2022

Tracking tangible asset ownership and provenance with blockchain

Mark D. Sheldon

Tracking Tangible Asset Ownership and Provenance with Blockchain

Mark D. Sheldon, CPA, CISA
Associate Professor
Kramer School of Accountancy and Information Sciences
Boler College of Business
John Carroll University
6 Bruening Hall
University Heights, OH 44118
msheldon@jcu.edu

April 5, 2022

Running Head: Tracking Tangible Assets with Blockchain

Acknowledgements: I thank Graham Gal (editor) and two anonymous reviewers for their helpful comments and suggestions. I also thank Reza Barkhi, John "Jack" Castonguay, Greg Jenkins, and Karen Schuele for their helpful comments and suggestions. Finally, I am grateful for the research support provided by the Arthur Andersen Fellowship at John Carroll University.

Tracking Tangible Asset Ownership and Provenance with Blockchain

ABSTRACT

Blockchain transactions are recorded in a shared and append-only repository that multiple parties verify, validate, and agree-upon. While initially used to keep track of digital assets, blockchains now track the ownership and provenance of tangible assets. An inherent challenge in using blockchain for this task involves keeping the status of a tangible asset in the physical world in sync with its non-fungible token on a blockchain. While several blockchains are already being used in this manner, specific implementation details are fragmented. In response, this study examines four stages of tracking tangible assets using a consortium's permissioned blockchain, including: design and governance of a blockchain, asset creation, asset transfer, and asset retirement. Based on this analysis, this study proposes a framework of risk considerations and control objectives to evaluate the extent to which a unique blockchain serves as a reliable transaction repository for tracking the ownership and provenance of tangible assets.

Keywords: blockchain; provenance; ownership; tangible asset; non-fungible tokens.

I. INTRODUCTION

A growing number of blockchain implementations demonstrate that the technology can help companies track the ownership and provenance of tangible assets (Higginson, Nadeau, and Rajgopal 2019). For example, Walmart uses blockchain to track the provenance of some food items (Hyperledger 2020a), while Everledger tracks the provenance of diamonds, wine & spirits, and luxury goods (Austin 2020). In many cases, non-fungible tokens (NFTs) on a blockchain represent unique tangible assets.[1] However, an inherent challenge is how to keep an NFT and its tangible asset in sync (McKinsey & Company 2018) as discrepancies can lead to issues with inventory valuation and/or conflicts in ownership claims. To date, details on how existing blockchains address this challenge are sparse. In response, this study examines four essential stages of tracking the ownership and provenance of tangible assets with blockchain, focusing on assets to which an identification (ID) tag can be directly attached.[2] Following the approach used by Sheldon (2021), the objective of this study is to develop a framework of risks and control objectives to evaluate the extent to which a permissioned blockchain used by a consortium serves as a reliable transaction repository for tracking tangible assets.[3,4]

Blockchain provides a self-contained environment that enables exchanges of value online and resists threats from the outside world (Coyne and McMickle 2017; Warburg, Wagner, and

[1] NFTs "identify something or someone in a unique way" (Ethereum Foundation 2022), which can include digital or physical assets (Entriken, Shirley, Evans, and Sachs 2018). On Ethereum, an open-source blockchain commonly used as a code base to create permissioned blockchains, these tokens are defined under Ethereum Request for Comment 721, *Non-Fungible Token Standard* (Ethereum.org 2021).

[2] Assets with ID tags attached to only packaging and/or shipping containers are beyond the scope of this study.

[3] While this study focuses on risks and controls specific to using a permissioned blockchain to track tangible assets, there are other risks and controls to consider when evaluating an entire blockchain ecosystem (e.g., private key security, change management, system interfaces). Interested readers can see COSO (2020) for a broad range of blockchain risks and internal controls, and Sheldon (2019) for information technology general controls (ITGCs) relevant to a permissioned blockchain.

[4] This study refers to blockchain as a distributed transaction "repository" rather than "ledger" to convey the fact that it tracks details about tangible assets beyond simple exchanges (i.e., debits and credits). The notion of a distributed transaction repository remains consistent with terminology used in a recent publication from the International Organization of Standards (ISO 2020). I thank an anonymous reviewer for this suggestion.

Serres 2019). However, when used to track tangible assets, a blockchain ecosystem requires external inputs to keep the physical and digital worlds in sync. While the practice of recording digital representations of tangible assets is not new (e.g., scanning barcodes), blockchain enables end-to-end tracking of NFTs from asset origin, through exchanges in the supply chain, and ultimately between different owners using a repository that is shared, append-only, verified, validated, and agreed-upon by key stakeholders. This tracking allows companies to maintain real-time views into their own tangible asset holdings and to view records of each asset's provenance.[5] A reliable record of provenance is important to establish an asset's origin and authenticity, which can have a direct impact on its valuation. For example, the retail value of a smartphone will likely decrease if customers discover that its raw materials include conflict minerals (Hyperledger 2020b).

While a single enterprise might implement a blockchain to track tangible assets,[6] parties in a horizontal or vertical ecosystem can also form a consortium to accomplish this task (Deloitte 2019). Various parties typically have an interest in proving an asset's authenticity throughout its life (e.g., manufacturer, wholesaler, retailer, customer). Given the level of control a consortium would want to maintain over its blockchain, a permissioned (rather than permissionless) design would allow only authorized users to submit transactions, verify/validate transactions, participate in the consensus to add transactions to the repository, and maintain a copy of the blockchain repository (Drescher 2017; IBM 2019; Warburg et al. 2019; Stein Smith and Castonguay 2020).[7]

[5] Permissions to view content on a blockchain can be defined at the participant level. This study focuses on consortium blockchains with authorized participants, and assumes all participants can view all data and records.

[6] Given that blockchains were initially conceived to avoid centralized control (e.g., Nakamoto 2008), a blockchain owned and controlled by a single enterprise might be challenged on its classification as a blockchain.

[7] This study makes several assumptions about the types of transactions that would be recorded in a blockchain used to track tangible assets. Specifically, the term "transaction" in this study can refer a financial exchange (e.g., of digital currency) or an event (e.g., the creation, sale, modification (enhancement or damage), or retirement of an asset, as well as any asset recertifications). In terms of asset value, this blockchain would track historical cost established as part of sales or modifications, but would not be used to track asset market values or book values. As

Such control makes permissioned blockchains appealing in a business setting (AICPA and CPA Canada 2017; Dai and Vasarhelyi 2017; Lewis 2018; Warburg et al. 2019), as evidenced by the prominent permissioned blockchains currently being used to track tangible assets (e.g., IBM Food Trust and Everledger).[8] As such, this study focuses on permissioned blockchains used by consortiums to track the ownership and provenance of tangible assets.

This study follows the Design Science Research Methodology (DSRM) (Hevner, March, Park, and Ram 2004; Peffers, Tuunanen, Rothenberger, and Chatterjee 2007), as applied in an accounting information systems (AIS) setting by Geerts (2011). Several recent AIS studies also apply this methodology (e.g., Nehmer and Srivastava 2016; Appelbaum and Nehmer 2017; Rozario and Thomas 2019; Appelbaum and Nehmer 2020; Sheldon 2021). DSRM includes six phases: (1) Problem identification and motivation, (2) Define the objectives of a solution, (3) Design and development, (4) Demonstration, (5) Evaluation, and (6) Communication (Geerts 2011). The problem identified in this study (Phase 1) is that blockchain can be used as the record of tangible asset ownership and provenance, but the extant research does not offer a framework to evaluate the extent to which blockchain serves as a reliable repository for tracking tangible assets. As motivation to study this problem, blockchain users might rely on incorrect information from a technology labeled a "truth machine" (Casey and Vigna 2018). However, a blockchain deemed reliable to track tangible assets can provide strong support for (1) an asset's origin and authenticity, (2) an owner's claim to the asset, and (3) key accounting documentation about the asset (e.g., purchase date and cost) (Hoare 2015). The question of reliability can be solved/clarified (Phase 2) by examining the process of tracking tangible assets with blockchain,

such, this study assumes that more involved accounting procedures (e.g., depreciation and mark-to-market) would be handled separately by a firm's internal accounting system(s).

[8] Recent arguments suggest, when designed properly, permissioned blockchains can achieve higher decentralization of control than permissionless blockchains (e.g., Bakos, Halaburda, and Mueller-Bloch 2021).

then creating a framework of risks and control objectives relevant to each stage of the asset's life (i.e., creation, transfer, and retirement); both tasks are performed in this study (Phase 3). As it is not always feasible for individual studies to address every aspect of the DSRM (Peffers et al. 2007), this study does not demonstrate or evaluate its framework in a live setting (Phases 4 and 5).[9] However, a Big-4 practitioner working on that firm's blockchain product provided suggestions on ways to improve the framework, which are incorporated in the final version. Furthermore, key open issues with the framework appear in Section IV, Research Opportunities. Finally, writing this study accomplishes communication (Phase 6). Table 1 provides a mapping and further discussion of how this study follows the DSRM.

[Insert Table 1 about here]

To develop a framework of risks and control objectives, this study examines four stages of tracking a tangible asset's ownership and provenance using blockchain. Stage One, Design and Governance Considerations, addresses technical details and key processes a consortium's charter should define before implementing a blockchain to track tangible assets. This stage also discusses three pervasive supporting processes: privileged access provisioning, smart contract deployment, and smart contract retirement.[10] Stage Two, Asset Creation, examines the creation of a tangible asset, participants' verification and validation of the creation, and minting (i.e., creating) the asset's NFT. Stage Three, Asset Transfer, considers the transfer/sale of an asset, participants' verification and validation of the transfer, and the role of smart contracts in transfers. This stage also considers the process to recertify the quality/condition of a tangible

[9] While publicly available documentation for how some blockchains track the ownership and provenance of tangible assets is more thorough (e.g., the IBM Food Trust, www.ibm.com/food), proprietary details are not made public. As such, it is not currently feasible to demonstrate (i.e., Phase 4) the framework against one of these implementations.

[10] References to "smart contracts" throughout this study are interchangeable with "decentralized applications" (or Dapps), which are applications on a blockchain built by combining several smart contracts.

asset and attach this recertification to the respective NFT. The final stage, Asset Retirement, considers the retirement of both the tangible asset and its NFT. If the risks posed throughout these four stages are addressed, blockchain has the potential to provide a reliable record of ownership and provenance for a tangible asset as it moves between owners/custodians. However, even if all of these risks are addressed, some traditional procedures remain applicable such as periodically confirming the existence/custody of an asset and inspecting the asset's physical condition (and applying valuation adjustments).

This study is important to practitioners (i.e., managers, accountants, and internal/external auditors), standard setters, and researchers. For practitioners, the study proposes a framework of risks and control objectives to evaluate the extent to which a consortium's permissioned blockchain serves as a reliable repository for tangible assets.[11] Here, reliability should increase when the consortium addresses more of the identified risks and implements controls to achieve the proposed control objectives. If a tangible asset and its NFT are not kept in sync, practitioners could be confronted with issues of (1) whether physical possession or the blockchain record serves as a more appropriate claim of asset ownership and/or (2) unexpected impairments if the market value of the asset falls below its cost due to being identified as counterfeit or having an unreliable provenance. This study also informs standard setters as they develop guidance on risks that auditors must address when evaluating the reliability of an asset's ownership/provenance as recorded on a blockchain. Finally, this study extends existing research on blockchain in the accounting literature (e.g., Dai and Vasarhelyi 2017; Appelbaum and Nehmer 2020; Sheldon 2021) by examining the creation, transfer, and retirement of an asset that exists both in the physical world and as an NFT, and proposes directions for future research in this area.

