HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

ABOUT HYPERLEDGER

Hyperledger is an open source effort created to advance cross-industry blockchain technologies. It is a global collaboration including leaders in banking, finance, Internet of Things, manufacturing, supply chains, and technology. The Linux Foundation, the nonprofit organization enabling mass innovation through open source, hosts Hyperledger. The Linux Foundation also enables a worldwide developer community to work together and share ideas, infrastructure, and code.

LF EDGE

ABOUT LF EDGE

LF Edge is an umbrella organization that aims to establish an open, inter-operable framework for edge computing independent of hardware, silicon, cloud, or operating system. By bringing together industry leaders, LF Edge will create a common framework for hardware and software standards and best practices critical to sustaining current and future generations of IoT and edge devices.

Decentralized ID and Access Management (DIAM) for IoT Networks

Purpose of this Solution Brief

This document describes a decentralized identity and access management (DIAM) system for IoT devices, based on open source blockchain frameworks from Hyperledger. This decentralized approach can help IoT providers build a secure and cost-effective environment to support millions of IoT devices in the near future.

Intended Audience

The audience for this solution brief includes any vendors or users interested in reducing the complexity, cost, and risk of large-scale IoT networks. Participants in these networks will include enterprise customers, OEMs of IoT devices and equipment, and network software and service providers.

V1.0 published February 2021.

Abstract

The ever-growing number of IoT devices means data vulnerability is an ongoing risk. Existing centralized IoT ecosystems have led to concerns about security, privacy, and data use. This solution brief shows that a decentralized ID and access management (DIAM) system for IoT devices provides the best solution for those concerns, and that Hyperledger offers the best technology for such a system.

1. Introduction

The exact definition of the Internet of Things (IoT) can vary depending on the context. However, most definitions agree on these key characteristics:

- A "thing" is a connected object that can collect data, such as a robot in a factory, a pacemaker placed in a human, or a temperature sensor in a food package
- Each object has a unique ID
- Each object can automatically collect and share data
- Some objects are programmable
- Some objects can make certain decisions on their own without human intervention
- The Internet of Things is a group of these objects all connected and accessed via the Internet

The IoT is growing quickly. IDC predicts that by 2025 there will be 55.7 billion connected devices in the world.[1]

IoT devices are the bottom layer of the IoT stack (the physical layer), while applications sit in the top layer. These IoT applications provide a range of advanced and intelligent services. Since these services can be critical, the accuracy and integrity of the data provided by IoT devices must be protected.

Scaling and securing a network of billions of IoT devices starts with a robust device. Data security also requires a strong access management framework that can integrate and interoperate with existing legacy systems. Each IoT device should carry a unique global identifier and have a profile that governs access to the device.

In this solution brief, we propose a decentralized approach to validate and verify the identity of IoT devices, data, and applications.

In particular, we propose using two frameworks from the Linux Foundation: Hyperledger Fabric for the distributed ledger (DLT) and Hyperledger Indy for the decentralized device IDs. These two blockchain frameworks provide the core components to address end-to-end IoT device ID and access management (IAM).

2. The Problem: IoT Data Security

As the number of IoT devices increases quickly, managing and protecting these devices and the data they generate becomes more challenging. This challenge spans multiple domains, from people accessing services to organizations responsible for authenticating access to devices and data.

One example is the automotive industry, where a massive volume of vehicle-to-vehicle (V2V) and vehicle-to-road communications must be safeguarded to prevent malicious activity and malfunctions due to single points of failure.

Because no robust, industry-grade IoT device management scheme exists, devices are exposed to risks such as identity theft and unauthorized manipulation of data. This situation becomes even more grave when dealing with personalized services where issues such as consent, ID validation, trust, and attribute sharing become very important.

At the industry level, the proliferation of IoT devices in heterogeneous networks has resulted in fragmentation in the ID management space. Numerous silos of ID management have been created that significantly limit interoperability.

Since the majority of IoT devices will be used by consumers in peer-to-peer applications, a centralized approach raises many issues of trust related to privacy, control, and censorship. A decentralized approach addresses the trust issue better.

