

NISTIR 8419

Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability:

Needs and Industry Perspectives

Keith Stouffer
Michael Pease
Joshua Lubell
Evan Wallace
Harvey Reed
Vivian L. Martin, Ph.D.
Steve Granata
Andrew Noh
Connor Freeberg

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8419>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8419

Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability:

Needs and Industry Perspectives

Keith Stouffer
Michael Pease
*Smart Connected Systems
Communications Technology Laboratory*

Joshua Lubell
Evan Wallace
*Systems Integration Division
Engineering Laboratory*

Harvey Reed
Vivian L. Martin, Ph.D.
Steve Granata
Andrew Noh
Connor Freeberg
*The MITRE Corporation
McLean, VA*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8419>

April 2022



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
*James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce
for Standards and Technology & Director, National Institute of Standards and Technology*

National Institute of Standards and Technology Interagency or Internal Report 8419
119 pages (April 2022)

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8419>

Certain commercial entities, equipment, 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, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

Submit comments on this publication to: blockchain_nccoe@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

As supply chains 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 and related technologies. This NIST NCCoE publication explores the issues that surround traceability, the role that blockchain and related technologies may be able to play to improve traceability, and several case studies in use today.

Keywords

Blockchain; Cyber-physical anchor; Decentralized; Pedigree; Provenance; Supply Chain; Traceability.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's Cybersecurity programs, projects and publications, visit the [Computer Security Resource Center](#). Information on other efforts at [NIST](#) and in the [Information Technology Laboratory](#) (ITL) is also available.

Acknowledgments

The authors would like to acknowledge and thank a number of individuals and organizations who provided valuable input into this publication, including: Arnaud Brolly, SITA; Daniel Eliot, MITRE; Chris Fabre, Sky Republic; DUST Identity; Jim Wetzel; Pierre-Yves Benain, SITA; Sean Hanlen, Guardtime Federal, Inc.; and Ujjwal Guin, Auburn University.

Table of Contents

1 Introduction 1

 1.1 Purpose 1

 1.2 Scope..... 1

 1.3 Target audience 1

 1.4 Foundational practices 2

 1.5 Relationship to other programs and publications 2

 1.6 Methodology overview 3

 1.7 Summary of insights 3

 1.8 Organization of this paper..... 4

2 Manufacturing Supply Chain Overview and Imperatives 6

 2.1 Introduction 6

 2.2 Supply chain risk..... 6

 2.3 Relevant NIST Special Publications..... 7

 2.4 Product provenance and pedigree 7

 2.5 Ecosystem perspective 8

 2.6 Industrial control system example..... 9

 2.7 Traceability challenges 10

 2.8 Decentralized information sharing..... 12

3 Traceability 14

 3.1 Potential benefits of improved traceability..... 14

 3.2 Applicable domains..... 15

 3.3 Metrics 17

4 Technologies Supporting Traceability 18

 4.1 Blockchain 18

 4.2 Cyber-physical anchors 21

 4.3 Other technologies..... 23

 4.4 Summary 24

5 Considerations for Adoption of Blockchain 25

 5.1 Metrics 25

 5.2 Information exchange standards..... 25

 5.3 Minimum viable ecosystem..... 25

5.4 Multiple blockchains..... 26

5.5 Intellectual property..... 27

5.6 Privacy 28

5.7 Identity for supply chain partners 28

6 Industry Case Studies & Analysis 31

6.1 From Field to Fork..... 31

6.2 Sky Republic with SITA..... 31

6.3 Guardtime Federal and “Perspectives from a Prime”..... 31

6.4 DUST Identity 32

6.5 MediLedger..... 32

6.6 Chain Integration Project (CHIP) 33

6.7 Methodology 33

7 Future Research Opportunities 39

7.1 Identity 41

7.2 Message content standards..... 42

7.3 Barriers to entry 42

7.4 Supply chain traceability ecosystems 43

7.5 Metrics 44

7.6 Patterns in supply chain traceability..... 44

7.7 Ecosystem scale and interoperability..... 45

7.8 Opportunities cross reference..... 46

8 Conclusions..... 50

List of Appendices

References..... 52

Appendix A— Case Study Analysis Models and Lenses..... 56

A.1 Cyber supply chain risk management..... 56

A.2 Technology lenses & adoption curve 57

A.3 Win/win and production possibility frontier 60

A.4 Intermediation, disintermediation, classic make/buy 61

A.5 Centralized and decentralized 62

Appendix B— Submitted Case Studies..... 65

B.1 Case Study: Guardtime Federal, Inc..... 65

B.2 Case Study: Perspectives from A Prime 69

B.3 Case Study: Sky Republic 74

B.4 Case Study: Manufacturing Supply Chain Traceability from “Field to Fork” .. 81

B.5 Case Study: DUST Identity 86

Appendix C— Case Study Individual Analysis Notes 93

C.1 Field to Fork..... 93

C.2 Sky Republic..... 94

C.3 Guardtime Federal 95

C.4 Large Prime 96

C.5 DUST Identity 97

C.6 MediLedger FDA Pilot Project..... 99

C.7 Chain Integration Project (CHIP) 100

Appendix D— Mental Models Analysis Candidate Areas for Research 102

D.1 Supply chain risk management candidates..... 102

D.2 Marketplace positioning candidates 103

D.3 Win/win and the production possibility frontier candidates..... 104

D.4 Intermediation and disintermediation, make or buy candidates 105

D.5 Centralization and decentralization candidates..... 105

Appendix E— Analysis notes from Standards and Solution Experts..... 107

E.1 Linking physical objects to data 107

E.2 Data integrity..... 107

E.3 Data traceability 107

E.4 Ecosystems of cooperation 107

E.5 Enabling distributed coordination 108

E.6 Analysis and trade space of decentralization, distribution, and consensus. 108

E.7 Analysis method to quickly discover/form/implement a blockchain enabled ecosystem 108

E.8 Identity 108

E.9 Need to incorporate classified networks 108

E.10 Minimum viable ecosystem..... 108

E.11 Cross blockchain transactions 109

E.12 Standards 109

E.13 Cooperation with logistics and IP blockchain records 109

E.14 Decentralized information sharing (trusted, attributed, resilient) 109

E.15 Metrics 109

E.16 Data patterns of external repositories (from legacy to Solid, IPFS, etc.)..... 110

List of Figures

Figure 1 - Overall methodology 3

Figure 2 - "Intermediate manufacturers" and "higher level manufacturers" 6

Figure 3 - Ecosystem sources of traceability requirements 10

Figure 4 - Traceability records shared using a trusted data layer across an ecosystem 13

Figure 5 - Basic blockchain principle 19

Figure 6 - A simple scenario of blockchain usage to validate product data 20

Figure 7 - A more complex scenario of blockchain usage to validate product data 21

Figure 8 - Cyber-physical anchor verification flow 22

Figure 9 - (Left) Current centralized style of web applications vs. (Right) Proposed
access-controlled data pods..... 23

Figure 10 - Network of traceability ecosystems 27

Figure 11 - Community of Interest contributions 39

Figure 12 - NIST's acquirer viewpoint 57

Figure 13 - Characterizing value and impact with lenses 59

Figure 14 - Paths to value: implementation tracks and diffusion 60

Figure 15 - Win/win and PPF 61

Figure 16 - Visuals of decentralization 63

Figure 17 - DUST Identity technical approach..... 88

1 Introduction

Manufacturing supply chains are increasingly critical to maintaining the health, security, and the economic strength of the United States. 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 publication uses supply chain traceability case studies and the outcome of NIST engagement with an associated community of interest, to assess the current state of supply chain traceability and offer several research opportunities.

1.1 Purpose

This publication seeks to catalyze the understanding of traceability in manufacturing supply chains as an ecosystem-wide concern, and to recommend directions of future research in manufacturing supply chain traceability, enabled by blockchain and related technologies.

1.2 Scope

This publication covers topics including existing factors that inhibit manufacturing supply chain traceability, analysis of nascent blockchain-enabled supply chain traceability initiatives in progress, and recommendations for future research in manufacturing supply chain traceability enabled by blockchain and related technologies.

1.3 Target audience

The target audience of this publication encompasses the needs and interests of all stakeholders in the U.S. national manufacturing supply chain. The target audience includes:

- **Businesses engaged in manufacturing:** Manufacturing cuts across a wide array of goods and services, with stakeholders ranging in size from small businesses to large multinational concerns.
- **Regulatory agencies:** Multiple regulatory offices, across federal, state, local, and tribal agencies in the U.S. and internationally, operate under legal authority to assure product safety, and/or prohibit or prosecute fraudulent or malicious supply chain disruptions.
- **Government and industry standards bodies:** Multiple standards bodies span technology domains, industry sectors, supply chain types, etc.
- **Academic researchers:** Many academic institutions contributed to the existing body of knowledge and may desire to pursue future research.

- **Product consumers:** Private individuals, businesses, governments, or other institutions procure products for their individual needs and unique operating environments, driving their specific interests in supply chain traceability.

The target audience of this publication also includes stakeholders in the supply chain for operational technology (OT) including industrial control systems (ICS) utilized in manufacturing plants, utility service operations, and other elements of national critical infrastructure including:

- System engineers, integrators, and architects that design or implement OT
- Administrators, engineers, and other information technology (IT) professionals that manage or secure OT
- Security analysts that assess or test OT security
- Industrial managers responsible for OT, including managers responsible for OT cybersecurity and those responsible for mitigating operational impacts to OT disruption
- Researchers and analysts working to understand unique security aspects of OT
- Technology and industry suppliers that develop OT or OT-related products

1.4 Foundational practices

There are no well-established foundational approaches to improving traceability throughout a manufacturing supply chain ecosystem. Instead, numerous nascent examples of improved traceability in subsets of the manufacturing supply chain were observed and explored in the case studies later in this paper. These provide an initial ecosystem and establish a semantic understanding and implementation for key concepts including identity and traceability.

1.5 Relationship to other programs and publications

This paper builds upon, yet has a different target audience than, related NIST publications dedicated to supply chain security and risk management.

Related NIST publications establish the foundations of supply chain security and supply chain risk management. This paper builds on these foundations, adds a blockchain-enabled ecosystem perspective, and provides recommendations for future research in manufacturing supply chain traceability. NIST publications related to this publication include Special Publication 800-161 [1], Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Supply Chain Risk Management control family in Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations [2], and Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations.

1.6 Methodology overview

The methodology used for this paper is based on community of interest stakeholder engagement as described below and illustrated in [Figure 1](#).

Overall Methodology

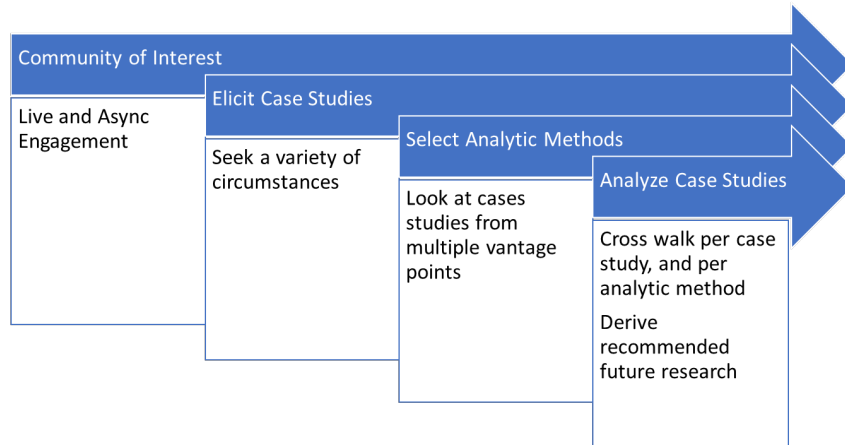


Figure 1 - Overall methodology

2. Survey traceability concerns across microelectronics, aerospace, food and agriculture, and other domains and their end-use operating environments. Elicit knowledge using a combination of live events, individual meetings, and soliciting written case studies which describe their efforts.
3. Select analytic methods for case studies. Seek multiple vantage points to get a comprehensive perspective. Considerations for the analysis include individual concerns, challenges, and benefits and extend to the ecosystem perspective for win-win outcomes.
4. Analyze and compare case studies to gain insights. Derive recommendations for future research directions.

1.7 Summary of insights

1. Traceability (including pedigree and provenance records) needs to be shared via ecosystems of supply chain participants to transcend the limitations of bi-lateral message exchange. Further, tagging physical objects to the traceability record provides more

complete linkage. Operating as a multi-lateral ecosystem assures traceability records can be read and understood even if the participants are separated by multiple tiers.

2. These ecosystems can use blockchain and related technologies to exchange traceability records to cryptographically assure that traceability records are properly attributed, data is tamper-evident, and data cannot be deleted. While it is possible to exchange and record messages without blockchain (or similar cryptographic technology with proofs of data integrity), critical infrastructures and the supply chains that supply them are under increasing pressure to assure integrity of goods used.
3. This approach is already being adopted in some areas, and this paper contains seven case studies and analysis. Each case study is different; however, some common traits emerge indicating that further research is required in these areas:
 - a. Identity
 - b. Message Content Standards
 - c. Barriers to Entry
 - d. Supply Chain traceability Ecosystems
 - e. Metrics
 - f. Patterns in Supply Chain Traceability
 - g. Ecosystem Scale and Interoperability
4. The authors encourage further research, experimentation, and discussion in manufacturing domains to explore the topics above and discover further innovations to improve traceability of manufacturing supply chains.

1.8 Organization of this paper

The remaining sections of the paper are:

[Section 2](#) “Manufacturing Supply Chain Overview and Imperatives” reviews the current state of supply chain risk analysis and introduces an ecosystem perspective to complement the current per stakeholder perspective in Supply Chain Risk Management (SCRM) analysis.

[Section 3](#) “Traceability” reviews the desired benefits traceability may offer and example domains for which traceability is applicable.

[Section 4](#) “Technologies Supporting Traceability” reviews technologies, both mature and emerging, which can be used to link goods and services to data records, then share the data records across a wide set of supply chain stakeholders.

[Section 5](#) “Considerations for Adoption of Blockchain” reviews the challenges and risks associated with establishing a blockchain capability for a subset of the supply chain and the

resulting ecosystem. Blockchain is one technology with features corresponding to drivers for supply chain traceability, such as pedigree and provenance for products and records.

[Section 6](#) “Industry Case Studies & Analysis” reviews the methodology for industry engagement, organizations who submitted case studies, and the summaries of the submitted case studies. Following are the analyses of the case studies viewed through perspectives or mental models selected in the methodology. Full description of the analysis methods and full case studies are found in the Appendices.

[Section 7](#) “Future Research” summarizes indications of future research needed. Future research is intended to be directional, not specific, and performed by a variety of stakeholders including but not limited to industry, academia, and government organizations.

[Appendices](#) for Case Study Methodologies and Case Study submissions are provided as supporting documentation of the synthesis of inputs into the future research themes. They include researcher notes from case study observations and candidate subjects of interest, as well as resources for the models and lenses employed. These are the data underlying the paper’s discussions and conclusions.

2 Manufacturing Supply Chain Overview and Imperatives

2.1 Introduction

In this document, the term *supply chain* refers to the linked set of resources and processes between and among multiple levels of enterprises, each of which is an acquirer that begins with the sourcing of products and services and extends through their life cycle. A manufacturing supply chain begins with its most fundamental elements of raw materials and basic commodities, and flows through tiers of added value, product integration, and secondary/tertiary/etc., manufacturing. Eventually the supply chain flows through distribution to the point of product procurement or consumption by private individuals, businesses, governments, and other institutions. The supply chain is not linear as the word “chain” implies, rather it is more of a graph or web. The diagram below, [Figure 2](#), shows a simplified view of the supply chain with one branch to emphasize the web or graph nature. Activities occurring in the end operating environment (e.g., post-sale), are not depicted but also contribute to the de-facto network of supply chain management. These include claims, returns, callbacks, and maintenance services, all of which add to the richness of use cases in supply chain traceability that have potential implementations in blockchain.

Supply Chain Flow of Materials and Goods

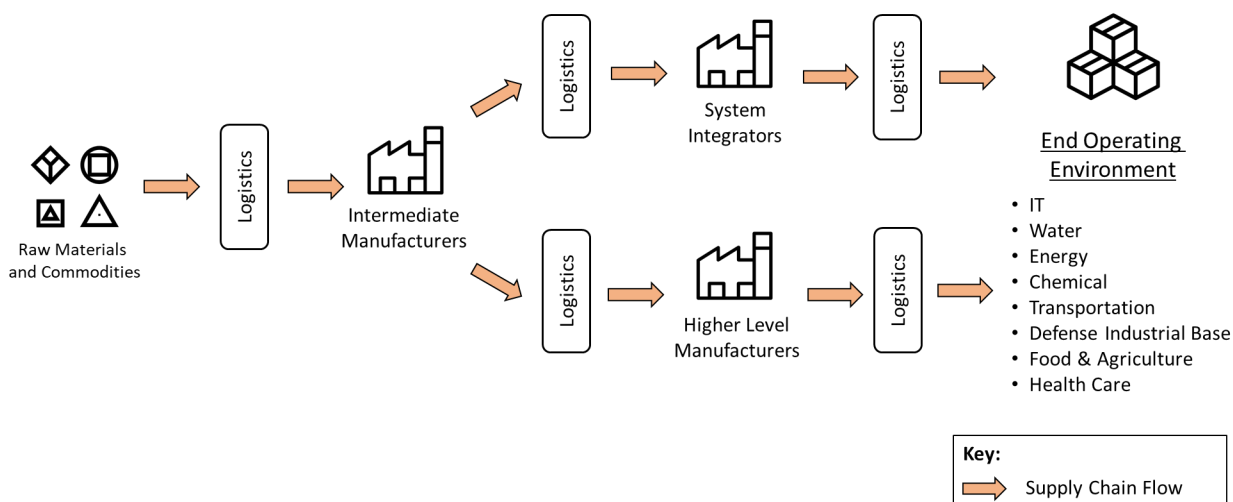


Figure 2 - "Intermediate manufacturers" and "higher level manufacturers"

2.2 Supply chain risk

The U.S. national supply chain of manufactured products faces growing risks to its resiliency and continuity, driven by economic, logistical, and technological factors. Supply chain risks increase when parties are unstable financially, or during times of economic, cyber, or logistical disruption to the operations and continuity of key supply chain elements. The global manufacturing supply chain presents significant economic benefits including low cost and robust competition, while

simultaneously posing the inherent risk of low-visibility or opaque threats to manufactured product quality, authenticity, and fraudulent or nefarious activity.

Exposure to supply chain risk increases when parties lack sufficient visibility and understanding of development, sourcing, production, distribution, deployment, and eventual disposal of products moving through all tiers. Actors with insufficient visibility into the supply chain face a gamut of risks that include production of substandard products, nefarious product counterfeiting, malicious product tampering, insertion of cybersecurity exploits, and/or loss or compromise of trade secrets and intellectual property (IP).

2.3 Relevant NIST Special Publications

NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations [1], and 800-53 Revision 5 [2], Security and Privacy Controls for Information Systems and Organizations, each include foundational material covering enterprise supply chain risk management (SCRM) methods. These documents include measures for enterprises at all tiers of the supply chain to increase their overall visibility across the entire supply chain, thereby illuminating and reducing threats to manufactured product quality, authenticity, and fraudulent or nefarious activity. Both documents cover the information and communications technology and operational technology (ICT/OT) sectors and are written to an audience of ICT/OT system developers and acquirers.

2.4 Product provenance and pedigree

NIST SP 800-161 [1] recommends that enterprises establish measures to track the provenance of products flowing through their supply chains. NIST SP 800-161 and NIST SP 800-53 define *provenance* as: “...the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data.” NIST SP 800-53 includes a supply chain security control covering product acquirer identification of provenance, as follows:

SR-4 PROVENANCE

Control: Document, monitor, and maintain valid provenance of the following systems, system components, and associated data.

Discussion: Every system and system component have a point of origin and may be changed throughout its existence. Provenance is the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. Organizations consider developing procedures (see SR-1) for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and system components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations have methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data. These actions help track, assess, and document any changes to the provenance, including changes in supply chain elements or configuration, and help ensure non-repudiation of provenance information and the provenance change records. Provenance considerations are addressed throughout the system development life cycle and incorporated into contracts and other arrangements, as appropriate.

NIST SP 800-53 control SR-4 includes a sub-control [SR-4(4)] that defines *pedigree* in terms of the linkage between the visibility of supply chain provenance with product acquirer determination of trust in product authenticity:

SR-4(4) PROVENANCE | SUPPLY CHAIN INTEGRITY — PEDIGREE

Employ...and conduct...organization-defined analysis...to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services.

Discussion: Authoritative information regarding the internal composition of system components and the provenance of technology, products, and services provides a strong basis for trust. The validation of the internal composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software this includes the composition of open-source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid. The validation of the internal composition and provenance can be achieved by various evidentiary artifacts or records that both manufacturers and suppliers produce during the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of technology, products, and services.

NIST SP 800-53 also contains an additional supply chain security control, SR-11, that emphasizes the importance of product authenticity to enterprises in the supply chain, as follows:

SR-11 COMPONENT AUTHENTICITY

Discussion: Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code.

Taken together, the foundational NIST SCRM definitions and recommendations establish the need and utility for product acquirers throughout the supply chain to establish product provenance. NIST recommendations compel product acquirers to use provenance as a strong measure of assurance for the pedigree of products against supply chain-based threats to quality, authenticity, and fraudulent or nefarious activity. Traceability is the key enabler to assure provenance and pedigree.

2.5 Ecosystem perspective

This document portrays an ecosystem-oriented manufacturing supply chain perspective layered atop the existing “per acquirer” perspective. The ecosystem perspective serves to define traceability for a subset (an ecosystem) of the manufacturing supply chain, and to share and store data records used to establish traceability. Traceability requirements and their means of implementation will be unique for each ecosystem. Traceability data includes information about product provenance, pedigree, and other data as needed.

Industry contributions to this inquiry indicate that an ecosystem perspective is necessary to enable multi-lateral supply chain information sharing and migrate away from existing linear information flows based on numerous bi-lateral agreements. The existing status quo of information sharing is susceptible to incomplete coverages, differing implementation, and

potential semantic gaps in data elements. A semantic gap may occur when a stakeholder multiple tiers away writes 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.

Another potential gap arising from chained bi-lateral agreements is trust transitivity. This occurs as a broken “chain of trust” induced by point-to-point exchanges. If Company A sends data to Company B and B transmits to Company C, the original traceability information from A may not be transferred to C. At that point C is faced with trusting A by way of having trusted B. Maintaining traceability information sharing at the ecosystem level can allow participants to verify data in a variety of traceability situations. Ecosystem-wide use of a trusted means to exchange traceability data records ensures trust in the traceability data records.

Prior NIST documents treat each supply chain tier as having a “per acquirer” perspective which provides risk analysis context and highlights the challenge of establishing pedigree and provenance across multiple tiers. This document builds on that approach with an ecosystem perspective, and it recognizes the importance of certain acquirers who establish foundational traceability requirements for a subset (ecosystem) of the supply chain.

2.6 Industrial control system example

Supply chain traceability enables the product acquirer to verify the provenance and subsequently establish the pedigree of goods and services flowing through ecosystems of potentially overlapping manufacturing supply chains. Each manufacturing supply chain ecosystem has a set of end-operating environments, each of which itself drives traceability requirements from those environments back through multiple tiers of the supply chain. The end-operating environment establishes risks unique to that environment. These risks drive criticality of traceability of pedigree and provenance to assure genuine and uncompromised parts as an aspect of risk mitigation. Establishment of traceability including provenance and pedigree enables component authentication and non-repudiation.

For example, nuclear power generation plants must ensure that the industrial control systems (ICS) they use to regulate nuclear fuel and manage handling of spent fuel rods, are secure and not compromised with fraudulent or malicious components, including actuators and microelectronics. The end operating environment generates traceability requirements which are successively conveyed back to upstream stakeholders. Traceability requirements then inform developmental activities for applicable stakeholders in the ecosystem, who in turn update their computing resources.

This perspective of an end operating environment generating traceability requirements for an ecosystem is illustrated in [Figure 3](#). It is not shown, but is important to note, that additional traceability requirements can be generated at any point in the supply chain from failure analysis and adversarial test activities which may further expose supply chain vulnerabilities.

Once traceability requirements are implemented, then live traceability information can flow with goods from upstream to downstream stakeholders.

Ecosystem Sources of Traceability Requirements

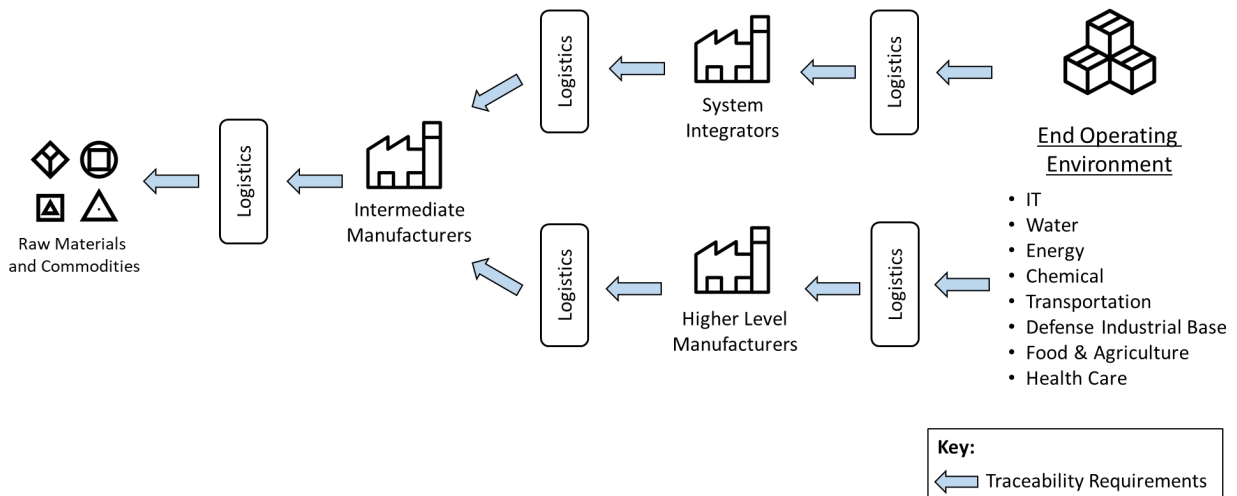


Figure 3 - Ecosystem sources of traceability requirements

This simple example highlights that:

- End operating environments (e.g., nuclear power plants) generate traceability requirements which flow down to multiple tiers of their OT supply chains (e.g., industrial control systems, mechanical control systems, microelectronics, and devices).
- Manufacturing supply chains often provide goods and services to multiple consumers in a myriad of operating environments, each with unique security and resilience requirements.
- No individual perspective taken in isolation is sufficient to determine the full requirements of supply chain traceability, nor can it determine the methods and means to achieve traceability across supply chain ecosystems.

Note that the diagram includes the end operating environment as a single construct, to focus on the supply chain which generates the product that the end operating environments use. In the end operating environment, there are numerous activities such as maintenance and repair that are not shown. In the end operating environment, the concept of trust transitivity (introduced above) applies as well, so that activities such as repair can proceed knowing genuine parts are being used.

2.7 Traceability challenges

Product manufacturing supply chains are multi-faceted and built on a variety of business, economic, and technological factors. Manufacturers choose their suppliers, and consumers choose their sources based on a range of factors that vary from corporate preferences and existing/ongoing business relationships to more discreet considerations such as the existence of limited sources of supply and/or unique characteristics of one product versus another.

Manufacturers often consider the composition of their supply chain to be proprietary business information. In many instances the composition of a manufacturer's supply chain indicates its trade secrets and/or telegraphs proprietary IP to outside parties. The inherent desire of parties in a supply chain to safeguard sensitive business information often overrides their interest in supply chain illumination for risk reduction purposes. Put simply, manufacturers often are inclined to tolerate supply chain risk in their greater interest of safeguarding sensitive business information.

