SYM-AM-21-104

Excerpt from the Proceedings of the Eighteenth Annual Acquisition Research Symposium

Blockchain Mergence for Distributed Ledgers Supporting Fleet Logistics and Maintenance

May 11–13, 2021

Published: May 10, 2021

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

Blockchain Mergence for Distributed Ledgers Supporting Fleet Logistics and Maintenance

Britta Hale—is a Cryptographer and Assistant Professor in Computer Science at the Naval Postgraduate School. Hale has a PhD from the Norwegian University of Science and Technology and a Master of Science in Mathematics of Cryptography and Communications from Royal Holloway University of London. Specialization areas include cryptographic key exchange and authentication protocols, protocol self-healing, post-quantum hybrids, unmanned vehicle security, and secure channels within constrained settings. Hale is currently a member of the Message Layer Security working group of the Internet Engineering Task Force. [britta.hale@nps.edu]

Don Brutzman—is a Computer Scientist and Associate Professor of Applied Science working in the Modeling Virtual Environments Simulation Institute, Undersea Warfare Academic Group, and Information Sciences Department. He leads the Network Optional Warfare project, exploring fleet stealth using efficient messaging, optical signaling, semantic coherence, and ethical control of unmanned systems. His research interests include underwater robotics, real-time visualization using the Extensible 3D Graphics International Standard, artificial intelligence, and networking for distributed large-scale virtual environments. [brutzman@nps.edu]

Terry Norbraten—earned a Master of Science in Modeling, Virtual Environments and Simulation (MOVES) at the Naval Postgraduate School in 2004. Terry retired from active duty in the U.S. Navy in 2005 and has served as a Research Associate with the MOVES Institute by instructing in the Java and JavaScript programming languages and working on various software projects involving stand-alone and web-based scenario generation, discrete event simulation, and training and analysis for fleet and field requirements. [tdnorbra@nps.edu]

Jonathan Culbert—completed his master's degree at Naval Postgraduate School in 2020. His thesis was titled *Toward Understanding the Longitudinal Stability of an IP Geolocation Database*. [jaculber@nps.edu]

Abstract

Blockchain is highly adaptable and enables distributed transaction logging through its cryptographic underpinnings, making it an attractive technology for diverse suppliers and acquisition integrators. Supply chain tracking using blockchain must, however, support updates to item records throughout the life cycle—including repair and carcass tracking within Depot Level Repairable (DLR) and back into operation. Unmanned systems, additive manufacturing of parts, and version-control of software updates are all exemplars related to the supply chain requiring addition, deletion, updating, and mergence of a wide array of records. This raises the question of how to build and integrate an integrity-protected item history record that is updateable regardless of when or where changes may occur. We call this approach to updateable record management *blockchain mergence* and investigate how item tracking can be achieved throughout the full item life cycle, even under intermittent connectivity of deployed assets in combat environments. We demonstrate blockchain mergence through an interweaving of dual chains—an authenticated local history signature chain and a global blockchain—and apply it to an unmanned aerial system repair case. Blockchain mergence offers significant opportunities for distributed decentralized trust among diverse producers and consumers of both materiel and information, ashore and afloat.

Background

Blockchain has been widely researched for applications due to the technology's ability to support consensus among distributed participants. The chain is, by design, required to be a single, forward path of events; if branches appear, the chain consensus ensures that all but one branch is discarded (Zheng et al., 2017). A supply chain, in comparison, particularly on the production side, is a reversed architecture. In this case, small parts are used to build larger parts, hence requiring a form of *mergence* (e.g., a final ready-for-use vehicle is comprised of multiple smaller parts sourced from various vendors, manufacturers, and even countries). Blockchain, according to its current design, fundamentally disallows this. Assuring supply chain integrity and visibility requires an adaptation of blockchain use to allow for the mergence that the original concept was not designed to handle. Such adaptive blockchain solutions provide new capabilities and support the potential for future manufacturing changes.

Approach

We survey existing blockchain solutions for forms of mergence, that is, solutions for merging chains into a single blockchain, such as would be necessary for supply chain assurance.

We analyze potential solutions using partner signatures (where supply chain partners commit to chain addenda by digitally signing new blocks while also committing to the entire previous chain). This requires analysis of security considerations based on different commitment variants. Furthermore, it requires consideration of potential time lines and time line collisions of block production.

The above solutions are evaluated with respect to formal blockchain integration. In particular, we investigate whether mergence of distributed ledgers is possible within exiting blockchain architectures or if it is feasible as a parallel assurance mechanism, such that commitments are uploaded to an existing blockchain. This evaluation will be made on mathematical feasibility as well as use case comparison.

Current Research on Ledger Mergence

Blockchain technology has been often touted as a solution to various challenges since its inception under Bitcoin and cybercurrency. An interesting question is how blockchain technology might benefit Navy logistics. In essence, blockchains are a list of records, or blocks, cryptographically linked as a distributed ledger for recording transactions among parties in a permanent and verifiable way (Zheng et al., 2017). Blockchain might also support “smart contracts,” which may be a way to reduce the administrative friction associated with honoring requirements across a large enterprise.

The hallmarks of a robust Distributed Ledger Technology (DLT) are decentralization between blockchain networks and the individual nodes in those networks, as well as the consensus reached when validating individual blocks when added to a network’s blockchain ledger (Khan, 2019). Khan (2019) also noted that characteristics such as the number of transactions per second (TPS) that a network can process, the network’s scalability, and how a particular network guards against malicious attempts to add false information are also key to a good system.