The starting point for any device management scheme is a universal way to identify each unique device to help manage access to and from it throughout its lifecycle.

IoT device ID management must be part of a larger end-to-end architectural framework that manages access and control in human-to-device, device-to-device, and device-to-services interactions.

Such a framework should provide the following capabilities:

- Unique universal identifiers compatible with the internet namespace convention
- Device ownership and lifecycle management from manufacturing to retirement
- Authentication and authorization
- Governance of data access, provenance and privacy
- Advertising of supported “services”
- Ability to adapt and participate in various trust models

3. The Solution: Decentralized Identity

IoT devices collect, handle, and act on data as proxies for a wide range of users, such as a human, a government agency, or a multinational enterprise.

With tens of billions of IoT devices to be connected over the next few years, numerous IoT devices may represent a single person or institution in multiple roles. And IoT devices may play roles that no one has yet envisioned.

For example, with the rise of autonomous computing powered by machine learning, an IoT device may be able to change roles, ownership, or affiliations dynamically based on external triggers. IoT devices will likely communicate on an ad hoc basis with numerous entities without any pre-existing business relationships.

Decentralized Identifiers (DIDs) enable a standards-based, globally interoperable identity system that puts IoT device owners in control. DIDs enable multiple identifiers to be created at will to help manage anonymity, auditability, correlation across contexts, privacy, revocability, and traceability.

A decentralized ID management system removes the need for any central governing authority and makes way for new models of trust among organizations. All this provides more transparency, improves communications, and saves costs.

4. High-Level Overview of the Solution

As shown in Figure 1, the three main components of identity management are authorization, authentication, and accounting.

These three components correspond to three important questions:

- How is the identity of an IoT device actually managed?
- Who has authorized rights over any particular IoT device?
- What costs are assessed for managing the identity of an IoT device?

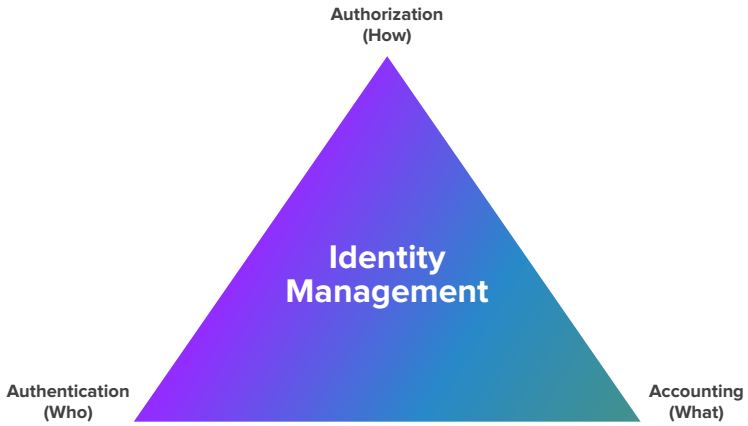

FIGURE 1: THE THREE COMPONENTS OF IDENTITY MANAGEMENT

Ideally, any decentralized scheme is built from the ground up. We propose a four-layer approach to build a decentralized identity and access management (DIAM) framework for IoT.[2]

As shown in Figure 2, the bottom layer provides the basic infrastructure of the blockchain and decentralized storage. The next layer handles ID management through decentralized identifiers (DIDs). The third layer features peer-to-peer (P2P) authentication, and the top layer is P2P authorization for access control.