For end-to-end traceability, data records must be able to be shared among all parties in the supply chain, product manufacturers must have high confidence in the existence of robust data protection measures and must have satisfactory constraints on the sharing of their business information. Manufacturers' confidence in data safeguards must be high enough to enable them to participate in shared technology platforms such as distributed ledgers and blockchains, that illuminate the supply chain and reduce all parties' exposure to supply chain risks.

Traceability across manufacturing supply chains requires:

1. An information sharing approach that transcends the typical business-to-business (B2B) bi-lateral exchanges of information that is exchanged in supply chains. The existing bi-lateral exchanges are well-supported by existing IT, legal, contractual, and liability methods and means. In contrast, blockchain and related technologies have potential to share information in a wider yet trusted scope, but are not yet widely supported in IT, legal, contractual, and liability methods and means.
2. Agreement and cooperation to share traceability information across relevant stakeholders, sufficient to correlate traceability with each relevant stakeholders' internal enterprise systems. The tradeoff is between minimal information shared with potentially redundant information in enterprise systems, or more information shared but with increased requirement for fine grained and rules-based access control. The analysis of tradeoff alternatives must include time, effort, and resilience to future changes.
3. Linking physical objects to cyber records. Validation of authenticity of a physical part, requires that the part is inspected (independent of its packaging and labeling) to detect a unique characteristic or signature which can be linked to electronic records. This can occur at 2 layers. The first is an actual physical marking (see [Section 4.2](#), Cyber-Physical Anchors) and the second is a trusted data layer or hardware root of trust. For example, the operator of a nuclear power plant can verify the authenticity of an ICT/OT microelectronic component by comparing the traceability signature on the component with the matching traceability data record in the trusted data layer, before using that component during routine maintenance.
4. Cooperation across the supply chain to write and read traceability records, and adoption of technology, methods, and means to mark and inspect goods and services for linkage with electronic records.
5. Analysis to ensure that incentives for participants across relevant supply chain ecosystems are sufficient to motivate adoption of blockchain and related technologies. Sufficient incentives to write traceability records, combined with a critical mass of early adopters, are necessary to achieve a Minimum Viable Ecosystem (MVE) [3] for traceability information.

MVE is an initial starting condition to subsequently grow participation, strength of incentives, and trust in the supply chain. As the ecosystem establishes the need for traceability, measures must be employed to gauge progress and close gaps.

2.8 Decentralized information sharing

The hypothesis for this paper is that use of trusted decentralized information sharing (Decentralized Ledger Technology, blockchain, etc.) by stakeholders across the manufacturing supply chain, can enable the sharing of traceability data records. A corollary is that blockchain can enable sharing additional data records which may help to incent sufficient stakeholders to form an MVE.

For example, in the diagram below, stakeholders separated by multiple tiers can both write and read traceability records as goods flow toward integrators and end operating environments. Additional data records could be written to attract stakeholders far away from the integration and end operating environments, such as retail or sales records as a form of market intelligence. This may incent broad participation and enable the formation of an MVE. The exchange of traceability and market intelligence data records require protections of both IP (for traceability) and privacy (for market intelligence).

In [Figure 4](#), note that the flow of goods and services can include traceability markers (see Cyber-physical anchors below) which can then be correlated with traceability data records throughout the ecosystem. Beyond the ecosystem, the traceability records may not be understood due to semantic and other gaps, see [Section 5.4](#), Multiple Blockchains below and in [Section 7](#), Future Research Themes.

Traceability Records Shared using a Trusted Data Layer Across an Ecosystem

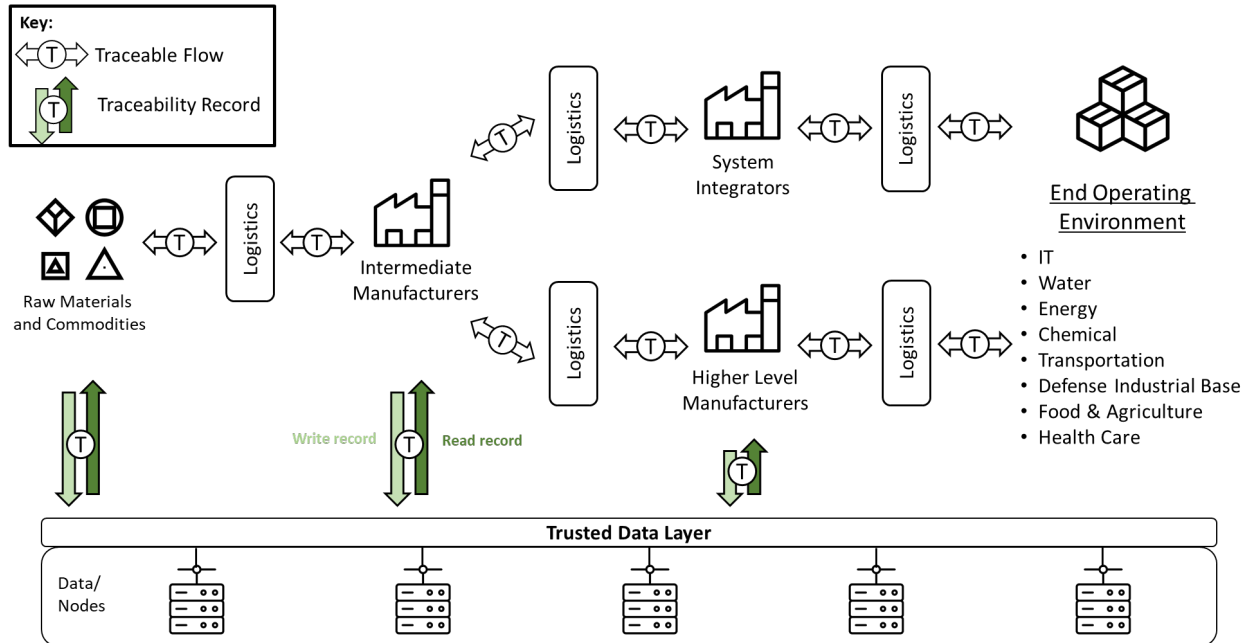


Figure 4 - Traceability records shared using a trusted data layer across an ecosystem

The Trusted Data Layer could be implemented by blockchain and related technologies, see [Section 3](#), Traceability.

3 Traceability

Industry and academic engagement in this inquiry indicates that traceability of goods and materials flowing through a supply chain could be improved with the exchange of traceability data records using blockchain or similar distributed ledger technologies. Traceability confers benefits on the supply chain and is accompanied by challenges to resolve such as IP protections, and the role of standards and metrics, as discussed below. It is important to note that in addition to improved exchange of traceability records, this in no way diminishes the need for accurate data collection and data quality measures, although data collection and data quality considerations are beyond the scope of this paper.

3.1 Potential benefits of improved traceability

[Section 2.4](#) of this publication discussed foundational NIST SCRM recommendations that establish the need and utility for product acquirers throughout the supply chain to establish product provenance. NIST recommendations inform product acquirers regarding information about product provenance as a SCRM measure, providing assurance against supply chain-based threats to product quality, authenticity, and fraudulent or nefarious activity.

Improved supply chain traceability enables producers to provide acquirers with a level of assurance of product provenance and implied pedigree, up to and including a formal warranty of provenance and pedigree. Shared technology platforms such as distributed ledgers and blockchains that illuminate the supply chain are necessary for entities in the supply chain to realize product assurance enabled by supply chain traceability.

3.1.1 Smart contracts

Many supply chains are unique to the entities within them, such that the entities enter into specific contracts with unique terms for the development, production, and/or delivery of manufactured products. NIST Internal Report (NISTIR) 8202, *Blockchain Technology Overview* [4], defines a *smart contract* as follows:

A smart contract is a collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network...The smart contract is executed by nodes within the blockchain network; all nodes that execute the smart contract must derive the same results from the execution, and the results of execution are recorded on the blockchain.

NISTIR 8202 goes on to enumerate some of the benefits of smart contracts:

The smart contract code can represent a multi-party transaction, typically in the context of a business process. In a multi-party scenario, the benefit is that this can provide attestable data and transparency that can foster trust, provide insight that can enable better business decisions, reduce costs from reconciliation that exists in traditional business to business applications, and reduce the time to complete a transaction.

NISTIR 8202 describes the benefits of supply chain entities utilizing smart contracts in multi-party business transactions, which occur often in supply chains characterized by business or government/institutional acquisition of manufactured products. Entities at all tiers of these supply chains participate in smart contracts, including utilizing cryptographically signed transactions on the blockchain network. In these instances, the blockchain-enabled smart contract

acts to document product provenance and illuminate the supply chain, thereby serving as a product acquirer SCRM measure.

The benefit of smart contracts in blockchain is that many blockchains (e.g., Enterprise Ethereum, Tendermint, Cosmos, and Polkadot) execute the smart contract code within the virtual machine of each blockchain node during transaction validation. Smart code execution validates the transaction and prevents subversion by external code running in processes outside the blockchain. Further, the smart contracts in effect form the backbone of new additional processes which must be complemented by external code. External distributed apps use the native blockchain smart contracts in the overall process architecture.

3.1.2 Standards-based approach to protecting proprietary information

A standards-based approach is necessary to facilitate widespread adoption of blockchain-enabled smart contracts. The standard must include specific supply chain data elements that multiple parties may share among the parties to a smart contract or within a particular supply chain, without exposing their proprietary and/or business-sensitive information. For example, Guardtime Federal's immutability features choices in protection of data by using on- and off-chain means of persistence for proprietary information. The benefit of such sharing would be for parties engaged in all tiers of the supply chain to assure product provenance and implied pedigree by means of supply chain illumination.

While smart contract practices are maturing and could potentially benefit from standards, in the absence of standards numerous studies of smart contracts are being published, with a meta-study [5] (study of smart contract studies) proposing a taxonomy for smart contracts. Table 10 in [5] identifies numerous smart contract studies related to manufacturing and supply chain.

3.2 Applicable domains

There are numerous domains for which traceability as described above is applicable. Some of these domains are substantiated by case studies included in the paper, discussions with the community of interest, and some by case studies not suitable for public release.

- Parts / components,
 - Track physical parts in pedigree and provenance electronic records (e.g., cyber-physical anchors)
 - Share pedigree and provenance electronic records across ecosystem partner stakeholders
 - Distribution and Retail (Auburn CHIP case study, [Section 6.6](#))
 - Cyber-physical anchors (DUST Identity case study, [Section 6.4](#))
- Food, batch, continuous flow
 - Track bulk food goods from farm to processing plants

- Gluten-free oats (Agribusiness case study, [Section 6.1](#))
- Pharma
 - Track controlled drugs through forward and reverse logistics (MediLedger case study, [Section 6.5](#))
- Software
 - Product functionality is increasingly delivered using software and the software development process itself can be considered as a supply chain
 - NIST is developing preliminary draft version of NIST Cybersecurity Practice Guide SP 1800-34, Validating the Integrity of Computing Devices, which focuses on trusted devices for computing
 - Track software development process (Aerospace and Defense, Guardtime Federal and Large Prime case study, [Section 6.3](#))
- Data
 - Digital twins [6] are a digital representation of a physical machine or system, and the manufacturing process itself.
 - Digital twin models (Aerospace and Defense memo¹) are being encouraged to accelerate developmental processes; however, digital twins are also susceptible to supply chain vulnerabilities.
 - Additive manufacturing is being rapidly adopted to shorten production cycle time, however additive manufacturing data is vulnerable to corruption (Aerospace and Defense Small Business Innovation Research (SBIR) project²)
 - AI training requires curation and stewardship of AI/ML training data including assuring that training data is not corrupted (Aerospace and Defense summary of classified AFCEA International brief³)
 - Sensor-to-shooter connections are a form of supply chain that performs targeting functions; the dynamics of connecting devices in ways that were unanticipated at

¹ <https://software.af.mil/wp-content/uploads/2021/05/Digital-Building-Code-and-Scorecard-Memo-v15.pdf>.

² <https://blog.simbachain.com/blog/bringing-blockchain-enabled-additive-manufacturing-to-battlefields>.

³ <https://www.afcea.org/content/ai-key-cyber-operations-caveat>.

the time of initial fielding⁴, raises questions about assuring provenance and pedigree of data exchanged between them.

3.3 Metrics

Traceability metrics are a requirement for an MVE to be established and later evolve to meet dynamic needs of the supply chain. Traceability gaps express whether the ecosystem has met a traceability requirement or not, and potentially the proportion of completion (coverage). An MVE will use traceability metrics to motivate participants to marshal the resources and cooperation needed to achieve traceability goals for that ecosystem. Traceability metrics are discussed in [Section 5](#), and as a topic for future research.

⁴ <https://www.af.mil/News/Article-Display/Article/2369626/army-air-force-form-partnership-lay-foundation-for-cjadc2-interopability/>.

4 Technologies Supporting Traceability

Blockchain is the primary data sharing and storage technology to enable traceability as considered in this paper. In addition to blockchain, the following technologies were also identified as potentially useful to enable traceability:

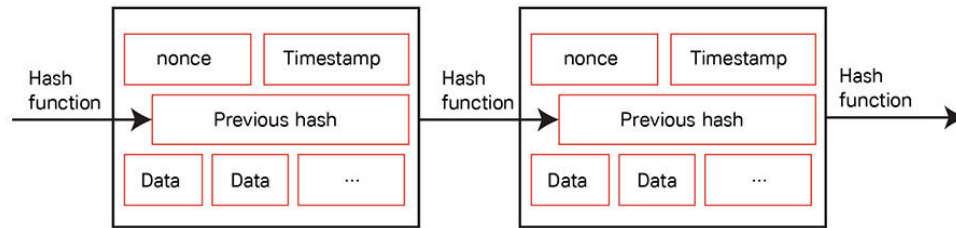
- Cyber-physical anchors – goods which need to be matched to traceability records may need to be identified with a Physically Unclonable Function (PUF) to assure a unique identification [55]. Cyber-physical anchors provide unique electronic identifiers which are associated with goods, where the identifier has integrity against spoofing. This identifier can then be incorporated into electronic data recorded on the blockchain to combine the data integrity offered by the blockchain with the unique goods identification provided by the cyber-physical anchor.
- Solid Pods – an internet-based innovation (from Tim Berners Lee) on storage, may offer an alternative mechanism to the current per stakeholder enterprise repositories. The relevance is that blockchain can store only small amounts of information, so additional storage (e.g., full provenance information) may be required for traceability data records in a blockchain. Full traceability data would need to be stored in a form and manner agreed upon by the ecosystem stakeholders, which currently would be an off-chain repository in one of the stakeholder’s enterprise networks. Solid pods may offer a storage and access means that are suitable for shared access within the ecosystem.
- Decentralized Social Network Protocol (DSNP) – in addition to exchanging traceability and market intelligence data records, there is a need to share discoveries, findings, and emerging new traceability requirements across the ecosystem. These new traceability requirements need to be understood and widely shared as a precursor to adoption. Sharing related supply chain information can be performed using existing means (email, website), or using a social network approach. This emerging protocol may serve as a foundation for ecosystem-wide sharing of ecosystem intelligence, and traceability refinements.

4.1 Blockchain

With increasing demand on manufacturers and global supply chains, blockchain has been introduced as a viable solution. Blockchain is described in NIST.IR 8202 [4] as a tamper evident and tamper resistant distributed ledger, which stores all the details of a network's activity. This enables the data to be trusted by blockchain participants. Blockchains are usually stood up without a central authority, such as a bank or government. The first blockchains were public (or permissionless) and in use today as cryptocurrencies. However, the blockchains in consideration below and through this paper are permissioned and restricted to a well-known and vetted set of participants.

The trust lies in the validator nodes across the permission blockchain network, which is how the data is secured and transactions validated on the blockchain [7]. New transactions added to the blockchain are verified by validator nodes through a consensus algorithm, where it is confirmed by a quorum of validators in the blockchain (e.g., 2/3 validators in the Byzantine Fault Tolerant consensus algorithm). The blockchain peer-to-peer network allows its users to post transactions

which are written to blocks, which are themselves linearly and chronologically linked to other blocks which make up the shared ledger. Each block contains a set of data, a timestamp, and a hash [7] from the previous block and is placed next to it, then the process repeats itself, as seen in Figure 5. Once the blockchain is published, no chain in the network can be altered, creating a permanent, open record for everyone to access.



Source: Yaga [4]

Figure 5 - Basic blockchain principle

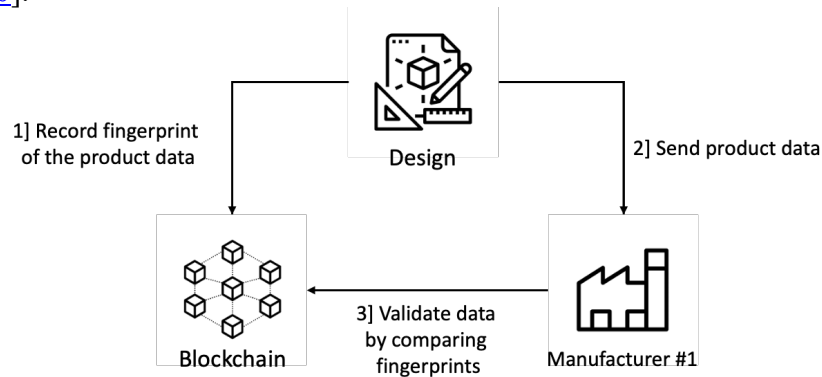
The two-step validation process is an added benefit to blockchain’s reliability. The first step validates the transaction data against pre-defined domain-specific business rules [10]. The second step requires a consensus agreement by peers on the network to include validated transactions in the next block, which is then added to the blockchain data. This agreement is reached through a consensus mechanism [4], preventing bad actors from adding and/or accepting fraudulent blocks [11]. Another way the blockchain mitigates the effects of potential malicious activity is by replicating data across all nodes on the network so that it can withstand loss of nodes due to attack or accident. This in part, allows blockchain to be distributed, replicated, and maintained as a log of transactions that are well suited for sharing information among diverse stakeholders, such as in manufacturing supply chains.

Table 1 Example Metrics of Manufacturing Supply Chains

Metrics	Information that could be included on a block
Economic	a. Smart contract executed transactions (i.e., payments and deliveries) b. Bank access to network c. Age of material or resource d. Market resources and commodities prices
Environmental	a. Raw materials used b. Waste, byproducts, and coproducts produced
Social	a. Responsible care instructions b. Responsible disposal instructions c. Worker age and hour restrictions
Functional	a. Intended use b. Warranty information c. Repair information d. Quality control information

Adapted from: Rogaway [8]

Generating digital signatures of product data is a possible method where blockchain can be utilized to support manufacturing supply chain traceability [12]. The signature stores a digital fingerprint of various identifiers and metrics. Table 1 shows some examples of information that could be stored in an individual block. To secure the digital fingerprint, storing the associated metadata on a blockchain can “track both the existence and ownership of a digital asset at a certain time” [10].



Source: Krma [10]

Figure 6 - A simple scenario of blockchain usage to validate product data

Blockchain can be used to track several types of digital assets. [Figure 6](#) shows a simple traceability example where “blockchain can help to secure proof of existence and ownership of data associated with a specific instance of product that can be critical to solve future engineering and/or legal issues” [5]. In more complex scenarios, if the source and destination metadata are included, the product data exchange can be recorded on the blockchain. The resulting unique data transaction can be easily verified as secure, and the ownership of the transaction is clearly attributed on the blockchain. [Figure 7](#), Step 5 would raise red flags if the data was manipulated by the bad actor in Step 4. A bad actor is depicted, implying nefarious intent; however, it is also possible a good actor may have inadvertently caused a bad event. The blockchain allows determination of loss or change in either case.

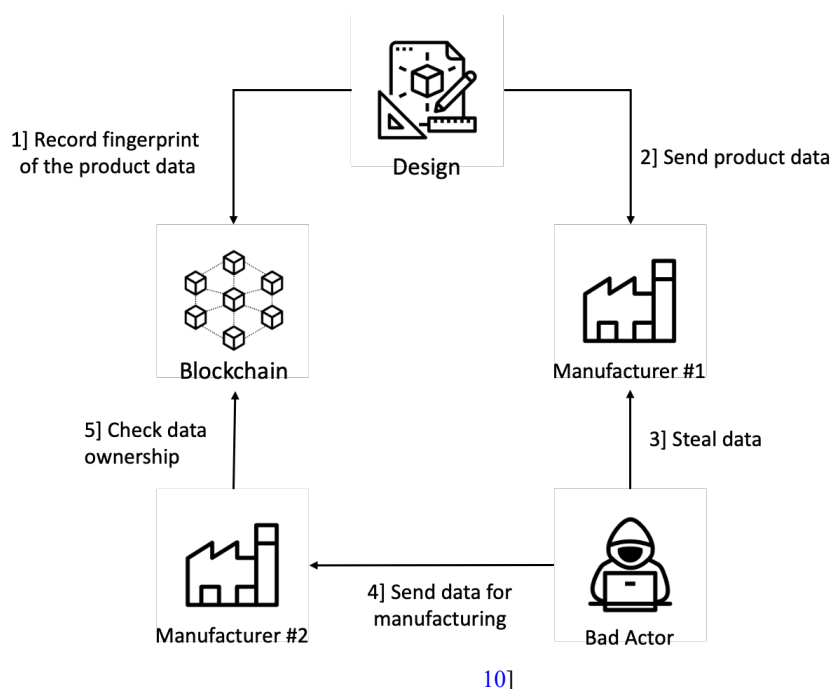


Figure 7 - A more complex scenario of blockchain usage to validate product data

Posting validated manufacturing traceability data records on the blockchain provides trusted data across an ecosystem which can be used to determine pedigree and provenance of goods and services in the supply chain.

4.2 Cyber-physical anchors

The initial concept and usage of public (permissionless) blockchain validates transactions strictly against data records already stored on the blockchain (e.g., cryptocurrencies). However, using permissioned blockchains for manufacturing traceability data records requires associating the traceability data records with goods and services which are external to the blockchain. This association must be unique and provable. If not, this reduces trust in the shared traceability data. For example, one scenario might be to mitigate counterfeit and fraudulent products mixed in with authentic items. Another case is anti-tamper detection to ensure that genuine items are not manipulated by bad actors. In a complex supply chain across multiple countries, identifying these inauthentic items is a difficult task. Therefore, it is essential to provide a trusted link between the physical products and its associated traceability data record on the blockchain.

For associating cyber products, such as documents and software files, techniques such as hash fingerprints can inform traceability records. The goal is the same, which is to record a provable and immutable traceability record in a blockchain that can be used to compare against cyber and physical products later downstream and establish authenticity.

For associating physical products, techniques such as serial numbers, QR Codes, and RFID could be used since these have been demonstrated to work with many different manufactured goods

today. However, for physical products which require a higher degree of proof of identification and resistance to tampering and counterfeiting, alternative technologies are emerging and discussed next.

Cyber-physical anchors are a product authentication technology [13], which acts as a unique digital fingerprint for physical objects to be used as an identifier in blockchain records associated with that good. The cyber-physical anchors are tamper-resistant and non-transferable to another good or object, and any attempt to modify or destroy the anchor can be detected (tamper-evident) [14].

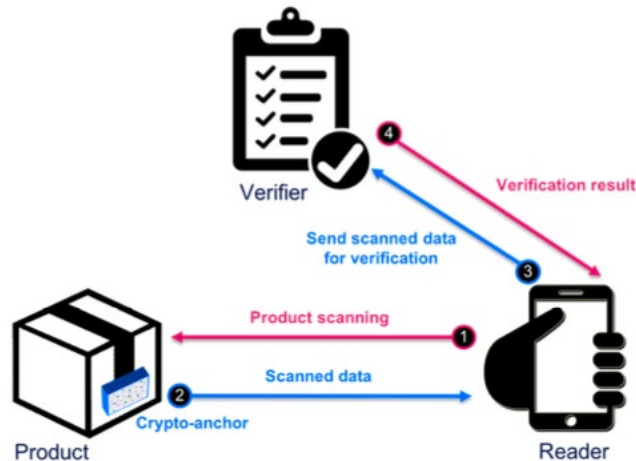


Figure 8 - Cyber-physical anchor verification flow

Source: Prada-Delgado [13]

Generally, the cyber-physical anchor verification process involves the Reader/User, the Product, the Cyber-physical anchor, and the Verifier. A simple scenario is depicted in [Figure 8](#). A user first scans the cyber-physical anchor on the product using a reader device, then it receives the scan result. Next, the scanned data is sent for verification to a verifier where the verifier authenticates the data and validates the result.

Preliminary research conducted by IBM, and companies such as DUST Identity and others has resulted in a framework to enhance security, transparency, efficiency, and resiliency in supply chain management [13]. Their solutions consist of 3 layers [14]:

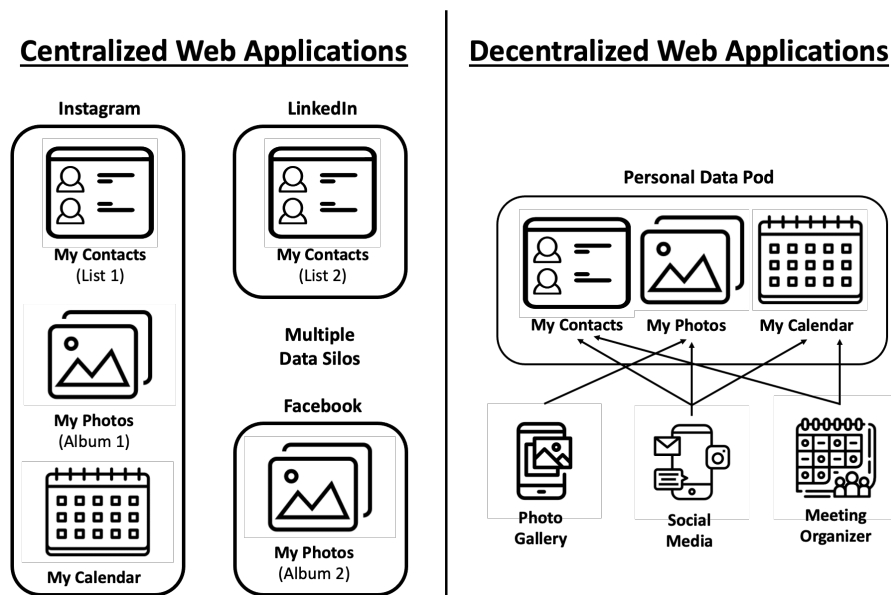
- an ecosystem blockchain to digitally store and track traceability data transactions (with cyber-physical anchor instance and physical goods and services instance association included), and data ownership and access rights for the ecosystem participants
- a layer of cyber-physical anchors attached to or embedded in the instances of goods and services which connect their digital identity to a physical item
- blockchain data (shared by applicable supply chain ecosystems) to enable consistent semantic understanding and syntactic use of cyber-physical anchor types across ecosystems (e.g., consistent cyber-physical anchor reading of codes on parts)

In summary, a blockchain network used by a supply chain ecosystem allows for users to check the data records in the blockchain ledger. However, to be useful, the blockchain data record must include a link to the cyber-physical anchor instance which is associated with the goods and services instance flowing through the supply chain.