We focus on authentication of changes at the micro-level, with transparency in a ledger for support of supply chain assurance. Industry is working on a number of efforts involving supply chain logistics and supply chain management (SCM)—such as Hyperledger (2020), Everledger (2020), and Ethereum (2020)—that may have an application to the Navy’s logistical systems and perhaps could contribute to an agile logistical system. The central challenge is applying such efforts beyond acquisitions to the whole life cycle of the supply chain.

A Quick Look at DLT Then and Now

Nakamoto (2009) is considered the conventional originator of the original description of blockchain technology, although it is focused on the financial and Bitcoin applications. One should note, however, that the concepts surrounding blockchain predate this by a decade or so, and there is other research available on distributed ledgers before that time frame. Beyond Bitcoin, DLT and blockchain have been researched for various financial and operational tracking purposes. Zheng et al. (2017) and Natarajan et al. (2017) provided a general and fairly informal introduction into DLT and how it might integrate into mainstream day-to-day operations in the financial, private, and government sectors. Natarajan et al. (2017) also provided a sense of how "decentralized records of flow of commodities and materials across a supply chain by using trusted stakeholders to validate flows and movements" could benefit those stakeholders, lending credence to adopting DLT, which would enhance trust in the supply chain. For an overview of blockchain research, we point to Fosso Wamba & Queiroz (2020), which highlights the benefits of the creation of value in operations and supply chain management (OSCM). Statistics such as the number of published papers by country, topic, keyword summary, and relationships are recorded.

Although not explicitly addressing blockchain technology, Bonanni (2011) discussed supply chain discovery/awareness, concepts and concerns that motivate our work. Bonanni argued for "Radical Transparency" in the context of sustainable (carbon cost) supply chains, carbon-footprint measured supply chains, and product life cycle awareness and optimization. This runs into a similar problem set that Department of Defense (DoD) acquisition may encounter—companies' unwillingness to reveal their supply chain details as trade secrets, or an inability to do so because the companies are unaware of the source of their sources.

There has also been a line of research covering direct application of blockchain to SCM. Korpela et al. (2017) provided an analysis of how blockchain could be used to solve or ameliorate the issues of concern of the major stakeholders involved in a very large supply chain operation. The main contribution of the paper is the proposed elimination of a third party to mediate/handle supply chain inter-business and then address these popular concerns. Meanwhile, Banerjee (2018) provided an overview/summary of the use and benefits of blockchain in supply chain operations, such as

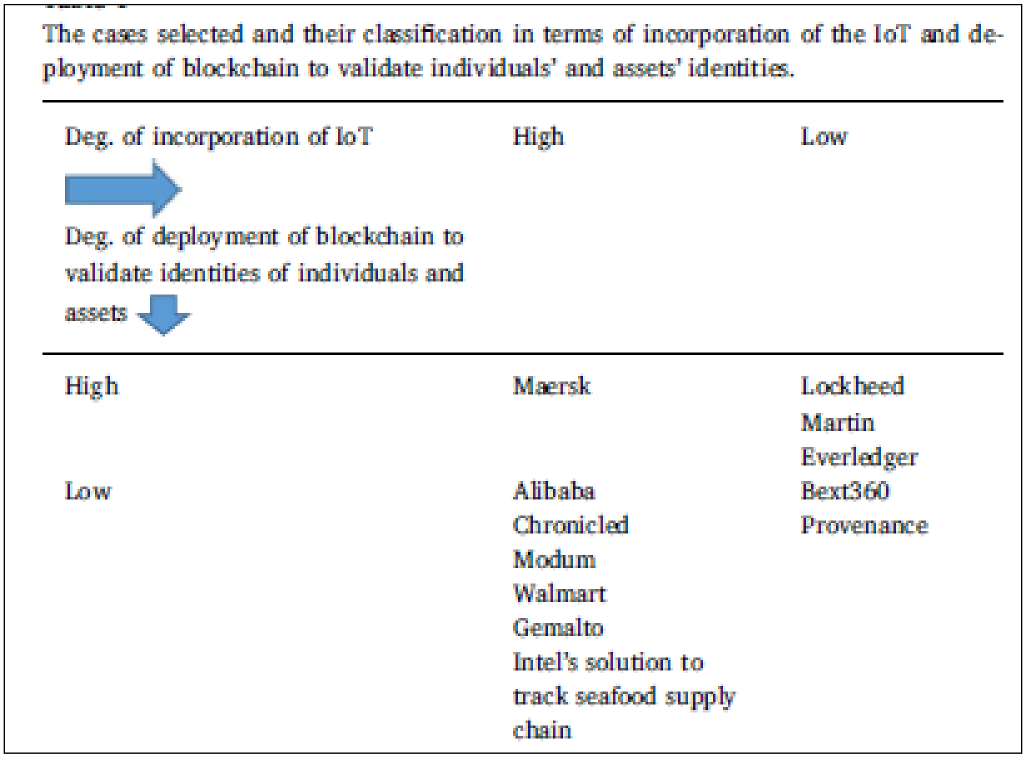
- reduced counterfeiting and origin tracing
- digital product details/life cycle
- custom-built provenance solutions: Software service providers can use the blockchain framework to build provenance solutions for its customers (permission blockchain)

Based on Banerjee's work, custom-built solutions appear to have gained traction within industry. For instance, Infosys has developed a product provenance solution using Oracle Blockchain Cloud Services that is based on Hyperledger Fabric. Infosys has also developed a coffee bean tracking provenance solution for its customers. Such examples point towards a demand for custom-built provenance solutions that can be developed with product- or industry-specific validations. It is important to note that the concept of provenance only functions when all the supply chain stakeholders are part of the blockchain network. The architecture of blockchain inherently traces products as they pass from one supply chain entity to another. These transactions are stored as blocks and chronologically linked according to the physical movement of "the goods." Supporting such tracking technologies motivates our solution (see the section titled A

Ledger Mergence Either in Blockchain or as a Module Approach Leveraging Existing Blockchain Solutions).