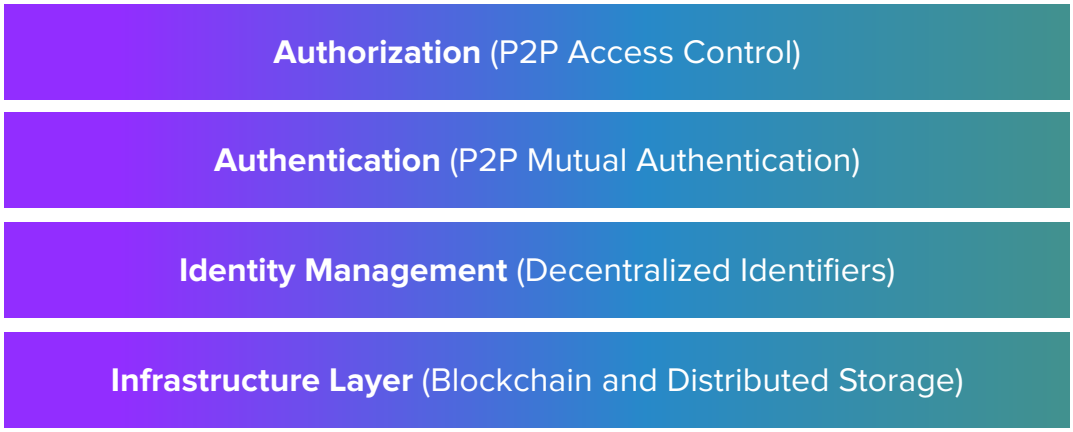

FIGURE 2: THE FOUR LAYERS IN DIAM

The ID management layer uses a specific DID method to create ID documents for IoT devices, as well as a DID resolver to retrieve DID documents as needed.

DID documents can be stored on any system. However, to speed up performance we suggest using a decentralized storage system such as the InterPlanetary File System (IPFS).

Although the DID documents are stored off-chain on the decentralized storage system, the DID itself must be stored on-chain.

A smart contract is the self-executing contract with the terms agreed between buyer and seller written directly into lines of code. The system's smart contract contains the main logic for authenticating ownership before performing any update to any DID document. The smart contract is also used to commit transactions to the blockchain for auditing purposes.

5. The Advantages of Hyperledger Fabric

Anyone, anywhere can join a public blockchain such as Ethereum. But since IoT networks are typically used by consumers or P2P applications that need not be accessible to the general public, a private blockchain is a better choice.

Some other advantages of a private blockchain:

- No malicious actors can join the network because all members must be verified and approved
- Transactions are private
- The smaller size means it uses less computing power
- The consensus mechanism is simpler because all members are trusted

We have chosen the private blockchain Hyperledger Fabric in part because it is open source. IoT services using open-source code enjoy these key advantages:

- Reasonable network set-up costs
- No need to rely on a commercial entity to issue software updates
- Open source is typically more innovative and tends to add new technologies regularly
- Quick and responsive support is available from the open source community when needed for updates, bug fixes, and testing

The blockchain built using Hyperledger Fabric coupled with Hyperledger Indy to create the many IoT device IDs becomes the trust root of the DID.

6. Use Case: IoT Security and Data-Sharing Platform

Many consumers resist buying IoT devices such as smart speakers[3] and smart doorbells[4] because of well-founded concerns around security and privacy.[5]

And as corporate customers become aware of the value of their data, they are starting to demand more transparency from service providers on how their data will be used.

IDC predicts that by 2025, connected devices will generate more than 73.1 zettabytes of data every year[6]—where each zettabyte is a billion terabytes.

How can telecom service providers secure all these devices, manage the integrity of each device, and provide the transparency that consumers and enterprises want about how their data is used?

In the marketplace of smart home and IoT services, telcos must deliver these new services with transparency in order to win customers' trust, and that is possible only when consumers are in control of their data.

Current IoT supply chain and service challenges

The current IoT supply chain is complex and inefficient due to the lack of information exchange among multiple parties. This results in delays in fulfilling orders, uncertain timelines, limited visibility into orders, and mismatches during settlements.

The IoT supply chain also faces potential threats, including device tampering, theft, and unauthorized modifications by an external party. Therefore, IoT services must be secured end-to-end, covering all the physical and virtual network components that make up a network, including all end-point devices.

These security provisions must include:

- Protecting identity and integrity
- Securing both agent and agent-less devices
- Maintaining a database for recording violations
- Managing permissions

Proposed Solution

The solution is to use Hyperledger to create a trusted platform for a telecom ecosystem that can support IoT devices throughout their entire lifecycle and guarantee a flawless customer experience.