4.3 Other technologies

Typically, minimal shared traceability data is stored directly on the blockchain, with links to full traceability data stored in off-chain storage. The off-chain storage can be a stakeholder system, or shared storage for the ecosystem, including decentralized storage. Decentralized technologies continue to rapidly evolve and currently, there are numerous decentralized storage technologies in related projects under development. One such emerging decentralized storage specification is the Solid Project led by Professor Berners-Lee [51] [52] [53] [54]. The Solid Project attempts to change how web applications interact and utilize user’s data, by giving the users ownership of their data, and enhanced privacy. The importance of considering technology options such as Solid for data storage is that shared traceability data in an ecosystem needs to be stored somewhere, and an open-source specification helps preserve accessibility. The Solid specification is starting to be productized [44], with initial users considering how to use Solid in their enterprise, such as the National Health Service (NHS) in the United Kingdom (UK) [45]. The description below is not a recommendation to use Solid; however, its decoupled architecture (app and data decoupling) as an approach may prove useful in traceability ecosystems, whether Solid per se is used or not.

The Solid Project is user centric. For the purpose of supply chain, the user could be a supply chain participant or even the whole ecosystem. For example, the ecosystem could choose to store data in a manner agnostic to any given participant. The Solid Project may inform such an approach.



[15]

Figure 9 - (Left) Current centralized style of web applications vs. (Right) Proposed access-controlled data pods

“Solid Linked Data” also known as the Solid Project is a web decentralization project, as shown in [Figure 9](#). Solid Project envisions a decentralized, user (e.g., supply chain participant or ecosystem) controlled platform for linked-data applications, rather than the application or a third-party controlling access. Solid Project is attempting to achieve three goals:

- True data ownership: Users should have the right to decide where their data is stored and who has access to it. Solid Project decouples data and content from the application.
- Modular design: Since “applications are decoupled from the data they produce, users will be able to avoid vendor lock-in, seamlessly switching between apps and personal data storage servers, without losing any data or social connections” [\[17\]](#)
- Reusing existing data: Developers will be able to easily create new applications or improve existing ones, by reusing existing data that was produced by other applications.

This decentralized structure allows users to have increased control of their data, including access and storage. To achieve this, they are proposing a “set of conventions and tools for building decentralized social applications based on Linked Data principles” [\[17\]](#).

Decentralized approaches such as Solid may bring advantages of decentralized data sharing and storage to manufacturing supply chain ecosystems. For example, traceability data and marketing intelligence data (ecosystem incentives) could be stored in Solid (or summary) in the future. Adoption of such approaches provides an alternative to siloed back-office data or highly centralized data.

4.4 Summary

As supply chains grow to be even more complex, bad products and actors will inevitably enter, causing economic losses in addition to other disruptions and safety concerns. Some of the technologies mentioned above are workable solutions to connect the physical domain with the digital environment, enhancing traceability.

5 Considerations for Adoption of Blockchain

From the case studies, several key topics regarding adoption were raised and discussed with the community of interest, summarized below.

5.1 Metrics

Traceability metrics are required to measure progress toward implementing traceability across an ecosystem. For example, what are the minimum viable traceability data elements which constitute traceability for any set of goods and services? Present traceability metrics as implemented in the case studies are generally straightforward, meaning either the pedigree/provenance data records for the ecosystem are written and read, or not. Another possible metric of traceability is “time to data,” which measures the speed with which an operator can acquire the information they need about any given product in the moment that the information is needed. Time to data is often a crucial measure of the effectiveness of a supply chain in its ability to deliver information and trust, in addition to physical goods.

Future traceability efforts may be more complex with overlapping needs. For example, an ecosystem which needs to incrementally add traceability records to improve coverage needs to first enumerate gaps, then prioritize which traceability records to implement by which participant in what order will close those gaps and to what extent. The coverage across stakeholders may need to be prioritized or at a minimum reported, so that the ecosystem governance has good situational awareness. Metrics could be expressed as either quantitative or qualitative (or both) measures and are discussed further in [Section 7](#), Future Research Opportunities.

5.2 Information exchange standards

Standards are required for the exchange, and semantic and syntactic understanding of data records shared beyond typical B2B bi-lateral information exchanges. One of the case studies (MediLedger) featured a partnership with GS1 US, a standards organization. While use of standards can accelerate adoption, future standards requirements may be more complex, see [Section 7](#) Future Research Opportunities. Proprietary or private data may be linked via identifiers rather than directly stored on the blockchain, enabling flexibility in protecting information, a consideration in standards for exchanges, for example the Guardtime Federal approach.

5.3 Minimum viable ecosystem

Traceability requirements are often established by end operating environments, failure analysis, and adversarial testing results. Conversely, issuance of traceability data records is performed by the contributing goods and services supply chain participants. The benefit of writing/reading traceability data records using blockchain and related technologies, needs to be complemented with incentives for the contributing supply chain participants to participate (e.g., access to market intelligence data records). This tradeoff will be unique to each sector and domain.

The purpose of an MVE is to provide a starting point, then subsequently grow and refine the ecosystem. Of particular concern is to balance the incentives and effort across the ecosystem of participants who will have differing perspectives (e.g., upstream versus downstream participants). An MVE must also include an end operating environment(s), the contributing

goods and services supply chain, associated minimum viable traceability data elements to constitute traceability, and sufficient incentives like marketing records to incent all participants to work together. If the MVE cannot be initially established, then the ecosystem cannot function and maintain coherency.

Once established, the MVE will then incrementally evolve within the constraints and guidance of the associated governance, informed by traceability metrics. MVEs are adapted to evolving traceability needs of the end operating environments and other supply chain participants. As requirements demand increased traceability, this may impact techniques of linking physical goods with blockchain data records and linking off-chain data with the blockchain data records.

Identification and measurement of traceability gaps, and strengthening of traceability methods and means, must be expressed and driven using traceability metrics and analysis methods. See [Section 7](#), Future Research Opportunities below.

5.4 Multiple blockchains

As blockchain enabled supply chain ecosystems are instantiated and grown, driven by metrics and governance, ecosystems will soon intersect. Intersection means that one or more stakeholders is included in more than one ecosystem where traceability in one ecosystem needs to be carried over to the adjacent ecosystem. For example, a secure software supply chain traceability ecosystem and a secure microelectronic traceability ecosystem (see case studies below) could both feed into a secure avionics supply chain ecosystem. One or more participants from the feeder ecosystems may also participate in the assembly ecosystem. In addition, one upstream supplier (e.g., electronics) may supply to two different feeder ecosystems. Having consistent approaches, practices, and standards for individual participants as well as entire ecosystems, will help to assure interoperability and transitive trust across the web of supply chain ecosystems.

When ecosystems intersect, then the exchange of traceability data records can be facilitated by either:

- (a) The relevant individual intersecting stakeholder's "copy" the applicable traceability records from the upstream ecosystem to the dependent downstream ecosystem.
- (b) The relevant ecosystem blockchains directly send applicable traceability records from the downstream ecosystem blockchain to the upstream ecosystem blockchain.

Multiple traceability ecosystems that need to exchange traceability records give rise to another complexity scale level often referred to as a network of ecosystems. The grouping of ecosystems into ecosystem networks will be driven by the needs of the relevant end operating environments and supply chain participants. [Figure 10](#) illustrates ecosystem linkages of exchanging traceability data records. The connections between ecosystems will arise as (a) individual participants in each ecosystem supply goods to multiple ecosystems and/or (b) ecosystem participants (and end operating environments) consuming products from one or more ecosystems. The intersection or linkage between ecosystems should assure understandability and durability of traceability records across ecosystems to achieve transitive trust.

Linked Ecosystems

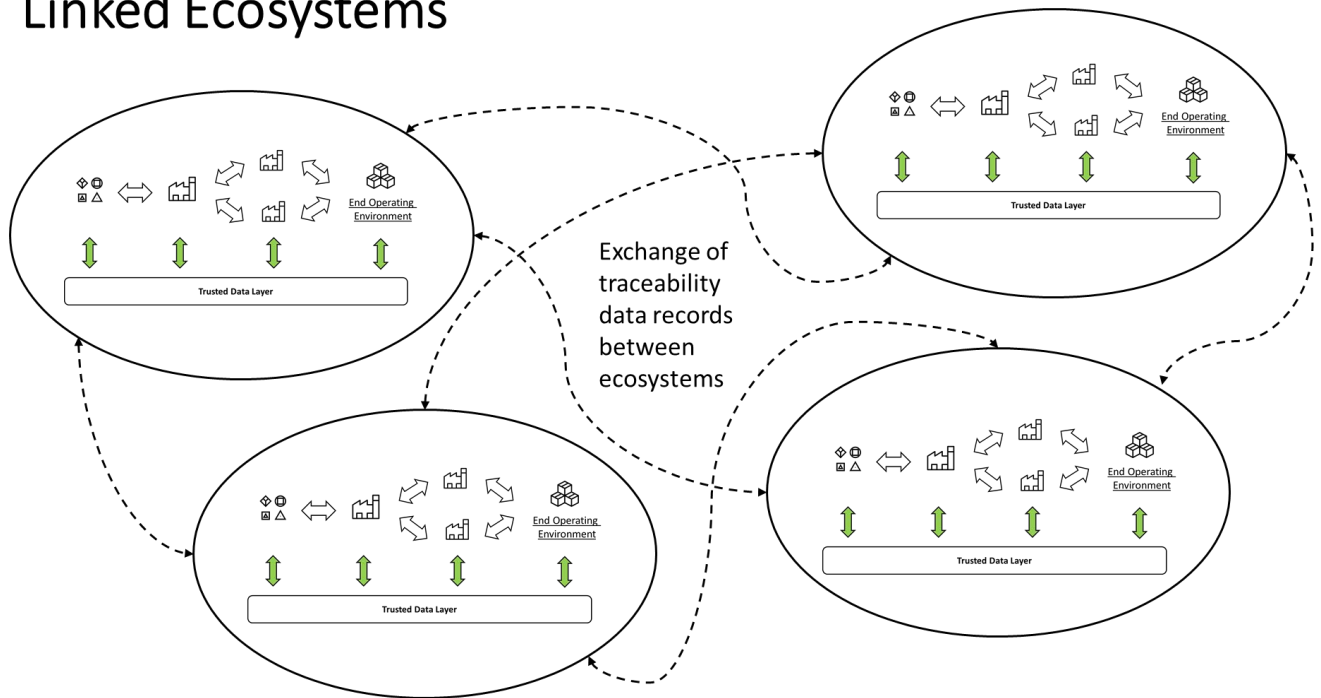


Figure 10 - Network of traceability ecosystems

Challenges with exchanging traceability data records across ecosystems arise from dissimilar governance, blockchain and related technology, regulatory environment, and accepted practices. This is an outgrowth from the current state of unconnected blockchain ecosystems operating independently from each other. Indications are that the ecosystems will continue to grow and will soon need to intersect and align traceability records.

Further, use of logistics (shipping) providers in between supply chain steps is an added level of complexity. While use of logistics can simplify supply chain operations, assuring the traceability of manufactured goods through logistics may require the participation of logistics providers in traceability ecosystems. Many logistics providers are already using blockchain data records to improve their coordination and reduce lost goods, and there may be opportunity to include use of logistics. See [Section 7](#) Future Research Opportunities.

5.5 Intellectual property

Ecosystems require IP protection to enable participants to freely exchange traceability records. This is a multi-dimensional concern as follows:

- Ecosystem participants seek to safeguard proprietary business information and IP to the maximum extent. Supply chain information often acts as, or itself is, proprietary business information and/or indicates IP. Ecosystem participants must design the data elements in traceability records to achieve traceability while minimizing sharing IP information. The

goal is to achieve desired supply chain ecosystem traceability while still protecting proprietary information and IP. The MediLedger and Guardtime Federal case studies are good examples of this strategy. In the MediLedger case, the ecosystem blockchain stores minimal traceability identifiers which complement the participant's legacy B2B ERP systems. Guardtime Federal's approach employs hash values and digital signatures on the blockchain as links to immutable IP data stored elsewhere. In these cases, protection of IP is accomplished by avoidance of sharing IP information in exchanged traceability data records. Further, note that marketing or sales intelligence records, as incentive to participate in the ecosystem, may inadvertently contain proprietary organizational information, such as what office in what company is purchasing what and how many goods. Mitigations include de-identifying marketing or sales intelligence records so that the minimal amount of information which still provides sufficient incentive is recorded, leaving organizational proprietary information minimized.

- Complementary, and separate from writing and reading traceability data records using an ecosystem blockchain, ecosystem participants may also want to establish and record IP ownership (e.g., Digital Rights) using a blockchain. Establishing and protecting IP using blockchain could be performed using a purpose built blockchain (perhaps distinct from the ecosystem blockchain) offered as a service to a sector of industry. This is an active area of research and patent development [47] in industry [48] and academia, and beyond the scope of this paper.

The interplay between supply chain traceability blockchain records and IP is discussed in [Section 7](#), Future Research Themes.

5.6 Privacy

Privacy, as discussed earlier in the paper, is focused on market or sales intelligence data records written to the ecosystem blockchain. This is an optional activity as the data records do not strictly provide or enhance traceability. However, market intelligence records may be needed to provide incentives to upstream supply chain participants so that they are motivated to write traceability data records for the benefit of downstream participants, especially those in the end operating environment. The market intelligence records then provide sufficient incentives to establish an MVE, and ideally maintain the incentives through incremental growth of the ecosystem. The term privacy as used here, focuses on Personally Identifying Information (PII).

The privacy risk arises when the market intelligence records (e.g., sales or distribution information on who is using upstream goods and services) are specific to the extent that downstream participant information is unnecessarily disclosed to upstream participants. Mitigations include de-identifying market intelligence records so that the information still provides sufficient incentive while also protecting PII.

The interplay between supply chain traceability, blockchain records, and privacy is discussed in [Section 7](#), Future Research Themes.

5.7 Identity for supply chain partners

Supply chain partner identity is required for supporting data exchange regardless of the

technology utilized (e.g., EDI/VAN, B2B ERP, or blockchain). Blockchain uses public keys (see [Section 4](#), Technologies Supporting Traceability) which are managed on a per ecosystem/blockchain basis. Management functions include vetting participants, training participants how to safeguard their private keys, assuring participants know each other's derived public keys, etc. The NIST White Paper, "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems" [18] describes the components of blockchain enabled decentralized identity management.

In the case studies below, blockchain identity is established and managed within the pertinent blockchain ecosystem. This ecosystem-unique identity is sufficient for isolated ecosystems; however, as discussed above, some blockchains will start to intersect. At this point, if traceability records (and market intelligence records) are to be exchanged across ecosystem boundaries, then:

(a) Ecosystem identities must be mapped to maintain coherence. For example, if participant A is included in two ecosystems which start to intersect, the key for A in the first ecosystem may be different from the key for A in the second ecosystem, unless the independent governances for the two ecosystems coordinate. When a traceability (or market intelligence) record is exchanged, the attribution in the exchanged data records from the first ecosystem should be matched (with proof) to the same participant in the second ecosystem.

Or,

(b) Participants from both ecosystems must use a common shared identity scheme provided elsewhere.

Complicating traceability is the path of goods through logistics partners. Thus, traceability needs to track goods and services not only through supply chain participants, but also tracked through steps in the logistics process. This may be needed for fine grain provenance information (e.g., countries visited) if goods and services are of a sensitive nature.

If we seek to coordinate identities across ecosystems which seek to exchange traceability records, then either the relevant ecosystems must coordinate their identity processes, or both ecosystems use a common or global identity service. Some global blockchain-enabled identity projects like Sovrin Network⁵ seek to establish a global decentralized identity which (theoretically) could provide identity for all individuals across the globe. However, since identity projects require consent of the participants, it is understandable and in fact the case, that there will be multiple "global" efforts each originating with hubs of influence (e.g., U.S. and Europe). In fact, on 30 June 2021, Sovrin signed an agreement of cooperation and alignment with European Self-Sovereign Identity Consortium (ESSIC) to enable a network of identity networks⁶.

⁵ [Home - Sovrin](#)

Full disclosure, MITRE is a steward of a test node in the Sovrin Network

⁶ [Sovrin aligns with European Self-Sovereign Identity Consortium \(ESSIC\) in order to enable a network-of-networks. - Sovrin](#)

Self-Sovereign Identity is based on emerging standards such as Decentralized ID from W3C (World Wide Web Consortium). The most recent draft of decentralized identifier standards is dated July 2021, which includes core architecture, data model, and representations⁷.

The distinction between global identity networks is establishing trust to attract participants and build the network. In the case of Sovrin, the constituency is primarily North America, and ESSIC is primarily European. Further, there is cooperation among identity providers to provide trust across the internet, via entities such as Trust over IP⁸. For example, Evernym (who operates Sovrin Network) is a Steering Member of Trust over IP.

While the Sovrin and ESSIC efforts help to establish identities for individuals via ID wallets, institutional ID wallets are still in their infancy with complex topics to solve such as delegation and replacement of individuals associated with organizational ID wallets.

For more, see [Section 7](#), Future Research Themes.

⁷ [Decentralized Identifiers \(DIDs\) v1.0 \(w3.org\)](#)

⁸ [Trust Over IP - Defining a complete architecture for Internet-scale digital trust](#)
Full disclosure, MITRE is a Steering Member of Trust over IP

6 Industry Case Studies & Analysis

Industry case studies were used to learn about current and emerging efforts which are using blockchain and related technologies to improve traceability of manufacturing supply chains. The community of interest discussions and elicited case studies form the basis of recommended research in [Section 7](#), Future Research Themes. The case studies are viewed and analyzed objectively and subjectively with selected mental models (further explained in [Section 6.7](#)) to establish a means of comparison to discover findings of similarities and dissimilarities. Peers, subject matter experts, stakeholders, industry leaders, each have offered considerable insights to this process.

This section opens with a summary of each case study, including the goal of the project, who was involved, and the technologies utilized to address the problem. The full case study submissions are in [Appendix C](#) of this paper. The remainder of the section addresses the analysis methodology and a summary of its resulting discussion.

6.1 From Field to Fork

The goal of the Field-to-Fork initiative was to improve the yield of gluten-free raw materials as they are processed through the supply chain from supplier to consumer. Because the product needed to be gluten free, the process required a purification step. However, the supply chain of the raw materials was not designed to ensure 100% purity of the raw material, which means the raw material needed to be processed and filtered to a 100% purity level at the manufacturing site. Additionally, the supply chain was not designed to capture the transformed state of the material as it moved through the supply chain. As a result, the current process resulted in a significant amount of wasted material thus leading the company to research other technologies to improve the yield of the gluten free product. The research resulted in a process that did not utilize blockchain, but instead built a material ledger developed with a graph database to capture the relationships of the material flow.

6.2 Sky Republic with SITA

The Sky Republic case study includes four different Proofs of Concept (PoC) that were conducted with SITA [\[49\]](#) in 2020. The efforts focused on four different aviation supply chains: Aircraft MRO Track & Trace, Aircraft MRO Digital Passport, Air Cargo Shipment EDI/IoT Tracking, and Air Cargo ULD Interlining. Each of the participants within each PoC had their own process they wanted to improve. For example, in the Aircraft MRO Track & Trace PoC, the airline wanted to improve detection and mitigation of disruptions and OEM wanted to improve retrieval of operational and configuration data related to the parts to accelerate repairs. Each of the four projects aimed to demonstrate that a blockchain-based platform can provide end-to-end automation, visibility, and transparency for supply chains more efficiently than legacy technologies and infrastructures. The participants followed a set of guidelines which included: identify business benefits, define the prototype to be experimented, develop, integrate, and set up prototypes, experiment with actors utilizing the prototype, and finally, a post-mortem analysis.

6.3 Guardtime Federal and “Perspectives from a Prime”

As described in the Guardtime Federal questionnaire, each participant submitted a case study for

a blockchain pilot they conducted to ensure traceability in the Prime's digital supply chain. The Prime's driver behind implementing a blockchain-based solution is that the company's computer networks, the software supplier's networks, and the Prime's customer, the Department of Defense (DoD), provide critical information even on unclassified networks. Blockchain offers an opportunity to layer on additional data integrity to further enhance existing measures. Guardtime Federal provided the platform for this additional layer and incorporated their own digital integrity and digital provenance solutions like the KSI® Calendar. The KSI® Calendar acted as a public, widely witnessed, common anchor that utilized hash functions to verify the provenance and integrity of the digital supply chain data.

6.4 DUST Identity

DUST Identity partnered with Manufacturer X, a Fortune 500 multinational-supplier that participates in several industries (e.g., electronics, electrical components, and highly engineered components for the automotive and consumer electronics spaces), to support their initiatives on integrating blockchain into their manufacturing lines with a strong cyber-physical anchor and digital thread⁹ solution [56]. Manufacturer X was encountering an increasing number of non-genuine and non-compliant parts being sold under their brand name. These issues were negatively impacting their business and brand reputation, causing the manufacturer to realize that they needed a secure traceability solution to address the problem. After selecting blockchain to securely record provenance data with entities in their supply chain, Manufacturer X determined that, to truly trust the data on their blockchain, they would need to immutably connect part data to individual products through the use of a unique and unclonable cyber-physical anchor. DUST Identity filled this need through the Diamond Unclonable Security Tag (DUST), which binds physical parts to their unique digital records using a persistent, secure identifier composed of microscopic diamond crystals. Now, authorized parties can scan the DUST marking on the part to access the blockchain and DUST ledger to validate the integrity of the part and access the part's data record.

6.5 MediLedger

The MediLedger project was conducted in response to a Food and Drug Administration (FDA) request for pilots addressing the requirements of the Drug Supply Chain Security Act (DSCSA). Compliance means that package-level tracing and the interoperability among systems enabling the tracing will drive technology enhancements. Industry stakeholders have been engaged since 2017 exploring achieving interoperability with blockchain technology. The pilot project tackled the challenges of interoperable systems tracing a saleable unit and the homogenous case packaging levels. The report [19] covered the findings of the 23 participating entities from the pharmaceutical domain. Their ten findings cover a range of concerns including how blockchain technology can enable transaction verification, authenticity validation, and expediting suspect investigations while keeping transactions fully obfuscated, i.e., confidential, transactional privacy, and ensured immutability. Social constructs addressed include governance from the industry, strong participation and adoption from stakeholders, and pursuit of additional standards agreements. For the blockchain technology employed, a single blockchain solution for the parties

⁹ The label of digital thread is useful for the information flow in a product's lifecycle and supply network [56]

performed adequately, the solution's architecture should be open in order to remain interoperable, capabilities support additional business applications, and a technology stabilization period is advisable prior to DSCSA enforcement activities.

6.6 Chain Integration Project (CHIP)

Auburn University's RFID Lab conducted a proof of concept targeting challenges of tracking RFID serialized data pertaining to products moving from brand distribution centers to retailers [20]. The proof of concept employed blockchain technologies and included a step to standardize data streams. The GS1 Electronic Product Code Information Services (EPCIS) [50] standard allowed data from numerous company systems to post transactions to the blockchain solution. Some participants produced data streams for the EPCIS standard while others relied on an AU-developed translator. Among the findings of the proof of concept are opportunities valued at \$181 billion associated with claims processing, shrink, and counterfeiting.

Additionally, Auburn University and others conducted previous research, which is also relevant, and described below:

Traceability of Microelectronics [21]: The authors proposed a prototype permissioned blockchain-based framework using Hyperledger Fabric to provide comprehensive and reliable device traceability so that tracking and verification of microelectronics can be done for different manufacturers, distributors, and end-users. The traceability must be ensured using an electronic chip ID (ECID) or unclonable ID generated from a PUF. The origin of a device, the trace of travel in the supply chain, and its bill of materials can be accurately tracked and used for verifying its authenticity.

Traceability of IoT Devices [22]: The authors proposed integrating blockchain technology to authenticate resource-constrained, low-cost edge devices for the Internet of Things (IoT). Static Random-Access Memory (SRAM) based physically unclonable functions were used to generate unique and unclonable device IDs. Registered manufacturers can upload a cryptographic hash of each device ID in a permissioned blockchain instance managed globally. The end-user needs to read the ID of a new edge device and search the ID hash in the blockchain before registering it in the IoT infrastructure.

6.7 Methodology

The methodology used for the case studies has two phases. The first is case study knowledge acquisition, and the second is case study analysis. Throughout the acquisition and analysis of case study knowledge, considerations for future research topics are captured for further discussion in [Section 7](#), Future Research Opportunities. Peers, subject matter experts, stakeholders, industry leaders, each have offered considerable insights to this process.

Two phases were used to illuminate the topic of manufacturing supply chain traceability; based on the goals of this effort and the current environment of supply chain risk as described in previous sections and references. The goals of high engagement and building a community of interest were drawn from the purpose of discussing and ratifying key issues experienced in practice. For this reason, a broad aperture accompanied by means of synthesis, pointed to collecting case studies and applying mental models to their combined characteristics.

The first phase, case study knowledge acquisition, yielded submissions from several organizations representing a range of stakeholders in supply chain security. Industries represented were agriculture, aircraft manufacturing, software development, OT/ICT solution providers, distribution, and retail, pharmaceutical, and industry consortia.

The second phase, analysis of the case studies, produced a discussion with suitable context for needs and industry perspectives.

6.7.1 Methodology of case study knowledge acquisition

The authors sought to engage organizations that represent a variety of industry sectors and sizes in their effort to collect case studies. Beginning with a series of events in 2020 and continuing into 2021, the authors engaged an active Community of Interest (COI) whose makeup consists of individuals and organizations that hold a high degree of blockchain expertise, to elicit knowledge, to share insights, and to request participation in the case study process.

The authors began by developing a series of questions that were designed to capture an organization's experience(s) deploying blockchain and related technologies for manufacturing supply chain traceability. Once the questions were finalized, a COI meeting was held March 30, 2021, to provide attendees with an overview of the questions, and of the case study collection process. Attendees who expressed interest in submitting a case study were emailed the list of questions for response.

Once the authors collected responses, the authors held semi-structured interviews with each submitting organization to elaborate upon or clarify submitted content. All notes taken by the authors during these semi-structured interviews were combined and sent back to the interviewee for review and final sign-off.

Case study content in this publication represents the views and perspectives of the submitting organizations themselves, and not necessarily that of NIST. The authors' goal was to hear from industry and to do a deep dive into the experiences of a few organizations who have deployed blockchain and related technologies for manufacturing supply chain traceability, their tactics, their challenges, and their lessons learned.

The full case study submissions and analysis notes can be found in the Appendices [C](#) and [D](#).

6.7.2 Phase 2: Methodology of case study analysis: leveraging mental models

The second part of the methodology, mental model viewpoints,¹⁰ is built from a selection of works that describe or organize by simplifying reality to promote understanding. The expectation is that perspectives that the models or lenses evoke lead to candidate topics worthy as key issues

¹⁰ Using mental models to explore has a tradition that can be reviewed starting with Senge [23], with a summary of his titles at Bui [24]. There are many branches of this network of literature, Google Scholar reports 71,975 citations for the 2006 work, as of 4 Jun 2021. In this spirit, models from across disciplines were used as means of understanding aspects of the case studies. An additional motivation is the discovery of intersections as described in Johansson [25] in which deliberate intersections of disciplines reveal potential for innovation.

or research areas. The resulting proposed topics may be stated as loosely formed hypotheses, challenge statements, driving industry characteristics, or simply thought-provoking discussion.

The [mental model process](#) is listed below and includes references to summaries and analysis notes from completing the activities:

- a. Select models with promise for illuminating some aspect of manufacturing supply chain traceability. Selections are summarized in [Section 6.7.2.1](#) and further explained in [Appendix B](#).
- b. Summarize and use keywords among the case studies to present and characterize the set of cases. Analysis notes from this activity are found in [Appendix D](#).
- c. Step through each of the models selected and qualitatively discuss its application across the cases. Discussions are summarized in [Section 6.7.2.2](#) and analysis notes are found in [Appendix E](#).
- d. Synthesize observations into candidate future research topics. Candidate topic discussions are found in [Appendix E](#) and the results are integrated in [Section 7](#).

6.7.2.1 Selected models

In the first step (select models), the list of potentially useful models would undoubtedly fill many volumes. The basic description of the models proffered and the reasoning for choice are addressed in this section. [Appendix B](#) contains additional discussion of the models and their relevance.