[11] The framework proposes control objectives, but not control activities nor testing procedures to evaluate control activities, as auditors would need to identify/develop these based on the unique blockchain implementation.

II. BACKGROUND

Accounting Research on Blockchain

A growing body of research examines blockchain and its implications for the accounting profession (e.g., Coyne and McMickle 2017; Cong, Du, and Vasarhelyi 2018; Rozario and Thomas 2019; Sheldon 2019; Liu, Wu, and Xu 2020; Stein Smith and Castonguay 2020). Three recently published works are particularly relevant to this study.

Dai and Vasarhelyi (2017) discuss how blockchain can be used alongside other emerging technologies such as Internet-of-Things (IoT) devices. Specifically, objects from the physical world can be virtually represented in a mirror world, with their physical "conditions, locations, surrounding environment, history, and activities" continuously updated in the mirror world by transmissions from IoT or similar devices (Dai and Vasarhelyi 2017, 15). Building from Dai and Vasarhelyi (2017), the current study examines the process used to ensure that a tangible asset and its NFT remain in sync so a reliable record of asset ownership/provenance can be maintained by a blockchain.

Appelbaum and Nehmer (2020) discuss the challenge of blockchain participants being able to observe/verify an event in the physical world, and then contribute to the blockchain consensus vote as to whether the event actually occurred. They argue that a more restricted internal private blockchain would be best suited for such challenges, because "if participants are not able to directly verify for themselves that the blockchain activity as recorded accurately represents the physical activity or asset, consensus may not occur" (Appelbaum and Nehmer 2020, 10). Based on this argument, the current study focuses on tracking tangible assets with permissioned consortium blockchains. Furthermore, this study builds off Appelbaum and

Nehmer (2020) by examining the various points in a tangible asset's life when an event in the physical world needs to be recorded as part of the asset's provenance on a blockchain.

Sheldon (2021) examines the use of oracles to observe events in the physical world and make this information available on a blockchain. Oracles collect data from various sources to generate information about a tangible asset using devices such as IoT or radio frequency identification (RFID). The author highlights several risks of using hardware devices as a data source such as whether they remain attached to the intended asset, they are configured to capture the intended occurrence, the devices store data securely, and these data are completely and accurately transmitted to the relevant oracle. These external data source considerations inform the current study as it examines blockchain vulnerability to exogenous inputs and processes.

Blockchain Technical Considerations

Today, the owner of a tangible asset typically maintains the only record of an asset's provenance, meaning subsequent buyers must trust this record or exert effort to validate the seller's claims.[12] With blockchain, participants work to maintain a complete provenance that is shared, append-only, verified, validated, and agreed-upon.[13] If a party chooses to leave the blockchain, remaining participants maintain the asset's provenance. Furthermore, participants have incentives to behave honestly, as dishonest behavior can result in losing access to the blockchain or business partnerships established along the supply chain.

Blockchains use devices such as IoT and RFID to integrate with the physical world (Dai and Vasarhelyi 2017). If controlled properly, these devices make it possible for an NFT and tangible asset to remain in sync. As the digital representation of an asset, an NFT can carry

[12] In some cases, a central party might also maintain asset records, such as when CARFAX collects oil change, owner, accident, and damage history for a vehicle from sources such as state Departments of Motor Vehicles.

[13] Here, and throughout the remainder of this study, discussion of blockchain functionality is specific to permissioned blockchains used by consortiums (unless otherwise specified).

specific attributes (e.g., asset name, serial number, date of creation) and attach to various (re)certifications (e.g., asset origin, quality, or condition) (De Poli 2021). Furthermore, an NFT can be transferred to a new owner, a process typically aided by smart contracts that release payment to the seller once the buyer takes possession of the tangible asset (Coyne and McMickle 2017). Each time an NFT moves between parties or attaches to a (re)certification, blockchain adds the transaction to a chronological history of the asset's provenance.

Several configurable features also make blockchain an appropriate repository for tangible assets. For example, parties running a blockchain can pre-define in its protocol and/or in individual smart contracts the evidence required to verify and validate transactions. These parties can also define what proportion of participants must come to a consensus that a transaction is valid before it can be added to the shared repository (Warburg et al. 2019).[14] Clearly defining what constitutes appropriate evidence and consensus is critical because transactions added to the blockchain repository are difficult to modify or delete.

Given the discussed features, several permissioned blockchains now exist to track tangible assets. However, specific implementation details are not widely available. In response, the following section examines essential stages of tracking tangible assets with blockchain.

III. STAGES AND EVALUATION FRAMEWORK

This study takes the position that tracking tangible assets using blockchain involves four stages. The first stage includes design and governance considerations of a blockchain, while the second stage considers the creation of a tangible asset and its associated NFT. Stage three

[14] Warburg et al. (2019) define a blockchain consortium as "a blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node, and of which ten must sign every block for the block to be valid" (p. 350).

involves transfers and recertifications of an asset, while the fourth and final stage addresses asset retirement.

Stage One – Design and Governance Considerations

The design and governance stage addresses the consortium's charter, including the processes it defines to provide permissioned access and create and retire smart contracts.[15]

Consortium Charter

A critical component in the creation and continued operation of a consortium is its charter. Formalizing a charter helps ensure that key governance and operational details about the consortium and its blockchain are clearly defined and agreed to by all participants and member organizations.[16] While the charter can include a wide range of details, those most critical to this study include the blockchain technical details and the processes used to support blockchain operations.

In terms of technical details, the charter should define the types of permissioned access rights that exist on a blockchain, such as abilities to (1) verify the occurrence of transactions, (2) submit transactions, (3) validate transactions and participate in the consensus to add transactions to the repository, and/or (4) maintain a copy of the blockchain repository (Drescher 2017; IBM 2019; Warburg et al. 2019; Stein Smith and Castonguay 2020). The charter should also specify which participants may possess permissioned access rights or combinations of permissioned access rights. Furthermore, a charter needs to define criteria for selecting oracles, acceptable forms of evidence to verify and validate the creation/transfer/retirement of a tangible asset, and

[15] Stage one does not discuss all possible governance considerations, but rather those that are uniquely important in the context of using a consortium's permissioned blockchain to track the ownership and provenance of tangible assets. For a broader discussion of governance considerations, see Stein Smith and Castonguay (2020).

[16] This study distinguishes consortium member organizations from network participants, in that member organizations create and sustain the consortium, while network participants perform activities on the consortium's blockchain. As such, network participants can be from member organizations or can be authorized outsiders. References to "participants" are shorthand for "network participants".

the minimum level of consensus required to record transactions to the blockchain repository. For NFTs, the charter should specify the attributes that must be assigned to each token (e.g., tangible asset's name, ID tag, serial/model number, creation date, creation location, and picture), which attributes are only visible to restricted parties, and the data standards for assigning/attaching information to NFTs (i.e., for interoperability purposes).

Consortium charters also must define the processes used to support and maintain the blockchain. To begin, a defined process should exist for how to request, approve, and implement logical access, including who has the authority to request, approve, and/or implement the access. The charter should also define the process used to design, test, and implement new smart contracts, specify who has the authority to approve and deploy new smart contracts, and define how to remove/avoid retired smart contracts. Additionally, the charter should specify when smart contracts should be audited, how they should be audited, and who may perform these audits. It is also necessary to define the parties allowed to recertify the quality/condition of different assets and the process for attaching this recertification to the respective NFT. Further, the charter should include a resolution process to resolve discrepancies between the physical world (i.e., who possesses the tangible asset) and digital world (i.e., who controls the NFT). Finally, there must be a process for how to amend the charter, including how many member organizations must approve the change(s). While all processes are essential to support and maintain the blockchain, at least three require further examination due to their high frequency and pervasive nature: provisioning permissioned access, implementing smart contracts, and retiring smart contracts.

Provisioning Permissioned Access

In contrast to permissionless blockchains, permissioned blockchain participants are typically fewer in number, have known identities, and are explicitly granted access to the blockchain (IBM 2019; Warburg et al. 2019). Each participant has the potential to exert relatively more influence on blockchain operations, which increases the need to tightly control who obtains permissioned access rights.[17] The access provisioning process should involve an authorized party submitting a formal/documented request for a separate participant's new/modified/removed access rights, which should then be reviewed by a separate authorized party or committee to determine whether the requested access is appropriate based on rules set forth in the charter (Sheldon 2019). Part of this evaluation should include whether the new access (1) concentrates higher-power abilities among too few participants and (2) assigns the least privilege necessary for a participant to perform their role in the ecosystem (ISACA 2019). For example, if a participant's role is to verify the creation of a tangible asset, it might be appropriate to allow this party to submit evidence of creation to the blockchain, but not validate the event or vote in its consensus.[18] If approved, access should be implemented by an authorized security administrator. Finally, an expedited process should be in place for emergency removal of access from identified/potential bad actors (ISACA 2019).

While access rights determine who has specific authorizations on a blockchain, smart contracts create much of the on-chain functionality available to these participants.

Implementing and Retiring Smart Contracts

Smart contracts are short software programs on a blockchain available for one-time or repeated uses. In this study, smart contracts act as escrow agents that hold the buyer's and seller's assets until certain conditions are achieved as part of an exchange agreement, and also

[17] Stein Smith and Castonguay (2020) point out that "admitting an unprepared or lower quality member can lead to information issues" that harm the other members (p. 122). The authors emphasize that "enterprises must determine, prior to the acceptance of network members, how the identities of different network members – individuals or institutions – will be verified and authenticated prior to being admitted as nodes to the private blockchain" (Stein Smith and Castonguay 2020, 122).

[18] The issues discussed in this paragraph allude to questions of appropriate segregation of duties, which are later discussed in Section IV, Research Opportunities.

mint NFTs that represent tangible assets. Once deployed, smart contracts are difficult to modify and have a unique address to call their functionality. Furthermore, smart contracts that execute are nearly impossible to reverse. As such, smart contracts must be subject to robust design, development, testing, approval, and release processes.[19] It is also possible that, as operations change, legacy smart contracts will need to be replaced by new smart contracts that are more tailored to current needs. By calling a smart contract that is no longer relevant, participants are exposed to the risk that the smart contract does not adhere to current regulatory/contractual agreements and that assets might be transferred to an unintended party. It is therefore necessary to define processes to sunset retired or outdated smart contracts.

Level of adherence to the following control objectives can help reveal the extent to which risks are mitigated in Stage One, Design and Governance Considerations. Specific control activities to achieve these objectives will vary based on the unique blockchain implementation:

- ***Control Objective #1.1*** *– Controls provide reasonable assurance that the consortium has a charter in place that is agreed to by all original and subsequent network participants and member organizations. The charter should address technical details about the blockchain and any relevant processes used to support blockchain operations.*

- ***Control Objective #1.2*** *– Controls provide reasonable assurance that the (level of) permissioned access granted to network participants remains appropriate.*

- ***Control Objective #1.3*** *– Controls provide reasonable assurance that smart contracts deployed to the blockchain are subject to a formal design, development, testing, approval, and release process.*

- ***Control Objective #1.4*** *– Controls provide reasonable assurance that smart contracts are retired/blocked when they are no longer applicable to the consortium's operations.*

See the appendix for the framework that maps these control objectives to risk considerations.