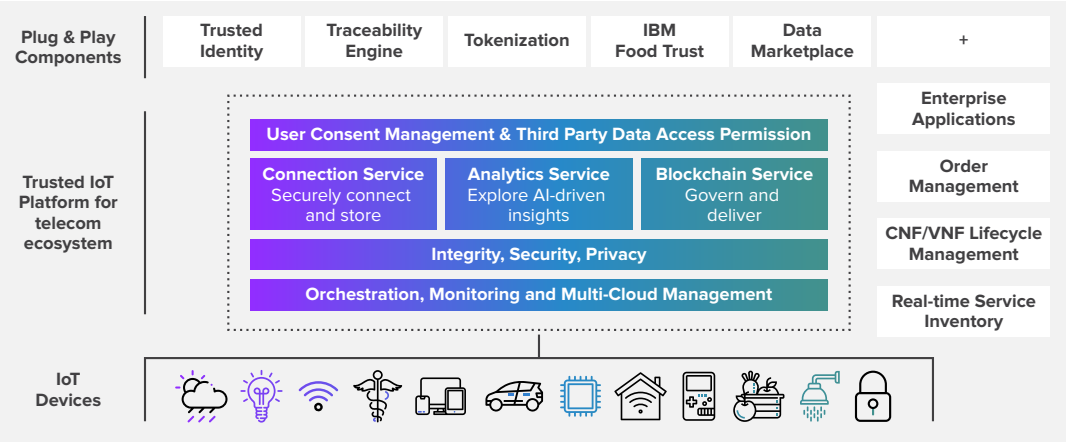

FIGURE 3: A TELECOM ECOSYSTEM FOR IOT USING HYPERLEDGER

At the bottom of Figure 3, the icons show that any type of IoT device can be connected to the network: weather sensors, smartbulbs, medical devices, smartphones, connected cars, and so on.

In the middle layer, Hyperledger Fabric provides a decentralized platform for IAM with all the benefits of a private blockchain. This platform can support telecom use cases such as real-time service inventory, CNF/VNF lifecycle management, order management, and other mission-critical enterprise applications.

At the top, Hyperledger Fabric supports plug-and-play components for specific markets or use cases including trusted identity networks, traceability engines, tokenization of real-world assets such as autonomous cars, the IBM Food Trust system, and any sort of data marketplace.

These applications can be extended to other markets or use cases as required.

Benefits of the Solution

This architecture offers many important benefits for IoT device security, network quality assurance, customer experience, visibility and transparency, and user data access and consent.

IOT DEVICE SECURITY

- The identity of all IoT devices is managed by a device or asset registry
- All IoT devices are monitored to prevent unauthorized access or configuration changes

NETWORK QUALITY ASSURANCE

- The identity of all service components is managed by a registry
- The function of all network components is continuously validated
- Every device and service update is easily tracked and its provenance maintained
- Service providers and vendors gain full visibility into IoT device status and lifecycle

CUSTOMER EXPERIENCE

- Shorter wait time from order to installation
- Service level agreements are monitored and managed by smart contracts
- Consumption-based pricing is managed by smart contract, which reduces errors and provides a single view for all partners

VISIBILITY AND TRANSPARENCY

- Network members gain complete visibility into the status of IoT devices, services consumed, and data generated
- Network members gain better visibility into what customers are charged and what providers are paid

DATA ACCESS AND USER CONSENT

- All user consent is managed on the blockchain
- Any user data stored on- or off-chain is governed by user consent
- Third-party access to user data is governed by policies and agreements managed by the blockchain

7. Reference Architecture

This section provides a high-level architecture view of the proof of concept (PoC) that IBM is working on with some enterprise clients. This PoC uses Hyperledger Fabric as described above.

Figure 4 shows the integration of blockchain components with various BSS/OSS systems, such as order management, CRM, billing, user and enterprise dashboards. This implements the end-to-end lifecycle management of IoT devices and user/application data.