Supply Chain Risk Management

NIST Draft Special Publication 800-161 [\[1\]](#), addressing risk in cyber supply chain scenarios, includes two important, foundational, and descriptive models that together aid in framing the proceeding discussions across other models. The first perspective orients the acquirer, and the second perspective frames the assessment process.

These two perspectives are described in [Appendix B](#). They are important to the synthesis of case studies because they highlight an organization's risk exposure due to its internal information, its relationship information, and the importance of being open to advantages in sharing what would otherwise be guarded, when seeking a safer ecosystem of operations among manufacturers and suppliers. The trade-off between guarding and sharing data traces to risk management practices performed within organizations. Supply chain risk and data sharing concerns are expected to surface in case study submissions and can aid in synthesis across the collection.

Pace Layered Architecture & Adoption Curve

The lenses of Strategic Innovative, Differentiator, and Routine Administrative are loosely based on Brand's Pace Layering concepts [\[26\]](#) and Gartner's Pace Layered Architecture; the combination of the ideas is described in Isotta-Riches & Randell [\[27\]](#). These three categories in turn, dovetail with the technology diffusion model, described in Rogers [\[28\]](#), to provide a model

of pursuit of business value.

The joined perspectives of the lenses (strategic innovative, differentiator, and administrative routine) and the classic diffusion curve are important to the synthesis of the case studies because they create a basis for compare-and-contrast exercises. A case study submission may explicitly state its strategic imperatives, or a reader may be able to discern them. The combined positioning may enlighten differences and similarities, presenting possible explanations or predictions of need, such as alleviating barriers to entry.

Win/Win & the Production Possibility Frontier (PPF)

Gharajedaghi [29] describes casting opposing tendencies in social systems as dimensional, a case where more of both tendencies creates the win/win scenario: the <and> rather than <or>. Similarly in economics, the concept of a PPF [30] illustrates how, even when it seems that production of one thing results in less of another, i.e., <or>, more of both are feasible. This concept is due to the introduction of technology or other factors that improve the capacity of production.

The importance of this perspective is to avoid assumptions of mutual exclusivity and encourage the possibility of two seemingly opposed concepts potentially coexisting. For example, two opposing concepts that are frequently juxtaposed are sharing data versus protecting data.

Intermediation, Disintermediation, Classic Make/buy

A useful marketing domain concept is the disintermediation effect, often provoked by disruptive technology or a quality of an environment prone to disruption, and movement through a cycle of intermediation, disintermediation and reintermediation [31]. For a discussion specific to the disintermediation portended by blockchain see Quiniou [32]. Space for new products or services follows and presents manufacturers with new scenarios for make-versus-buy strategic decisions.

This perspective is important to the synthesis of the case studies because new and emerging forms of services and products related to supply chain traceability are potentially reported. These may benefit from consideration of their overall impact on the supply chain.

Centralized and Decentralized

A traditional view of decentralization is simply the shape of a particular network described classically by Baran and reported in Schneider [33]. The semantics of the concepts centralized and decentralized; however, quickly become problematic. Polycentricity is described by Ostrom [34] in the field of public administration as the naturally arising interaction of otherwise formally independent decision-making centers (p. 52). Since these independents did not begin as centralized, decentralized confuses further discussion.

This perspective is important to the synthesis of the case studies because aspects of blockchain tend to be described as decentralized. Additionally, the formation of supply chains can be said to be decentralized because, in a canonical free market, autonomous buyers and sellers decide to cooperate. Both ideas are relevant to the discussion.

6.7.2.2 Mental model analysis summary

Even across a few voluntarily provided case studies, a wide variety of activities in supply chain traceability surfaced. We have settled on a handful of mental models to use as aids in looking across the case studies for research indicators and precursors to tomorrow's standardization needs. Using the models has highlighted potentially market-driven motivations arising from current supply chain circumstances (e.g., counterfeit products) and classic business drivers for improved profitability, market share, efficiency, and scale. In this section, each of the five mental models will be used to structure a conversation spanning the activities of our respondents. Each conversation concluded with one or more candidate research areas which are provided in [Appendix E](#).

Supply Chain Risk Management Summary

NIST 800-161 is a foundational reference for risk assessment in acquiring organizations. An organizational orientation to risk assessment highlights when, in fact, the means to mitigate some risks must be addressed by a community or domain of stakeholders. As described in most case-cited situations, risk abatement appears to be an activity of the community as well as an internal pursuit. Some projects and proofs of concept are described as being partnerships between a solution provider and a single company pursuing business improvement, while others assembled groups that constitute a supply chain use case.

As a result, research could move to address broader ecosystem views rather than focusing on whether communities recognize the need for cooperation in contending with supply chain risks

Marketplace Positioning Summary

Our respondents easily display the qualities of innovators as well as an appreciation for technology adoption cycles. The variety of pursuits and experiences in solution and value seeking included: internally run custom projects with research and development partners, outsourcing to specialist vendors, and hybrid solutions as the technology expands in use and incentivizes cooperation. In line with the diffusion model, the strategic minded can forecast potential market share as the numbers of, and scale of, uses in tandem create profit opportunities. In turn, reaching larger audiences as well as anticipating needs of new entrants and latecomers enters the equation of strategic planning.

Win/Win and the PPF Summary

Traceability technologies can be said to move the PPF such that the Win/Win situation of having more of both can be realized. For some, this is counter-intuitive because protecting data has been a traditional method of securing it. As suggested in cases, efforts to share data to protect the objectives of an ecosystem can encounter a myriad of existing assessments, controls, and procedures, all enforced at the data owner's level. The responsibility for data and associated information can be burdensome as it can reflect IP (such as a bill of materials) or national security concerns as in export-controlled technology data. While we see from our respondents their recognition of the value in cooperating to share data across supply lines, there is still the hard work of determining what information is crucial to the success of traceability efforts.

Intermediation and Disintermediation, Make or Buy Summary

Opportunities for intermediation are potentially dominant, given the experiences described by our respondents. These discussions surfaced:

- Intermediation resulting from potential profitability for companies offering supply chain traceability solutions that include operations.
- An external operator of a blockchain solution can be attractive, where teaming of companies is variable and commonplace, as in government monopsony conditions.
- Strengthening existing intermediators as their roles in data collection are enhanced, such as co-ops.
- Willingness to outsource on the part of supply chain participants. As technologies mature and solution sets become more complete, innovators and the subsequent majority of interested adopters may see outsourcing as viable to strategy.

Fewer suggestions of disintermediation surfaced. These primarily relate to existing security measures that are displaced by improved circumstances of traceability. Examples are improved physical-component identity reducing physical security roles and un-needed administrative services for tracking and responding to supply chain discrepancies. The degree to which displacement of currently profitable roles is portended appears overshadowed by the opportunities to fill solution niches.

Centralization and Decentralization Summary

Defining decentralization, on its own footing, begs for research into its semantics and application. Introducing decentralization as a desirable characteristic of traceability solutions compounds the dilemma.

Our respondents' businesses have characteristics that can be cast variously as centralized or decentralized. Farms are both geographically dispersed and regional. Maintenance facilities are scaled to serve multiple operational units. A dominant buyer is a central figure in a supply chain. Events with ripple effect have a central point of origin, such as demurrage and other logistics situations. Responsibility for performance coalesces with the prime contractor. And so on. It is not clear from our respondents that decentralization, as when used to describe blockchain solutions, is particularly interesting. Instead, business drivers and strategic commitments attract attention.

7 Future Research Opportunities

The future research themes below were synthesized from three activities (see [Figure 11](#)) driven by the methodology described in [Section 6](#), Industry Case Studies & Analysis above including:

1. Engagement with community of interest practitioners and interested parties.
 - Engagement ranged from large live virtual meetings, down to small group and individual discussions and asynchronously via email. This activity is called “Standards and Solution Experts” in the diagram below. The philosophy was to build on the reality of successes today.
 - See [Section 5](#), Considerations for Adoption of Blockchain which captures highlights of those discussions.
2. Engagement with case study respondents
 - interview to solicit written case study
 - individual and group discussion
 - submitted written case study (or publicly available)
 - see [Section 6](#), Industry Case Studies & Analysis and the Appendices capture the discussions and case studies
3. Analysis by authoring team
 - down selected several comparative models which provide a variety of perspectives to consider the case studies
 - applied the models to the case studies, and extracted take-aways from analysis
 - See [Section 6](#), Industry Case Studies & Analysis and the Appendices capture the discussions and case studies.

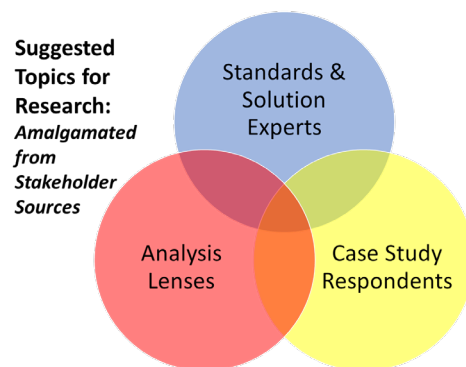


Figure 11 - Community of Interest contributions

The result is a set of seven broad research areas described below which will address areas of uncertainty and concern based on traceability activities of supply chain participants today.

The most striking observation is that the case studies indicate a mega-trend toward participants self-forming ecosystems to share sufficient data records to implement traceability. Further, some of the ecosystems appear on a path to intersect soon. The path shows the formation of scale levels of complexity¹¹, common in natural systems.

The traceability scale factors discovered in this paper are:

- Individual supply chain participant
 - This is most often an enterprise or company which recursively has its own scale levels. For example, a common information system strategy for an enterprise is to manage identities internal to and across the enterprise.
- Supply chain traceability ecosystem
 - See [Figure 4](#)
 - This is the scale level of the case studies where a set of participants agree to cooperate to the extent that they can implement traceability across the ecosystem (see [Section 2.5](#), Ecosystem Perspective).
- Network of supply chain traceability ecosystems
 - See [Figure 8](#).
 - In discussion with some of case study contributors it became clear that some of these nascent ecosystems will likely need to intersect.
 - In observation of “global” identity providers, there are already examples where ecosystems choose to align and intersect, rather than to try and take over the other. See [Section 5.7](#), Identity for Supply Chain Partners.
 - The goal in connecting and intersecting the identity ecosystems is to further the reach of identity beyond the original ecosystem. This creates a network of “global” identity.
 - In analogous fashion, a network of supply chain traceability ecosystems may be able to further the reach of traceability beyond a single ecosystem.

The future research topics are organized as themes to support the multi-scale level findings and listed in [Table 2](#):

¹¹ [Concepts: Scale — New England Complex Systems Institute \(necsi.edu\)](#)

Table 2 - Research Opportunities

Research	Opportunity
Identity	Identity is core to any ecosystem, and mapping identities across ecosystems is critical to enable networks of ecosystems, and for traceability to scale as well. See Section 5.7 .
Message Content Standards	Traceability is expressed as data records, and the semantics and syntax must be agreed upon within an ecosystem and understood or mapped across ecosystems (similar to the “global” identity network discussion above).
Barriers to Entry	In addition to identity and traceability data records, the ecosystem needs participants to achieve an MVE. Minimizing barriers to entry is key to maximizing participation which benefits not only the affected participant, but the ecosystem and network of ecosystems as well.
Supply Chain Traceability Ecosystem	What are the key aspects of an MVE? What types of incentives are beneficial to consider? How sensitive is the ecosystem to changes?
Metrics	Ecosystems will start small, and incrementally grow. The incremental growth must be driven by metrics which all participants in the ecosystem agree to use as the basis for development, test, and operations.
Patterns in Supply Chain Traceability	The implementation of ecosystem identity, traceability records, blockchain, and other aspects such as off-chain storage will benefit from development of patterns which give future ecosystems a jump start to instantiate themselves.
Ecosystem Scale and Interoperability	This scale level is where supply chain wide traceability occurs. Also, many unknowns may surface regarding identity and making the ecosystem-to-ecosystem connection. As examples: what constitutes the cyber-attack surface of newly interoperating blockchain ecosystems? What contract requirements are needed to address such types of cyber attacks including roles and responsibilities?

The seven themes, above, that emerged from the discussions are presented in this section for consideration for their potential as inputs to research formulation. The following theme discussions were designed such that they may be restated or developed into hypotheses, challenge statements, driving industry characteristics, or simply thought-provoking discussion for a working group. While at the same time there is a cohesion to the set of themes that provides a sense of completeness as a research agenda, as it progresses from pointed prerequisites (identity), through emergence of patterns, to anticipation of great scale (ecosystem interoperability).

7.1 Identity

The theme of identity relates to long standing challenges arising from digital representations in cyberspace. The digital aspects of accountability and its consequences make the challenges particularly difficult. Two areas arise: assured links between uncommunicative physical objects and their data records and likewise, linkage of digital identities to human individuals, communicating sensors, and organizational entities.

Two aspects of the identity emerging technology field are: 1.) Non-invasive means of marking physical objects without corrupting them (e.g., cyber-physical anchors), 2.) Privacy respecting means allowing humans and organizational entities to assert their identities for accountability.

Additionally, identity as linkage to physical objects and human individuals may be very well-known within an ecosystem but uncertainty may be introduced when mapping across intersecting ecosystems or by other challenges. Further challenges arise when inspecting parts virtually / remotely when uncertainties can be introduced. Consider including probabilistic aspects with identity with potential utilities such as cost functions.

Impacts: Traceability is strengthened when an ecosystem provides: 1.) Provable linkage between physical goods and data records, 2.) Consistent, repeatable, and understandable means of establishing and using identity.

7.2 Message content standards

The theme of message content standards encompasses the form and vocabulary for traceability transactions. What is the minimum set of data elements and the associated message or process context to support a successful traceability project? Can strategies from previous efforts at design criteria, such as an hour-glass model [35] serve as guidance? Existing business exchange standards provide solid footing for incremental improvements, such as the Open Applications Group Integration Specification (OAGIS), and GS1 EPCIS and Core Business Vocabulary (CBV)¹².

Context for transactions and requests traversing the supply chain can include: 1.) traceability as provenance is established and 2.) market intelligence as end operating environments explore demand. Further, message content should be considered in the context of the supply chain participant processes that generate and consume these data records. The participants may not have coordinated processes or messages prior to joining the ecosystem. The act of joining requires participating in negotiating message content standards. After adopting the ecosystem messages, increased traceability may have impacts to these processes, and successive iterative improvements by individual supply chain participants will improve overall ecosystem traceability.

Impact: Discovering the stable attributes of traceability qualities can potentially improve success rates and longevity of standards for transaction vocabularies. Pinpointing the necessary and sufficient alleviates data sharing concerns and avoids translation steps encouraging participation in supply chain traceability ecosystems.

7.3 Barriers to entry

Our discussions revealed recognition that risks are reduced, and business efficiency can be improved with cooperation among suppliers, manufacturers, distributors, and end operating environments. For this reason, removing barriers to entry is particularly of interest in cultivating successful supply chain traceability ecosystems. Small and niche suppliers can be instrumental in production scenarios and are courted as sources of innovation. Barriers include:

¹² <https://www.gs1.org/standards/epcis>

- 1) the degree of investment needed to meet a minimally competitive level of traceability operations,
- 2) the necessity of sophisticated knowledge, expertise, and resources (which may be scarce) in operating or participating in new solutions, and
- 3) the undue disruption to existing operating models.

Additionally, the quicker that traceability arrangements can be agreed upon, the quicker risk reduction measures can take effect. Speed to solution can include onboarding procedures for participants and other ecosystem creation aids such as message content standards and data sharing agreement templates. Overall, rate of adoption can increase through identification of and removal of barriers to entry.

Impact: Burdensome supply chain traceability solutions potentially reduce the flow of innovation and freshness of competition by minimizing participation of start-ups, small, and niche players.

7.4 Supply chain traceability ecosystems

With cooperation among the supply chain participants comes the emergence of an ecosystem with scope (or perhaps boundary) commensurate with the participants' objectives. The ecosystem draws in levels of commitment from its participants that potentially imply thresholds for effectiveness. An MVE likely can be characterized in terms both qualitative and quantitative, such as:

- 1) degrees of cooperation
- 2) data sharing
- 3) connectedness
- 4) mutual benefit

The governance associated with traceability could have recognizable patterns within its scope of membership, market share, economic conditions, etc. There are likely dynamics and complexities that are difficult to characterize. Complexity sciences and study of socio-technical systems could offer means of quantifying the minimally viable ecosystem, such as with graph theory metrics and other metadata for modeling and simulation. Existing research contributors include Chauhan, Frayet, & LeBel [36], Tachizawa & Wong [39], Vernon & Keeling, [38].

Further, consideration should be given to incentives used within an ecosystem, especially when initializing the MVE. Additionally, roles and responsibilities for ecosystem capabilities need to be established. This could include outsourcing delivery and sustainment of the ecosystem blockchain to a third party, and use of industry consortia to negotiate business rules and message content standards.

Impact: Employing graph theory and exploring connectedness could lead to improved

appreciation of risk and effectiveness in the emergence of an ecosystem.

7.5 Metrics

For our respondents, measurements in the context of supply chain traceability tended toward alleviation of business operations pain points and solution performance specifics. The potential for project management metrics in progress tracking for traceability implementation efforts which can be applied within a single participant's scope is also notable. Traceability metric development drives discovery and measurement of desirable qualities of the MVE, and informs governance or dashboard displays that relay information about ecosystem operations monitoring or improvement.

As traceability is implemented across larger regions of the supply chain, metrics will be required to measure:

- 1) coverage of requirements and
- 2) effectiveness of mitigating supply chain risk associated with individual and combined traceability efforts.

A traceability ecosystem may contain information beyond traceability, such as connectedness and flow of goods through an ecosystem. This opens the potential for introducing metrics from the disciplines of complexity science and graph theory, for example resilience and supply chain reconfigurability [46].

Impact: Metrics are required to reliably identify traceability gaps, understand sensitivity to them, and measure progress in addressing those gaps. Measurements of cost and effectiveness could reveal that traceability is akin to quality measures that tend to pay for themselves in the avoidance of rework and waste. The more complete traceability is, the more rework and waste is avoided.

7.6 Patterns in supply chain traceability

As technology adoption progresses and the business value of supply chain traceability takes shape with numbers and dollars, emerging patterns make for opportunity to move traceability from craft to repeatable best practice. As tacit and internal knowledge forms, identifying patterns is a method of making best practice explicit and further contributes to metrics development and operational awareness. Patterns in the context of supply chain traceability that would potentially contribute to repeatable best practice may take form as patterns of use, implementation, and solution architecture.

- 1) Patterns of use include collecting conditions that highlight the need for traceability. Examples could include the phrases such as: As a quality control user, I need to find and expose introduction of counterfeit components in the supply chain. These patterns of use start with ecosystem-wide concept development, and drive user stories with individual stakeholders as they use agile and other methods to update capabilities and how they interact with the traceability ecosystem.

- 2) Patterns of implementation examine the trade space of incremental deployment of solutions. Our respondents were not fans of disruptive solutions, and, instead, preferred initial experimentation followed by increments of value delivered in a sequence. These build outs give form to creation of viable ecosystems of traceability for repeat performances and longevity of benefit.
- 3) Architectural patterns arise from the needs of particular ecosystems and how they relate to the choices from among solutions and the resulting structures. These portend to be highly strategic, encompassing organizational variations, levels of data visibility (e.g., on and off chain storage trades), accommodation of industry volumes, membership, and IP concerns. The glimpse of a potential architectural driver could arise from whether the ecosystem derives from a strict avoidance of risk or a disciplined business approach to profit and efficiency. The trade space analysis and success measures are likely different.

Impact: Consistently applied patterns become best practices that can accelerate adoption, speeding benefit and risk avoidance. Additionally, the pattern that is “supply chain” or is “supply network” is a driver of scale as ecosystems discover benefit in interoperability. Patterns may emerge to inform supporting the lifecycle of a product beyond initial delivery. Implementation patterns that can be expressed as standards can accelerate adoption.

7.7 Ecosystem scale and interoperability

Traceability ecosystems will tend to grow both members, and types of traceability information tracked, creating new scenarios of scale and interoperability. Such scenarios may relate to intersections of traceability information needs and to cyber vulnerabilities in expanded surface area.

As some of these traceability ecosystems grow, they will intersect and need to exchange traceability information between them. A simple example is where an industrial control traceability ecosystem and a microelectronic traceability ecosystem both contribute to a nuclear power ecosystem. In this case, the microelectronics are used in the industrial controls which are then used in the nuclear power plants (serial exchanges). Other situations could have parallel exchanges as well.

Once ecosystems intersect and exchange traceability information, either serially or in parallel, the need for understandability of syntax and semantics arises. The patterns of traceability use cases may or may not scale along with the activities. New patterns may emerge as the interacting solutions cope with dynamics of business relationships.

The emergence of great scale among intersecting and interoperable ecosystems introduces a need for updated definitions of cyber-attack surfaces and exploration of new attack vectors. In one view, the addition of blockchain solutions layers in complexity impacting characteristics of system coupling which can lead to trade-offs between resilience and inherent propensity to cascading attack consequences [57] [58]. Other considerations include:

- Need for specific cybersecurity related requirements [4] to incorporate updated ecosystem cybersecurity roles and responsibilities expressed in associated contracts [59].

- Consideration of typically centrally administered cyber certifications, such as granting an Authority to Operate (govt) or the equivalent in commercial settings, and applicability to decentralized capabilities.
- Overcoming cybersecurity practices which may result in siloing cyber knowledge in specific domains, e.g., industrial controls, space satellites.
- Security and life cycle management concerns associated with dependence on open-source software [60].

Impact: The mechanics and patterns of linking traceability between blockchain solutions, for example to accommodate logistics, must ultimately stand up to the demands of multiple end operating environments and traceability ecosystems. The experience need not be the only teacher. Experiments, further proofs of concept, modeling and simulation could improve readiness and cyber resilience. By probing with adaptive models, we may anticipate constitution of transactions, in scope, identity solutions, content, vocabulary, synchronicity, and perhaps unforeseen characteristics when market forces and cyber adversaries are on the move.

7.8 Opportunities cross reference

As an aid in using the themes, Table 3 leads from the themes into specific observations, applicable literature citations, and probing narratives intended to inform or inspire research proposals.

Table 3 - References for More Granular Discourse

Theme	References
Identity, 7.1 Keyword: identity	Sections: 1.4 , Foundational practices 4.2 , Cyber-physical anchors 5.7 , Identity for supply chain partners 6.4 , DUST Identity 6.6 , Chain Integration Project (CHIP) 6.7.2.2 , Mental model analysis summary 7 , Future Research Opportunities 7.7 , Ecosystem scale and interoperability 8 , Conclusions Case Study: DUST Identity , CHIP Appendix: C.5 , Dust Identity D.4 , Intermediation and disintermediation, make or buy candidates E.4 , Ecosystems of cooperation E.8 , Identity
Message content standards, 7.2 Keywords: message, transaction, standard	Sections: 1.3 Target audience 1.7 , Summary of insights 3.1.1 , Smart contracts 3.1.2 , Standards-based approach to protecting proprietary information 4.1 , Blockchain

Theme	References
	<p>4.2, Cyber-physical anchors 5.2, Information exchange standards 5.4, Multiple blockchains 5.7, Identity for supply chain partners 6.5, MediLedger 6.6, Chain Integration Project (CHIP) 7, Future Research Opportunities 7.3, Barriers to entry 7.4, Supply chain traceability ecosystems 7.7, Ecosystem scale and interoperability 8, Conclusions Case Study: CHIP, MediLeger, Sky Republic Appendix: A.5, Centralized and Decentralized C.5, DUST Identity C.6, MediLedger FDA Pilot Project D.1, Supply chain risk management candidates D.2, Marketplace positioning candidates D.3, Win/win and the production possibility frontier candidates E.11, Cross blockchain transactions E.12, Standards E.15 Metrics</p>
<p>Barriers to entry, 7.3 Keywords: barrier, small business</p>	<p>Sections: 1.3, Target audience 1.7, Summary of insights 3.2, Applicable domains 6.7.2.1, Selected models 7, Future Research Opportunities 8, Conclusions Case Study: DUST Identity, Sky Republic Appendix: A.2, Technology lenses & adoption curve C.2, Sky Republic C.6, MediLedger FDA Pilot Project D.2, Marketplace positioning candidates</p>
<p>Supply chain traceability ecosystems, 7.4 Keywords: ecosystem, lateral</p>	<p>Sections: 1.1, Purpose 1.4, Foundational practices 1.5, Relationship to other programs and publications 1.6, Methodology overview 1.7, Summary of insights 2.5, Ecosystem perspective 2.6, Industrial control system example 2.7, Traceability challenges 2.8, Decentralized information sharing 3.2, Applicable domains 3.3, Metrics 4, Technologies Supporting Traceability 4.1, Blockchain 4.2, Cyber-physical anchors</p>

Theme	References
	<p>4.3, Other technologies 5.1, Metrics 5.2, Information exchange standards 5.3, Minimum viable ecosystem 5.4, Multiple blockchains 5.5, Intellectual property 5.6, Privacy 5.7, Identity for supply chain partners 6.7.2.1, Selected models 6.7.2.2, Mental model analysis summary 7, Future Research Opportunities 7.1, Identity 7.2, Message content standards 7.3, Barriers to entry 7.5, Metrics 7.6, Patterns in supply chain traceability 7.7, Ecosystem scale and interoperability 8, Conclusions Case Study: Sky Republic, Field to Fork Appendix: A.3, Win/win and production possibility frontier C.1, Field to Fork C.2, Sky Republic C.5, DUST Identity D.1, Supply chain risk management candidates D.3, Win/win and the production possibility frontier candidates E.3, Data traceability E.4, Ecosystems of cooperation E.6, Analysis and trade space of decentralization, distribution, and consensus E.7, Analysis method to quickly discover/form/implement a blockchain enabled ecosystem E.8, Identity E.10, Minimum viable ecosystem E.11, Cross blockchain transactions E.12, Standards E.14, Decentralized information sharing (trusted, attributed, resilient) E.15, Metrics</p>
<p>Metrics, 7.5 Keywords: metrics, measure</p>	<p>Sections: 1.7, Summary of insights 2.3, Relevant NIST Special Publications 2.4, Product provenance and pedigree 2.7, Traceability challenges 3.1, Potential benefits of improved traceability 3.1.1, Smart contracts 3.3, Metrics 4.1, Blockchain 5.1, Metrics 5.3, Minimum viable ecosystem 5.4, Multiple blockchains 6.3, Guardtime Federal and “Perspectives from a Prime” 6.7.2.2, Mental model analysis summary</p>

Theme	References
	<p>7, Future Research Opportunities 7.3, Barriers to entry 7.4, Supply chain traceability ecosystems 7.6, Patterns in supply chain traceability 8, Conclusions Case Study: Guardtime Federal and Large Prime, Field to Fork Appendix: A.2, Technology lenses & adoption curve D.2, Marketplace positioning candidates D.5, Centralization and decentralization candidates E.10, Minimum viable ecosystem E.15, Metrics</p>
<p>Patterns, 7.6 Keyword: pattern</p>	<p>Sections: 7, Future Research Opportunities 7.4, Supply chain traceability ecosystems 7.7, Ecosystem scale and interoperability 8, Conclusions Case Study: Sky Republic Appendix: A.5, Centralized and decentralized C.2 Sky Republic D.1, Supply chain risk management candidates E.2, Data integrity E.4, Ecosystems of cooperation E.10, Minimum viable ecosystem E.16, Data patterns of external repositories (from legacy to Solid, IPFS, etc.)</p>
<p>Scale and ecosystem interoperability, 7.7 Keywords: scale, interoperability</p>	<p>Sections: 1.7, Summary of insights 4, Technologies Supporting Traceability 5.4, Multiple blockchains 5.7, Identity for supply chain partners 6.5, MediLedger 6.7.2.2, Mental model analysis summary 7, Future Research Opportunities 7.6, Patterns in supply chain traceability 8, Conclusions Case Study: DUST Identity, Field to Fork, Guardtime Federal and Large Prime, MediLedger Appendix: A.2, Technology lenses & adoption curve C.1, Field to Fork C.5, DUST Identity C.6, MediLedger FDA Pilot Project D.1, Supply chain risk management candidates D.2, Marketplace positioning candidates D.5, Centralization and decentralization candidates E.15 Metrics</p>

8 Conclusions

Improving traceability in manufacturing systems holds the promise of mitigating critical risks to our increasingly interdependent supply chains. Traceability encompasses both pedigree and provenance assertions about goods and services, and most importantly requires agreement from the supply chain participants to define and implement a solution. As in many domains of human activity, traceability agreements can start locally and expand in scope over time.