Stage Two – Asset Creation

[19] Sheldon (2019) examines the specifics of smart contract development and change management processes in evaluating information technology general controls (ITGCs) in a blockchain environment.

In general, ID tags can be attached to (1) the physical asset, (2) the asset's packaging, or (3) the asset's shipping container. Given the heightened risk that an asset can be separated from its ID tag when the tag is attached to the asset's packaging or shipping container, this study focuses on tangible assets directly attached to an ID tag.

A wide variety of tangible assets can be directly attached to an ID tag (e.g., a large industrial stamping machine or a car). However, the benefits of tracking tangible assets with blockchain become more apparent when (1) it is important to demonstrate the authenticity/origin of the asset, and/or (2) the asset will be sold/transferred several times throughout its life. A large industrial stamping machine might not benefit from blockchain tracking as buyers likely purchase the machine from the manufacturer and it will not be sold frequently throughout its life. However, a car will likely be sold several times throughout its life and the authenticity/origin of component parts remains important. Here, blockchain can track the authenticity/origin of component parts (e.g., a separate NFT for the frame, engine, and body), and any sale/transfer of the asset as an assembled unit.[20] Given the importance of ID tags to this process, various types of ID tags and associated risks must be considered.

Asset Identification Tags

The asset ID tag plays a key role in uniquely identifying a tangible asset and keeping it in sync with its NFT. One of the simpler forms of ID tags remains a one-dimensional barcode (i.e., a barcode with parallel vertical lines of varying widths), but this format limits the amount of information a tag can directly store/represent about an asset. More information can be

[20] Smart contracts provide a solution to track the origin/authenticity of component parts used to create an assembled and finished tangible asset (cf. EY 2021). Specifically, when parts are combined, a smart contract can burn (i.e., destroy) the component NFTs and mint (i.e., create) a single new NFT to represent the in-process or completed asset. A blockchain repository records the trail/log for these types of activities, and thus maintains evidence about the origin/authenticity of a finished product's component parts.

stored/represented within a confined space using a two-dimensional barcode, such as a QR code (Baum, n.d.). RFID and near-field communication tags more commonly track specific information about a unique item (Dai and Vasarhelyi 2016), such as with supply chain smart label tracking (Baum, n.d.). Other methods are also emerging to uniquely identify tangible assets, such as taking high resolution images, recording specific metrics and attributes (Warburg et al. 2019), using synthetic DNA (e.g., Everledger),[21] or placing quantum dot security inks on an asset (e.g., Ubiquitous Quantum Dots).[22]

Several features of asset ID tags and their implementation should be considered. To begin, what data does the tag store, can the data be used to uniquely identify the specific tangible asset, and can this data be changed in an unauthorized manner? Next, is it possible for data on the tag to be copied to a different tag and attached to a different asset in an unauthorized manner (e.g., creating fraudulent assets or spoofing an RFID tag)? Similarly, how permanently is the tag attached to the asset, and is it possible for the ID tag to be removed and placed on a different asset without showing signs of tampering or misuse? Once these issues are addressed, the next step is to verify details about the asset's creation.

Verify and Validate Creation of Tangible Asset

Tracking tangible assets with blockchain presents the challenge of how to observe when something happens in the physical world and then convince participants that the event occurred (Appelbaum and Nehmer 2020). As part of this, only authorized and appropriate participants and/or oracles (per the charter) should be allowed to verify the creation of a tangible asset and submit this information to the blockchain. It is important to consider how this party observes the

[21] For more information on Everledger, see: www.everledger.io
[22] For more information on Ubiquitous Quantum Dots, see: https://ubiqd.com/security/

asset's creation, and whether this observation is persuasive in the specific circumstance. Evidence of this observation might include one or more of the following:

- A live or recorded video, from a stationary camera or drone, showing the creation of the asset at a specific location (Appelbaum and Nehmer 2020),
- A neutral third party observing and certifying the creation (Campbell, Omietański, and Southwell 2018),
- For a geographically concentrated blockchain, live observation of the creation by participants (Appelbaum and Nehmer 2020).[23]

It is also relevant to consider how a blockchain receives evidence of the tangible asset's creation. For example, if a smart device observes the creation, is the device protected from unauthorized access (i.e., physical access to the device and logical access to its data and software) (Sheldon 2019). Furthermore, does the device directly interface with a blockchain node or does information about the transaction get passed to another intermediary that should also be evaluated for security issues, similar to how Sheldon (2021) describes the risks of intermediary blockchain oracles. Finally, one must consider how the observer correctly routes evidence of asset creation to the smart contract that mints an asset's NFT.

With creation verified and evidence of this event submitted to the blockchain, participants must review this evidence to determine whether it validates creation. Here, an important consideration includes what forms of evidence participants are allowed to use to validate the creation of different types of tangible assets, and how blockchain enforces this requirement (e.g., by protocol or smart contracts). Also, at this point, consider different ways a specific blockchain achieves consensus. For example, some blockchains require that only a small

[23] Plausibly, there could be a hierarchy of evidence, such that certain forms can stand alone while others must be combined with one or more other forms.

number or proportion of participants approve a block for it to be valid, increasing the risk of incorrectly recording the creation of an asset due to error or fraud. However, this risk might be offset by requiring higher quality and/or more objective forms of evidence to validate an asset's creation. Finally, it is important to evaluate how the relevant smart contract enforces the required level of consensus among authorized participants before it mints an asset's NFT, as any failure to enforce this consensus could result in minting an unauthorized NFT.

Assign Attributes to Non-Fungible Token

Smart contracts should require that certain attributes about a tangible asset (e.g., the asset's name, ID tag number/reference, serial/model number, creation date/location, and picture) be assigned to its NFT as part of minting. Assigning these attributes as part of NFT minting is critical because delays in assigning attributes can lead to errors or inaccuracies, which could introduce challenges in later defending the asset's authenticity. In some situations, it might also be appropriate for the manufacturing plant or other origin to be inspected, certified, and/or otherwise licensed to demonstrate authenticity of the asset. For example, the IBM Food Trust blockchain tracks certifications and licenses that "a facility is properly inspected, that livestock have been treated according to law, that a supplier is legally able to do business, and that a farm is certified as conforming to industry standards" (IBM 2019). Only authorized parties should submit certification/inspection/license records to the blockchain, and these records should include the date of certification/inspection/licensing, the time period covered, and how long these should be considered valid (IBM 2019). It is also necessary to determine how certification/inspection/license details are properly recorded and submitted to the blockchain, as well as how they are attached to a specific NFT.

Maintaining Asset ID Tag

Asset ID tags should be regularly maintained given their role as the physical unique identifier that associates a tangible asset with its NFT. Here, it is relevant to consider how long the tag will be usable relative to the life of the tangible asset and what procedures are in place to maintain the tag so as to sustain a continuous link between the tangible asset and its NFT. As this relates to RFID and near-field communication tags, also consider whether the tags are active and have their own power source, or if they are passive and require energy from the scanning device to share information (Baum, n.d.). Although all tags run the risk of damage over time, active tags also run the risk that the battery or other power source might fully deplete, thus preventing the tag from sharing information. To replace an ID tag, procedures should be in place to decommission the legacy tag and associate the replacement tag with its existing NFT.

Devices other than ID tags can also help accumulate details about a tangible asset throughout its life, such as IoT devices.

Internet-of-Things Devices

IoT represents a broad category of technologies that includes the asset ID tags already discussed, as well as other devices that provide "computing functionality, data storage, and network connectivity for equipment that previously lacked them" (NIST 2019, iv). For example, when shipping a piece of art, IoT devices can uniquely identify the asset (e.g., RFID tag), monitor its surrounding temperature and humidity (e.g., temperature and humidity sensors), determine the speed at which is it being moving (e.g., accelerometer sensor), monitor changes in its physical orientation (e.g., angular rate sensor), and pinpoint the origin, path, and final destination of its journey (e.g., GPS device). When combined, IoT devices can provide an expansive history of an asset's physical status, which blockchain can record as part of the asset's provenance.

IoT devices pose several unique risks. To begin, some IoT devices include network interface capabilities, meaning the device can interact over a communications network (e.g., Wi-Fi or Bluetooth) (Dai, Zheng, and Zhang 2019; NIST 2019). If an IoT device includes network connectivity, it becomes vulnerable to the collection of risks and threats that other internet-connected devices face (e.g., cyberattacks, loss of control of the device, unauthorized changes to stored data) (NIST 2019). In these cases, all custodians of an asset should have hardware and software internal controls in place to protect the device (Sheldon 2019). Furthermore, IoT devices must be properly configured to observe and capture an intended event, store data securely, and transmit collected information completely and accurately to an intermediary device or directly to a blockchain (Sheldon 2021).

Level of adherence to the following control objectives can help reveal the extent to which risks are mitigated in Stage Two, Asset Creation. Specific control activities to achieve these objectives will vary based on the unique blockchain implementation:

- ***Control Objective #2.1*** *– Controls provide reasonable assurance that when a tangible asset is created, it is attached to a secure asset identification tag that uniquely identifies the tangible asset.*

- ***Control Objective #2.2*** *– Controls provide reasonable assurance that only authorized network participants or oracles (1) verify the creation of a tangible asset and (2) submit evidence of this event to the smart contract used to mint the asset's non-fungible token.*

- ***Control Objective #2.3*** *– Controls provide reasonable assurance that participants validate the creation of a tangible asset using approved forms of evidence.*

- ***Control Objective #2.4*** *– Controls provide reasonable assurance that network participants must reach the required level of consensus on the tangible asset's creation before the smart contract will mint the asset's non-fungible token.*

- ***Control Objective #2.5*** *– Controls provide reasonable assurance that the smart contract accurately assigns all required attributes to the non-fungible token upon its minting (e.g., asset name, identification tag number/reference, serial/model number, creation date/location, and picture).*

- ***Control Objective** #2.6 – Controls provide reasonable assurance that the asset identification tag is serviced regularly. If the tag must be replaced, the legacy tag is decommissioned and the new tag is associated with the respective non-fungible token.*

- ***Control Objective** #2.7 – Controls provide reasonable assurance that IoT devices used to track tangible assets adhere to the same controls as asset identification tags, and also maintain secure network connectivity, data storage, and configurations.*

See the appendix for the framework that maps these control objectives to risk considerations, and Figure 1 for an example of a tangible asset moving through Stage Two, Asset Creation.[24]

[Insert Figure 1 about here]

Stage Three – Asset Transfer

While asset transfers can happen between many different parties along a supply chain or between owners of a finished product, the critical element from a recording perspective remains the same in each exchange: is the asset released by the seller the same as the asset received and paid for by the buyer? Stage Three, Asset Transfer, considers the elements of a transfer and the risks that threaten a blockchain's ability to provide a reliable record of these events. This study assumes that a smart contract assists in transfers by releasing the NFT and payment once physical transfer of an asset takes place.[25]

Asset Recertification

[24] For aggregated assets (i.e., those comprised of several component parts/inputs), it might not be feasible for all manufacturing/sourcing parties to tag each component part and/or participate in the consortium's permissioned blockchain (e.g., due to contributing low-cost parts or not having the necessary technology resources). In these situations, it will be important for designated parties in the consortium to tag remaining component parts (of meaningful value) and submit any required evidence to the blockchain to create the associated NFT(s). By doing so, this party stakes its own reputation to signal to the rest of the consortium, supply chain, and consumer market that the component parts are authentic. Similar to the underlying incentive structures in popular consensus protocols (e.g., proof-of-work and proof-of-stake), this party has incentives to maintain a reliable blockchain repository as any signs of fraud or tampering would hurt its own financial condition.