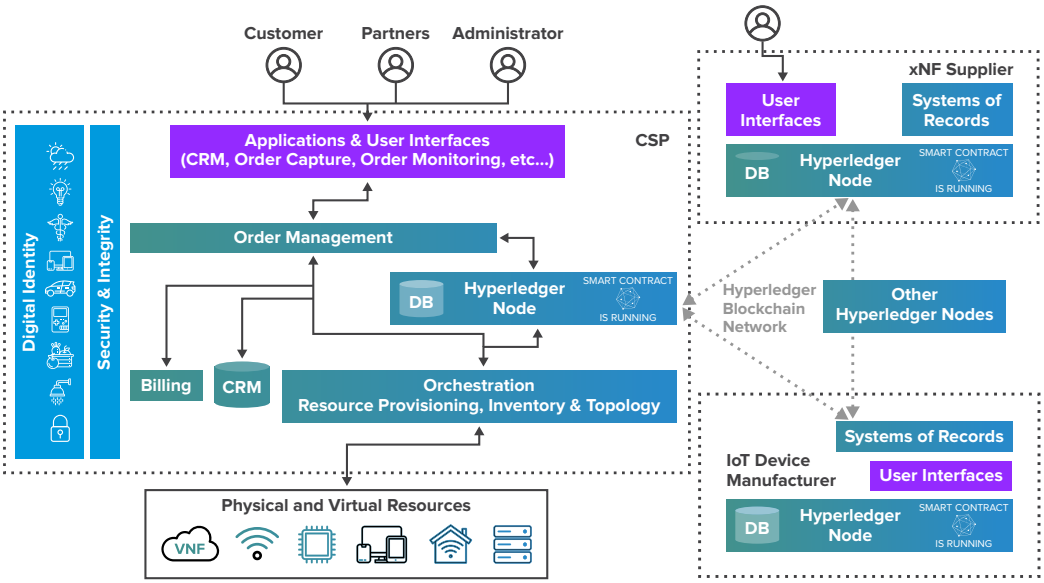

FIGURE 4: REFERENCE ARCHITECTURE FOR END-TO-END LCM FOR IOT USING HYPERLEDGER

Participants, Key Assets, and Transactions in the PoC

Using three tables, this section shows the high-level details of the blockchain model used in IBM's PoC: the participants, the key assets, and the transactions.

Table 1 shows all the roles for each of the different participants on the network, listed in alphabetical order.

Table 2 shows the key asset types defined in the model file. Each asset is listed chronologically with a description, its key properties, and the participants who would touch that asset.

Table 3 shows in chronological order the key transactions defined in the business model and managed by the smart contract. As appropriate, these transactions are performed on one or more assets by one or more of the network participants.

TABLE 1: PARTICIPANTS DEFINED IN THE BLOCKCHAIN MODEL

ABBREVIATION	DESCRIPTION
Cloud Provider	Cloud platform provider
CSP	Communications service provider
Customer	Enterprise IoT customer
FieldAgent	Vendor that provided IoT field services like installation or maintenance
OEM	Original equipment manufacturer of IoT devices or other physical items
VNFProvider	Virtual Network Function software provider

TABLE 2: KEY ASSETS DEFINED IN THE BLOCKCHAIN MODEL

ASSET	DESCRIPTION	KEY PROPERTIES	PARTICIPANTS
Quote	Customer quote created for the requested service, identified by quoteID	Offering name, sellerID, list of components (physical, virtual, and logical)	CSP, Customer
CustomerOrder	Finalized customer order created for the requested service, identified by orderID	ProductID, location, list of service orders, creation time, completion time, total bill, status	CSP, Customer
ServiceOrder	Service order for individual components and tasks as part of customer order, identified by serviceorderID	Service name, list of components (physical, virtual, or logical), creation time, completion time, bill, status	CSP
PhysicalElement	Physical hardware elements identified by unique element ID	Version, type, license assigned, count, and notes	OEM
VirtualElement	Software element identified by unique element ID	Version, type, license assigned, count, and notes	VNFProvider
PhysicalComponent	Physical hardware component that forms part of a service, identified by componentID; encapsulates one or more physical elements	List of physical elements, location, last seen timestamp, notes	CSP, Customer, FieldAgent
VirtualComponent	Virtual/software component that forms part of a service, identified by componentID; encapsulates one or more virtual elements	List of virtual elements, location, last seen timestamp, notes	CSP, Customer, CloudProvider
LogicalComponent	Logical component that forms part of a service, identified by componentID	Location, last seen timestamp, notes	CSP, Customer
PhysicalOrder	Order for physical hardware elements, identified by orderID	Physical element involved, order time, completion time, delivery manifest, bill, status	CSP, OEM
PhysicalInstall	Order for installation and activation of physical component, identified by orderID	Physical component involved, order time, completion time, location, bill, status	CSP, FieldAgent
RegisterPhysicalElement	Registers a physical element on activation; also updates the component asset with the right configuration present at the device	Asset id, version, count and device status	CSP, OEM
PresenceDetectedPhyEle	An event triggered by the physical component that affects the service and updates the blockchain	Asset id, device status, timestamp of event	CSP, Customer, OEM, FieldAgent
CreatePhysicalElement	Creates a new physical element; occurs at the OEM's end	Asset id, version, device status	OEM
VirtualOrder	Order to acquire license for virtual component, identified by orderID	Virtual component involved, order time, completion time, location, bill, status	CSP, VNFProvider
License	License assigned for components, identified by licenseID	Type, number	CSP, VNFProvider