This paper effort engaged a community of interest (industry, academia, government) who are actively working traceability challenges, and who offered several case studies. The goal is to learn what is happening now (as exemplified by case studies), where efforts will go (emerging trends), and what challenges may be encountered, including these candidate research opportunities:

1. Identity
2. Message Content Standards
3. Barriers to Entry
4. Supply Chain Traceability Ecosystems
5. Metrics
6. Patterns in Supply Chain Traceability
7. Ecosystem Scale and Interoperability

The case studies and associated discussion notes are available in full in the appendices, as researchers may find the source material useful. The cases studies offered a rich variety of committed supply chain participants addressing traceability using innovative approaches. Several conclusions arise from the case studies and analysis:

1. The evolutionary path of improving traceability follows the path of forming local ecosystems to develop and agree on traceability language and establish definitions of traceability terms in data records exchanged.
 - a. This trend is observed.
 - b. The tradeoffs between IP protection and privacy are more likely to initially be settled locally versus supply chain wide, where top-level agreements without organic lower-level support are likely be over-constrained and difficult to achieve.
2. These traceability ecosystems can internally use decentralized information sharing to overcome the restriction of typical bi-lateral business-to-business (B2B) connections (tiers).
 - a. This trend is observed.

- b. The decentralized information sharing technology can range from DLT (Decentralized Ledger Technology) to blockchain.
 - c. The benefit of DLT is that the ecosystem can operate redundant nodes to add resiliency.
 - d. However, if the ecosystem needs more decentralization due to not entrusting any one participant with control over the data, then blockchain can be used (ledger + decentralized control).
 - e. Overcoming bi-lateral connections enables traceability data records to be shared as widely as agreements can be forged. This scope naturally forms an ecosystem and shares a common purpose, common agreement on language, and a common means to exchange data records.
3. These traceability ecosystems will soon start to connect and form a network of ecosystems.
 - a. This is the trend anticipated in manufacturing supply chains.
 - b. This trend has been recently observed in global identity networks.
 - c. A network of traceability ecosystems, together with a means to measure progress and make incremental improvements will grow the network.
 - d. Cybersecurity measures and perspectives will be influenced by the scale of interoperable ecosystems and redistribution of cyber responsibilities among participants.
 4. The emergent growth of networks of ecosystems can be accelerated by larger feedback loops (hypothesis).
 - a. A feedback loop of observations, lessons learned, pattern derivation, and updated proposed research areas will grow the scope of networks of traceability ecosystems across the manufacturing supply chain.
 - b. This paper is the first step of feedback and proposed research areas.

The authors of the paper anticipate vigorous and constructive discussion regarding the research themes, leading to formation of beneficial research efforts. The results of these research efforts will inform the greater manufacturing supply chain community to:

- enable growth of traceability ecosystems, while reducing barriers to entry
- enable growth of networks of traceability ecosystems as needed
- lead to increase breadth and scope of sharing traceability information for manufacturing supply chains

Regardless of the numerous research questions to answer, initial observations indicate that an approach of growing traceability ecosystems enabled by blockchain and related technologies could contribute significantly to increasing the traceability of manufacturing supply chains.

References

- [1] Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. <https://doi.org/10.6028/NIST.SP.800-161>.
- [2] Joint Task Force (2020). *Security and Privacy Controls for Information Systems and Organizations*. (National Institute of Standards and Technology, Gaithersburg, MD). NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of September 23, 2020. <https://doi.org/10.6028/NIST.SP.800-53r5>. Available at <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>.
- [3] Adner, R (2012) *The Wide Lens: What Successful Innovators See That Others Miss* (Penguin Group, New York, NY).
- [4] Yaga D, Mell P, Roby N, Scarfone K (2018). *Blockchain Technology Overview*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8202. <https://doi.org/10.6028/NIST.IR.8202>.
- [5] Khan SN, Loukil F, Ghedira-Guegan C, Benkhelifa E, Bani-Hani A. (2021) Blockchain Smart Contracts: Applications, Challenges, and Future Trends. *Peer-to-Peer Networking and Applications*. pp 1-25. doi: <https://doi.org/10.1007/s12083-021-01127-0>.
- [6] Thilmann J (2021) Identical Twins. *The American Society of Mechanical Engineers*. [Web Site]. Available at <https://www.asme.org/topics-resources/content/identical-twins>.
- [7] Tian F (2017) A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain & Internet of Things. *International Conference on Service Systems and Service Management*, (IEEE,7/31/2017), pp 1-6. <https://doi.org/10.1109/ICSSSM.2017.7996119>.
- [8] Rogaway P, Shrimpton T (2004) Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. *Fast Software Encryption, 11th International Workshop* (New Delhi, India). pp. 371-388. <https://www.iacr.org/archive/fse2004/30170373/30170373.pdf>.
- [9] Rusinek M, Zhang H, Radziwill, N (2018) Blockchain for a Traceable, Circular Textile Supply Chain: A Requirements Approach. *Software Quality Professional* 21(1):4-24.
- [10] Krima S, Hedberg T, Barnard Feeney A (2019) *Securing the Digital Threat for Smart Manufacturing: A Reference Model for Blockchain-Based Product Data Traceability* (National Institute of Standards and Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.AMS.300-6>.
- [11] Dwork C, Naor M (1993) Pricing via Processing or Combatting Junk Mail. *Advances in Cryptography: 12th Annual International Cryptology Conference*, (Santa Barbara, California). <https://web.cs.dal.ca/~abrodsky/7301/readings/DwNa93.pdf>.
- [12] Hedberg T, Krima S, Camelio J A (2016) Embedding X.509 Digital Certificates in Three-Dimensional Models for Authentication, Authorization, and Traceability

- of Product Data. *Journal of Computing and Information Science in Engineering* 17(1):11008– 11011 <https://doi.org/10.1115/1.4034131>.
- [13] Prada-Delgado M, Dittmann G, Circiumaru I, Jelitto J (2021) A Blockchain-Based Crypto-Anchor Platform for Interoperable Product Authentication. *International Symposium on Circuits and Systems*, (IEEE 4/27/2021) <https://doi.org/10.1109/ISCAS51556.2021.9401582h>.
- [14] Jelitto J, Dittman G, Angel Prada Delgado M. (2019) Crypto Anchors and Blockchain: a Strong Alliance against Supply Chain Fraud. *IBM Research-Zurich* [Web Site]. Available at www.ibm.com/blogs/research/2019/12/crypto-anchors-and-blockchain-a-strong-alliance-against-supply-chain-fraud/.
- [15] Ghent University, *Solid: Taking Back the Web Through Decentralization*. Available at <https://rubenverborgh.github.io/Slides-FOSDEM-2019/#views>.
- [16] Crosby PB (1996) *Quality is Still Free: Making Quality Certain in Uncertain Times* (McGraw-Hill Companies, New York, NY).
- [17] Massachusetts Institute of Technology, *Solid* [Web site]. Available at <https://solid.mit.edu>.
- [18] Lesavre L, Varin P, Mell P, Davidson M, Shook J (2020) *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*. (National Institute of Standards and Technology, Gaithersburg, MD).
- [19] Sample M (2019) *MediLedger DSCSA Pilot Project* (AmerisourceBergen, Chesterbrook, PA). <https://www.mediledger.com/dscsa-fda-pilot-project>.
- [20] Auburn University RFID Lab (2019) *Chain Integration Project (CHIP) Proof-of-Concept Whitepaper*. [Web Site]. Available at: <https://rfid.auburn.edu/chip-project-chain-integration-pilot/>.
- [21] Cui P, Dixon J, Guin U, DiMase D (2019) *A Blockchain-Based Framework for Supply Chain Provenance*. (IEEE Access, 10/28/2019), pp 157113-157125. DOI: <https://doi.org/10.1109/ACCESS.2019.2949951>.
- [22] Guin U, Cui P, Skjellum A (2018) Ensuring Proof-of-Authenticity of IoT Edge Devices using Blockchain Technology. *IEEE International Conference on Blockchain*. (IEEE, 6/3/2019), pp. 1042-1049. DOI: https://doi.org/10.1109/Cybermatics_2018.2018.00193.
- [23] Senge P (2006) *The Fifth Discipline: The Art and Practice of the Learning Organization* (Doubleday/Currency, New York, NY), 2nd Ed.
- [24] Bui H (2020) From the Fifth Discipline to the New Revolution: What We Have Learnt from Senge’s Ideas Over the Last Three Decades. *The Learning Professional* 27(6):495-504. <https://doi.org/10.1108/TLO-04-2020-0062>.
- [25] Johansson, F (2017) *The Medici Effect, With a New Preface and Discussion guide: What Elephants and Epidemics Can Teach Us About Innovation* (Harvard Business School Press, Boston, MA:), 2nd Ed.
- [26] Brand S (2008) *The clock of the Long Now: Time and Responsibility* (New York, NY: Basic Books).
- [27] Isotta-Riches B, Randell J (2014) Architecture as A Key Driver for Agile Success: Experiences at Aviva UK in *Agile Software Architecture: Aligning Agile Processes and Software Architectures*. Ali Babar M, Brown A, Mistrik, I, Eds. (Burlington, MA: Morgan Kaufmann), pp. 357-374. <https://doi.org/10.1016/B978-0-12-407772-0.00014-9>.

- [28] Rogers EM (2004) A Prospective and Retrospective Look at the Diffusion Model. *Journal of Health Communication* 9(1):13-19. <https://doi.org/10.1080/10810730490271449>.
- [29] Gharajedaghi J (2011) *Systems thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture* (Elsevier, Burlington, MA), 3rd Ed.
- [30] Lipsey RG (1975) *An Introduction to Positive Economics* (University Press, New York, NY: Oxford) 4th Ed, pp. 57-58.
- [31] Chircu A M, Kauffman R J (1999) Strategies for Internet Middlemen in the Intermediation/Disintermediation/Reintermediation Cycle. *Electronic Markets* 9(1-2):109-117.
- [32] Quiniou M (2019) *Blockchain: The Advent of Disintermediation* (John Wiley & Sons Incorporated).
- [33] Schneider N (2019) Decentralization: An Incomplete Ambition. *Journal of Cultural Economy* 12(4):265-285. <https://doi.org/10.1080/17530350.2019.1589553>.
- [34] Ostrom V “Polycentricity” in *Polycentricity and Local Public Economies: Readings from the Workshop in Political Theory and Policy Analysis*. McGinnis M, Ed. (Ann Arbor, MI: University of Michigan Press, 1999), pp. 50-74.
- [35] Beck, M (2019) On the Hourglass Model. *Communications of the ACM* 62(7):48-57.
- [36] Chauhan, SS, Frayret JM, LeBel L (2009) Multi-Commodity Supply Network Planning in the Forest Supply Chain. *European Journal of Operational Research* 196(2):688-696.
- [37] Tachizawa EM, Wong C Y (2015) The Performance of Green Supply Chain Management Governance Mechanisms: A Supply Network and Complexity Perspective. *Journal of Supply Chain Management* 51(3)18-32.
- [38] Vernon, MC, Keeling MJ (2009) Representing the UK's Cattle Herd as Static and Dynamic Networks. *Proceedings of the Royal Society B: Biological Sciences* 276(1656):469-476. doi: <https://doi.org/10.1098/rspb.2008.1009>.
- [39] Allison GT, Zelikow P (1999) *Essence of Decision: Explaining the Cuban Missile Crisis* (Addison Wesley Longman, Inc. New York, NY), 2nd Ed.
- [40] Iowa-State College (1957) The Diffusion Process, *Special Report 24*. <https://lib.dr.iastate.edu/specialreports/24>.
- [41] Mukherjee N. (2018) Block Propagation, Scaling and Adoption—Maturing Blockchains. *Medium* [Web Site]. Available at <https://medium.com/coinmonks/block-propagation-scaling-and-adoption-maturing-blockchains-99218260b7b8>.
- [42] Karlsruhe Institut für Technologie, *DSN Bitcoin Monitoring* [Web Site]. Available at <https://www.dsn.kastel.kit.edu/bitcoin/videos.html>.
- [43] European Union Agency for Cybersecurity (2020) *Guidelines for Securing the Internet of Things: Secure Supply Chain for IoT*. Available at <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>.
- [44] Bruce, J (2020) *Proving the Possible: Introducing the Inrupt Enterprise Solid Server*. Available at <https://inrupt.com/enterprise-server-release>.

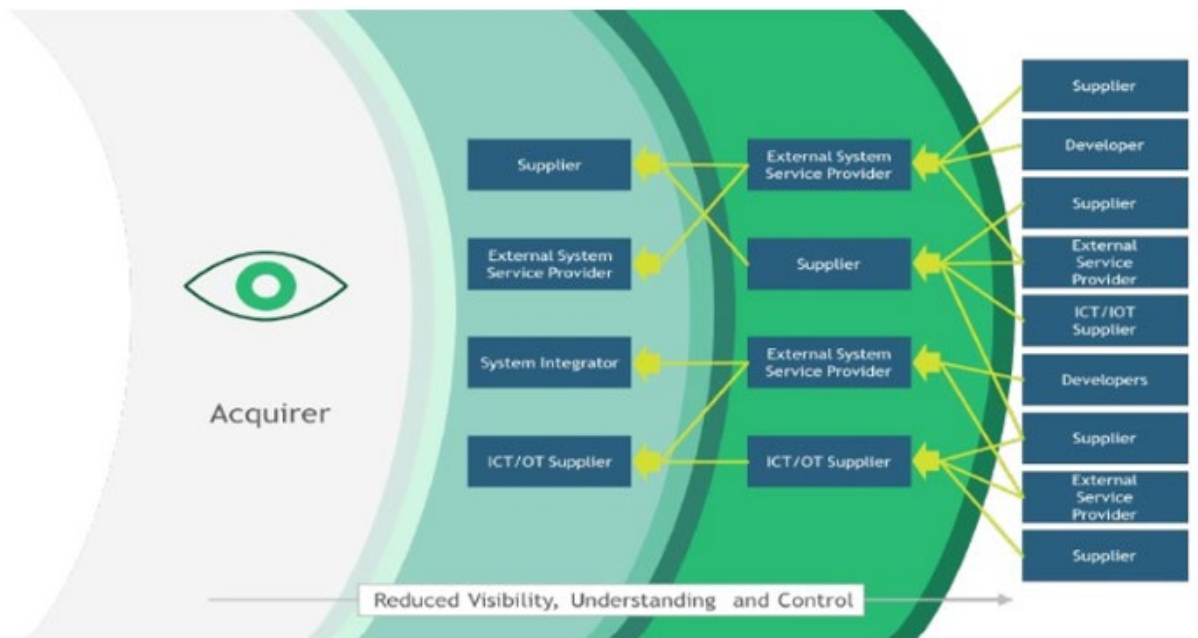
- [45] Cellan-Jones, R (2020) *NHS Data: Can Web Creator Sir Tim Berners-Lee Fix It?* BBC News. Available at <https://www.bbc.com/news/technology-54871705>.
- [46] Zidi S, Hamani N, Kermad L (2021) New Metrics for Measuring Supply Chain Reconfigurability. *Journal of Intelligent Manufacturing*. <https://doi.org/10.1007/s10845-021-01798-9>.
- [47] Patent Kinetics (2021) Kim and Inje Blockchain, Smart Contracts, and DRM Patent Applications. *Managing Rights Management* [Web Site]. Available at: <https://www.managingrights.com/2021/10/kim-and-inje-blockchain-smart-contracts-and-drm-patent-applications.html>.
- [48] Prasad S (2021) The Future of Blockchain in Intellectual Property. Automation.com [Web Site]. Available at: <https://www.automation.com/en-us/articles/january-2021/the-future-of-blockchain-in-intellectual-property>.
- [49] SITA [Web site]. Available at <https://www.sita.aero>.
- [50] Electronic Product Code Information Services [Web site]. Available at <https://www.gs1.org/standards/epcis>.
- [51] SOLID Project [Web site]. Available at <https://solidproject.org>.
- [52] Bingham J, Zagidulin D, Coburn A (2021) *Solid Protocol, Version 0.9.00, 2021-12-17*. (W3C Solid Community Group), Available at <https://solidproject.org/TR/protocol#abstract>.
- [53] W3C Solid Community Group (2021). *Solid/Specification* [Web site]. Available at <https://github.com/solid/specification>.
- [54] W3C Solid Community Group (2021) [Web site]. Available at <https://www.w3.org/community/solid/>.
- [55] Maes R., Verbauwhede I. (2010) Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. In: Sadeghi AR., Naccache D. (eds) *Towards Hardware-Intrinsic Security*. Information Security and Cryptography. (Springer, 10/12/2010), pp 3-37. https://doi.org/10.1007/978-3-642-14452-3_1.
- [56] Feeney AB, Simon PF, Vijay S. (2015) A Portrait of an ISO STEP Tolerancing Standard as an Enabler of Smart Manufacturing Systems. *Journal of Computing and Information Science in Engineering* 15(2). <https://doi.org/10.1115/1.4029050>.
- [57] Perrow C (2011) *Normal Accidents: Living with High Risk Technologies* (Princeton University Press).
- [58] Perrow C (1990) Organizing to Reduce the Vulnerabilities of Complexity. *Journal of Contingencies and Crisis Management* 7(3):150-155. <https://doi.org/10.1111/1468-5973.00108>.
- [59] United States Government Accountability Office (GAO), *Weapon Systems Cybersecurity: Guidance Would Help DoD Programs Better Communicate Requirements to Contractors*, Report to Congressional Committees GAO-21-179, March 4, 2021. Available at: <https://www.gao.gov/products/gao-21-179>.
- [60] Kamp PH (2014) Quality Software Costs Money---Heartbleed Was Free. *Communications of the ACM* 57(8):49-51. <https://doi.org/10.1145/2631095>.

Appendix A—Case Study Analysis Models and Lenses

[Section 6.7.2](#) describes and provides the application of mental models to characteristics of the case studies. Cases are viewed individually and collectively under the umbrella of chosen mental models. The body of the paper summarizes key concepts from these models from a variety of disciplines to present case discussions in a cohesive form. This appendix contains additional information on the models and lenses employed in the analysis as a complementary resource. The models and lenses employed are Cyber Supply Chain Risk Management; Technology Lenses and the Adoption Curve; Win/Win and the PPF; Intermediation, Disintermediation, Classic Make/Buy; and Centralized versus Decentralized.

A.1 Cyber supply chain risk management

NIST Draft Special Publication 800-161 Revision 1 [\[1\]](#) addressing risk in cyber supply chain scenarios supplies two important, foundational, and descriptive models that together aid in framing the proceeding discussions across other models. In addition to describing risk as a function of likelihood and impact, and delving into a comprehensive treatment of risk management, the NIST authors orient to an organization's span of control with respect to its cyber supply chain. The publication presents [Figure 12](#), NIST's Acquirer Viewpoint, illustrating the connections between types of suppliers as the acquisition process reaches out successively to providers. The risk management process is specific to the tasks and interests of a single organization, in keeping with the need for action at an organizational level. It emphasizes the progressive loss in clarity across visibility, understanding, and control as the supply chain expands outward. Consider for example, that at various points on the lines connecting boxes in [Figure 12](#), there are potentially multi-carrier transportation routes for raw materials, assemblies, and finished products.



Source: Fig. 1-3: An Organization's Visibility, Understanding, and Control of its Cyber Supply Chain. NIST SP 800-161 Rev. 1 (Draft)

Figure 12 - NIST's acquirer viewpoint

The publication's treatment of the risk management process of Frame, Assess, Respond, and Monitor, places the identification of threat and vulnerability analysis in the Assess step. Data assets internal to the organization are the object of threats and their exposure the essence of many vulnerabilities. Several categories of information are cited as in need of risk management (mitigation of exposure) leading to protective measures. The types of information include proprietary data, operational data, systems information, product data, payments data, and others. Relationships are also posed as impactful in threat and vulnerability scenarios involving shared suppliers, logistics, tier distance, etc. These relationships create an opportunity for improving visibility while also creating additional data assets. Particularly for the intended federal audience, this publication's models of analysis serve as useful means for identifying protective measures, which include an emphasis on supply chain information sharing related to risk experience across a sharing community to leverage its collective knowledge. [1] (pp. 38-40).

A.2 Technology lenses & adoption curve

Allison and Zelikow [39] refined an analytic approach based on the idea of a lens that captures a particular perspective and context useful in portraying and characterizing historical events. This section selects three lenses for technology, characterizing each as a layer in its potential value or impact to an organization.

The lenses Strategic Innovative, Differentiator, and Routine Administrative are loosely based on Brand's Pace Layering concepts [26] and Gartner's Pace Layered Architecture; the combination of the ideas is described in Isotta-Riches & Randell [27].

[Figure 13](#), Characterizing Value and Impact with Lenses, presents each lens with a short

definition. Each lens is further described below.

Viewing a technology or combination of technologies with the Strategic Innovative lens allows exploration of the potential for market-disrupting improvements that traceability technologies represent on a wide scale. Operating scenarios with this lens include an experimentation tempo within research and development functions. Results are quickly parsed for keepers and implemented on some scale. Brand originally described activities at an extreme pace, with multi-directional characteristics, as being on the order of changes in fashion [26] and this view is extended to include experiences in the presence of disruptive technologies potentially used in innovative ways. These discussions revolve around strategic use of supply chain traceability to further strategic goals of an organization:

- introducing new products or rebranding existing products
- protecting against unpredictable, marketplace security concerns due to increasing complexity
- accounting for classic business model rationales, such as degree of vertical integration, roles of intermediators and conversely, disintermediation
- forecasting and decision making for technology-enabled cooperation and trust
- casting service providers and suppliers in roles that vary in centralized and decentralized characteristics

The Differentiator lens refers to the skills and technology tools that establish a competitive edge for companies and organizations in their domains. These skills and tools set an organization apart from its competitors and/or adversaries. They may include tactics, techniques, tradecraft, or technologies specifically developed in the organization and may be subject to professional non-disclosure agreements or other industrial security measures. These skills and tools are carefully curated; however, responsiveness is a factor because of competitive or adversarial pressures and the pace of development quickens as a result. Measurements are devised and introduced as consistent improvement in quality and/or efficiency is to be demonstrated.

The Routine Administrative lens refers to internal, administrative functions that are fundamental to the accomplishment of everyday or foundational tasks. A high bar of performance is expected in these types of tasks, because without them, an organization's activities would fall short in accomplishing their objectives. Change comes slowly in this foundational area as these tasks are often based on the commonly accepted principles of a domain and have withstood the test of time and careful refinements. They can be barriers to entry, in terms of ability of contenders to join the domain. Additionally, though at a slow pace, tasks such as these are typically subjected to continuous process improvement toward maintaining efficiency and effectiveness. Thus, performance metrics and close cost accounting can be part of managing these kinds of routine tasks.

Lenses Can Relate Supply Chain Traceability to Impact




 Strategic Innovative	The Strategic Innovative lens is reserved for the potential of marketplace impact from improved supply chain traceability technologies. Characterized by rapid experimentation and disruptive technologies.
 Differentiator	The Differentiator lens refers to the skills and tools that establish a competitive edge for companies and organizations in their domains. Characterized by market responsiveness and refinement of advantage.
 Routine Administrative	The Routine Administrative lens encompasses internal, administrative functions of the firm that are fundamental to the accomplishment of everyday or foundational tasks. Characterized by utility and stability, a cost of doing business.

Figure 13 - Characterizing value and impact with lenses

A set of technologies and skills can be said to be institutionalized, if it begins as a product of a strategic innovative process, is proven as a valuable differentiator, and lands as a baseline of functionality that is utilitarian and essential. A start-up entity attracted to a particular marketplace could encounter this cost of doing business as a barrier to entry, since competition with market leaders will be difficult without the utility. A small or niche player will be similarly impacted as investment in the transition could overwhelm their existing business model and capital arrangements.

The maturation of an innovation in the direction of a utility and the effect of the innovation on the competitive environment, lead to motivations across communities to adopt the technology and its corresponding skills and metrics. The innovation adoption lifecycle (an interesting start for background is the 1957 Iowa State College special report [40], as pertains to agriculture) may be a helpful way to conceptualize about movement toward traceability technology in conjunction with that technology’s maturation. Rogers [28] defines diffusion as:

“Diffusion is the process through which an innovation, defined as an idea perceived as new, spreads via certain communication channels over time among the members of a social system.”

In [Figure 14](#) Paths to Value: Implementation Tracks and Diffusion, working left to right distinguishes how solution acquisition, including make/buy or insource/outsource decisions, differ with how an organization can be characterized in the adoption scheme. It also illustrates the differences in paths adopters may experience, using a lens to interpret their view of the technology’s strategic significance and use.

Paths to Value: Implementation Tracks and Diffusion

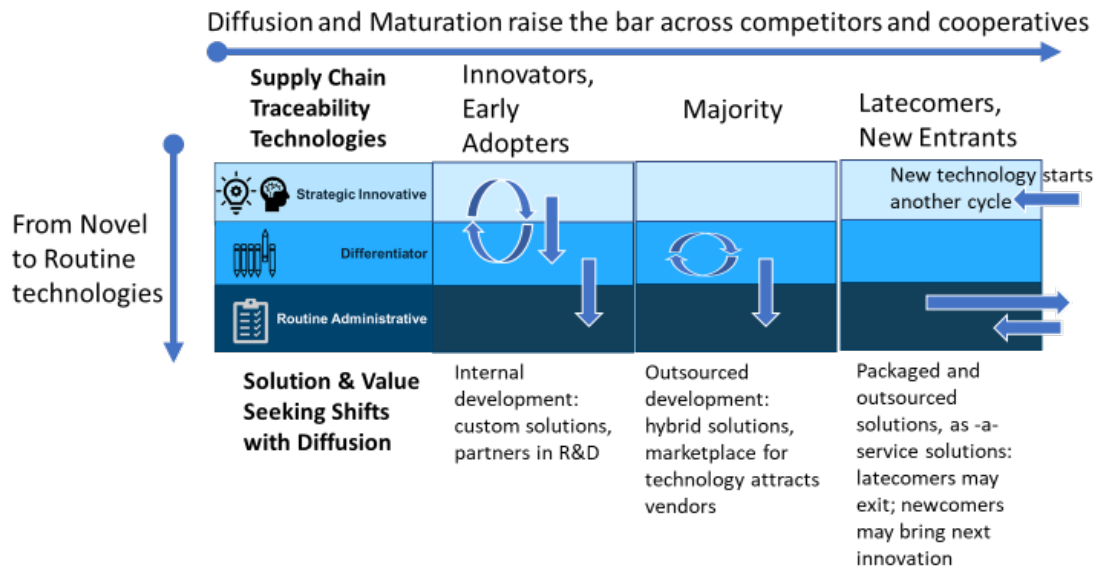
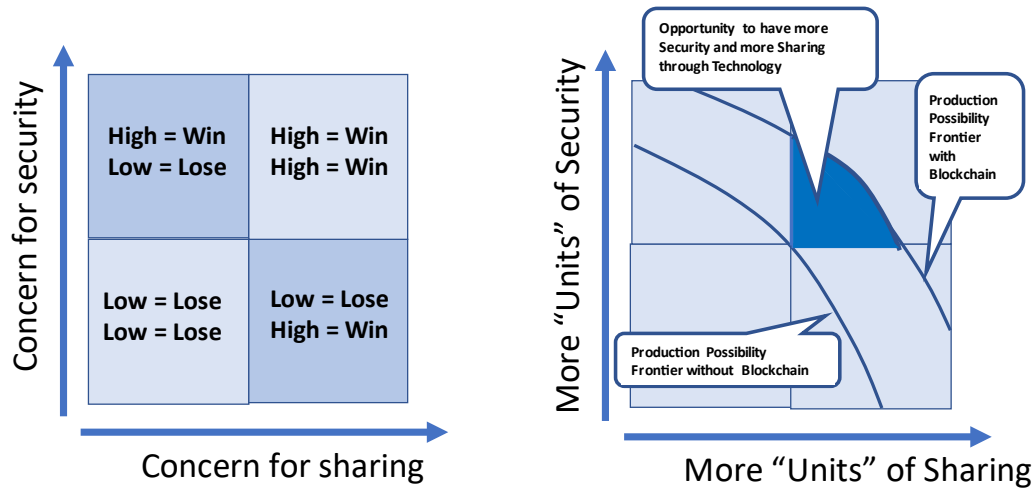


Figure 14 - Paths to value: implementation tracks and diffusion

A.3 Win/win and production possibility frontier

Gharajedaghi [29] (pp. 30-40) describes casting opposing tendencies in social systems as dimensional, a case where more of both tendencies creates the win/win scenario: <and> rather than <or>. Similarly in economics, the concept of a PPF [30] illustrates how, even when it seems that production of one thing results in less of another, i.e., <or>, more of both are feasible. This concept is due to the introduction of technology or other factors that improve the capacity of production. This shifts the frontier revealing an area under the curve that represents efficiency to be gained at given levels of production. **Error! Reference source not found.** Win/Win and PPF, applies these concepts to the employment of blockchain (and are generalizable to other technologies).