[25] Given the exchange of consideration, assets sold for scrap would follow the Asset Transfer process.

As a best practice, an expert should recertify the quality/condition of a long-lived tangible asset after it undergoes a significant change (e.g., a new engine) or prior to a transfer/sale.[26,27] The guidance/processes outlined in a consortium's charter should be followed as part of any recertification, including (1) who may serve as an expert to recertify different assets, (2) how to identify this expert (and have the buyer/seller agree on this expert if part of a transfer/sale), (3) required credentials of the recertifying expert, and (4) how to resolve any disagreements about the expert's recertification conclusion. Evidence of recertification (e.g., documentation and photos) should be uploaded to the blockchain by an appropriate party, such as the expert, and attached to the respective NFT.[28,29] Furthermore, if the expert determines that the asset should be retired prior to a transfer/sale, this status should be submitted to the smart contract used to facilitate the exchange, which should trigger the return of payment and NFT to their original owners. In such cases, a "retired" status should be attached to the NFT and/or the NFT should be burned (i.e., destroyed).

Verify and Validate the Transfer of a Tangible Asset

The process to verify and validate the transfer of a tangible asset is similar to the process used to verify and validate its creation. For example, only authorized participants and/or oracles should verify the transfer and submit evidence of this event to the blockchain. Such evidence might include one or more of the following:

[26] This does not recertify the asset's authenticity, as that is demonstrated by its provenance on the blockchain.

[27] Owners that make significant changes to assets that will not be imminently transferred/sold should still have the assets recertified on a timely basis (i.e., not wait until the next transfer/sale) so that the provenance accurately reflects what change happened, when it occurred, and when it was recorded to the blockchain/attached to the NFT.

[28] While it is possible for evidence of recertification to be kept off-chain, this presents risks of the evidence being manipulated, destroyed/lost, or not made available to participants. This study assumes the recertifying expert uploads this documentation, and has incentives to upload this documentation, to the blockchain on a timely basis.

[29] For example, Honeywell Aerospace displays recertification documents for used parts on its GoDirect Trade blockchain as part of creating a marketplace for used airplane parts (Hyperledger 2020c).

- A live or recorded video, from a stationary camera or drone, showing the delivery of an asset to a specific location (Appelbaum and Nehmer 2020),
- A neutral third party observing and certifying the transfer (Campbell et al. 2018),
- For a geographically concentrated blockchain, live observation of the transfer by participants (Appelbaum and Nehmer 2020),
- The recipient scanning the asset's ID tag to acknowledge possession of the asset for a transfer (Christidis and Devetsikiotis 2016),
- A GPS device attached to the asset showing the asset arrived at a specific location for a transfer (Christidis and Devetsikiotis 2016).

Similar to asset creation, it is necessary to consider how a verifying party/device submits evidence of transfer to the blockchain (i.e., directly or via an intermediary), and how a smart contract receives notice of a completed transfer.

Once the transfer has been verified and evidence of this event has been submitted to the blockchain, participants must validate the transfer. Similar to asset creation, this involves reviewing evidence of the transfer and determining whether it validates the event. Once again, it remains important to consider the forms of evidence participants may use to validate the transfer of different types of tangible assets, and how a blockchain enforces requirements for specific evidence. Finally, also consider the consensus required to record a transfer (per the charter) and how the relevant smart contract enforces this consensus before it transfers the NFT.

Smart Contract Assisted Transfer

As mentioned, a smart contract likely acts as an escrow service to assist in asset transfers. Here, the seller sends the respective NFT to the smart contract, and the buyer sends payment to the smart contract. Once participants verify and validate the transfer (as previously described), the smart contract releases the NFT to the buyer and payment to the seller. Here, it is necessary to consider how the smart contract is set up to collect sufficient payment from the buyer and the correct NFT from the seller. Furthermore, the trigger event used to release the payment and NFT should be subject to verification and validation by participants. Finally, consider when this trigger event must happen (i.e., does the smart contract remain active indefinitely), and if not by a specified date/time, whether the escrowed payment and NFT are returned to the original owners.

Level of adherence to the following control objectives can help reveal the extent to which risks are mitigated in Stage Three, Asset Transfer. Specific control activities to achieve these objectives will vary based on the unique blockchain implementation:

- ***Control Objective #3.1*** *– Controls provide reasonable assurance that longer-lived tangible assets that are prone to deterioration are recertified (quality/condition) by an expert when the asset experiences a significant change and/or prior to a transfer/sale of the asset, and this recertification is attached to the respective non-fungible token.*

- ***Control Objective #3.2*** *– Controls provide reasonable assurance that if an expert is recertifying the quality/condition of a tangible asset and determines that the tangible asset should be retired, this status is attached to the respective non-fungible token and/or the token is burned.*

- ***Control Objective #3.3*** *– Controls provide reasonable assurance that only authorized network participants or oracles (1) verify the transfer of a tangible asset and (2) submit evidence of this event to the smart contract used to transfer the asset's non-fungible token.*

- ***Control Objective #3.4*** *– Controls provide reasonable assurance that network participants validate the transfer of a tangible asset using approved forms of evidence.*

- ***Control Objective #3.5*** *– Controls provide reasonable assurance that network participants must reach the required level of consensus on a tangible asset's transfer before the smart contract will transfer the asset's non-fungible token.*

- ***Control Objective #3.6*** *– Controls provide reasonable assurance that the smart contract used to enable the transfer is configured to simultaneously release the payment and non-fungible token when the required conditions are met. Otherwise, the payment and non-fungible token are returned to their original owners.*

See the appendix for the framework that maps these control objectives to risk considerations, and Figures 2 and 3 for an example of a tangible asset moving through Stage Three, Asset Transfer.

[Insert Figure 2 about here]

[Insert Figure 3 about here]

Stage Four – Asset Retirement

Asset retirements identified as part of a recertification process were discussed in Stage Three, Asset Transfer, but there will also be instances in which an asset should be retired outside of a formal recertification event. While asset owners should take responsibility for changing the status of an asset to retired on a blockchain, they might also have a motive to avoid declaring this status because it is a signal that an asset no longer has value in an exchange. As such, retirement processes should specify how often to evaluate an asset for potential retirement, how owners make retirement records available on a blockchain, how to attach a retirement record/status to an NFT, and whether/how to burn an NFT upon retirement.

Level of adherence to the following control objective can help reveal the extent to which risks are mitigated in Stage Four, Asset Retirement. Specific control activities to achieve this objective will vary based on the unique blockchain implementation:

- ***Control Objective #4.1*** *– Controls provide reasonable assurance that if a tangible asset has reached the point of retirement outside of a transfer or recertification event, this status is attached to the respective non-fungible token and/or the token is burned.*

See the appendix for the framework that maps this control objective to risk considerations.

IV. RESEARCH OPPORTUNITIES

Several research opportunities emerge from issues examined in this study:

1. *What should be considered sufficient evidence to validate the creation or sale/transfer of a tangible asset?*

   Researchers familiar with the auditing profession have an opportunity to study the evidence necessary to validate the creation or sale/transfer of a tangible asset, knowing that blockchains will likely be subject to audits and auditing standards (e.g., PCAOB Auditing Standard No. 1105, *Audit Evidence*). One way to approach this issue might be to study the objectivity/neutrality of different observation methods (i.e., a device is more objective/neutral than a human observer) and rank the desirability of available methods. Such a study would need to consider the risk that devices used to witness these events are prone to attacks from bad actors (e.g., cyberattacks), and could examine the impact of requiring multiple forms of evidence (e.g., human and device witnesses) to validate transactions.

2. *Should permissioned blockchains include a segregation of specific duties?*

   Internal control environments should include a segregation of duties (SoDs), and require specific separations between those with the ability to authorize transactions, record transactions, and maintain custody of the underlying assets (Turner, Weickgenannt, and Copeland 2016). With public and permissionless blockchains (e.g., Bitcoin and Ethereum), participants do not need to trust one another in order to trust the underlying repository, and any user is free to submit new transactions, verify/validate transactions, vote in the consensus to approve new transactions, and maintain a copy of the repository. Here, a participant can have all three duties that are often intentionally kept separate, as the blockchains are large enough that a single participant could not submit a fraudulent transaction and then have meaningful influence on recording the transaction or custody of the related asset (due to widespread validation and consensus). In contrast, permissioned consortium blockchains have fewer participants, meaning individual actions have more influence on the appropriateness of recorded transactions. With consortium blockchain SoDs, researchers can study the appropriateness of (1) the abilities maintained by individual participants within a member organization, as well as (2) the abilities maintained across participants from the same member organization (i.e., a member organization's collective abilities). Such a study can inform which duties should be kept separate at both a participant and member organization level (e.g., the ability to submit a transaction, but then not validate it nor participate in its consensus vote). This study could also reveal whether a lack of SoDs in blockchain consortia presents a meaningful risk to the reliability of the underlying repository.

3. *How will discrepancies between the physical world and blockchain repository be resolved?*

In discussing the consortium's charter, this study calls for a process to resolve discrepancies between the physical world (i.e., possession of a tangible asset) and blockchain (i.e., control of an asset's NFT). However, it remains unclear how this resolution process should be defined. For example, should the party in physical possession be required to deliver an asset to the owner of record per blockchain, or should the owner per blockchain be required to send the NFT to the party in possession of the tangible asset? If the owner per blockchain refuses to release the NFT, should certain participants be allowed to force this transaction, or does that level of centralized power go against the very purpose of having a blockchain in the first place? Further, who legally owns the asset when there are discrepancies, and what happens when these parties are in different countries with different laws?

4. *How should blockchain interface with downstream internal reporting systems?*

While this study focuses on maintaining reliable blockchain data, participants and/or member organizations will likely need to incorporate this data into downstream internal reporting systems (Sheldon 2019). Currently, no widespread agreement exists on how to extract, transform, and load blockchain data to other reporting systems, making this area ripe for future research. One solution involves manually accessing assets/balances in a digital wallet (or by using a block explorer), copying and transforming this data, then loading it to the target system. Another solution involves using a smart contract or decentralized application (Dapp) to collect details on specific assets/balances in a format that can be easily extracted, transformed, and then loaded elsewhere. A robotic process automation (RPA) task could also be used to extract specific data, transform it, then automatically load it to target systems. Finally, an application programming interface (API) could be developed specific to the consortium blockchain and downstream internal reporting system. With any of these solutions, controls must be in place to ensure data remain complete and accurate.

5. *What are immediate challenges for assets that are processed, assembled, or divisible?*

When combining component parts that each have an NFT, a smart contract can burn the component NFTs and mint a new NFT to represent an assembled asset. However, current NFT standards (i.e., those available for the Ethereum blockchain, such as ERC-721) do not work in the reverse direction, and thus NFTs are not designed to allow an assembled asset's NFT to be disassembled back into its component NFTs (Ethereum Foundation 2022).[30] Ways to disassemble an asset's NFT back into its component NFTs represents an area for future examination and collaboration among researchers and practitioners. One solution to this issue might be to not burn the component NFTs but rather attach them to the newly assembled

[30] Still, participants can view the record of a smart contract minting the assembled asset's NFT, which should show the component NFTs burned in the process.

