain smart contracts are optional for the MVP.

Blockchain Data

The traceability record data in the MVP ecosystem blockchains will be notional and representative of industry domain traceability data however, will not be based on specific standards (see "Data Standards" below) in order to facilitate rapid implementation. The new concept in the MVP is the mechanism to create and read a traceability chain (tree) across manufacturing ecosystems.

The MVP blockchain transaction data (traceability records) is intended to be minimal in size and complexity. The transaction data can include notional pointers to manufacturer's private manufacturing data to indicate that a critical infrastructure operator could, if mutually agreed, use the traceability data to access internal manufacturer process data. Access to the private manufacturing data is controlled by the manufacturer, is expected to be negotiated with purchasers (other suppliers and critical infrastructure operators), and is not written to the ecosystem blockchain. This notional pointer can be used in scenarios below to illustrate anticipated real world forensic activities to verify authenticity in certain traceability use cases.

Data Standards

This MVP is intended to be a foundational starting point for refinement of future manufacturing supply chain traceability ecosystem data standards. Subsequent refinements to the MVP could incorporate future traceability record standards, specific to each industry. The section High-Level Architecture above discusses a set of notional traceability record data types for use in this project.

Integration

This MVP includes integration as well as technology. This MVP is a starting point for researching and demonstrating cross manufacturing supply chain exchange of traceability information. Future research could explore data and identity standards, and different modes of organizing and governing ecosystems.

Component List

All components below are intended to be implemented in software and data (not physical components).

- MEP Ecosystem
  - Instance of blockchain technology (can be the same technology across ecosystems)

    - Instance of query facility (can be the same technology across ecosystems)
    - Stakeholders (e.g., MEP-001), each with MVP-wide unique identity
    - Chips, each with unique identity, synthetic factory pedigree data
- ICT Ecosystem
    - Instance of blockchain technology (can be the same technology across ecosystems)
    - Instance of query facility (can be the same technology across ecosystems)
    - Stakeholders (e.g., ICT-001), each with MVP-wide unique identity
    - Software, each with unique identity, synthetic factory pedigree data
    - Assemblies (chip + software + [optional: sensors, mechanical device]), each with unique identity, synthetic factory pedigree data
- CI Ecosystem
    - Instance of blockchain technology (can be the same technology across ecosystems)
    - Instance of query facility (can be the same technology across ecosystems)
    - Stakeholders (e.g., CI-001), each with MVP-wide unique identity
    - Critical infrastructure, each with unique identity, synthetic pedigree data
- MVP Dashboard with functions:
    - Initialize (clear data)
    - Scenario 1, execute scenario, display activity, save results
    - Scenario 2, execute scenario, display activity, save results
    - Scenario 3, execute scenario, display activity, save results

MVP Requirements

1. Create ecosystems and actors per Component List above and in concordance with the high-level architecture.
2. Create data types per Table 1: Traceability Record Sub-type Data Fields above.
3. Execute scenarios per the Scenario section above and capture results.

4 Relevant Standards and Guidance

List of standards used for this project:

Table 2: Standards and Guidance

Standards Body	Nomenclature	Name
Global Semiconductor Alliance	WP-19	Using a Virtual Identifier Thread for Root of Trust and Reliability

5 Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity, and to other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices but does not imply that products with these characteristics will meet an industry's requirements for regulatory approval or accreditation.

Table 3: Security Control Map

Cybersecurity Framework v1.1			SP 800-53 R5
Function	**Category**	**Subcategory**	
Identify (ID)	Supply Chain Risk Management (ID.SC)	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.	SA-9, SA-11, SA-12, PM-9 SR-6
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	AU-2, AU-6, AU-12, AU-16, PS-7. SA-9, SA-12 SR-6
	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8, PM-5
Protect (PR)	Identity Management, Authentication, and Access Control (PR.AC)	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	MP-8, SC-12, SC-28
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SC-16, SI-7
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	CM-2
Detect (DE)	Detection Processes (DE.DP)	DE.DP-2: Detection activities comply with all applicable requirements	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
NA	NA	NA	SR-4
NA	NA	NA	SR-7
NA	NA	NA	SR-11

Appendix A References

[1] K. Stouffer, M. Pease, J. Lubell, E. Wallace, H. Reed, V. Martin, S. Granata, A. Noh and C. Freeberg, "Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives," National Institute of Standards and Technology, Gaithersburg, MD, 2022. Available: https://doi.org/10.6028/NIST.IR.8419. [Accessed 12 April 2023].

[2] "Supply Chain Integrity, Transparency, and Trust (scitt)," Internet Engineering Task Force (IETF), [Online]. Available: https://datatracker.ietf.org/wg/scitt/about/. [Accessed 3 April 2023].

[3] "Decentralized Identifiers (DIDs) v1.0," World Wide Web Consortium (W3C) , [Online]. Available: https://www.w3.org/TR/did-core/. [Accessed 3 April 2023].

[4] "Trusted IoT Ecosystem Security (TIES)," Global Semiconductor Alliance (GSA), [Online]. Available: https://www.gsaglobal.org/iot/ties/. [Accessed 3 April 2023].

[5] "Supply Chain Traceability," MIT Sustainable Supply Chain Lab, [Online]. Available: https://sustainable.mit.edu/supply-chain-traceability/. [Accessed 8 March 2023].

[6] "Information and communications Technology Supply Chain Risk Management," DHS CISA, [Online]. Available: https://www.cisa.gov/information-and-communications-technology-supply-chain-risk-management. [Accessed 8 March 2023].

[7] "Supply Chain Assurance," National Institute of Standards (NIST) National Cybersecurity Center of Excellence (NCCoE), [Online]. Available: https://www.nccoe.nist.gov/supply-chain-assurance. [Accessed 8 March 2023].

Appendix B Acronyms and Abbreviations

CI	Critical Infrastructure
DID	Decentralized Identifier
ICT	Industrial Control Technology
MVP	Minimum Viable Product
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
POC	Point of Contact
RI	Reference Implementation
W3C	World Wide Web Consortium