Kshetri (2018) provided a theoretical framework related to key objectives of SCM. Kshetri's work covers several corporate case studies of how the Internet of Things (IoT) blockchain SCM can be used by companies with differing levels and areas of interest in supply chain verification/source confidence (see Table 1). Such case studies, including the Chipotle E. coli outbreak ingredient tracing case study, may shed light on potential parallel solution behaviors involving a faulty/compromised hardware component recall in the DoD. Under a similar formal goal, Queiroz and Fosso Wamba (2018) covered blockchain SCM adoption in the United States and India. The study advocated for drawing on emerging literature on blockchain, supply chain and network theory, and technology acceptance models (TAMs). Queiroz and Fosso Wamba (2018) introduced a model based on a slightly altered version of the classical unified theory of acceptance and the use of technology (UTAUT).

Table 1. Cases Selected and Their Classification in Terms of Incorporation of the IoT and Deployment of Blockchain to Validate Individuals' and Assets' Identities (Kshetri, 2018)



The cases selected and their classification in terms of incorporation of the IoT and deployment of blockchain to validate individuals' and assets' identities.

Deg. of incorporation of IoT → Deg. of deployment of blockchain to validate identities of individuals and assets ↓	High	Low
High	Maersk	Lockheed Martin Everledger
Low	Alibaba Chronicled Modum Walmart Gemalto Intel's solution to track seafood supply chain	Bext360 Provenance

A Method for Adapting Distributed Ledger for Supply Chain Use

Unmanned Aerial Vehicle Use Case: Systems Deployed by U.S. Navy Ships

Littoral combat ships (LCS) have two classes of relatively small surface warships designed for operations near shore by the U.S. Navy ("Littoral combat ship," n.d.). Modern designs allow for flexible mission execution, various mission payloads, and other tasking. Reduced crew complements mean individuals are assigned yet with reduced inventories of spare parts and supplies.

The use of unmanned aerial vehicles (UAVs) help in this regard. These vehicles are employed for scouting and other rapid response detailing that minimize risk to the overall mission, ship, and crew. The ecosystem for a typical UAV consists of four categories of components:

- *hardware:* airframe, sensors, computers
- *software:* communication, guidance and control
- *additive manufacturing (AM):* 3D printed wings, tails and other small parts for ad hoc repair
- *information:* keys, training, repair instructions, feedback, safety

Within these four categories of components, each is different and necessary for aggregation into a complete device, and each has different stakeholders and supply chains feeding ships' supplies. Thus, four parallel supply chains of interest exist, and each is interdependent; therefore, any mergence solution should necessarily support all four aspects, as seen in Figure 1. Note that even with acquisition of a device as a single unit, the nature of updates, potential repairs, and parts reuse between devices imply that it must be possible, for tracking purposes over the device lifetime, to handle the mergence of all four aspects.

System Constraints and Requirements Identification

In this section we explore the various system requirements in the context of the UAV use case.

Scenario: UAV Deployment, Repair, and Operations

Suppose that a ship deploys with stock gear and consists of two distinct yet similar versions of a UAV. The ship must maintain its current pace of operations until return to port or resupply.

Under normal operations, the following issues may affect device history—in that they impact the integrity of the device or its trustworthiness—and, therefore, should be added in an authenticated manner to the device history:

- software updates
- training and safety updates to ship tactics, training, and procedures (TTP) and standard operating procedures (SOP)

Now suppose that a collision occurs during testing between the two UAVs, causing damage to each vehicle. The following may also be important changes to the device history, requiring authenticated changes in device records:

- hardware replacements on board, including classified components
- 3D printing for upgraded tail assemblies
- maintenance feedback to shore commands

Any mergence solution must, therefore, support per minimum such a variety of changes to the item history.