NFT, which then maintains control over the component NFTs. This way, should a component need to be removed (e.g., selling a salvageable engine from an otherwise destroyed car), the owner of the assembled NFT could remove the component NFT and transfer it to a new owner. In doing so, the provenance of a component NFT would remain intact and show any instances in which it was attached to, or removed from, an assembled NFT.

As a related issue, some assets undergo processing before reaching an intended form. For example, minerals might be processed into metals, while cattle might be divided into various cuts of beef. Future research can address when various assets are at a viable point to be tracked with an NFT and who should create the NFT. In doing so, it will be important to consider whether the party that creates the NFT has incentives to record the asset's provenance correctly (e.g., the counterfeit fish market), and whether the blockchain is set up to provide an audit trail to investigate any instances of fraud or tampering.

6. *What are possible next steps in evaluating blockchain for assurance/attestation purposes?*

Relying on a consortium's permissioned blockchain involves relying on multiple participants to consistently apply agreed-upon policies and procedures (as defined in the consortium's charter). Current auditing standards from both the American Institute of Certified Public Accountants (AICPA) and Public Company Accounting Oversight Board (PCAOB) do not address this level of inter-company dependence, and instead focus largely on intra-company risks and controls.[31] Today, a firm that relies on another firm's processes often obtains a system and organization control (SOC) report, which is the output of a specific type of engagement performed under the AICPA's Attestation Standards. SOC

[31] In fact, Appelbaum, Cohen, Kinory, and Stein Smith (2022) suggest that an impediment to blockchain adoption is a lack of specific rules or guidance from parties like the Financial Accounting Standards Board (FASB), Securities and Exchange Commission (SEC), PCAOB, and AICPA.

reports have evolved to address emerging issues in the audit/attest space. For example, the AICPA recently released a SOC for Cybersecurity engagement (AICPA 2022a), which can be augmented by the AICPA's Trust Services Criteria (i.e., security, availability, processing integrity, confidentiality, and privacy) to provide a more wholistic evaluation of a firm's IT environment. The AICPA also recently released a SOC for Supply Chain engagement (AICPA 2022b), which provides a mechanism for interdependent firms to communicate risks and controls that might impact other supply chain members and stakeholders. This study provides the foundation for a SOC-like engagement specific to tracking tangible assets with blockchain that can also be augmented by existing frameworks (e.g., the AICPA's Trust Services Criteria) and/or used as a reporting mechanism for multiple interdependent firms (e.g., SOC for Supply Chain). If consortium blockchains like the one in this study follow a SOC-like attestation path, research will need to address how many (or which) consortium participants must receive such an evaluation before the entire blockchain can be relied upon from an audit standard setter perspective (i.e., the AICPA and PCAOB).

7. *What are potential scaling issues with a permissioned blockchain used to track tangible assets?*

A permissioned blockchain like the one described in this study could quickly expand and encounter scaling issues, making it difficult to manage and maintain. As more assets are tracked and more parties participate, one possible solution is to create side chains to track unique assets. Here, pre-determined parties could act as full-nodes and access administrators to validate transactions and ensure access is only granted to parties with verified and authorized identities. Access administrators could also ensure each participant only creates one account to help prevent any single user from moving assets within their own accounts to create an artificial market for an asset. Each side chain could track and manage a specific asset, which includes components that ultimately become part of a larger assembled asset on a higher-level blockchain. For instance, a blockchain used to track the provenance of ACME truck engines might include side chains for component parts such as valves and pistons, thus providing a more manageable mechanism to track the various parts and parties involved. In doing so, each side chain would need to address the risks outlined in this study. Researchers can consider the implications of scaling issues with a permissioned blockchain like the one described in this study, and further evaluate the potential use of side chains as a viable solution.[32]

V. CONCLUSION

This study examined the use of blockchain to track the ownership and provenance of tangible assets through four stages, including (1) design and governance of a blockchain, (2) asset creation, (3) asset transfer, and (4) asset retirement. In doing so, the study proposes a framework of risks and control objectives to evaluate the reliability of a permissioned blockchain used by a consortium to track tangible assets. Here, reliability should increase when a consortium addresses more of the identified risks and implements controls to achieve the proposed control objectives. Finally, the study concluded by suggesting research opportunities related to the use of blockchain to track tangible assets, including (1) what evidence blockchain participants need to validate the creation or sale/transfer of a tangible asset, (2) are segregation of duties necessary on permissioned blockchains, (3) what happens when blockchain and the physical world are not in agreement, (4) how should blockchain interface with downstream reporting systems, (5) what are

[32] I thank an anonymous reviewer for suggesting the use of side chains to address scaling issues.

immediate challenges for assets that are either assembled or divisible, (6) what are possible next steps in evaluating blockchain for assurance/attestation purposes, and (7) what are potential scaling issues with a permissioned blockchain used to track tangible assets.

The processes, risks, and control objectives discussed in this study can be used as a guide to evaluate the reliability of a consortium's permissioned blockchain to track the ownership and provenance of tangible assets. By design, these blockchains are tailored to meet specific needs of a consortium, and as such, many variations of these blockchains will ultimately exist, thus making it impractical to develop an overly specific framework for their evaluation. Still, the processes, risks, and control objectives presented herein should apply across most variants of these blockchains and the various types of tangible assets they would be used to track. Unique scenarios will emerge and asset tracking technologies will evolve, but the topics addressed should remain applicable as a baseline for evaluation purposes.

This study is subject to several limitations. To begin, it does not demonstrate or evaluate the framework in a live setting (i.e., Phases 4 and 5 of the DSRM). Further, there is limited information available on how current blockchains accomplish tangible asset tracking, and emerging details might change how specific components of the presented process work. Next, this study only speaks to a few types of asset ID tags and IoT devices, and acknowledges that these are entire fields of study in their own right. Future research can consider a broader range of ID tags and IoT devices, and how these might help address open issues or concerns. Finally, this study focuses on tangible assets that are directly attached to an ID tag, as risk of separation increases when tags are attached to packaging or shipping containers. Future research can examine ways to mitigate risks of separation.

REFERENCES

American Institute of Certified Public Accountants (AICPA). 2022a. *SOC for Cybersecurity*. Available at: https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative (last accessed January 2022).

American Institute of Certified Public Accountants (AICPA). 2022b. *SOC for Supply Chain*. Available at: https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/soc-for-supply-chain (last accessed January 2022).

American Institute of Certified Public Accountants (AIPCA) and the Chartered Professional Accountants of Canada (CPA Canada). 2017. *Blockchain technology and its potential impact on the audit and assurance profession*. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf (last accessed May 2020).

Appelbaum, D., and R. A. Nehmer. 2017. Using drones in internal and external audits: An exploratory framework. *Journal of Emerging Technologies in Accounting* 14 (1): 99-113.

Appelbaum, D., and R. A. Nehmer. 2020. Auditing cloud-based blockchain accounting systems. *Journal of Information Systems* 34 (2): 5-21.

Appelbaum, D., E. Cohen, E. Kinory, and S. Stein Smith. 2022. Impediments to blockchain adoption. *Journal of Emerging Technologies in Accounting*. Forthcoming.

Austin, S. 2020. *Blockchain asset tracking: A growing number of opportunities*. Available at: https://www.everledger.io/blockchain-asset-tracking-a-growing-number-of-opportunities/ (last accessed July 2020).

Bakos, Y., H. Halaburda, and C. Mueller-Bloch. 2021. When permissioned blockchains deliver more decentralization than permissionless. *Communications of the ACM* 64 (2): 20-22.

Baum, H. (n.d.). *Bar, QR, and RFID Codes, Oh My!!*. Available at: https://www.uc.edu/content/dam/uc/ce/docs/OLLI/Page%20Content/PRODUCT%20IDENTIFICATION%20CODES%20BAR%20QR.pdf (last accessed March 2022).

Campbell, R., A. Omietański, and K. Southwell. 2018. *Digitalising the Mining & Metals Global Supply Chain: Rise of Blockchain and the Smart Contract.* White & Case, London.

Casey, M., and P. Vigna. 2018. *The Truth Machine: The Blockchain and the Future of Everything*. St. Martin's Press.

Christidis, K., and M. Devetsikiotis. 2016. Blockchains and smart contracts for the internet of things. *IEEE Access* 4: 2292-2303.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2020. *Blockchain and internal control: The COSO perspective*. Available at: https://www.coso.org/Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf (last accessed January 2022).

Cong, Y., H. Du, and M. A. Vasarhelyi. 2018. Technological disruption in accounting and auditing. *Journal of Emerging Technologies in Accounting* 15 (2): 1-10.

Coyne, J. G., and P. L. McMickle. 2017. Can blockchains serve an accounting purpose? *Journal of Emerging Technologies in Accounting* 14 (2): 101-111.

Dai, J., and M. A. Vasarhelyi. 2016. Imagineering Audit 4.0. *Journal of Emerging Technologies in Accounting* 13 (1): 1-15.

Dai, J., and M. A. Vasarhelyi. 2017. Toward blockchain-based accounting and assurance. *Journal of Information Systems* 31 (3): 5-21.

Dai, H. N., Z. Zheng, and Y. Zhang. 2019. Blockchain for internet of things: A survey. *IEEE Internet of Things Journal* 6 (5): 8076-8094.

De Poli, F. 2021. *Designing tokens for supply chain assets*. Proceedings from the 2021 EY Global Blockchain Summit, Virtual Conference.

Deloitte. 2019. *Deloitte's 2019 global blockchain survey: Blockchain gets down to business*. Available at: https://www2.deloitte.com/content/dam/insights/us/articles/2019-global-blockchain-survey/DI_2019-global-blockchain-survey.pdf (last accessed July 2020).

Drescher, D. 2017. *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress, New York.

Entriken, W., D. Shirley, J. Evans, and N. Sachs. 2018. *EIP-721: ERC-721 Non-Fungible Token Standard – Ethereum Improvement Proposals, no. 721*. (January). Available at: https://eips.ethereum.org/EIPS/eip-721 (last accessed April 2021).

Ernst & Young (EY). 2021. *What happens when government, industry and investors seek common digital ground? Withholding tax distributed ledger report: A look inside the testing of an innovative application of distributed ledger technology to solve a costly and decades-old tax problem*. Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/tax/tax-pdfs/ey-withholding-tax-distributed-ledger-report.pdf (last accessed August 2021).

Ethereum.org. 2021. *ERC-721 Non-Fungible Token Standard*. (April 11). Available at: https://ethereum.org/en/developers/docs/standards/tokens/erc-721/ (last accessed April 2021).

Ethereum Foundation. 2022. *Non-fungible tokens (NFTs)*. Available at: https://ethereum.org/en/nft/ (last accessed January 2022).

Geerts, G. L. 2011. A design science research methodology and its application to accounting information systems research. *International Journal of Accounting Information Systems* 12 (2): 142-151.

Hevner, A., S. T. March, J. Park, and S. Ram. 2004. Design science in information systems research. *MIS Quarterly* 28 (1): 75 – 105.

Higginson, M., M. Nadeau, and K. Rajgopal. 2019. *Blockchain's Occam problem*. Available at: https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem (last accessed May 2020).

Hoare, D. 2015. *Internal Controls – Fixed Assets*. (July 6). Available at: https://businessecon.org/internal-controls-fixed-assets/ (last accessed April 2021).

Hyperledger. 2020a. *Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric*. Available at: https://www.hyperledger.org/resources/case-studies (last accessed May 2020).