Taking an Ecosystem View of Industry Security Suggests Opportunity



Applied from: Gharajedaghi (2011) and Lipsey (1975)

Figure 15 - Win/win and PPF

The win/win and PPF models open possibilities in protecting data and sharing data that create ecosystem value as employment of blockchain influences risk assessments. This perspective is important to the synthesis of the case studies because the consideration of additional and/or reduced sources of risk differ when considering technology. Risk perceptions among the case study submissions are expected to vary based on industry. Discussion of the variations in perception and the variation in sources of risk present a means of discovering research worthy topics obscured by assumption.

A.4 Intermediation, disintermediation, classic make/buy

This section presents the idea of market mediation and the potential for traceability in creating new make/buy possibilities for supply chain participants.

For some use cases in supply chain traceability, blockchain technology may create mediation disequilibrium. For blockchain, the combined benefits of cooperation and decentralized resilience create a trust bond among participants which acts to eliminate the need for a central intermediary, perhaps an authoritative source, responsible and accountable for trust in the system, if one already exists. In the marketing domain, this would be described as a disintermediation effect, and thus, presents an environment prone to disruption, or movement through a cycle of intermediation, disintermediation and reintermediation [32]. The disruption occurs as intermediary roles (such as a service provider or broker) are made obsolete or changed significantly by actors attracted to or nudged out of the marketplace or industry.

For a discussion specific to the disintermediation portended by blockchain see Quiniou [32]. Quiniou reports the blockchain’s automation becomes a substitute form of mediation. He draws a

parallel between the disintermediation driven by the enabling technology of the internet, which is now followed by reintermediation. Those that employed the benefits of directly connecting members of communities (e.g., buyers and sellers, via the internet) to their advantage are positioned to grow. Exploiting the substituted automation becomes fertile ground for vertical integration to achieve further competitiveness or control (pp 52-54).

Likewise, in situations where no intermediaries play a role in the supply chain, one may be attracted, perhaps for the task of collecting data or supplying sensor readings. New intermediators whose constructions of control, attraction, and exchange of assets create new forms of sharing environments that in turn can require new skills, tools, and visibility needs. The space for these new products or services presents manufacturers with new scenarios for make-versus-buy strategic decisions.

A.5 Centralized and decentralized

Constructing a mental model of centralization and decentralization that aids in synthesizing across the supply chain traceability cases proves quite challenging. Nevertheless, perhaps an attempt can help focus on what is salient about using the designation of “decentralized,” which although problematic, does communicate a theme if not a well-defined characteristic. Three perspectives to demonstrate the situation are classical network, polycentricity, and equilibrium seeking.

A classical view of decentralization is simply the shape of a particular network that resembles (B) in **Error! Reference source not found.**, Visuals of Decentralization, with critique from Quiniou (p.9) at (B.1) observing that the absence of the circled node severely disables the network. An observation from Schneider adds that the pattern of nodes and edges in (C) more closely capture a “...maximally redundant and egalitarian distributed mesh” [33] (p.15). Further, Mukherjee describes the propagation of block transactions to the destination databases in a blockchain [41]. A network depiction of the propagation mechanism could look like (D) in the figure; however, the dynamics of network use are obscured in favor of the conceptual structure. More realistically, animations of block propagation are presented in DSN Bitcoin Monitoring [42].

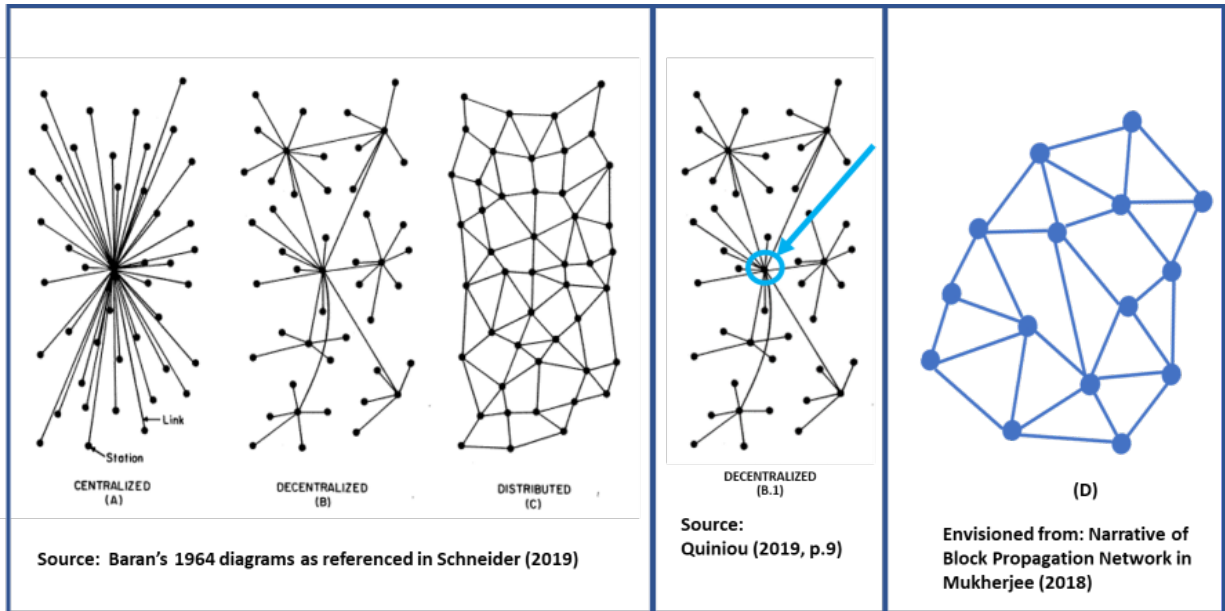


Figure 16 - Visuals of decentralization

Polycentricity is described by Ostrom [34] in the field of public administration as the naturally arising interaction of otherwise formally independent decision-making centers (p. 52). Rather than describe the pattern as decentralized, since it did not begin as centralized, polycentric became the modifier. “Multinucleated” was also considered (p. 50). This perspective highlights the semantic confines of describing a condition as something it is not. It also alludes to the possibility that emergent behavior across previously unrelated centers of activity can result in systems of interaction. These systems of interaction may be transient or more permanent in nature. The behaviors of entrepreneurship and supply chain building may have similar qualities in the private sector.

Equilibrium seeking is an attempt to label centralization and decentralization as being a dynamic activity among socio-technical systems such that for multiple aspects of a firm’s activities, conditions of operations move between (and/or simultaneously display) centralized and decentralized characteristics. Along these lines, Schneider’s research in decentralization [33] covers historical use of the term and provides many examples of accompanying human behavior and rationale for pursuit. Additionally, Gharajedaghi’s [29] systems-thinking approach to business architecture offers this summation:

“A three-dimensional architecture recognizes the need for centralization and decentralization, integration and differentiation, and interdependency and autonomy at the same time.” p. 304

A useful observation is that degrees in the presence or absence of centralization are pursued for a myriad of reasons. Decentralization appears more attractive when centralization becomes burdensome and vice versa. The pursuit is dynamic with perhaps pauses (equilibrium) when a performance level is satisfied.

For this attempt to surface topics of interest, it is perhaps a case study's characterization of why (or even if) traceability decentralization is considered to have business value. This contrasts with an attempt to align an organization's one or more operational aspects as being suitable for decentralization. A result may be that resilience to stressors could be a better way to talk about the expected value of decentralization, e.g., mitigation of risk.

This perspective is important to the synthesis of the case studies because aspects of blockchain tend to be described as decentralized. Additionally, the formation of supply chains can be said to be decentralized because, in a canonical free market, autonomous buyers and sellers decide to cooperate. The subject matter pertaining to a discussion of centralization and decentralization, i.e., the generalizable ideas, can quickly become entangling. In a comparison of what makes a blockchain decentralized and what makes the formation of supply chains decentralized, the ambiguity of the term begins to surface. The decentralized characteristics of blockchain are its distributed databases and its lack of a center of control since updates are made by consensus. In supply chain, as buyers and sellers connect to achieve profitable production levels their decisions are independent, and they operate within agreed-upon norms. With this brief comparison of ways to interpret decentralization, an invitation to explore the topic arises.

Appendix B—Submitted Case Studies**B.1 Case Study: Guardtime Federal, Inc.****Case Studies in Manufacturing Supply Chain Using Blockchain and Related Technologies***Observations from Industry***Author(s):** Sean Hanlen**Name of Organization:** Guardtime Federal, Inc.**DISCLAIMER:**

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendations or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose. Perspectives expressed in these case studies are views of the authors, and do not necessarily reflect the viewpoint of the National Institute of Standards and Technology.

Addressing Supply Chain Challenges:

Traceability in the supply chain requires integrity and trust in the digital data used throughout the supply chain process. A supply chain's digital data, no matter if the supply chain is physical, software, information, or some combination of these three types of supply chains, necessitates integrity protections at every step throughout the supply chain to ensure the resultant end item is authentic and free from unauthorized manipulations, disruptions, or modifications. Confidentiality and availability cybersecurity protections such as encryption and cloud-based architectures do not guarantee digital integrity of data in a federated supply chain system that crosses organizational and domain boundaries. Guardtime Federal's unique implementation of blockchain establishes a common anchor of trust throughout the supply chain to assure digital integrity and provenance thereby achieving traceability for physical, software, and information supply chains.

Approaches to deploying blockchain or related technologies for manufacturing supply chain traceability:

To assure digital integrity and provenance in the supply chain, Guardtime Federal's unique implementation of blockchain technology enables mathematically provable digital integrity and provenance solutions that rely only on secure hash functions, cryptographically linked to a public, widely witnessed, common anchor of trust known as the KSI® Calendar. By signing the fingerprint of digital data using KSI Signatures, digital information is immutably linked to the KSI Calendar and enables integrity verification of that data at any time in the future across any organizational or domain boundaries. KSI Signatures and participation in the KSI

Calendar do not require a supplier, manufacturer, or end user to share any of their data with Guardtime Federal. Data remains completely private from the KSI Calendar and in the control of the supplier, manufacturer, and end user. Only the supplier, manufacturer, and end user decide what information is shared with the rest of the supply chain.

Recognizing that the supply chain includes information from defense industry manufacturers that is proprietary, sensitive, or even classified data, Guardtime Federal developed a purpose-built security gateway appliance called a Black Lantern®. The Black Lantern gateway is designed to operate on the boundary of sensitive and classified networks enabling access to the KSI Calendar for signing and verifying KSI Signatures on classified networks. This gateway device establishes a common anchor of trust for the supply chain between unclassified and classified networks. The Black Lantern is designed with the required security protections in place for accreditation and operations on the boundary of sensitive or classified network domains. Like the KSI Calendar, a Black Lantern Appliance never receives any customer data as only the unclassified cryptographic hash of the data is passed through the Black Lantern gateway to the KSI Calendar.

Challenges to implementing blockchain or related technologies for manufacturing supply chain traceability:

Technological

Manufacturing supply chains make significant investments in their product lifecycle management (PLM), enterprise resource planning (ERP), and manufacturing execution system (MES) tools. Supply chains also integrate software development environments and repositories to integrate software into a manufactured end item. These tools and infrastructures in place today support the manufacturing supply chain's digital data during the end-to-end supply chain process. One challenge with traceability is how to integrate integrity and provenance technology into these existing tools and infrastructures and extend this same technology out to suppliers, subcontractors, and end users for full end-to-end traceability through the entire supply chain. Guardtime Federal is focused on reducing the challenge of last mile adoption by integrating integrity and provenance technology into a variety of dedicated applications, plug-ins to existing tools and systems, as well as software development kits that can be integrated into existing processes and infrastructure. This enables a common anchor of trust that can be used to verify integrity and provenance at each step in the supply chain resulting in end-to-end traceability.

Non-Technological

One of the non-technological challenges for implementing blockchain technologies as mechanism for traceability into the Defense Industry Base supply chain is the lack of integrity and provenance cybersecurity requirements on contract between government program offices and their contractors. While NIST Special Publication 800-161 emphasizes the provenance policies and practices as a control mechanism that enables supply chains to have "greater

traceability in [the] case of an adverse event and is critical for understanding and mitigating risks,” a recent Government Accountability Office (GAO) report (March 2021) found that the Department of Defense (DoD) “does not specifically address how acquisition programs should include cybersecurity requirements” on their contracts. While the Department of Defense has developed instructions, policies, and regulations to address supply chain risk management, the GAO report emphasizes that “contracting for cybersecurity is key.” Without establishing cybersecurity requirements as contractual acceptance criteria for DoD acquisition programs, digital integrity and provenance in the supply chain is program dependent or, in some cases, non-existent as the GAO discovered when they identified multiple contracts that did not have any cybersecurity requirements on contract. Without contractual cybersecurity requirements, supply chain traceability is negatively impacted by the lack of sufficient digital integrity and provenance controls that enable traceability throughout the supply chain.

Desired standards or guidelines to support the planning or implementation:

The DoD continues to make significant investment in its digital transformation and increasing reliance on digital information for timely and informed decisions made both on the battlefield and inside the Pentagon. From sensors to artificial intelligence to digital engineering, the DoD’s Data Strategy, released in September 2020, directs that “it is the responsibility of all DoD leaders to treat data as a weapon system and manage, secure, and use data for operational effect.” In order to achieve a data-centric organization, the Data Strategy identifies seven goals for the DoD related to data. Data trustworthiness as one of the seven goals is achieved when the “DoD data has protection, lineage, and pedigree metadata bound throughout its lifecycle.” In other words, trust in data is achieved when provenance and traceability can be irrefutably verified throughout its supply chain and operations lifecycle. While the agency’s data strategy was published well after Guardtime Federal started developing digital integrity and provenance solutions for traceability in the supply chain, DoD’s Data Strategy further validates and confirms that digital integrity and provenance are critical enablers for making data trustworthy through the entire supply chain lifecycle.

Lessons Learned:

Integrating digital integrity and provenance technology into established and existing supply chain processes and infrastructure may seem daunting at first. Guardtime Federal has integrated digital integrity and provenance technologies into supply chains, and one of our best practices from these integrations is to focus on those supply chain processes that are most at risk or require significant resources if a failed part or software vulnerability is identified. By focusing on those critical systems and processes, the prime manufacturer and their suppliers can implement traceability with accuracy at those steps in the supply chain process that are most at risk. Ultimately, a supply chain that has integrated integrity and provenance technologies into their processes for traceability can realize a return on their investment by reducing the labor cost required to identify affected systems, compliance and quality control verifications, and auditing if and when a defect, vulnerability, or counterfeit part is discovered

Lessons Learned:

in the supply chain.

Another best practice for supply chain traceability is signing the attestation of new or updated supply chain data as close to the source of that information as possible and verifying the integrity and provenance as close to use as possible. By signing and verifying information early and often, this enables a higher fidelity of traceability throughout the supply chain if a defective part or software vulnerability is discovered. Upon discovering a defect, Guardtime Federal's integrity and provenance technology can then be used to determine which step in the supply chain process introduced the defect or vulnerability and contribute to a root cause analysis for determining if the defect is a result of unauthorized modification or manipulation of digital information used to support the supply chain.

Referenced Materials:

NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations—

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf>

GAO Report on DoD Weapons Systems (March 2021)—<https://www.gao.gov/products/gao-21-179>

DoD Data Strategy (Sept 2020)—<https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>

B.2 Case Study: Perspectives from A Prime

Case Studies in Manufacturing Supply Chain Using Blockchain and Related Technologies

Observations from Industry

Author(s):

Anonymous

DISCLAIMER:

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendations or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose. Perspectives expressed in these case studies are views of the authors, and do not necessarily reflect the viewpoint of the National Institute of Standards and Technology.

Addressing Supply Chain Challenges:

Prime Contractor development networks and those of software suppliers and Department of Defense (DoD) customers provide critical information within unclassified networks. Although there are significant data integrity technologies in use, blockchain technologies offer an opportunity to layer on additional data integrity to further enhance existing measures. The challenge is employing an end-to-end data provenance technology from software suppliers through the supply chain to the end customer platform.

A prime contractor will continually strive to innovate the state-of-the-art technologies used in platforms, products, and services. Key attributes blockchain technologies offer over existing data integrity technologies are the immutable ledgers, and cryptographic strength in some solutions.

A contractor must invest in technology it anticipates the end customer will eventually need while differentiating itself from competitors by adopting advanced technology early. After evaluating several promising technologies which utilized blockchains, the prime contractor opted to partner with Guardtime Federal and their Keyless Signature Infrastructure (KSI®) for these reasons:

1. Guardtime Federal provides, as a service, mathematically provable, immutable digital integrity at high volume, focused on data privacy and cross-boundary verification, making it an optimal solution for defense, intelligence, and high-assurance infrastructures.
2. The prime contractor and Guardtime Federal worked for over 6 years in an ever-increasing level of implementation and integration of KSI® capability across multiple programs to assure integrity of software and information in delivered systems.

Addressing Supply Chain Challenges:

The prime contractor integrated KSI® into the software development process from the reception of supplier software deliverables, through the process referenced as Software Factory, to the transport mechanism of an air vehicle. Verification of the entire software delivery process for select aircraft data loads was demonstrated, with an intended follow-on focus of software operational flight programs (OFPs).

Approaches to deploying blockchain or related technologies for manufacturing supply chain traceability:**Technological**

Identifying a starting point for KSI® technology insertion into a network of networks is a formidable task considering the number of enterprise and program networks operated by the prime contractor. The first effort was to develop a comprehensive block diagram depicting how enterprise networks are connected, and then partnering with Guardtime Federal, a plan was developed to integrate KSI technologies in the prime's networks. Block diagrams were used to identify where supplier networks connected to the prime's enterprise network (on the left) and interfaced customer networks (on the right). Areas in the network diagram were identified for subsequent KSI® integrity verification. An attractive feature of KSI® technology is that each integration builds upon previous integrations. A chain of verification points as the data file transits through networks establishes a chain of custody called data provenance.

Next, for initial deployment was to identify which data files or types were most critical needing additional data integrity. Various types of mission data files were evaluated and targeted for KSI® technology insertion. Questions posed included: What are the number of data files? Should all data files of a type be signed or select specific data files to apply KSI® signatures? The data files, whether unclassified, but especially if classified, must remain within data network. KSI® uses only hash-function cryptography, allowing verification to rely only on the security of hash-functions and the availability of a public ledger (commonly referred to as a blockchain) and not the data file itself. The program data is never in the ledger, just a hash of the data. Using Guardtime Federal's unique blockchain technology, the contractor's data remains within the prime's network and is key to why KSI® blockchain technology is a best fit for DoD applications.

Additional considerations were ease of effort of KSI® integration, hours required to integrate, and to be non-intrusive to existing development efforts. Even with program and subject matter expert support for integration, normal production operations cannot be adversely affected. The KSI® application layer (KAL) tools the prime contractor developed using Guardtime Federal SDKs had to be flexible to handle multiple use cases. The KAL tools were created to run in the application layer with limited human interaction and are deployable to all networks, not

Approaches to deploying blockchain or related technologies for manufacturing supply chain traceability:

being limited to a single platform or program. The scalability and reusability of KAL tools is precisely the information protection technology the DoD desires.

KSI® technology is intended to provide software integrity during development by automatically signing software source code during development. Those signatures can then be used to validate the data integrity during software build, integration, and release. Additionally, this technology is accessible to software suppliers so that they can digitally sign software before it is delivered to the prime contractor.

Non-Technological

The prime contractor identified software suppliers of significant data files and designed trials with these suppliers, to use KSI® technology to sign their data prior to delivery to the prime contractor. The suppliers willing to conduct the trials provided valuable feedback which matures the Guardtime Federal SDKs and verifies the tools handle all conditions and architecture types.

An important component for deploying KSI® technology was cultivating relationships between prime contractor cyber architects, developers, program managers, Guardtime Federal liaisons, and customer project managers. These relationships established trust in each other's work, and instilled appreciation for each other's constraints so we could be flexible when required to achieve the most desirable outcome despite constraints.

Challenges to implementing blockchain or related technologies for manufacturing supply chain traceability:**Technological**

There were no technological issues which couldn't be overcome by the ingenuity and familiarity of network architecture by the prime contractor cyber architects. Some solutions were deemed not desirable because they would require additional hardware or more budget allocated to integrate prime contractor's tools into the system, but all technical challenges encountered had at least one viable solution proposed.

Integration of new technologies into a network infrastructure can be a challenge when the technology is unfamiliar to those responsible for security and IT. The prime contractor planned to install a Guardtime Federal-developed hardware appliance called a Black Lantern onto the prime contractor corporate network. Black Lanterns are a purpose-built gateway appliance that allows protected or even classified networks to sign and verify data using the KSI® Calendar as a common trust anchor. Although physically connected between two networks, Black Lanterns only move cryptographic hash values of the data. To integrate the

Challenges to implementing blockchain or related technologies for manufacturing supply chain traceability:

Black Lanterns into the prime contractor network, several meetings were held with prime contractor security and IT SMEs who initially characterized the Black Lantern as a “cross-domain solution” (CDS) since it connects two networks at different classification levels. The prime contractor and Guardtime Federal team developed a concept of operations document for the using the KSI® technology in a classified environment that identified use cases for the technology and the technical details of Black Lantern operations. By documenting the capabilities and operations of the Black Lantern, the concept of operations document served as a source document for terminology and technical details for all subject matter experts to integrate the Black Lantern and KSI® technology into the prime contractor network.

Non-Technological

Guardtime Federal-developed products and prime contractor-developed products undergo free and open-source software (FOSS) reviews. A list of all included FOSS dependencies is contained in software product deliveries. The lists may be trivial to compile, but FOSS reviews can be lengthy and impact development or integration timelines. Authority to operate (ATO) permissions for hardware and software to operate on a network are required by prime contractor network administrators and program security representatives of any program network a contractor intends to incorporate KSI®. Each program has its own set of security considerations and personnel. It is possible one network owner may grant an ATO, but another network owner may reject the ATO request.

Complex programs with separate integrated product teams (IPT) make deployment of KSI® tools and technologies complex as well. Prime Contractor KSI® project managers must establish relationships with each IPT and understand their production schedules and staffing, how their cyber architecture fits within the larger air system, and what budget complexities exist within each IPT to incorporate KSI® technology even when all other roadblocks are eliminated.

A challenge for software suppliers may be that they don’t know which blockchain technology to adopt for their various customers. The prime contractor software suppliers were informed of the prime contractor-Guardtime Federal partnership and intent for KSI®-signed software deliveries at a supplier conference in 2020. KSI® technology development at the prime contractor was aligned with Sustainment imperatives for future growth. All programs and platforms have access to KSI® technology and customer outreach is informing the DoD of the benefits of the prime contractor-Guardtime Federal solutions available today.

Military commanders at all levels rely on data from trusted sources and at various classification levels as the foundation for informed and actionable decisions. Data exfiltration and, even more so, data manipulation are a threat to undermine the trust of this foundational data. When implemented to protect the data privacy and support development and operations in a multi-level security environment, blockchain and distributed ledger technologies are a

Challenges to implementing blockchain or related technologies for manufacturing supply chain traceability:

viable solution that support not only the traceability of the manufacturing supply chain but also the information supply chain for that weapons system through operations. By integrating the integrity and provenance technologies as intrinsic elements of the weapon system from development to operations, the data provided by this weapon system becomes a trusted source with verified integrity and provenance for decisionmakers at all levels.

B.3 Case Study: Sky Republic**Case Studies in Manufacturing Supply Chain Using Blockchain and Related Technologies***Observations from Industry***Author(s):**

Chris Fabre, Sky Republic

Arnaud Brolly, *Société Internationale de Télécommunications Aéronautiques (SITA)*

Pierre-Yves Benain, *SITA*

Name of Organization: Sky Republic

DISCLAIMER:

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendations or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose. Perspectives expressed in these case studies are views of the authors, and do not necessarily reflect the viewpoint of the National Institute of Standards and Technology.

Addressing Supply Chain Challenges:

This submission deals with case studies related to 4 Proof of Concepts (PoCs) which were conducted by Société Internationale de Télécommunications Aéronautiques (SITA), consortium leader and notary, and Sky Republic, platform & application provider, in 2020

- **Aircraft Maintenance Repair and Overhaul (MRO) Track & Trace:** SITA (Notary), Cathay Pacific, Haeco, Bolore Logistics, and Safran participated.
- **Aircraft MRO Digital Passport:** SITA (Notary), Safran, Willis Lease, and Fly Docs participated.
- **Air Cargo Shipment Electronic Data Interchange (EDI)/ Internet of Things (IoT) Tracking:** SITA (Notary), Singapore Airlines, Safran, Bollore Logistics, SATS, and WFS participated.
- **Air Cargo ULD Interlining:** SITA (Notary), ULD Care, Cathay Pacific, Emirates, Lufthansa, and Air New Zealand participated.

For each, participants proceeded in the following way:

1. identification of business benefits to be demonstrated compared to actual systems
2. definition of the prototype to be experimented with and relevant test cases:
 - a. standards to be implemented
 - b. participant's systems to be integrated or simulated
 - c. definition of the supply chain processes to be automated:
 - i. events to be exchanged: EDI or custom

Addressing Supply Chain Challenges:

- ii.records to be shared: Order, Invoice, AirWay bill, etc. in pdf or doc formats
 - iii.Sky Apps (~dApps) to be used: participant orchestration process to be performed through a WebApp or API integration
 - iv.Sky Contracts (~Smart Contracts): supply chain process choreography including alerts, errors, or SLA management to be performed and monitored.
3. development, integration, and set up of the prototypes by SITA and Sky Republic
 4. experimentation with the distributed prototypes by current supply chain actors of each participant company operating them in parallel of actual systems for selected repairs, parts, shipments, and interlinings.
 5. post-mortem

As of today, participants with Aircraft MRO PoCs are discussing the productization of the prototypes and participants of Air Cargo PoCs expressed their willingness to do the same. All use cases aim at demonstrating that a blockchain-based platform can provide end-to-end automation, visibility, and transparency for supply chains “faster, better, cheaper” than legacy technologies [(EDI)and Application Programming Interface (API)] and infrastructures (messaging networks and control towers).