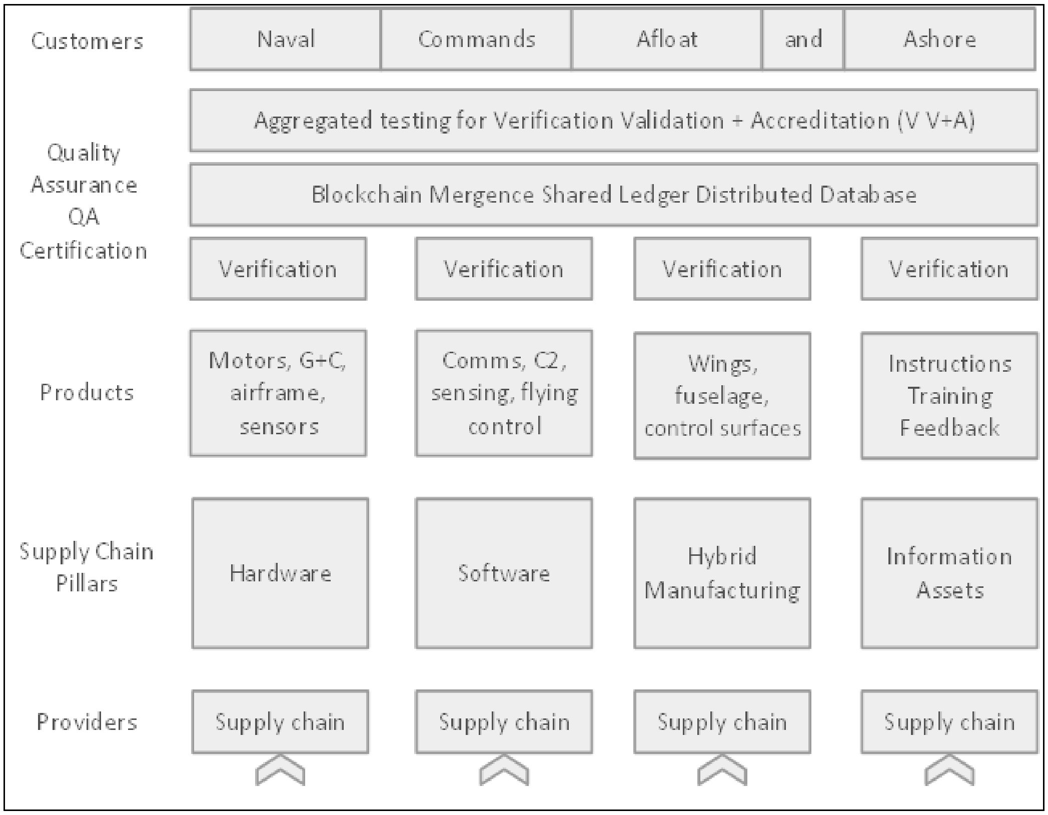

Customers
Naval
Commands
Afloat
and
Ashore
Quality Assurance QA Certification
Aggregated testing for Verification Validation + Accreditation (V V+A)
Blockchain Mergence Shared Ledger Distributed Database
Verification
Verification
Verification
Verification
Products
Motors, G+C, airframe, sensors
Comms, C2, sensing, flying control
Wings, fuselage, control surfaces
Instructions Training Feedback
Supply Chain Pillars
Hardware
Software
Hybrid Manufacturing
Information Assets
Providers
Supply chain
Supply chain
Supply chain
Supply chain

Figure 1. UAV Operational Assembly and Modification

Mergence Requirements Assessment: Verifiability

In addition to the aforementioned types of item record changes, there are also requirements in how a change is recorded. In particular, the record must be verifiable. In terms of verifiability, the following requirements are also essential and must be supported by a mergence solution:

- conformation that a given component X is on the ship
- conformation of all devices in the inventory that have X as a component
- conformation if and when X has been replaced/repaired and so on within a particular device
- conformation of the change entity—the responsible party to change/split/remove/combine X as a component within devices
- ability to add logs or metadata

The above requirements emerge from use case issues. For example, if a device component is found to be compromised and must be removed, the logged data associated with the device should indicate if it has been removed and by whom. Furthermore, it is important for administration purposes to identify all possible devices containing the compromised component for swift handling and damage mitigation. In these contexts, “components” may refer not only to hardware but also malicious software or poorly executed AM (e.g., 3D printed wings with vulnerable integrity).

Mergence Requirements Assessment: Flexibility

Finally, we list flexibility requirements associated with mergence. Since mergence solutions must support potential external (industry/non-DoD) supply chain tracking of unpredictable natures, the mergence solution must be fairly adaptable. Furthermore, external supply chain tracking may differ from internal (DoD) tracking, and the potential solution must support one or more blockchains used internally to the DoD. As many acquisition devices may be of a sensitive nature, the mergence solution must furthermore support various classification levels, such that unclassified devices may be administered in unclassified environments, while devices of higher classification levels can also be managed within the same mergence solution without sensitive information leakage. Finally, in addition to all of these, devices transfer hands between organizations, ships, and so on, requiring a flexibility to record management. This leads us to the following final four solution requirements:

- flexibility independent of source/industry in the external supply chain
- flexibility with internal blockchains(s) within the DoD
- flexibility with classification levels
- flexibility for device transfer between organizations, ships, and so on internally

Ledger Mergence Either in Blockchain or as A Modular Approach Leveraging Existing Blockchain Solutions

There is a natural separation between external-DoD and internal-DoD supply chain tracking. This intrinsically leads to a dual solution, with the acquisition boundary denoting a change in authenticity tracking. Even for internal supply chain tracking, satisfying all solution requirements appears, on the outset, to be impossible. Notably, a solution that crosses classification boundaries must be carefully handled, especially for full item records and tracking information. We handle this by further separating out the internal DoD authentication chain into two parts.

External and Internal Chains

DoD equipment is typically procured via outside commercial manufacturing vendors. The supply chain starts outside of the DoD, where parts and other equipment must be verified and validated before becoming available inside internal supply chains. Conceptually, manufacturers may require supply chain assurance as well, tracking purchased components for integration in building devices. This may take the form of various blockchains (see Figure 2). Minimally, manufacturers may be required to present verification on the types and sources of a device’s components. At acquisition, a new item record will be formed, such that the component history of the acquired device is verified and authenticated by the acquisition authority, who registers components under a digitally signed genesis block. Once a genesis block for the internal ledger is formed, tracking may proceed internally.

What is essential at the DoD boundary/component registration step is the actual verification of internal components to a device. Information on processing chips, software, and so on must be recorded. This enables future tracking such that if, for instance, a component is later discovered to be compromised in the manufacturing chain, all devices containing the critical component can be identified. The genesis block thus serves as an initial registration for all components, such that it is only necessary to record changes to that initial list within the device history record.