Hyperledger. 2020b. *Case Study: Circulor achieves first-ever-mine-to-manufacturer traceability of a conflict mineral with Hyperledger Fabric*. Available at: https://www.hyperledger.org/resources/case-studies (last accessed May 2020).

Hyperledger. 2020c. *Case Study: Honeywell Aerospace creates online parts marketplace with Hyperledger Fabric*. Available at: https://www.hyperledger.org/resources/case-studies (last accessed May 2020).

International Business Machines (IBM). 2019. *About IBM Food Trust*. Available at: www.ibm.com/food (last accessed May 2020).

International Organization of Standards (ISO). 2020. *ISO/IEC DIS 15944-21: Information technology – Business operational view – Part 21: Application of Open-edi business transaction ontology in distributed business transaction repositories*. Available at: https://standards.globalspec.com/std/14351378/iso-iec-dis-15944-21 (last accessed March 2022).

ISACA. 2019. *CISA Review Manual 27th Edition*. ISACA, Schaumburg, Illinois.

Lewis, A. 2018. *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers them*. Mango Publishing, Coral Gables, Florida.

Liu, M., K. Wu, and J. Xu. 2019. How will blockchain technology impact auditing and accounting: permissionless vs. permissioned blockchain. *Current Issues in Auditing* 13 (2): A19-A29.

McKinsey & Company. 2018. Blockchain explained: What it is and isn't, and why it matters. *The McKinsey Podcast*. Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-explained-what-it-is-and-isnt-and-why-it-matters (last accessed May 2020).

Nakamoto, S. 2008. *Bitcoin: A peer-to-peer electronic cash system*. Available at: https://bitcoin.org/bitcoin.pdf (last accessed May 2020).

National Institute of Standards and Technology (NIST). 2019. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. U.S. Department of Commerce. Washington, D.C.

Nehmer, R. A., and R. Srivastava. 2016. Using belief functions in software agents to test the strength of application controls: A software agent framework. *International Journal of Intelligent Information Technologies* 12 (3): 1-19.

Peffers, K., T. Tuunanen, M. A. Rothenberger, and S. Chatterjee. 2007. A design science research methodology for information systems research. *Journal of Management Information Systems* 24 (3): 45-77.

Rozario, A. M., and C. Thomas. 2019. Reengineering the audit with blockchain and smart contracts. *Journal of Emerging Technologies in Accounting* 16 (1): 21 – 35.

Sheldon, M. D. 2019. A primer for information technology general control considerations on a private and permissioned blockchain audit. *Current Issues in Auditing* 13 (1): A15 – A29.

Sheldon, M. D. 2021. Auditing the blockchain oracle problem. *Journal of Information Systems* 35 (1): 121-133.

Stein Smith, S., and J. Castonguay. 2020. Blockchain and accounting governance: Emerging issues and considerations for accounting and assurance professionals. *Journal of Emerging Technologies in Accounting* 17 (1): 119-131.

Stratopoulos, T., V. Wang, and H. Ye. 2021. Use of corporate disclosures to identify the stage of blockchain adoption. *Accounting Horizons*. Forthcoming.

Turner, L., A. Weickgenannt, and M. K. Copeland. 2016. *Accounting Information Systems: Controls and Processes (3rd Edition*). Wiley, USA.

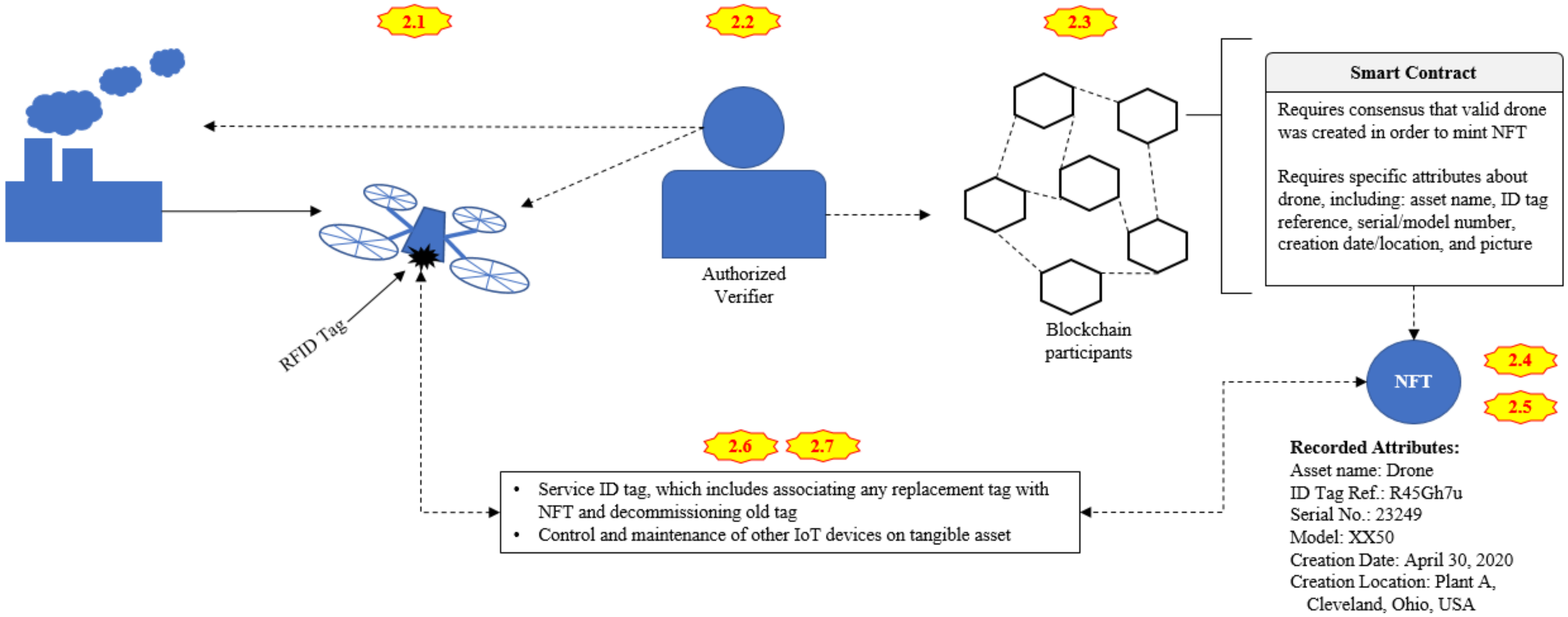
Warburg, B., B. Wagner, and T. Serres. 2019. *Basics of Blockchain: A Guide for Building Literacy in the Economics, Technology and Business of Blockchain*. Animal Ventures LLC, USA.

Table 1
Mapping of Design Science Research Methodology (Geerts 2011) to Current Study

DSRM Activities (Geerts 2011)	Activity Description (Current Study)	Knowledge Base (Current Study)
Problem identification and motivation	**Problem:** Blockchain can be used as the record of tangible asset ownership and provenance, but the extant research does not offer a framework to evaluate the extent to which blockchain serves as a reliable repository for tracking tangible assets. **Motivation:** Blockchain users might rely on incorrect information from a technology labeled a "truth machine" (Casey and Vigna 2018). However, a blockchain deemed reliable to track tangible assets can provide strong support for (1) an asset's origin and authenticity, (2) an owner's claim to the asset, and (3) key accounting documentation about an asset (e.g., purchase date and cost) (Hoare 2015).	Firms are investing in permissioned consortium blockchains (AICPA and CPA Canada 2017) and shifting their focus from cryptocurrencies to business applications (Stratopoulos, Wang, and Ye 2021), including the ability to track the ownership and provenance of tangible assets. Today, owners typically maintain the only record of an asset, and any subsequent buyer must trust that record (or exert their own effort to validate the seller's claims). Blockchain introduces the potential to provide a complete provenance of an asset that has been verified, validated, and agreed-upon by key stakeholders.
Define objectives of solution	The reliability of blockchain to serve as a record of tangible asset ownership and provenance can be solved/clarified by examining the process of tracking tangible assets with blockchain, then creating a framework of risks and control objectives relevant to each stage of the asset's life (i.e., creation, transfer, and retirement).	• Knowledge of blockchain functionality and limitations, as discussed in Section II, Background • Knowledge of a tangible asset's typical lifecycle, including its creation, transfer, and retirement • Knowledge of the role of control objectives to address risk, as informed by the AICPA's Attestation Standards, including AT-Cs 105, 205, and 320
Design and development	This study examines four stages of tracking tangible assets using blockchain, including (1) design and governance considerations, (2) asset creation, (3) asset transfer, and (4) asset retirement. The study then develops a framework of risk considerations and control objectives that can be used to evaluate the reliability of a blockchain to track the ownership and provenance of tangible assets.	Same as described in the "Define objectives of solution" phase
Demonstration	This study does not provide a demonstration of its framework in a live environment.	
Evaluation	This study does not evaluate its framework in a live environment. However, a Big-4 practitioner working on that firm's blockchain product provided suggestions on ways to improve the framework, which are incorporated in the final version. Key open issues with the framework also appear in Section IV, Research Opportunities.	
Communication	Writing this study accomplishes communication.	The ways in which this study is informed by, and extends, recent research on blockchain in the accounting domain appears in Section II, Background.

Figure 1
Example of Stage Two, Asset Creation*

Create tangible asset	Attach tangible asset to ID tag	Verify creation and submit supporting evidence to blockchain	Review evidence to determine if creation is valid	Mint tangible asset's NFT and assign required attributes



Smart Contract

Requires consensus that valid drone was created in order to mint NFT

Requires specific attributes about drone, including: asset name, ID tag reference, serial/model number, creation date/location, and picture

- Service ID tag, which includes associating any replacement tag with NFT and decommissioning old tag
- Control and maintenance of other IoT devices on tangible asset

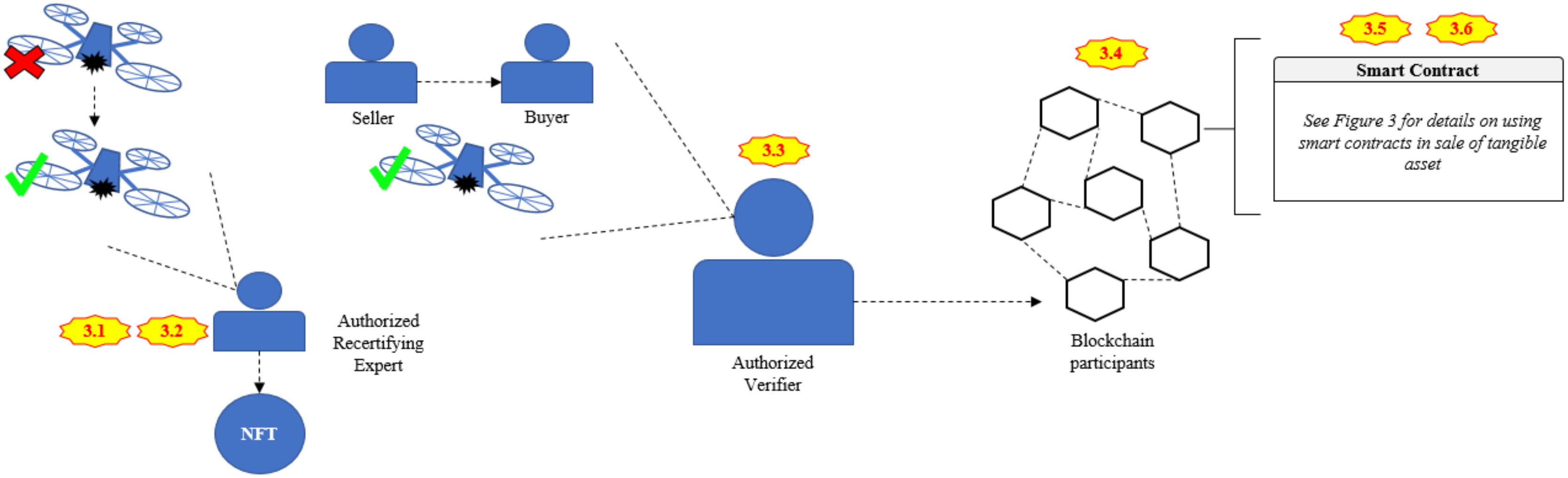
Recorded Attributes:
Asset name: Drone
ID Tag Ref.: R45Gh7u
Serial No.: 23249
Model: XX50
Creation Date: April 30, 2020
Creation Location: Plant A,
Cleveland, Ohio, USA

Assume a drone manufacturer produces a new unit. Upon completion the manufacturer attaches an RFID tag to the drone that records the official product name, serial number, model, and RFID tag reference. An authorized neutral party observes (verifies) the drone being built at a specific production facility, scans the RFID tag to collect product details, submits evidence about the creation and product details to the blockchain, and specifies the smart contract being used to mint the drone's NFT. Blockchain participants then review the provider and submitted evidence to determine whether the creation is valid (per the consortium charter). Once reaching consensus on a valid creation, the specified smart contract mints the drone's NFT and assigns it key details about the drone (e.g., RFID tag reference, serial number, and creation date). Finally, the RFID tag and other devices used to track and monitor the drone are regularly serviced.