Beyond these common goals and the willingness to co-innovate with business partners, each participant expressed specific business pains to be addressed depending on their role in the supply chain.

Aircraft Maintenance Repair and Overhaul (MRO) Track & Trace:

- Airline: detection and mitigation of disruptions (delays, errors, ...), optimization of repair turn-around to decrease inventory levels.
- MRO: digitization/automation of processes to increase operational efficiencies and better monitoring of subcontractor service level agreements (SLAs) to ultimately improve service-level to airlines.
- Logistics: better visibility in future demand to optimize resources and workforce planning.
- Original Equipment Manufacturer (OEM): retrieval of operational and configuration data related to the parts to accelerate repairs.

Aircraft MRO Digital Passport: record key data and documents of a part related to manufacturing, usage, maintenance, and change of ownership operations.

Addressing Supply Chain Challenges:

- Airline, OEM: protect part value by ensuring proper level of documentation, accelerate compliance & audit tasks related to safety regulations and leasing activities, share operational data and records with partners to maintain better and faster aircrafts.
- Lesser: decrease cost and time necessary to manage and transact assets by reducing manual tasks and automating record discovery. Increase revenue per asset by increasing availability.
- All: improve industry safety by blacklisting scrapped parts, potentially detect counterfeit and structural defects.

Air Cargo Shipment:

- Shipper: detect and mitigate disruptions earlier through correlation of EDI and IoT events to decrease financial impact and provide accurate estimated times of arrival (ETAs) to customers.
- Logistics: digitization/automation of processes to increase operational efficiencies and better monitoring of subcontractor SLAs to ultimately improve service-level to shippers.
- Ground-handler: better visibility in future demand to optimize resources and workforce planning, support more advanced digital processes to win more business.

Air Cargo Unit Load Devices (ULDs) interlining: open currently centralized and aging EDI platform used today exclusively for interlining between airlines:

- implement digital signatures to be able to onboard non-airlines entities (logistics, road/sea/rail carriers, etc.). “Trust” is today provided by a multilateral agreement restricted to airlines and the network operator.
- distribute comprehensive data for participants to optimize their processes (container routing and leasing for example).
- decentralize reconciliation, especially of demurrage computation and settlement, to provide transparency to network participants.

Approaches to deploying blockchain or related technologies for manufacturing supply chain traceability:**Technological****Demonstrate the value and feasibility of upgrading current supply chain processes and systems.**

Supply chains do not need commonly marketed blockchain characteristics like immutability or decentralization as such. In fact, nobody needs a blockchain, but most can benefit from the end-to-end digital consensus, automation, visibility, transparency, and agility that blockchain-based applications can provide “better faster cheaper” to supply chains.

Quickly after securing participants on the maturity of the underlying technology, we focused on designing the right processes and applications that would make a difference for participants’ businesses without inducing too much technical disruption.

Consider the blockchain platform as the only transacting system instead of a “recording layer.”

We started the first PoC by considering the blockchain platform as an additional layer to existing transactional systems and designed a “shadow” process that would be fueled by reporting business events from existing systems. First, the reporting events were usually simpler than the original events in terms of data content which limited the value of an end-to-end system. Second, we used the existing process constrained by the capabilities of existing systems. By construction, this approach does not unleash the true benefits of leveraging end-to-end data and events to upgrade the business process.

In the three other PoCs, we designed the ideal process right away reusing parts that were fine in current systems and fixing the others. We systematically recorded any piece of data or events in the Sky Contract to build a comprehensive single source of truth. This approach allowed to automate many advanced capabilities such as SLA computation/settlement or disruption recovery which are unfeasible when only shadowing existing systems (how to resync participant’s ERP systems when somebody realizes that a shipment was sent to the wrong address for example).

Non-Technological

Team spirit with a member in charge of governance.

The right environment for co-innovation was set up. SITA volunteered to project manage the initiatives, induced a consortium spirit, and organized workshops where participants from all companies could brainstorm and work together face-to-face.

Challenges to implementing blockchain or related technologies for manufacturing supply chain traceability:**Technological****Current process discovery**

Interestingly, it took some time and effort for the different entities to define accurately what is the current process in place (systems involved, format used, manual tasks, etc.)

EDI standard completeness

EDI standards (Spec 2000 for MRO, CargoXml for Air Cargo) cover the most frequently digitized tasks and records in business processes (order, invoice, etc.). On average, we found a standardized format for 70% of the events required to automate an end-to-end supply chain process.

We also noticed some weaknesses in:

- time zone management for dates and times which were problematic to monitor cross-continental processes which are common in Aerospace and Air Cargo
- universal identifier adoption where blockchain allows to manage coexistence between old but still in use non unique identifiers and newly defined unique identifiers

Confidentiality management

It is easy to automate a process end-to-end where permissioned participants can see everything.

The correct implementation of appropriate confidentiality rules (who can see prices of an order or the value of an SLA for example) is a key driver of the design of smart contracts and can be tricky.

Non-Technological**Stakeholder onboarding and management**

Numerous persons from numerous entities must be convinced, onboarded, and synchronized from the decision-making to the funding or the operation of a blockchain solution.

Blockchain is a team sport, and a team needs a coach.

Developing a Supply Chain Risk Management Strategy:

Risk management includes business and IT considerations.

Except for the fourth PoC where trust issues were easy to solve with classical digital signatures, our projects did not involve a structural change in the current supply chain ecosystem or procedures.

However, most drivers as explained above dealt with reducing supply chain risks by implementing unified processes on a new platform.

From a cryptography perspective, we used a technology compliant with Air Transport Association (ATA) Spec 42, which is recommended for all digital events and records in aerospace and air transportation.

Standards used for planning and implementation:

- ATA Spec 2000 which proposes format standards for MRO events and records
- International Air Transport Association (IATA) CargoXml which proposes format standards for Air Cargo events and records

We specified custom events in XML (eXtended Markup Language) or JSON (JavaScript Object Notation).

To reference supply chain organizations and locations, we used GS1, SITA, or IATA identifiers.

For specifying supply chain processes and Sky Contracts behaviors, we slightly expanded OMG BPMN (Business Process Model and Notation) choreographies. For Sky Contracts data repositories, we used UML (Unified Modeling Language).

For data exchanges (events, ledgers, etc.) between nodes and applications, we used representational state transfer application programming interfaces (REST APIs) or gRPC (gRPC Remote Procedure Calls)/TLS (Transport Layer Security).

Desired standards or guidelines to support the planning or implementation:

EDI standards could be extended with missing events to cover:

- good and bad paths in supply chain processes.
- IoT integration

Lessons Learned:

The main challenges are:

- form and manage a minimal group of motivated and sufficiently representative participants.
- upgrade existing processes to unleash real business benefits while ensuring confidentiality and maximal standard compliance.

B.4 Case Study: Manufacturing Supply Chain Traceability from “Field to Fork”**Case Studies in Manufacturing Supply Chain Using Blockchain and Related Technologies***Observations from Industry***Author(s):** *Anonymous***Name of Organization:** *Anonymous***DISCLAIMER:**

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendations or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose. Perspectives expressed in these case studies are views of the authors, and do not necessarily reflect the viewpoint of the National Institute of Standards and Technology.

Addressing Supply Chain Challenges:

The opportunity: Improve the yield of a raw material as it is transformed through the supply chain from field to fork.

The problem: A packaged consumer goods product was designed to have no gluten in the ingredients. However, the supply chain of the raw materials was not designed to ensure 100% purity of the raw material. Thus, the raw material needed to be processed and filtered to a 100% purity level at the manufacturing site. This purification step resulted in losses up to 50% of the raw material. The value of the raw material waste was in the 10's of millions of dollars.

The current purification process had no visibility to the attributes and manufacturability of the incoming ingredients. This forced the plant to run generic processing conditions there were not optimal for the yield of the plant. Having full visibility allows for the plant to develop optimal recipes (high yield) for the conversion of these raw materials into finished product efficiently.

Data needed to be captured along the supply chain both internal to the company and the external partners along the way from field to manufacturer. Thus, a real-time tracking system was needed.

The problem: The raw material was stored in up to 1500 silos and then sent to the purification process. Once the characteristics of the raw material were captured, a system to optimize the “blend” and/or optimized recipe for this blend was needed to maximize yield.

The problem: A second layer of defense was needed to release the purified material into a secondary manufacturing process. A positive release methodology was needed to ensure the integrity of the chain of custody of the material as it moved throughout the supply chain. This would consist of not releasing the product from the first stage until it had passed all of its quality and regulatory measures. Then and only then would it be dispatched to the second stage.

Approaches to deploying blockchain or related technologies for manufacturing supply chain traceability:**Technological****Raw Material Track and Trace:**

Looked at blockchain but not far enough along or broad enough use at the time, but many of the concepts were fleshed out. First, we understood that we needed a material ledger: the book of records of the characteristics, chain of custody, and transformation of the raw material from origin to end. What is a little unique is that the raw material is transformed as it passes from field to manufacturing and not only the original state, but the transformed state and its relationship must be maintained to be able to perform a track-and-trace. Again, the goal was to be able to trace backwards from the transformed material all the way back to its parents and origin even though blending and mixing that was happening throughout the flow.

The material ledger was developed with a graph data base to capture the relationships of the material flow.

Positive Release:

A material ledger was developed for this “finished” product as well since it had much of the same requirements as the original raw material and need a relationship to its source for full trace.

Manual Data Capture:

Some of the data was not available via instruments or networked devices. Tests on the raw material both in the field and at the manufacturing were manually performed. Data collection screens in either mobile format or fixed computer terminals were developed for manual entry of data, tests, etc.

Connecting to Existing Data sources:

There was some data that was flowing to programmable logic controllers (PLC’s) (i.e., bin measurements, weight belts conveyors, etc.) that needed to be captured as well as rail car and truck receiving information that was being collected in a SQL database. This information needed to be contextualized in the material ledger.

Bin Management and Blend Optimization:

A “smart” system was needed to take the data about the raw material in its 1,500 different locations and provide guidance on how to process optimally. An algorithm was developed to understand the best possible combinations of lots that would create the optimal yield with minimal waste.

Approaches to deploying blockchain or related technologies for manufacturing supply chain traceability:**Non-Technological**

Understanding the existing operation process and developing the new one that would meet the people where they were at and ensure their compliance. This project did not wipe the slate clean and start over; it was trying to use whatever the ecosystem had and only put in elements that were critical or gaps that needed to be invested in to achieve success.

The existing process from field to fork was not intimately understood by any one person. It took about 6 months of study, interview, field trips, etc. to map out the current process, sources of data, gaps in data or gaps in accurate information in order to be able to design the next generation system that would be able to be fully capable of meeting the track-and-trace requirements.

We leveraged a kaizen and value stream mapping process to vet this.

Challenges to implementing blockchain or related technologies for manufacturing supply chain traceability:**Technological**

1. Understanding the relationships in the data that was being collected. This was not a linear process flow. Data was collected by different organizations with different events and timestamps. Developing the semantic model that was able to contextualize the overall flow was challenging but resulted in a breakthrough technical approach to leverage Graph Database technology.
2. Developing manual data entry capability that would align with the contextualization needed and be as simple for a technician as writing data down on a piece of paper.
3. Developing the visualization of the flow in a trace approach. We ended up using Sankey diagrams for this.
4. Understanding the flow of mixtures and what “might” be in the stream and how to analyze this in a track-and-trace utility. This means both a 1-to-many, many-to-1 and many-to-many relationships were possible in this process flow.
5. Designing a system that would work for all material flow and track /trace, not just build for purpose of this project. A generic material ledger, Sankey visualizations and database were created so that technology could be deployed to other use cases (and has been since).

Challenges to implementing blockchain or related technologies for manufacturing supply chain traceability:

6. Visualizing bin management (1,500 silos) and executing an algorithm to provide guidance on optimal selection to blend for high yield and low waste.

Non-Technological

1. Manual entry as good as paper and not slowing down the decisions by digital intervention, but rather increasing the reliability of manual collected data.
 - a. Working with the workers to help design a simple and useable UX adoption was achieved. Adding in validation and preloading as much information as possible so that they only had to enter the specific test data that was new, greatly improved accuracy and speed.

Lessons Learned :

Need to meet people and technology where they are at. Add only what is needed and simplify as much as possible. At first glance, this opportunity would look to be an industrial internet of things (IIoT) project with lots of new sensors and technology to enable this. We started with chalkboards as data collection and upgraded to a manual entry screen on a tablet. Still no sensors. Retrofitting a massive legacy facility would cost millions and not be as reliable as people. We did a pilot using instrumentation instead of people for a specific measurement and found that people were more accurate and less expensive, more adaptable than instrumentation.

Lesson learned... truly behave like it is a balance of people, process, and technology. We tend to give lip service to that in real life and just work on technology as the solution.

The project over-delivered in value creation in unexpected areas. Having transparency and visibility along the supply chain, the quality of the raw materials and thus the yield increased. The supplier saw the manufacturability of the provided raw materials increase when they delivered a better material. They became a preferred supplier and got more business because their raw material ran better through the plant. They had no idea what happened to their material once it was sold. Now they do and are connected in the process. Everybody wins. Twice the anticipated value was achieved because of this.

The solution was not built for purpose, but for a generic case: track-and-trace. It has been deployed to additional streams with similar results. The lesson learned is not to design just for purpose, but generalize, if possible, so that it can be used in broader span and additional opportunities. Be available to be used for the problem you have not had yet.

Flexibility: semantics/taxonomies need to be able to be reworked and changed as the business, relationships, and physical assets change. If the system you create is static, the rework cost

will be staggering and/or the system will be irrelevant rather quickly. Creating a system that can reconfigure quickly, remodel, etc. is critical in this rapidly changing world.

B.5 Case Study: DUST Identity

Case Studies in Manufacturing Supply Chain Using Blockchain and Related Technologies

Observations from Industry

Author(s): *Anonymous*

Name of Organization: *DUST Identity*

DISCLAIMER:

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendations or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose. Perspectives expressed in these case studies are views of the authors, and do not necessarily reflect the viewpoint of the National Institute of Standards and Technology.

Addressing Supply Chain Challenges:

Manufacturer X is a Fortune 500 multinational-supplier that participates in several industries including telecom, electronics, and automotive. They have built a reputation for high quality products and cutting-edge manufacturing processes. Manufacturer X currently lacks the ability to securely verify components at scale as well as trace those parts as they move through the supply chain. Manufacturer X has encountered an increasing number of non-genuine and non-compliant parts being sold under their brand name. Even authentic parts are rerouted by third parties to take advantage of regional price differences (i.e., product diversion). This has led to a multitude of negative effects - impact on brand perception, loss of business opportunities, regulatory scrutiny, and additional costs in managing failures from non-genuine products. As a response,

Manufacturer X determined that they required a traceability solution that can enable an economical and scalable capability that is secured to ensure continued trust. This would allow participating organizations within the value chain to verify products and access pedigree and provenance data for products across their full lifecycle.

The leadership team of Manufacturer X selected blockchain to securely record and share item-level provenance data with entities in their supply chain. Furthermore, they determined that in order to truly trust the data on their blockchain they would need to immutably connect part of the data to individual parts through the use of a unique and unclonable physical anchor. This would provide data integrity in conjunction with hardware integrity and ensure that the part in someone's hand matched the one referenced in the blockchain. After performing vendor selection, Manufacturer X chose DUST Identity to support their initiatives on integrating blockchain into their manufacturing lines across multiple business units. DUST's unique compatibility with various form factors and its ability to meet the security and cost considerations in the context of large-scale deployment and use made DUST Identity an ideal partner for this engagement.

Addressing Supply Chain Challenges:

The Diamond Unclonable Security Tag (DUST) binds physical parts to their digital records using a persistent identifier composed of microscopic diamond crystals. The form-factor of the persistent identifier, the DUST Tag, is extremely flexible and allows for the same technology to be used consistently across the customer's diverse product lines and through all logistics hierarchies. Each time a user physically authenticates a part or digitally adds or edits information about the part (e.g., certification data, service history), that event creates a unique ledger transaction that can be recorded on both a distributed ledger and additional management and orchestration services such as those included in the DUST Solution. Replication of key data to a blockchain and the DUST ledger serves to reinforce and validate transaction data. Authorized parties can access the blockchain and DUST ledger records to reconcile the data and validate the integrity of the part.

Approaches to deploying blockchain or related technologies for manufacturing supply chain traceability:**Technological**

The technical approach for this effort was to store each product's Digital Thread in DUST's cloud-based application and on Manufacturer X's blockchain at the same time. Transactions (part verifications, metadata, etc.) would be synchronized via a Representational State Transfer (REST) API integration. When data entered the application, through a web interface or REST API integration, a real-time transaction would be sent to Manufacturer X's blockchain.

To perform the integration, Manufacturer X developed an application using Hyperledger Fabric and exposed read/write access to this blockchain via a REST API with supporting credentials. DUST Identity delivered cryptographic hashes of the data payloads to the Manufacturer X-owned blockchain triggered by physical authentication events or editing digital data within the DUST System. These triggers from DUST were sent to an auto-scaling queue-worker microservice to handle large volumes of data uploads to the Hyperledger channel to support scalability, throughput, and reliability. In future development, the team plans to use Hyperledger Fabric's record to be the primary data store, develop smart contracts for enforcing rules and policies around data access, and partner more closely in the blockchain with Manufacturer X (e.g., hosted endorsing peer nodes).

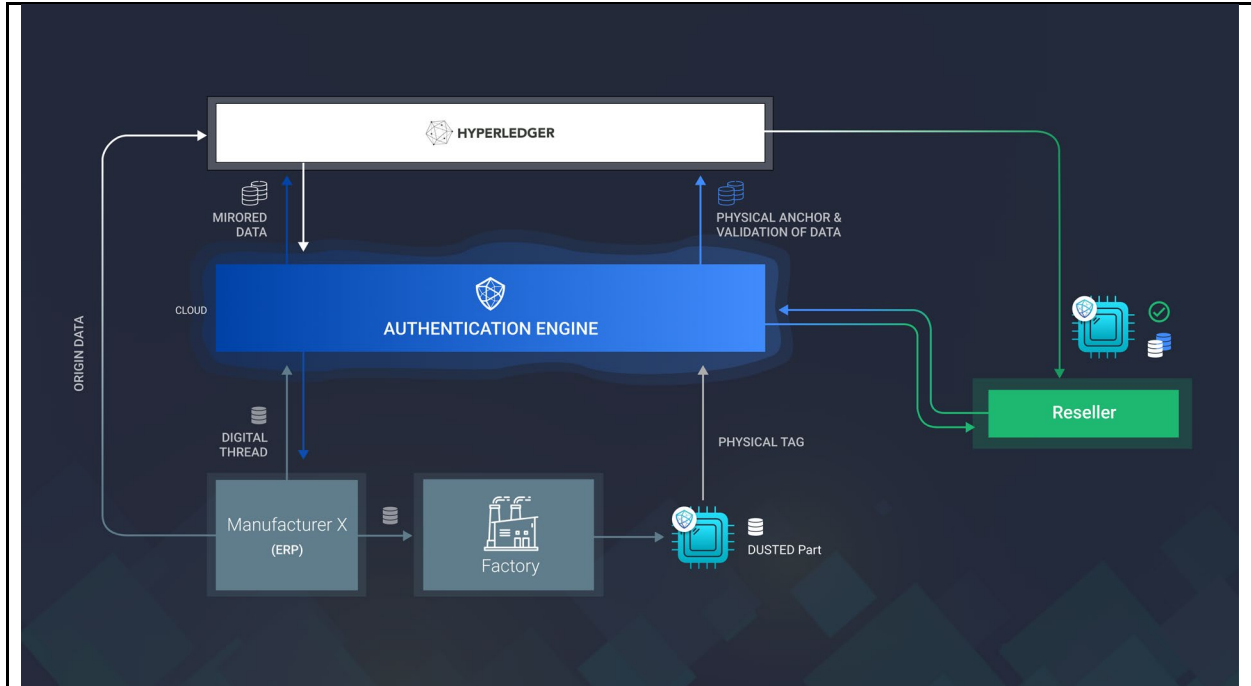


Figure 17 - DUST Identity technical approach

Challenges to implementing blockchain or related technologies for manufacturing supply chain traceability:

Technological

One key technological challenge related to scalability. To solve issues of scaling, DUST Identity developed a multi-threaded implementation that was sufficient for the volume of data at the time of implementation, then re-engineered it to use a queue-worker architecture which improved scalability, throughput, and reliability for the system at larger volumes.

Non-Technological

The main non-technological challenge related to communicating workflows between DUST Identity and Manufacturer X. As is often the case with system integration, the architecture needed several iterations for the parties to fully understand the dataflows. Since Manufacturer X is a global supplier of goods this required communication across multiple geographies, time zones and language barriers.

Developing a Supply Chain Risk Management Strategy:

In the implementation process, Manufacturer X and DUST Identity incorporated a number of standards that were important to the customer as well as those that are standard practice for DUST:

- NIST 800-171, which defines standards for Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. These standards help define the minimum standards for non-federal organizations interacting with and storing federal information. While the data stored was not federal information, DUST Identity utilized these standards as a guide to secure information and system access. As an example, to ensure the highest level of security possible, all sensitive identifiers were hashed before being broadcast to the blockchain. This standard is very important to DUST Identity and forms the basis by which all customer data is handled to ensure the highest level of cybersecurity.
- The *ENISA Guidelines for Securing the Internet of Things* [43] study defines guidelines for securing the supply chain for IoT. The study was developed to help IoT manufacturers, developers, integrators, and all stakeholders that are involved in the supply chain of IoT make better security decisions when building, deploying, or assessing IoT technologies. DUST Identity utilized these standards when considering IT infrastructure, data protection, and interface security.
- The METI Cyber/Physical Security Framework (CPSF) defines processes for maintaining risk management systems within and between organizations. Further, it defines a framework utilized by DUST Identity for correct transcription of data between physical spaces and digital spaces.

Standards used for planning and implementation:

DUST used several standards in implementation of the blockchain technology. The primary source utilized was Hyperledger Fabric, an open-source community of tools and libraries for enterprise-grade blockchain deployments that is hosted by The Linux Foundation. Its modular and versatile design satisfies a broad range of industry use cases and allows components, such as consensus and membership services, to be plug-and-play. Hyperledger Fabric offers a unique approach to consensus that enables performance at scale while preserving privacy. This emphasis on privacy makes it an ideal standard for manufacturing environments that are highly sensitive to external interference.

When building the API integrations, DUST Identity utilized the OpenAPI Specification (OAS) which defines a standard, programming language-agnostic interface description for HTTP APIs. It allows both humans and computers to discover and understand the capabilities of a service without requiring access to source code, additional documentation, or inspection of

network traffic.

Existing standards or guidelines that were not used in the planning or implementation, but could have been helpful:

While there are a number of standards for supply chain risk management and developing standards for blockchain, there is still a need for better standards relating to part integrity, ensuring trust, and having clarity about the tradeoffs between security, risk, and usability.

Two standards that were not used in this implementation but could be helpful in the future are:

- IEEE 2144.1-2020 is a standard for blockchain-based IoT Data Management. It identifies the common building blocks of the framework for a blockchain enabled IoT data lifecycle including data acquisition, processing, storage, analyzing, usage/exchange and obsolescence, and the interactions among these building blocks.
- The IEEE P3217 standard defines an application programming interface (API) collection and data transmission format between the chain layer and the application layer in a blockchain system. It standardizes the string, encoding, and request response format of the API. The standard specifies intrusion prevention, malicious code prevention, trusted execution of programs, data integrity, data confidentiality, access control, and management systems

Desired standards or guidelines to support the planning or implementation:

The lack of defined standards related to the interoperability between different ledger technologies led to a variety of challenges for the implementation team. For instance, the Hyperledger Fabric used in this implementation has fundamentally different definitions of permissions than other technologies such as R3's Corda. Standards that clearly define consensus on how certain blockchain technologies interact will be a critical need going forward.

Lessons Learned:

Participation in the blockchain is a growing strategic priority across supply chain leaders and innovators, many of whom are also exploring how to link that blockchain data securely to the parts themselves. Based on DUST Identity's partnership with Manufacturer X, these are the most important practices to adopt for any organization engaging in a blockchain implementation:

Lessons Learned:

1. Whenever entering a project with a large organization that has multiple needs that may be different across different business units, it is highly advised to ensure there is opportunity for all business units to collaborate on the architecture and specifications of the intended implementation. From technical parameters such as data flows to business goals and downstream value proposition, care should be taken to ensure all parties are aligned.
2. In order to establish supply chain traceability with blockchain, customers require a physical anchor to trust the integrity of the digital data on the blockchain. To meet the scalability and security needs of a blockchain for manufacturing environments, best practices dictate that this identification technology must possess a large serialization space of unclonable identifiers. Additionally, tagging technology must be widely distributable, suitable across form factors, and able to support multiple security environments.
3. It is critical that organizations assess technologies for feasibility at scale before starting PoC or pilot efforts. The key criteria to evaluate before starting any effort is a solution's ability to meet the demands of a production environment on scalability, security, cost, and usability. From the start, Manufacturer X was focused on rolling out its blockchain solution at scale, which led to a successful effort. We have a responsibility as a community to encourage organizations to focus on the long run when considering technologies and pilots and would urge everyone to increase their efforts in that regard.

Additional Comments:

In order to trust parts at scale, manufacturers require both Data Integrity and Hardware Integrity. The two elements are indelibly linked in that a trusted system cannot have one without the other.

Data integrity requires a secure, immutable source of truth to send and receive data between supply chain partners inside and outside of an organization. This is being addressed today through technologies like Blockchain. To ensure that data in those ledgers is associated with the correct part, supply chain organizations must reference a part's persistent identifier. This is where data integrity intersects with hardware integrity.

Hardware integrity requires knowledge of a product's pedigree (e.g., point(s) of origin, manufacturer certifications) and provenance (i.e., chain of custody). Pedigree and provenance are two elements of the digital thread that are stored in a blockchain, with the persistent identifier acting as the key that unlocks that digital thread. Without this key it is impossible to associate data with specific products meaning manufacturers are both unable to guarantee veracity of the supply chain and unable to prevent the manipulation of the production information. This presents a significant risk to the manufacturer and means that blockchain

Additional Comments:

alone is not enough to protect their products.

Having both data integrity and hardware integrity is impossible with products that rely on general part IDs, batch level IDs, or serial IDs that can be easily copied. This is because there is no simple, quick, or secure method to access a part's persistent identifier. This is also true for electronics that utilize software-based identifiers since it is difficult to access the part's persistent identifier without assembly into another product, as with microelectronics, or plugging the product in and potentially putting a platform at risk. A unique and unclonable physical anchor is the only method to trust that the product in your hand is genuine and has not been tampered with.

Engagement Results: Through the integrated system of Blockchain and DUST, the customer was able to maintain an ongoing, verifiable record of all activity associated with high-value components and end products. Going forward, Manufacturer X plans to further integrate this system with their manufacturing processes, expand to more product lines, and deploy the Blockchain/DUST solution to their reseller network.

Appendix C—Case Study Individual Analysis Notes

This appendix contains notes for each case within the context of the analysis method employing mental models. It is the as-is record of systematically considering each case study from the viewpoints of the mental models and lenses. See [Section 6](#) for the narratives that resulted from this raw data. See [Section 7](#) for the themes that surfaced from the narratives in combination with other sources of information. And see [Appendix B](#) for additional descriptions of the mental models and lenses employed. [Section 7.2](#) contains a cross reference table reflecting the aggregation of material into themes to satisfy a primary purpose of this paper.