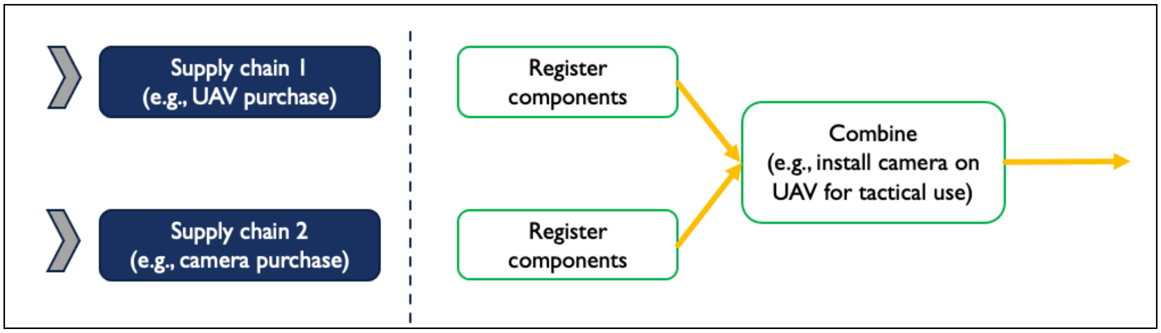


Figure 2. DoD Acquisition: Verification of External Input Chains(s), Registering of Devices to Initiate Internal Chains

Mergence Operations

We break internal tracking into two further chains to support classification boundaries. The *device chain* handles immediate time history and authenticates records as visible to the admin. Moreover, the device chain is designed to support the current Depot Level Repairable (DLR) system. Within the mergence solution, in addition to the device chain, we also support one or more internal blockchains. These may be organization level blockchains or classification level blockchains. Here we employ the term *blockchain* for a distributed immutable ledger, without specification that restricts to any particular ledger format or consensus method. This in turn meets the flexibility requirements specified in the section of this paper titled System Constraints and Requirements Identification.

We are motivated to show how blockchain technology might be applied to handle the full range of potential fleet resupply maintenance and modification requirements. We define the following device chain operations, in accordance with system requirements, as the fundamental primitive operations that together provide the general coverage necessary for distributed accountability of system modifications:

- *device registration*: adding a new, original item to a ledger. This creates the genesis block for the device chain.
- *device repair*: adding a new component onto an existing device. This differs from *device combine* in that the component being added has no registration history (i.e., no genesis block). This may occur if the repair takes place using AM.
- *device split*: separating components within an existing device. This supports potential reuse or disposal, such as when a component breaks and is removed from the current item record (device history is still maintained). This creates two separate device chains: one for each split component.
- *device combine*: integrating two components into a new combined device. This supports customization of devices after acquisition and parts replacement (e.g., a newly purchased component added to an existing device).

Device split can be employed if a device breaks but components can be reused. For example, suppose that a UAV (UAV1) malfunctions, but certain components can be used to repair another UAV (UAV2). The broken device would then have a device split operation in its item record, creating two new chains: one for the component that will be reused and one for the remaining unusable assembly UAV1. A device combine operation then integrates the split component into UAV2. As such, the item history of UAV1 is now linked to UAV2. If there were relevant repairs to the reused component or if it comes to light that the reused component was compromised during manufacture and must be pulled from use, it will be immediately clear from UAV2's record history that the part now resides within UAV2 instead of the UAV1 device carcass.

Each of the stated operations must be authenticated. For this, we use the public key infrastructure (PKI) already inherent in the DLR system. The operator responsible for the device signs the various operations. The signature covers the current record for the device(s) being operated on as well as what type of operation is performed. The authenticated transcript is stored as part of the device chain. These operations are shown in Figure 3.

The distributed ledger and shared memory exist beyond the immediate device chain history, such that an item record cannot be changed a posteriori. For this we employ a blockchain, which records the signatures from the device chain operations. Note that we only require the signatures, and not the related device information, to be stored on the blockchain, although the latter may be stored also. Storage of further information or metadata may be beneficial for device tracking but could also leak information (such as if the device or its location is sensitive). Instead, we require the minimum information on the blockchain concerning the current signature state.

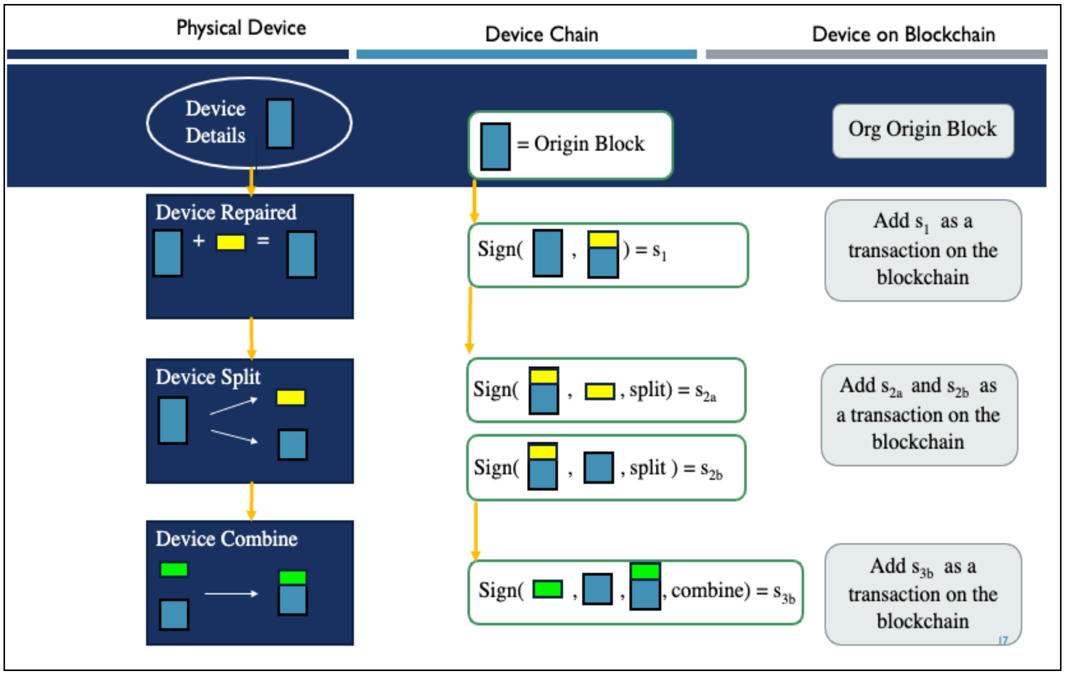

Physical Device
Device Chain
Device on Blockchain
Device Details
= Origin Block
Org Origin Block
Device Repaired
+ =
Sign(,) = s_1
Add s_1 as a transaction on the blockchain
Device Split
Sign(, , split) = s_{2a}
Sign(, , split) = s_{2b}
Add s_{2a} and s_{2b} as a transaction on the blockchain
Device Combine
Sign(, , , combine) = s_{3b}
Add s_{3b} as a transaction on the blockchain
17