* Numbers appearing in 10-point stars are control objectives (as defined in the study and listed in the appendix) that relate to the associated part of the asset creation stage.

Figure 2
Example of Stage Three, Asset Transfer*

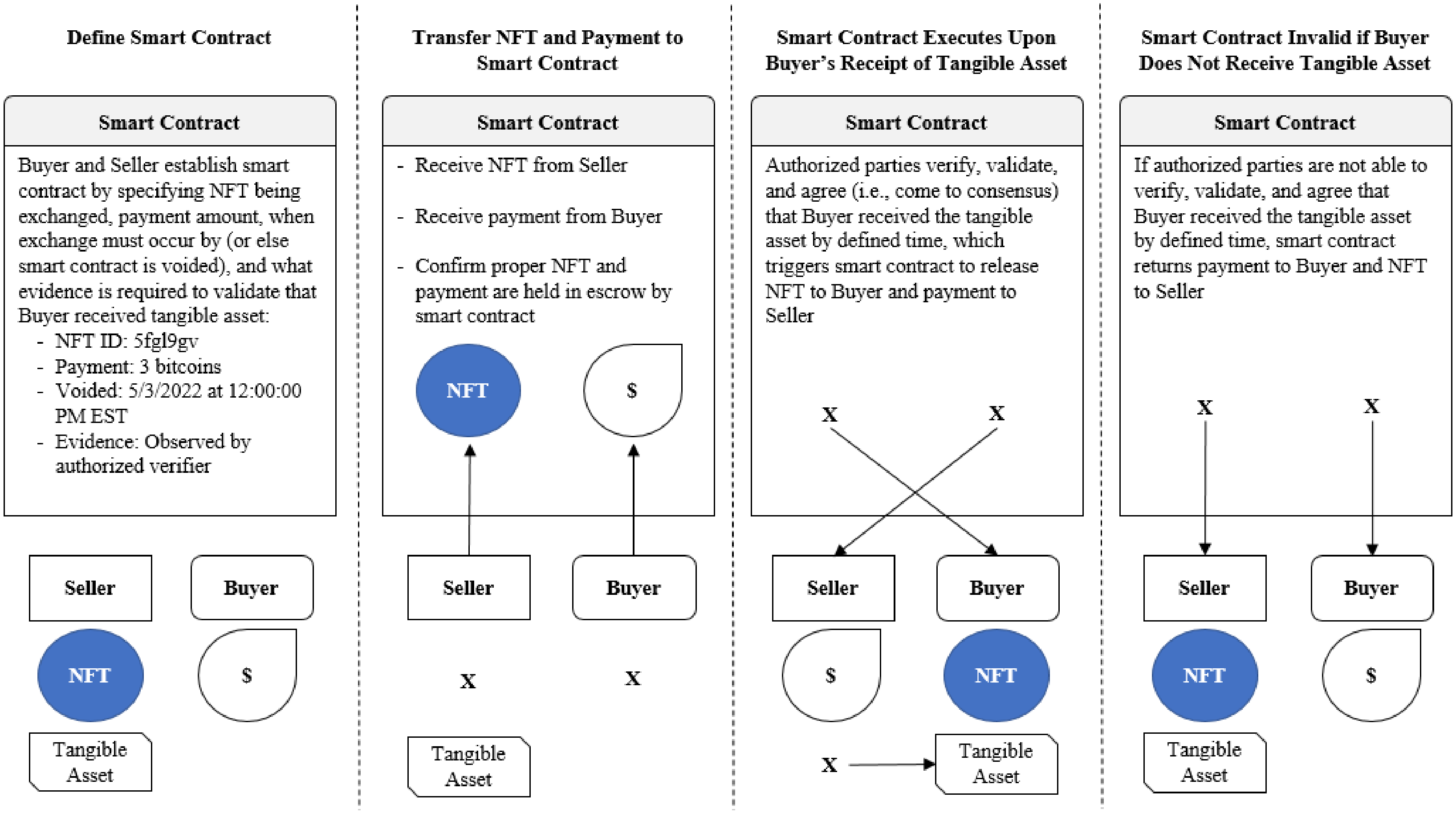
Recertify tangible asset following significant change and/or prior to transfer/sale; attach to NFT	Transfer tangible asset to new owner	Verify transfer and submit supporting evidence to blockchain	Review evidence to determine if transfer is valid	Transfer ownership of NFT to buyer and payment to seller


Seller
Buyer
3.5
3.6
3.4
Smart Contract
See Figure 3 for details on using smart contracts in sale of tangible asset
3.3
3.1
3.2
Authorized Recertifying Expert
Authorized Verifier
Blockchain participants
NFT

Assume the drone from Figure 1 is sold to a new owner. Prior to the sale, an authorized expert (per the consortium charter) recertifies the quality/condition of the drone and attaches this recertification to the respective NFT. An authorized neutral party then observes (verifies) the physical transfer of the drone, submits evidence about the transfer to the blockchain, and specifies the smart contract being used to transfer the drone's NFT. Blockchain participants then review the provider and submitted evidence to determine whether the transfer is valid (per the consortium charter). Once reaching consensus on a valid transfer, the specified smart contract releases the NFT to the buyer and payment to the seller (see Figure 3 for further smart contract details).

* Numbers appearing in 10-point stars are control objectives (as defined in the study and listed in the Appendix) that relate to the associated part of the asset transfer stage.

Figure 3
Detail on Use of Smart Contract in Sale of Tangible Asset



Define Smart Contract

Smart Contract

Buyer and Seller establish smart contract by specifying NFT being exchanged, payment amount, when exchange must occur by (or else smart contract is voided), and what evidence is required to validate that Buyer received tangible asset:

- NFT ID: 5fgl9gv
- Payment: 3 bitcoins
- Voided: 5/3/2022 at 12:00:00 PM EST
- Evidence: Observed by authorized verifier

Transfer NFT and Payment to Smart Contract

Smart Contract

- Receive NFT from Seller
- Receive payment from Buyer
- Confirm proper NFT and payment are held in escrow by smart contract

Smart Contract Executes Upon Buyer's Receipt of Tangible Asset

Smart Contract

Authorized parties verify, validate, and agree (i.e., come to consensus) that Buyer received the tangible asset by defined time, which triggers smart contract to release NFT to Buyer and payment to Seller

Smart Contract Invalid if Buyer Does Not Receive Tangible Asset

Smart Contract

If authorized parties are not able to verify, validate, and agree that Buyer received the tangible asset by defined time, smart contract returns payment to Buyer and NFT to Seller

Note that in either outcome (i.e., two events on the furthest right), both the tangible asset and its NFT reside with a single owner.

APPENDIX

Summary of Control Objectives and Risks Considerations when using Blockchain to Track Tangible Assets[1]

CO #	Control Objective Description *(Controls provide reasonable assurance that…)*	Risk Considerations
Stage One – Design and Governance Considerations		
1.1	… the consortium has a charter in place that is agreed to by all original and subsequent network participants and member organizations. The charter should address technical details about the blockchain and any relevant processes used to support blockchain operations.	As part of initiating a blockchain consortium, the originating member organizations should develop and agree to a charter that includes key technical details about the blockchain and the processes used to support the operation of the blockchain. Any subsequent member organizations should also be required to adhere to the charter. For purposes of this study, the most relevant technical details and processes to define in the charter include: Technical Details: - What types of permissioned access rights exist on the blockchain (e.g., verify the occurrence of events/transactions, submit transactions, validate transactions and participate in the consensus to add transactions to the repository, and/or maintain a copy of the blockchain repository)? - Which network participants may possess certain permissioned access rights (or combinations of permissioned access rights)? - Which oracles are allowed to provide the blockchain with exogenous data (or what are the criteria for selecting an oracle)? - What are the acceptable forms of evidence to verify and validate the creation/transfer/retirement of a tangible asset? - What is the minimum level of consensus required to record events/transactions to the blockchain repository? - What attributes must be assigned to each non-fungible token used to represent a tangible asset (e.g., asset name, asset identification tag, serial/model number, creation date, creation location, picture, etc.)? - Which attributes of a non-fungible token are visible to network participants and which attributes remain private to specific parties? - What data standards must be followed when assigning/attaching information to non-fungible tokens (i.e., for interoperability purposes)? Supporting Processes: - What is the process to provision permissioned access rights (i.e., request, approve, and implement), and who has the authority to request, approve, and/or implement these access rights? - What is the process to design, test, and implement smart contracts? Who has the authority to approve and deploy new smart contracts? - What is the process to retire smart contracts that are no longer used/relevant? - When should smart contracts be audited, how should they be audited, and who may perform these audits? - What is the process to recertify the quality/condition of a tangible asset and attach this recertification to the respective non-fungible token (including who is allowed to perform recertifications for different assets)? Note that recertification can be performed as part of a periodic valuation assessment of the asset, when there is a major change to the asset, and/or when the asset is about to be transferred/sold. Additional considerations include: • How is the recertification expert identified (and agreed to by the seller and buyer if recertification is part of a transfer/sale)? • Is the recertification performed by an expert that is credentialed to perform the task? • What happens if the owner/seller/buyer disagrees with the expert's conclusion that the asset qualifies as recertified? - What is the process to resolve discrepancies between the physical world (i.e., who possesses the tangible asset) and the blockchain (e.g., who controls the tangible asset's non-fungible token)? - What is the process to amend the original consortium charter, including how many member organizations must approve such changes?
1.2	… the (level of) permissioned access granted to network participants remains appropriate.	Permissioned abilities should be reviewed for reasonableness, while also considering the processes implemented to address: - How the permissioned access rights of new network participants are authorized and granted - How changes to permissioned access rights for existing network participants are authorized and granted/removed - How the permissioned access rights of terminated network participants are removed Following risks/practices should be considered: - Is there a concentration of higher-power permissioned access (e.g., voting in the consensus) shared among too few network participants?