C.1 Field to Fork

- Company / Business Drivers
 - Large agri-business organization wants to meet demand for GF (Gluten Free) products and branding them as such
 - Reduce cross-contamination waste and produce ultra-high purity cereal products (GF + branding)
- Supply Chain Risk Management
 - Risk could not be abated with actions within the agri-business organization, or within any single stakeholder
 - Agri-business organization initiates partnership (ecosystem) participation
- Marketplace Positioning Model (Lens and Diffusion)
 - Agri-business organization seeks innovation to meet goals, creating impetus, is willing to experiment and open to cooperation across supply chain.
- Win/Win and Production Possibility
 - Technologies increase usable raw materials, promising for most participants (buyers of byproduct (waste) grains foresee cost increases, attractive production improvement without PPF security/sharing
- Intermediation and Disintermediation
 - Roles of supply chain partners are enhanced with data collection duties, external to agri-business organization
 - Existing Co-Op intermediation role becomes enhanced and even more valuable
 - Tapped existing operational process across supply chain partners looking for gaps in which to invest
 - Sweeping clean and starting over not an option
- Centralized and Decentralized

- Semantic messiness with the terms
- (physical movement of material and movement (storage) of data) Data has context that effects appropriateness of storage decentralization?
- Control as key issue in "Field to Fork" example, or rather mutual benefit and cooperation?
- [sliding scale- one each for control span and data domain, which data domain or which subset of data (hourglass model)?] Beck [[35](#)]
- Traceability Consideration
 - Necessity to share data arises from the solution, strengthening traceability requirement.
 - Suppliers value sales and want to keep them as customers.
 - Changes farmers' view of quality of their product, and the need to prove the quality with traceability information to buyers
 - Is there a market need for lower quality product, with reduced cost?
- Candidate research topic
 - Do emerging data exchanges and tracking for continuous materials supply chains present data storage burdens?

C.2 Sky Republic

- Company/Business Drivers
 - Multiple business pains among participating supply chain actors
 - General acceptance that end-to-end processes in typical aircraft MRO and air cargo scenarios entailed inefficiency or pain points for each participant.
- Supply Chain Risk Management
 - Unified processes on a new platform theorized as reducing risk across the ecosystem
 - Risk asymmetry could occur; for example, one company decommissions a part at some low risk, but poses greater risk to the industry marketplace by accidentally acquiring a substandard part
- Marketplace Positioning Model (Lens and Diffusion)
 - Experimental proofs of concept each with a tracking scenario and multiple supply chain actors and innovation seekers at developmental stages.
 - Solution vendor attracted to market for considering blockchain technology and led proofs of concept to demonstrate value

- Win/Win and Production Possibility
 - Supply chain participants experience mutual benefit to participating in experiments.
 - Technology viewed as path to faster, better, cheaper (shift of PPF, with security a factor)
- Intermediation and Disintermediation
 - Participants did not appear sensitive to disruptions in roles for the end-to-end experiments.
 - Each participant sought specific upgrades and potential for improvement in current processing.
- Centralized and Decentralized
 - “Blockchain is a team sport, and the team needs a coach.” Willing participants cooperated but challenges in confidentiality rules arose during design of smart contracts.
 - Decentralization viewed as a blockchain marketing term, rather than a directly sought-after benefit. Operational drivers of faster, better, cheaper were sought after benefits. Reconciliation of demurrage computations cited as an interlining process seen as specifically to benefit from transparency attributed to decentralization.
- Traceability Consideration
 - Ecosystem of participants viewed as generally static with room for improvement. Automated processes joined with traceability from blockchain technology, a broad approach to sweep up various inefficiencies. Proofs of concept were designed to demonstrate broad value.
 - Will blockchain create or alleviate barriers to entry for new competitors in Air MRO and Air Cargo scenarios?
 - Can a case be made that an ecosystem is demonstrably safer as well as “faster, better, cheaper” due to improved traceability? (Safer is a byproduct or emergent quality, not to be sought specifically, perhaps) Would investment in core smart contract designs that include confidentiality management patterns reveal opportunities to standardize?

C.3 Guardtime Federal

- Company / Business Drivers
 - Guardtime Federal Inc./provided traceability solutions
 - Trust in data integrity even across organizational boundaries seen as generalizable
- Supply Chain Risk Management

- Federal space concerned with supplier quality and parts authenticity; risks cannot be abated by lone companies.
- Many “entry points” for integrity loss.
- Risk avoidance through trust structures spanning organizations.
- Marketplace Positioning Model (Lens and Diffusion)
 - Attracted to maturing use of traceability technologies, niche innovator seeking partnerships.
- Win/Win and Production Possibility
 - Information sharing rules are in hands of data owners.
- Intermediation and Disintermediation
 - Role of vendor: performs as new member of the supply chain, or could present as a new style of intermediation through the accompanying vendor technology and expertise
 - Similar to MediLedger case
- Centralized and Decentralized
 - Hard and formal delivery requirements between vendors and government PMOs (which are typical) make for centralized, hierarchical acquirers and loosely constructed, team building among supplier chains.
 - The government has many operating models for the notion of “end-operating environment.” They may have total system performance responsibility (TSPR) arrangements with contractor or “integrator” functions, or government leads operations, etc. Think about for “Perspectives from a Prime” case as well, re: intermediation and/or centralization
- Traceability Consideration
 - Will new outsourcing models arise for government traceability solutions? What would they look like? How would they differ by government domain (military, local government, treasury...)?

C.4 Large Prime

- Company / Business Drivers
 - Increasing need for data security and integrity
- Supply Chain Risk Management

- Highly structured and monitored risk and security arrangements due to military applications (SW&HW) and end-operating environments.
- Information acquisition and processing as a supply chain: A special case? The grandparent of good data –the database management system.
- Marketplace Positioning Model (Lens and Diffusion)
 - Market leader in the defense industrial base with sensitivities to national security. Government (monopsony conditions) acquisition strategies and contracting arrangements likely drivers for innovation seeking and pace of adoption.
- Win/Win and Production Possibility
 - Traditional constraints on sharing information coupled with many focal points arising from government program structures complicate outward motion of a PPF for security and sharing, even with solid technologies.
- Intermediation and Disintermediation
 - Interview discussions included intermediation topics related to responsibility for both contributing to a traceability solution and administering a solution.
 - Contractors’ teaming arrangements and IP protections contribute to attractiveness of an intermediary.
- Centralized and Decentralized
 - Inter-blockchain exchanges occurred in their solution setting, suggesting several interpretations regarding a centralized and decentralized discussion.
 - On one hand these exchanges highlight existing decentralized or distributed activities. On the other hand, attractiveness of an intermediary function (by requirement holders, i.e., government) reference central authority.
 - “Decentralized” is quite overloaded in meaning and application.
- Traceability Consideration
 - Free and open-source software plays into the prime’s deliveries (end deliveries to government and acceptance from suppliers).
 - Is a supply chain traceability solution for software products a complete risk reduction solution? Knowing that software hasn’t changed and where it came from may only cover a portion of risks specific to software products.

C.5 DUST Identity

- Company/Business Drivers

- Business Driver: rising incidence of counterfeit parts, resulting in increased support costs and brand reputation losses, among other things
- Focused on Identity and works out from it: central to broader array of traceability solutions
- Physical identity: gap in assurance between physical item and data about the physical item.
- Supply Chain Risk Management
 - Addresses risk associated with asserting genuineness and maintaining physical and digital data connections
 - NIST 800-171 given as a reference for cyber security guidance in securing information and access.
- Marketplace Positioning Model (Lens and Diffusion)
 - Innovator tackling traditionally hard problem of object identification (as in serialized parts) and partnering with blockchain developers (e.g., Manufacturer X).
 - Traditional solutions (serial numbers, stickers, barcodes, etc.) are not secure and are separable from objects, leaving them a mystery, and some parts are not subjectable to markings.
- Win/Win and Production Possibility
 - In addition to aiding a generalized security and sharing win/win by providing a way to uniquely identify objects, this technology moves the PPF by enabling ecosystem participants to maintain and share all their data, and also protect their IP by having a detailed and agile permissioning approach for the data.
- Intermediation and Disintermediation
 - Role of resellers is potentially impacted, how so exactly?
 - New API usage and process integration, potential adoption of Manufacturer X's solution outright.
 - Perhaps labor-intensive physical security is displaced or reduced, changed significantly by introduction of DUST. As a value-add to a traceability solution, intermediation currently satisfied with paperwork or streams of follow-up messages is greatly reduced.
- Centralized and Decentralized
 - Sensing the DUST Identity Tag is inherently tied to location of the physical object; however, data access and editing can happen without access to the physical object. This is tracked and reflects the lower level of security of the modifications since the

object was not present. Exposure of the data is an interesting proposition. Does the manufacturer have a business case for following its products to second-hand markets, for example? The supply chain in MRO scenarios may include the entire life cycle, but who “owns” that, with assemblies and such that change hands and may be installed repeatedly in different “end-operating environments?” DUST provided additional insight:

This is also something that DUST encounters regularly. There is significant incentive for upstream manufacturers to achieve higher visibility of downstream and end-usage of their products to better inform business decisions and potentially participate in downstream value creation.

As for data ownership, that is indeed an excellent question to raise, and we often see the best solution as the creators of the data owning their data and monetizing access to that data by other parties. This can be done by every member of a single product's supply chain, enabling all parties to monetize their data and share it as a revenue driver.

- Traceability Consideration
 - An enabling technology that fills a generic gap in traceability solutions, yet stands on its own as an identity solution, meeting internal manufacturing needs for example.
 - What is foreseeable about large scale growth of traceability solutions and the resulting large-scale implementations?
- Candidate Research Topic
 - Federation of solutions and data standards questions for research.

C.6 MediLedger FDA Pilot Project

- Company/Business Drivers
 - Search for legislation-driven solution in the pharmaceutical supply chain, examined a blockchain system in detail addressing multiple areas raised by a stakeholder group
- Supply Chain Risk Management
 - Concerns for transactional privacy and immutability
 - Poll found agreement that interoperability includes many trading partners as opposed to adjacent partners only.
 - Exception handling detail explored at the level of change of ownership
- Marketplace Positioning Model (Lens and Diffusion)
 - Wide net for participants cast due to impetus from legislation

- Poll reflects concerns related to diffusion and newness of blockchain technologies. Group split on whether newness is a barrier to adoption
- Recognition of thought leaders
- Win/Win and Production Possibility
 - Under barriers to adoption but related to PPF: Group poll reflected that an adoption rate of 80 to 90% of industry participants would be “critical mass.” Appearance of a shift in PPF, but only with sufficient participation.
 - Considerable attention given to minimizing what is shared for both transaction privacy concerns (also industry membership authorization) and appropriateness in volume for a blockchain solution
- Intermediation and Disintermediation
 - Three main industry roles addressed: manufacturers, distributors, and dispensers
 - Roles of solution providers included
- Centralized and Decentralized
 - Described solution as containing Private Nodes and Consensus Nodes, a hybrid concept, perhaps, of centralization and decentralization: Bearing resemblance to the polycentricity concept.
- Traceability Consideration
 - Changes in ownership as a chain of custody that has blind spots without full participation of chain members.

C.7 Chain Integration Project (CHIP)

- Company / Business Drivers
 - “Tremendous amount of effort and inefficiency in current supply systems” eliminating claims, shrink and counterfeiting worth some “\$181 billion” in business potential. Serialized data exchanges identified as a weak spot, even after 15 years of RFID solutions.
- Supply Chain Risk Management
 - “69% of ASNs [Advanced Shipping Notices] do not match purchase orders. Doing this faster is not a solution.
 - Supplier/retailer partnerships formed basis for examining an industry wide capability. A particular path representative of a frequently occurring serialized data exchange. Several hops, two partners.
- Marketplace Positioning Model (Lens and Diffusion)

- Auburn Blockchain Working Group established with membership of Consumer-Packaged Goods suppliers and retailers. Suppliers offered live data and paired with retailers for the proof of concept.
- Win/Win and Production Possibility
 - Shifting the PPF with respect to speed not seen as a helpful shift. Simply moving low quality (mismatched, out of sync, latent: process and identification issues) data around faster, not enough.
 - Outbound serialized data to inbound serialized data, a very focused scope. Also, an existing exchange with established means, like standards for RFID tags and barcode granularity.
 - Generally, agreements to share data already viewed as necessary. Improvement pursuit key.
- Intermediation and Disintermediation
 - Roles: suppliers (Consumer Packaged Goods), retailers and other supply chain stakeholders.
 - Solution providers considered necessary to the proof of concept for their role in serialized data management.
- Centralized and Decentralized
 - Cites “imbalance of control created by their centralized solutions or lack of scalability across the industry” as long-term impediments to exchange of serialized data.
 - Serialized data management solution providers considered central to processes.
- Traceability Consideration
 - Scope of project was partnerships, considered in combination to represent a commonly felt business pain, poor ASN and Receipt synchronization performance.

Appendix D—Mental Models Analysis Candidate Areas for Research

Even across a few voluntarily provided case studies, a wide variety of activities in supply chain traceability surfaced. As mentioned, we selected a handful of mental models, described in [Appendix B](#), to use as aids in analyzing the case studies for research indicators and precursors to tomorrow's standardization needs. Using the mental models has highlighted potentially market-driven motivations arising from current supply chain circumstances (e.g., counterfeit products) and classic business drivers for improved profitability, market share, efficiency, and scale. In this section, each of the five mental models will be used to introduce a conversation spanning the activities of our respondents. In addition, an "et cetera" section will capture traceability considerations that are not neat fits in model conversations. Additionally, each conversation concluded with one or more candidate research areas which are provided here:

D.1 Supply chain risk management candidates

An organizational orientation to risk assessment highlights when, in fact, the means to mitigate some risks must be addressed by a community or domain of stakeholders. As described in most case-cited situations, risk abatement appears to be an activity of the community as well as an internal pursuit. Some projects and Proofs of Concept are described as being partnerships between a solution provider and a single company pursuing business improvement, while others assembled groups that constitute a supply chain use case.

It may no longer be necessary to conduct further research into whether communities recognize a need for cooperation in contending with certain risks, but other related questions arise:

- What forms of cooperation are essential to successful supply chain traceability solutions and how do traditional ICT interoperability approaches help or hamper? This exploration could support pattern forming for implementation strategies amongst supply chain participants whose existing systems are vital to their operations. Some existing data exchange standards may prove more durable than may be obvious.
- If an organization pursues traceability specifically in response to risk assessment, how does that shape solutions? Is a solution with the key drivers expressed as risk mitigation significantly different than one that states its business drivers as new product lines or operational efficiency? This exploration could support solution architectural choices, thereby influencing traceability flows and subsequent calls for messaging standards.
- How sensitive is traceability reliability to gaps in information? Another angle for incremental risk reduction methods in applying traceability solutions is to examine situations that appear to be "all or nothing" but a closer look exposes interim value delivery. This value could take extra-curricular forms, so to speak, as well as emerge as a by-product rather than be directly attributable to a traceability component. This stems from viewing the supply chain in ecosystem and socio-technical system terms, that can be associated with cooperating in mutually beneficial ways. Alternatively, certain "gaps" are traditionally seen as a risk reduction measure. For example, a

digital asset such as a sensitive file, may be considered as inappropriate for an actual presence in the traceability solution, other than by proxy, as in a hash generated from the file.

- As supply chain participants gather to work across their networks, what short-list of terms would be helpful in reaching consensus quickly? What means of distributing knowledge of those basic, and few, terms would be valuable? The language itself of supply chain traceability is showing signs of a developing vernacular. For example, distinctions between integrity, provenance, trusted, immutable, etc. are arising due to entry of multiple solutions to specific pain points. The quicker traceability arrangements can be agreed upon, the quicker risk reduction measures can take effect. Terms related to quality of service and specificity of risk could be prioritized.

D.2 Marketplace positioning candidates

Our respondents easily display the qualities of innovators as well as an appreciation for technology adoption cycles. The variety of pursuits and experiences in solution and value seeking included: internally run custom projects with R&D partners, outsourcing to specialist vendors, and hybrid solutions as the technology expands in use and incentivizes cooperation. In line with the diffusion model, the strategic minded can forecast potential market share as the numbers of and scale of uses in tandem create profit opportunities. In turn, reaching larger audiences as well as anticipating needs of new entrants and latecomers enters the equation of strategic planning.

Discussion topics specific to industries or domains provide a sketch of potentially relevant issues and challenges where a decision to look closer could be fruitful:

- How will the architectures of solutions be influenced by the two dimensions of supply chain participants and technology components? Structures that crystalize into architectures also define the boundaries relevant to message content standardization and sequencing of business process. In the most generic sense, these divisions of labor define organizational boundaries and thus the discourse relevant to pursuit of standards. Industry or domain qualities may, or may not, significantly impact what communications and what shared data are vital to traceability needs. This may also be viewed as: To what degree can standardization pursuits be successful in this traceability realm, if variation (due to technologies and industry-specific formations) squeezes the space for opportunity?
- How does the complexity (in the scientific sense of complex adaptive systems, system of systems, behavioral economics) of the marketplace impact a proposed way ahead for even commonly understood elements? Conditions of complexity are characterized by difficulty of prediction and emergent behaviors. If an examination of the components of traceability in isolation does not (or cannot) account for what happens in practice, what can future proofs of concept, experiments, or perhaps modeling and simulation offer to inform and guide?

- What can ease a potential for barriers to entry, in the economic sense, that could pinch small or niche contributors? Barriers to entry that could arise include: degree of investment needed to meet a minimally competitive level of operations, necessity of sophisticated knowledge and expertise (which may be scarce) in operating or participating in new solutions, and disruption to existing operating models. In addition, why might it be important to be mindful of an active small and niche player community for any given industry? A result could be ongoing metrics and reporting the degree to which the pain points addressed by traceability place a drain on productivity, negate otherwise profitable investments, or impact national security. Start-ups are actively cultivated by government, military, academia, and venture capitalists for a variety of reasons. Start-ups, entering a technology cycle at the point where feedback from practical experience has begun, can position themselves with unique insights for smoothing implementations and even rough edges of the technology itself. For supply chain, the historical problem of marking physical objects combined with the traceability problem of matching a physical item with its digital thread, could be such an area.
- What standardized service levels of agreements, contract clauses in government domains, or other unanticipated forms of agreement can be constructed that would speed implementation of traceability across supply chains and networks? Speed of adoption may be an imperative for some end-operating environments that could be described as under attack. With improvements in multiple forms of cyber security detection methods, exposure of threats and their rate of exposure is likely to increase. If an organization didn't know they needed traceability yesterday but are acutely aware of it today, time is of the essence. Generic business models and agreement forms can dramatically shorten the distance between need and implementation.

D.3 Win/win and the production possibility frontier candidates

Traceability technologies can be said to move the PPF such that the Win/Win situation of having more of both can be realized. For some, this is counter-intuitive because protecting data has been a traditional method of securing it. As suggested in cases, efforts to share data to protect the objectives of an ecosystem can encounter a myriad of existing assessments, controls, and procedures, all enforced at the data owner's level. The responsibility for data and associated information can be burdensome as it can reflect IP (such as a bill of materials) or national security concerns as in export-controlled technology data. While we see our respondents' recognition of the value in cooperating to share data across supply lines, there is still the hard work of determining what information is crucial to the success of traceability efforts.

Several avenues of research surface as a result:

- What is the minimum set of data elements and associated message or process context to support a successful traceability project? Can strategies from previous efforts at design criteria, such as an hour-glass model (reference ACM on Hour-Glass Model) [36], or existing business exchange standards be leveraged to tackle this challenge. In one case an existing standards review did result in usable message types.

- What cryptographical or other means allow data to both be shared and obscured at the same time? Blockchain and other traceability technology could be improved in ways unimagined today.
- What other trade-offs between concerns exist that are today analyzed as zero-sum, but have technologies in the pipeline that would shift the PPF?

D.4 Intermediation and disintermediation, make or buy candidates

Opportunities for intermediation are potentially dominant, given the experiences described by our respondents. These discussions surfaced:

- Intermediation resulting from potential profitability for companies offering supply chain traceability solutions that include operations.
- An external operator of a blockchain solution can be attractive, where teaming of companies is variable and commonplace, as in government monopsony conditions.
- Strengthening of existing intermediators as their roles in data collection are enhanced, such as co-ops.
- Willingness to outsource on the part of supply chain participants. As technologies mature and solution sets become more complete, innovators and the following majority of adopters may see outsourcing as viable to strategy.

Fewer suggestions of disintermediation surfaced. These are primarily relating to existing security measures that are displaced by improved circumstances of traceability. Examples are improved identity of physical components reducing physical security roles and un-needed administrative services for tracking and responding to supply chain discrepancies.

The degree to which displacement of currently profitable roles is portended appears overshadowed by the opportunities to fill solution niches. With that in mind, these areas may be fruitful for research:

- How do industry or domain characteristics (microeconomics) influence what are the viable business models of intermediators in supply chain traceability? Do monopsony conditions necessarily indicate that the single consumer of the end-operations will absorb the cost of directing and transitioning improved traceability?
- Do the dynamics of improved conditions and efficiencies of introducing traceability have a net effect similar to the general pursuit of quality? In the respect that “Quality is Free” [16] is supply chain traceability also “free?”

D.5 Centralization and decentralization candidates

Defining decentralization, on its own footing, begs for research into its semantics and application. Introducing decentralization as a desirable characteristic of traceability solutions compounds the dilemma.

Our respondents' businesses have characteristics that can be cast variously as centralized or decentralized. Farms are both geographically dispersed and regional. Maintenance facilities are scaled to serve multiple operational units. A dominant buyer is a central figure in a supply chain. Events with ripple effect have a central point of origin, such as demurrage and other logistics situations. Responsibility for performance coalesces with the prime contractor. And so on. It's not clear from our respondents that decentralization, as when used to describe blockchain solutions, is particularly interesting. Instead, business drivers and strategic commitments attract attention.

For research:

- Is it the case that once the business need arises for cooperation, the differentiators among potential solutions do not hinge on the quality of decentralization? What are the key differentiators among solutions (features vs technology's inherent qualities) that aid in choosing among or designing a supply chain traceability solution? What determines a well-fitted solution?
- Do the various forms of connectedness in supply chains mean that graph theory is a useful source of descriptive and evaluative metrics? Existing research in this vein includes Chauhan, Frayet, & LeBel [36], Tachizawa & Wong [39], Vernon & Keeling, [38].

Appendix E—Analysis notes from Standards and Solution Experts

This listing is the result of compiling the material in Sections [4](#) and [5](#). These details provided inputs for themes in [Section 7](#), alongside other analysis notes in other Appendices.

E.1 Linking physical objects to data

Declared authenticity of physical objects in data records can only be verified by linking the physical object to a data record (e.g., cyber-physical anchor); current cyber-physical anchor technology uses both invasive (adding physical signature) and non-invasive (scanning) methods. Non-invasive methods hold the promise to expand the scope of objects which can be tracked. This is an emerging technology field.

Impact: Provable linkage between physical goods and data records are required for traceability.

E.2 Data integrity

Data integrity frequently implemented as “immutable ledger,” even linking to off-chain data with hash pointers to ensure off-chain data has not been tampered; consistent patterns and best practices will accelerate adoption.

Impact: Data integrity (immutability) of traceability data records, including across blockchains, is required for traceability.

E.3 Data traceability

Pedigree and provenance of data records (and hash linked data and physical objects) can be assured within a single blockchain effort (ecosystem scoped to agreed participants and shared blockchain enabled capability).

Further research required to link traceability between blockchain ecosystems. Further research required to understand the impact of part of a supply chain getting traceability requirements from multiple operating environments; can the traceability requirements be satisfied for all the operating requirements?

Impact: Data traceability required when tracing through multiple ecosystems.

E.4 Ecosystems of cooperation

Cooperation (e.g., governance, operations) can be achieved within an ecosystem, however cooperation across ecosystems (necessary for supply chain and other activities) is needed; consistent patterns and best practices (including identity and privileged access) will accelerate adoption.

Impact: Stable ecosystem governance including polycentric is required for traceability across ecosystems.

E.5 Enabling distributed coordination

Using blockchain and ledgers to bolster sensor-to-shooter data pedigree and provenance of data exchanged is being explored—can blockchain and ledgers also be used to help force coordination such as exchanging conditional delegated authorities in rapid tempo operations? In a joint/coalition environment? While environment is contested?

Impact: Data is part of a “supply chain of decision making” and traceability of data can increase confidence in using data to make decisions.

E.6 Analysis and trade space of decentralization, distribution, and consensus

As adoption tempo increases and blockchain ecosystems become linked, trusted, and repeatable methods to analyze trade space of options (e.g., centralized, DLT, blockchain) regarding benefit, cost, risk, level of effort must be developed and promulgated to achieve the desired effects including overall (across DoD and partner nation theaters) understanding of residual risks and vulnerabilities.

Impact: Greater understanding of decentralization, distribution, and consensus is required to create capabilities comprised of a network of ecosystems.

E.7 Analysis method to quickly discover/form/implement a blockchain enabled ecosystem

Impact: As traceability methods are discovered and championed, repeatable analysis and methods of practice are required to accelerate adoption.

E.8 Identity

Impact: Consistent, repeatable, and understandable means of establishing and using identity are required for traceability within and across ecosystems.

E.9 Need to incorporate classified networks

Impact: Traceability information is required to be ingested as needed by higher classification networks

E.10 Minimum viable ecosystem

Growth of ecosystems

Interlinking between ecosystems

Interlinking with logistics

Impact: Establishing an MVE must be a relatively routine process with supporting metrics, and data and governance patterns.

E.11 Cross blockchain transactions

Blockchain enabled ecosystems can be linked / bridged by either (a) individual participants write and read across the ecosystems, or (b) the blockchains mutually interact, potentially providing higher assurance of provable information exchange.

Impact: Traceability across ecosystems require means and methods to exchange transactions.

E.12 Standards

Consider developing a standard (NIST) or specification for adoption in blockchain-enabled 'smart contracting' or identifying as a gap that could be addressed by a NIST standard or additional research.

What is the role of standards to accelerate adoption? Who are the actors (by type)?

NEIM.gov is an interesting example whereby messages of a more specific type can be built on more generic types. Possibly supports incremental agreement.

Impact: Standards are required to establish traceability (e.g., goods identification). The standard can be used solely within the ecosystem or across ecosystems.

E.13 Cooperation with logistics and IP blockchain records

The interplay between supply chain traceability blockchain records and IP blockchain records

Impact: Traceability records may establish not only supply chain tracing, but also tracing through logistics, and potentially affirming ownership.

E.14 Decentralized information sharing (trusted, attributed, resilient)

In addition to exchanging traceability information with an ecosystem concurrent with flow of goods and services, there also is a need for ad hoc and event driven general information exchange to dynamically address threats; some examples of this are centralized (DSS, National efforts, etc.) and we also (not replacing the centralized efforts) need ad hoc support for ecosystems to immediately react to emerging threats; this information can be copied to national efforts.

Impact: Evolution of traceability depends in part on sharing supply chain intelligence.

E.15 Metrics

Multiple end operating environments may inform the same segments of supply chain. Further, blockchain enabled ecosystems may grow in scale and need to interact with each other. As traceability is implemented across larger regions of supply chain, metrics will be required to measure coverage of requirements and effectiveness of mitigating SCRM risk associated with individual and combined traceability efforts.

Impact: Metrics are required to reliably identify traceability gaps and measure progress in

addressing gaps. Metrics also required to describe the sensitivity of adding traceability (e.g., if traceability X is added, then the impact to ecosystem Y risk is Z).

E.16 Data patterns of external repositories (from legacy to Solid, IPFS, etc.)

Support for fusion and analytics (regimen to copy transactions and externally linked data into fusion/analytics for national security analysis)

Impact: High impact supply chain knowledge is enabled by fusion of attributed, trusted, and linked data.