Figure 3. Sequencing Operations for Blockchains

Multilevel Security Classification Agility Considerations

For hybrid devices used in the fleet, activities may occur and be needed across multiple levels and domains of security, such as UNCLASSIFIED, CONFIDENTIAL, SECRET, and TOP SECRET. For this, we map our solution to the multilevel security (MLS) classification system and demonstrate interoperability.

Note that while a distributed chain contains data blocks of potentially classified information, the information sent to the blockchain is comprised of merely the signature on the data rather than the data itself; any further additions are optional. Even with a time code associated to the signature object representation, there is no intrinsic value to the information outside of the context of the signed data, especially with a plentitude of blockchain transactions. Thus, the blockchain information can be shared across MLS systems since these codes are useless to an attacker without corresponding ledger (database) access.

In addition to the above observation, we can also allow for blockchains operating at different classification levels, such that more relevant device information than merely the signature may in fact be added to the blockchain. This in turn implies that any device may have a record with varying classification levels attached to different aspects of the associated information and that the associated data may be placed on the relevant blockchain. Naturally, higher classification can correlate same- and lower-level data records, but not write to them, per the properties of the MLS system. Figure 4 illustrates this framework in practice.

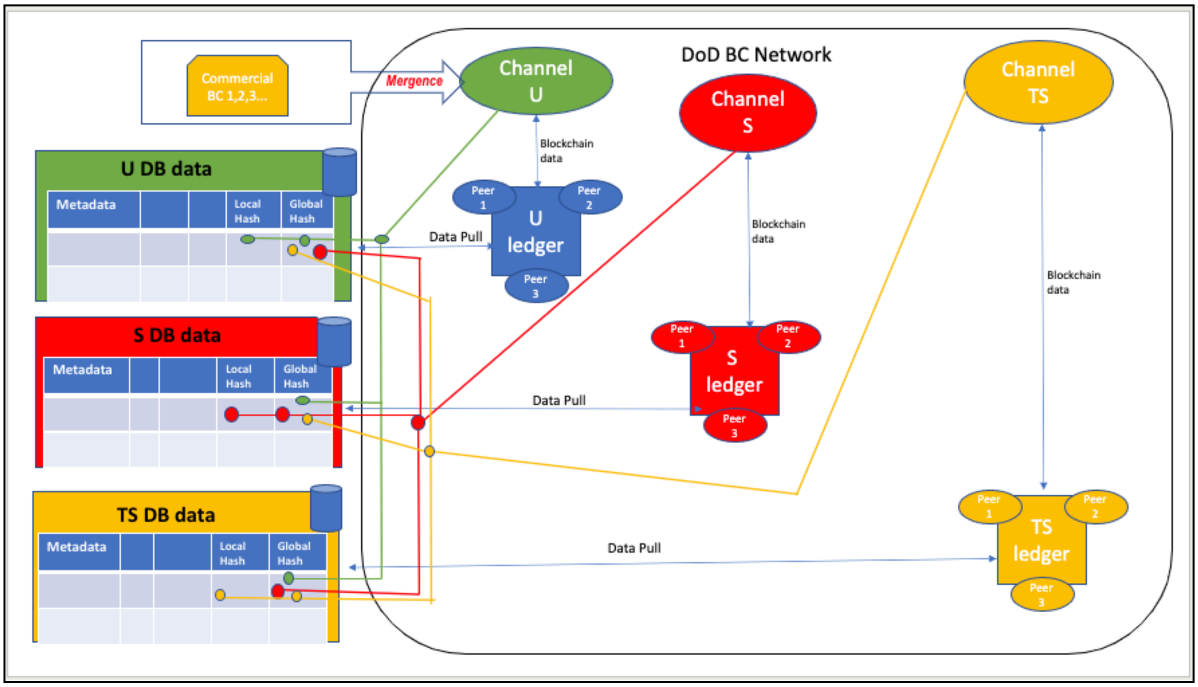


Figure 4. MLS Classification Agility Within a DoD Blockchain Network

To consider how this may work in practice, we walk through the following conceptualized steps for handling the mergence solution of device chains and blockchains within MLS:

1) A new item genesis record for an UNCLASS device is created for the device chain. This correlates to a device origin record with signature information populated to the various blockchains.
2) The device is transferred from an UNCLASS environment to a SECRET environment. The device chain is now maintained at SECRET.

3) The device is repaired, using a combine operation on the device chain. Necessary information is populated to the appropriate and corresponding SECRET level blockchain, while other chains record signature information only.

If it is later discovered that the device of interest contained a malfunctioning or compromised component (e.g., through manufacturer notification), then an operator might inspect all associated components in the device genesis block, recognizing that the critical component is present. It can then be seen that the device was associated to a different classification (or organization blockchain), and the appropriate authority for that blockchain can be contacted, who can then trace the device's history to identify if the component is still present or has been replaced.