		- Do network participants maintain higher-power permissioned access than necessary to perform a role (e.g., it might not be appropriate for network participants that provide certification records to vote in the consensus)? - Should network participants with permissioned access to verify the creation or sale/transfer of a tangible asset be restricted from other permissions, such as submitting this transaction to the blockchain or participating in its consensus vote? - Should network participants with permissioned access to validate the creation or sale/transfer of a tangible asset (i.e., participate in its consensus vote) be restricted from other permissions, such as submitting this transaction to the blockchain or verifying the transaction?
1.3	… smart contracts deployed to the blockchain are subject to a formal design, development, testing, approval, and release process.	Smart contracts may be used for critical events on the blockchain, such as minting non-fungible tokens and acting as an escrow agent that holds the buyer's and seller's assets as part of an exchange agreement. Once deployed, smart contracts are difficult to modify, and once executed, the resulting movement of assets is nearly irreversible. As such, any smart contract deployed on the consortium blockchain should be subject to a robust design, development, testing, approval, and release process. This applies whether the smart contact will be used for a single event such as a sale, or used for many events such as the minting of non-fungible tokens.
1.4	… smart contracts are retired/blocked when they are no longer applicable to the consortium's operations.	As operations change, it is likely that legacy smart contracts will need to be replaced by new smart contracts that are more tailored to the current environment. By calling smart contracts that are no longer relevant, users are exposed to the risk that the smart contract does not adhere to current regulatory/contractual agreements and that assets might be transferred to an unintended party. As such, there should be a process in place to either block smart contracts that are no longer relevant or to maintain a listing of smart contract addresses that should no longer be called.
Stage Two – Asset Creation		
2.1	… when a tangible asset is created, it is attached to a secure asset identification tag that uniquely identifies the tangible asset.	- Considering the need to uniquely identify the asset, is an appropriate asset identification tag used to convey the information stored on the tag (e.g., barcode, QR code, RFID/near-field communication tag)? - Has the asset identification tag been attached to the asset in a way that it cannot be inappropriately removed (or would such tampering be evident and flagged)? - What safeguards have been implemented to ensure the data stored/presented on the asset identification tag cannot be inappropriately modified or copied and placed on another asset identification tag (e.g., spoofing an RFID tag)?
2.2	… only authorized network participants or oracles (1) verify the creation of a tangible asset and (2) submit evidence of this event to the smart contract used to mint the asset's non-fungible token.	- Which network participants and oracles are authorized to verify the creation of a tangible asset and submit evidence of its creation? - How is the creation of the tangible asset observed, and is this persuasive in the unique circumstances? Evidence of this observation might include one or more of the following: • A live or recorded video of the creation • A neutral third party observing the creation • Live observation of the creation by network participants - How is this observation communicated to the blockchain (i.e., does the device used to observe the transaction interface directly with a blockchain node, or does the observation get communicated through an intermediary that should also be evaluated for security purposes)? - Are the devices used to observe the transaction protected from unauthorized access or use (i.e., physical access to the device and logical access to its data and software)? - How do the smart contract parties ensure that details of the physical creation are routed to the correct smart contract?
2.3	… network participants validate the creation of a tangible asset using approved forms of evidence.	- What forms of evidence submitted to the blockchain are network participants allowed to use in order to validate the creation of different types of tangible assets? - How are network participants forced to use approved forms of evidence in order to validate the creation of a tangible asset?
2.4	… network participants must reach the required level of consensus on the tangible asset's creation before the smart contract will mint the asset's non-fungible token.	- Given the number of network participants that vote in the consensus and the type(s) of evidence required to validate the creation of the tangible asset, it would be appropriate to revisit: • Is a lower-level of required consensus offset by requiring higher quality and/or more objective forms of evidence? • Are lower-quality and/or less objective forms of evidence (as used in validation) offset by requiring higher levels of consensus? - How does the smart contract that mints the asset's non-fungible token enforce the required level of consensus (as defined in the charter) among authorized network participants that the tangible asset has been created before minting the non-fungible token? • Any failure to enforce this consensus could result in the minting of unauthorized non-fungible tokens.

2.5	… the smart contract accurately assigns all required attributes to the non-fungible token upon its minting (e.g., asset name, identification tag number/reference, serial/model number, creation date/location, and picture).	- What attributes about the tangible asset does the smart contract require prior to minting its non-fungible token? For example: • Asset name • Asset identification tag reference • Serial/model number • Creation date/location • Picture of the asset - How does the smart contract ensure that the required attributes are accurately recorded and assigned to the non-fungible token? - Details about the tangible asset's inception will be more prone to error or inaccuracies the longer it takes to assign these attributes to the non-fungible token, potentially leading to challenges in defending the asset's authenticity at a later point in time. - In certain situations, it might be appropriate to obtain records of licenses, inspections, and/or certification of the manufacturing plant or other origin of the asset to further demonstrate the authenticity of the asset (and attach these records to the respective non-fungible token). • What party is responsible for submitting these licenses/inspections/certifications to the blockchain (or is responsible for making this information available to authorized network participants upon request)? • How are any licenses/inspections/certifications attached to the specific non-fungible token?
2.6	… the asset identification tag is serviced regularly. If the tag must be replaced, the legacy tag is decommissioned and the new tag is associated with the respective non-fungible token.	- How long is the asset identification tag expected to be in service as compared to the expected useful life of the tangible asset? - What procedures have been implemented to ensure the asset identification tag is routinely serviced before it becomes unreadable due to damage or loss of power (i.e., if the tag is active and has its own power source)? - What procedures are in place to replace the asset identification tag if it becomes unreadable, and how will the new tag be associated with the respective non-fungible token? - What are the procedures in place to retire the legacy tag, such that it is completely decommissioned (i.e., so it does not later send out signals after being replaced)?
2.7	… IoT devices used to track tangible assets adhere to the same controls as asset identification tags, and also maintain secure network connectivity, data storage, and configurations.	Internet-of-Things (IoT) devices used to track different aspects of the tangible asset (e.g., location, orientation, and surrounding temperature/humidity) should adhere to the same considerations as provided in Control Objectives 2.1 and 2.6. Furthermore, the following risks/practices should also be considered: - For IoT devices with network interface capabilities, what safeguards have been implemented to protect the device from the risks and threats faced by other internet-connected devices (e.g., cyberattacks, loss of control of the device, unauthorized changes to stored data)? - How have IoT devices been configured to capture the intended occurrence? - What measures have been taken to ensure the IoT device stores data securely? - How does the IoT device transmit collected information completely and accurately to an intermediary device or directly to the blockchain?
Stage Three – Asset Transfer		
3.1	… longer-lived tangible assets that are prone to deterioration are recertified (quality/condition) by an expert when the asset experiences a significant change and/or prior to a transfer/sale of the asset, and this recertification is attached to the respective non-fungible token.	- Is there a recertification of the longer-lived tangible asset when a significant change is made to the asset and/or prior to any sale/transfer of the asset in accordance with the consortium's charter? - What party is responsible for uploading the recertification record to the blockchain (or is responsible for making the recertification available to authorized network participants upon request)? - How is this recertification record/status attached to the respective non-fungible token?
3.2	… if an expert is recertifying the quality/condition of a tangible asset and determines that the tangible asset should be retired, this status is attached to the respective non-fungible token and/or the token is burned.	- What party is responsible for uploading the retirement record to the blockchain (or is responsible for making the retirement record available to authorized network participants upon request)? - How is this retirement record/status attached to the respective non-fungible token, and does this burn (i.e., destroy) the non-fungible token? - If the expert determines that the asset should be retired, is this status submitted to the smart contract used to facilitate the exchange and thus trigger the return of the payment and the non-fungible token to their original owners (and possibly burn the non-fungible token in the process)?

3.3	… only authorized network participants or oracles (1) verify the transfer of a tangible asset and (2) submit evidence of this event to the smart contract used to transfer the asset's non-fungible token.	- Which network participants and oracles are authorized to verify the transfer of a tangible asset and submit evidence of its transfer? - How is the transfer of the tangible asset observed, and is this persuasive in the unique circumstances? Evidence of this observation might include one or more of the following: • A live or recorded video showing the delivery of the tangible asset to a specific location/party • A neutral third party observing the sale/transfer • Live observation of the sale/transfer by network participants • The recipient scanning the asset's ID tag to acknowledge possession • A GPS device attached to the tangible asset showing it arrived at a specific location - How is this observation communicated to the blockchain (i.e., does the device used to observe the transaction interface directly with a blockchain node, or does the observation get communicated through an intermediary that should also be evaluated for security purposes)? - Are the devices used to observe the transaction protected from unauthorized access or use (i.e., physical access to the device and logical access to its data and software)? - How do the smart contract parties ensure that the results of the physical transfer are routed to the correct smart contract?
3.4	… network participants validate the transfer of a tangible asset using approved forms of evidence.	- What forms of evidence submitted to the blockchain are network participants allowed to use in order to validate the transfer of different types of tangible assets? - How are network participants forced to use approved forms of evidence in order to validate the transfer of a tangible asset?
3.5	… network participants must reach the required level of consensus on a tangible asset's transfer before the smart contract will transfer the asset's non-fungible token.	- Given the number of network participants that vote in the consensus and the type(s) of evidence required to validate the transfer of the tangible asset, it would be appropriate to revisit: • Is a lower-level of required consensus offset by requiring higher quality and/or more objective forms of evidence? • Are lower-quality and/or less objective forms of evidence (as used in validation) offset by requiring higher levels of consensus? - How does the smart contract that transfers the asset's non-fungible token enforce the required level of consensus (as defined in the charter) among authorized network participants that the tangible asset has been transferred before releasing the non-fungible token? • Any failure to enforce this consensus could result in the unauthorized transfer of non-fungible tokens.
3.6	… the smart contract used to enable the transfer is configured to simultaneously release the payment and non-fungible token when the required conditions are met. Otherwise, the payment and non-fungible token are returned to their original owners.	- How is the smart contract set up to collect sufficient payment from the buyer and the correct non-fungible token from the seller? - What is the trigger event for the smart contract to release the payment to the seller and the non-fungible token to the buyer (see Control Objective 3.3 for evidence to determine whether this event happened)? - When does the trigger event need to happen by? • What happens to the payment and non-fungible token held in escrow if the trigger event does not occur (or is not reported to the smart contract) by this time?
Stage Four – Asset Retirement		
4.1	… if a tangible asset has reached the point of retirement outside of a transfer or recertification event, this status is attached to the respective non-fungible token and/or the token is burned.	- What processes are in place to determine whether the tangible asset should be retired? - How does the owner upload the retirement record to the blockchain (or make the retirement record available to authorized network participants upon request)? - How is this retirement record/status attached to the specific non-fungible token, and does this cause the non-fungible token to be burned (i.e., destroyed)?

[1] This table is structured in the format used by Sheldon (2021) for Table 1. The final framework benefited from feedback provided by a Big-4 practitioner who is currently working on designing and implementing that firm's blockchain product.

Note – Any references to "smart contracts" in the above Control Objectives and Risk Considerations should be considered interchangeable with "decentralized applications" (or Dapps), which are applications on a blockchain built by combining several smart contracts. Furthermore, all Control Objectives are novel to using a blockchain to track tangible assets, other than Control Objectives #2.1 and #2.7, which were included to more fully demonstrate how risks related to existing technologies/processes need to be addressed when using blockchain in this manner.