TABLE 3: TRANSACTIONS DEFINED IN THE BLOCKCHAIN MODEL

ASSET	DESCRIPTION	PARTICIPANTS
QuoteCreation	Quote is created by customer request; initiated by the smart seller application	Customer, CSP
CustomerOrderCreation	Customer order is processed and finalized by the order management system	Customer, CSP
ServiceOrderCreate	Individual service orders are created under a particular customer order; triggered and processed automatically by order management system	CSP
ServiceOrderUpdate	Service orders are updated as the supply chain process moves along; triggered and handled by order management system	CSP
CustomerOrderUpdate	Customer orders are updated as the supply chain process moves along; triggered and handled by order management system	Customer, CSP
PhysicalComponentAssign	Physical components are assigned to the service order and customer order; orders are created for physical elements	CSP, OEM
PhysicalComponent AcceptShip	Physical element orders are processed as the order is accepted and hardware is shipped; the element and component status are updated, as are the service and customer orders	CSP, OEM
PhysicalComponentInstall Activation	Physical element installation orders are processed as the order is installed and activated; the element and component status are updated, as are the service and customer orders	CSP, OEM
VirtualOrderPlace	Orders are placed to acquire software components and licenses from the VNF provider	CSP, VNFProvider
VirtualComponentAssign	Virtual element is assigned to a particular customer order; virtual element, component, service order, and customer order are all updated	CSP
VirtualComponentProvision	Virtual component is provisioned and activated via a NFV-Orchestrator, in this case IBM Agile Lifecycle Manager	CloudProvider, CSP
VirtualComponentLifecycle	Lifecycle events of a virtual component, such as configuration, heal, scale, and policy compliance, are tracked via a NFV-Orchestrator, in this case IBM Agile Lifecycle Manager	CSP

Writing to the Blockchain

As any transaction is executed, the corresponding blocks are written to the shared ledger on the blockchain. Figure 5 shows the step when an agent completes the installation and activation of a piece of physical equipment, triggering the PhysicalComponentInstallActivation transaction. The corresponding block is then recorded on the blockchain.