DOD Equipment Repair Transactions Using the Hyperledger Fabric Framework for Distributed Blockchain Ledger Keeping

Using the open-sourced Hyperledger Fabric framework (Hyperledger, 2020) hosted on GitHub (2020), we have constructed a case study exemplar using open-source software and demonstration records that shows how various repair level organizations might use blockchain mergence solutions to record supply chain transactions between participants using blockchain as a distributed ledger technology.[1]

UAV Camera

For our case study, we have an organizational level (O-level) end user that currently possesses a UAV that houses a camera subcomponent, a DLR that requires repair at the depot level (D-level). The client application transactions that take place and are recorded on the blockchain ledger are

1. O-level issues the nonfunctional DLR camera to D-level for repair
2. D-level accepts and conducts the required repairs for the DLR camera
3. D-level reissues the repaired DLR camera back to O-level

The intent is to show chain of custody for the DLR camera subcomponent, camera metadata (i.e., serial number), and status of repair of the DLR in the supply chain. The blockchain network (N) is comprised of the following consortium organizations, components, and entities (illustrated in Figure 5):

- Organizations R1 (D-level), R2 (O-level), and R4 (blockchain network administrator).
- Client applications A1 (D-level transactor) and A2 (O-level transactor). Client applications conduct transactions on behalf of their respective organizations.
- Certificate authorities CA1, CA2, and CA4. Each organization can prefer their own vetted certificate authority.
- Peers P1 (D-level) and P2 (O-level). Peers maintain local copies of and record blockchain ledger transactions in accordance with agreed upon smart contracts (chaincode) within the consortium.
- Blockchain ledger L1. Each peer maintains and communicates with other network peers to ensure local blockchain ledger copies are kept uniform throughout the network.
- Smart contract (chaincode) S5. Peers are able to maintain blockchain ledger uniformity through consortium member agreed upon smart contracts.

[1] Details can be found at https://gitlab.nps.edu/tdnorbra/blockchain-mergence

- Network ordering service O4. The ordering service serves as the initial administrative gateway between consortium members upon network standup.
- Network configuration NC4. Consortium members R1, R2, and R4 all agree upon the blockchain network configuration policies administered by ordering service O4 via NC4.
- Channel configuration CC1. The channel configuration allows for network peers to accept and distribute blockchain ledger transactions between authorized organizations in accordance with NC4.
- Channel 1. The communications channel where organizational peers accept and record transactions between client applications A1 and A2 on Channel 1.

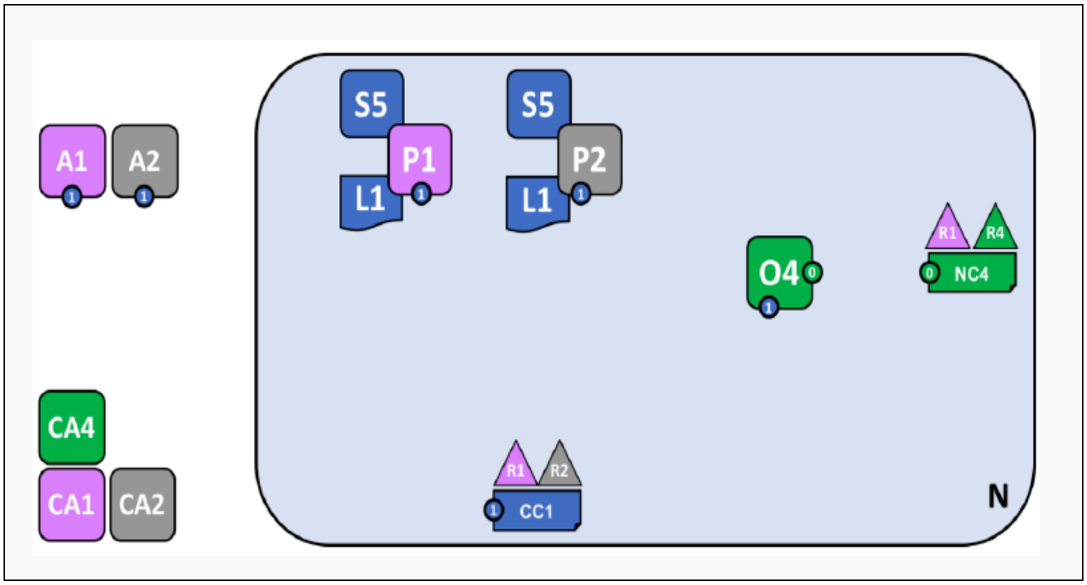


Figure 5. DoD Equipment Repair Blockchain Network (N) Configuration Topology

Using the Fabric Test Network

We apply the Hyperledger Fabric test network for our case study test benchmarking (Hyperledger, 2020). Depending on the operating system of the developer's choice, a specific environment may first be set up on a local machine to leverage the Hyperledger Fabric framework. Once the prerequisites are complete, the test network is invoked via command line scripts and the demonstration can proceed. In our case, the demonstration code was modified locally to mimic our UAV camera scenario.

DLR Transactions in Action

The codebase and a demonstration video for this contribution is maintained in open-source version control, located on the Naval Postgraduate School's GitLab server (Norbraten, 2020). In particular, we trialed the following case study stages:

1. Upon network standup/startup, the various organizational peers, admins, and so on are defined, registered, enrolled, and assigned certificate authorities, which then issue authenticating certificates for each

respective network node. The agreed upon smart contract (chaincode) is deployed to each organizational peer node and tested. Finally, each organizational peer node is given local custody of the blockchain ledger, which is then readied for acceptance and recording of ledger transactions.

2. The network facilitates transactions. Each client application (authorized organizational transaction entity) submits their authentication data to the network before the network authorizes the transaction to take place.
3. Finally, the network is operational, and authorized organizational entities are recognized. Transactions may begin, but only those that are delineated in the smart contract (an O-level entity submitting a UAV camera to D-level for repair). We run three example transactions, as per the smart contract constructs initiated from each of the O-level and D-level authorized entities. These transactions are initiated from each client gateway interface application that has knowledge of the network from their respective remote locations.

Basic Network Timing Data

For any system component introduction, computational expense is valuable to assess. We performed distributed ledger testing on commodity hardware, and delays were tolerable once system initialization was complete. Table 2 below annotates various local network timing data benchmarks for tests performed. Experiments were run using a 2015 Apple MacBook Pro laptop with a 3.1 GHz dual-core Intel i7 and 16 GB of RAM running the latest macOS operating system.

Table 2. Network Timing of Various DLR Transactions on Network (N)

Network Action	Time Units
Blockchain Network Startup/Standup	2 min 19 sec
Client Application Authentication	19.4 sec
O-level DLR Issue Transaction	18.3 sec
D-level Acceptance/Receipt ACK of DLR	17.8 sec
D-level Reissue of RFI DLR	18 sec

Conclusions and Recommendations

The span of device life cycle and rapid evolution from design to development, prototype testing, requirements approval, acquisition testing, deployment, casualty response, and system upgrades is immense. Automated authentication and change logging within this life cycle support human-mediated checkpoints. Industry is looking to blockchain solutions for supporting the ecosystem, which opens an opportunity for leveraging the technology for parts tracking within the DoD. Blockchain mergence provides a bridge between local device repairs and blockchain integrity. In essence, it builds on the DLR system with similar fine-grain parts replacement and carcass tracking by means of hard-coded integrity stamps on the blockchain as a defense against adversarial or even undesired but accidental changes to a device's logged history.

We investigated the logistics challenges that a blockchain mergence solution must address, including pre- and post-acquisition concerns, procedural modifications, preventative and corrective maintenance, and field repair. Furthermore, we evaluated potential solutions against fundamental requirements for interoperability, such as with the existing DLR system and MLS. Finally, our initial open-source, Hyperledger Fabric–

based simulation of the refined blockchain mergence solution demonstrates proof-of-concept capabilities by applying a widely used industry software library for blockchain configuration, simulation, and confirmation.

Recommendations for Future Work

This proof-of-concept exemplar work is ready for further development to match the full logistics life cycle. A real-world prototype case study emulating multiple participants (ashore hardware suppliers, operational forces, and unmanned systems with hardware-dependent software updates) might further test and demonstrate necessary capabilities and ledger distribution. Using the preexisting CAC infrastructure for individual identification further enables a full, ready-to-test blockchain mergence solution.

System engineering assessments can include potential augmentation of existing systems to better support the increased requirements accompanying the fast-growing deployment of unmanned systems. Use case considerations may also be assessed for trusted deployment and updates to hardware and software, as well as inclusion of additive manufactured parts. Future work might then emulate the full life deployment cycle for a fleet-critical system of interest to explore operational parallels in data-centric security for human–machine tactical deployments.

The blockchain mergence solution is designed for smooth integration with the existing DLR system. Feasibility testing of the combined system comprised of blockchain mergence, with the DLR system, and CAC infrastructure is a logical next step for future work.

References

Banerjee, A. (2018). Blockchain technology: Supply chain insights from ERP. *Advances in Computers*, *111*, 69–98. https://doi.org/10.1016/bs.adcom.2018.03.007

Bonanni, L. (2011). Sourcemap: Eco-design, sustainable supply chains, and radical transparency. *ACM Crossroads*, *17*, 22–26. https://doi.org/10.1145/1961678.1961681

Enterprise resource planning. (n.d.). In *Wikipedia*. Retrieved December 22, 2020, from https://en.wikipedia.org/wiki/Enterprise_resource_planning

Ethereum. (2020). *Ethereum is a global, open-source platform for decentralized applications*. https://ethereum.org/en/

Everledger. (2020). *Meet the Everledger platform*. https://www.everledger.io

Fosso Wamba, S., & Queiroz, M. (2020). Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. *International Journal of Information Management*, *52*. https://doi.org/10.1016/j.ijinfomgt.2019.102064

GitHub. (2020). *Repository for the open-sourced Hyperledger Fabric Framework source code*. https://github.com/hyperledger/fabric#releases

Hyperledger. (2020). *Open, proven, enterprise-grade DLT*. https://www.hyperledger.org/wp-content/uploads/2020/03/hyperledger_fabric_whitepaper.pdf

Kahn, F. (2019, February 14). *What are the different types of DLTs & how they work?* Data Driven Investor. https://www.datadriveninvestor.com/2019/02/14/what-are-the-different-types-of-dlts-how-they-work

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. *Proceedings of the Hawaii 50th International Conference on System Sciences*, 4182–4191. https://doi.org/10.24251/HICSS.2017.506

Kshetri, N. (2018). 1 blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, *39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Littoral combat ship. (n.d.). In *Wikipedia*. Retrieved December 3, 2020, from https://en.wikipedia.org/wiki/Littoral_combat_ship

Nakamoto, S. (2009). *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin. https://bitcoin.org/bitcoin.pdf.

Natarajan, H., Krause, S., & Gradstein, H. (2017). *Distributed ledger technology and blockchain*. World Bank Group. https://doi.org/10.1596/29053

Norbraten, T. (2020). *Developer code hosted on the Naval Postgraduate School's GitLab repository for this NRP project*. NPS GitLab.

Queiroz, M., & Fosso Wamba, S. (2018). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *International Journal of Information Management*, *46*, 70–82. https://doi.org/10.1016/j.ijinfomgt.2018.11.021

Shahaab, A., Lidgey, B., Hewage, C., & Khan, I. (2019). Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review. *IEEE Access*, *7*, 43622–43636. https://doi.org/10.1109/ACCESS.2019.2904181

Zheng, Z. Xie, S. Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net