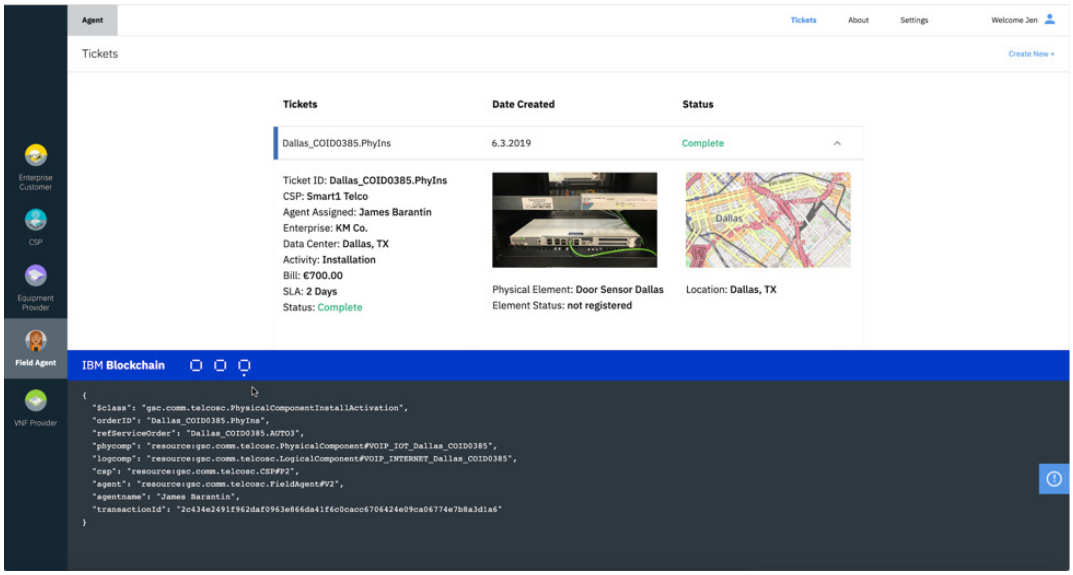

FIGURE 5: SAMPLE TRANSACTION WRITTEN TO THE BLOCKCHAIN

Successful Implementations of Hyperledger IoT Networks

IBM and its partners have successfully developed several global supply-chain ecosystems using IoT devices, IoT network services, and Hyperledger blockchain software.

Two examples of these implementations are Food Trust and TradeLens.

Food Trust seeks to make the world's food supply chain safer, smarter, and more sustainable. This network uses blockchain technology to provide unprecedented visibility and accountability for the food supply.

Food Trust is the world's only network of its kind that connects growers, processors, distributors, and retailers through a permissioned, permanent, and shared record of food system data.

For more information on Food Trust, visit **https://www.ibm.com/blockchain/solutions/food-trust**

TradeLens enables digital collaboration among the many parties involved in moving goods in international trade. Shippers, shipping lines, freight forwarders, port and terminal operators, inland transportation, and customs authorities can all interact more efficiently through near-real-time access to shipping data and shipping documents.

For more information on TradeLens, visit **https://www.tradelens.com/**

Acknowledgements

The Hyperledger Telecom Special Interest Group would like to thank the following people who contributed to this solution brief: Nima Afraz, David Boswell, Bret Michael Carpenter, Vinay Chaudhary, Dharmen Dhulla, Charlene Fu, Gordon Graham, Saurabh Malviya, Lam Duc Nguyen, Ahmad Sghaier Omar, Vipin Rathi, Bilal Saleh, Amandeep Singh, and Mathews Thomas.

Sources

1. "IoT Growth Demands Rethink of Long-Term Storage Strategies, says IDC." Press release. IDC. 27 July 2020. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prAP46737220

1. Ahmad. Sghaeir Omar and Otman Basir, "Capability-Based Non-fungible Tokens Approach for a Decentralized AAA Framework in IoT," in Blockchain Cybersecurity, Trust and Privacy (K.-K. R. Choo, A. Dehghantanha, and R. M. Parizi, eds.), pp. 7–31, Cham: Springer International Publishing, 2020 https://doi.org/10.1007/978-3-030-38181-3_2

2. Dorian Lynskey. "'Alexa, are you invading my privacy?'–the dark side of our voice assistants." The Guardian. 9 October 2019. Retrieved from https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants

3. Melanie de Klerk. "Amazon Ring: Explaining concerns about the smart, controversial doorbell, from privacy to hacking." Global News. 5 March 2020. Retrieved from https://globalnews.ca/news/6633045/amazon-ring-privacy-security-explained/

4. Janet Morrissey. "In the Rush to Join the Smart Home Crowd, Buyers Should Beware." The New York Times. 22 Jan 2019. Retrived from https://www.nytimes.com/2019/01/22/business/smart-home-buyers-security-risks.html

5. "IoT Growth Demands Rethink of Long-Term Storage Strategies, says IDC." Press release. IDC. 27 July 2020. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prAP46737220