Trusted and Transparent Asset Tracking on the Edge

An Industry IoT Consortium Tech Brief

2022-01-27

Authors:
Xinxin Fan
Head of Cryptography, IoTeX
xinxin@iotex.io

Raullen (Qi) Chai
CEO, IoTeX
raullen@iotex.io

Industry IoT Consortium

Supply chains are the principal arteries of the global economy playing a crucial role in enabling international trade flows. Today's supply chains are a globally interconnected supply-and-demand networks with profound interdependencies among suppliers, distributors, retailers and consumers. Businesses rely on it to move their assets from one part of the world to another in a timely manner. But a lack of visibility, traceability, integrity and transparency has plagued supply-chain operations for decades. This has led to poor quality control across the value chain, low administrative efficiency, long and tedious reconciliations among stakeholders, etc., thus increasing overall cost and affecting customer satisfaction significantly.

To tackle these industry-wide challenges, we need to focus on three aspects of supply-chain data:

1. *Untrusted data*: IoT devices (e.g., RFID tags, wireless sensors) that are attached to physical assets in the supply chain are subject to a wide range of attacks that can alter the supply-chain data arbitrarily and jeopardize the integrity of asset-status data.
2. *Fragmented data*: A supply chain involves multiple stakeholders that might not trust each other, which creates data silos and prevents optimal decision making. Data silos and opacity of supply chains can result in broken trust and compromised value chain integrity among stakeholders.
3. *Non-interoperable data*: Due to third-party IT systems and ERP solutions for data processing and storage in the supply chain, custom integrations are often needed to parse supply-chain data, which incurs overhead and decreases supply-chain efficiency.

The untrusted, fragmented and non-interoperable data is the root cause for many common problems faced by the supply chain industry today, so an asset-tracking solution that can ensure end-to-end trust and transparency across multiple tiers of the supply chain is highly desirable.

This technical brief describes how to build a trusted and transparent asset-tracking solution by combining three technical components: secure edge devices, consortium blockchain[1] and standardized supply chain data formats. The resulting solution facilitates collaboration among supply chain stakeholders, improves supply chain efficiency and user experience, and achieves substantial cost savings.

1 TRUSTED AND TRANSPARENT ASSET TRACKING: THE THREE KEY PILLARS

1.1 SECURE EDGE DEVICES

IoT devices are widely used in physical asset tracking applications for monitoring location, temperature, humidity, movement, handling, etc. Since the data reported by IoT devices reflects the real-time status of physical assets in the supply chain, the integrity of the data collection and

[1] Consortium blockchain refers to a blockchain platform operated by multiple organizations (see *https://cointelegraph.com/explained/private-public-and-consortium-blockchains-the-differences-explained*).

transmission process is critical. To ensure data trustworthiness, edge devices must be secure. The components of a typical secure edge device are illustrated on the left side of Figure 1-1.

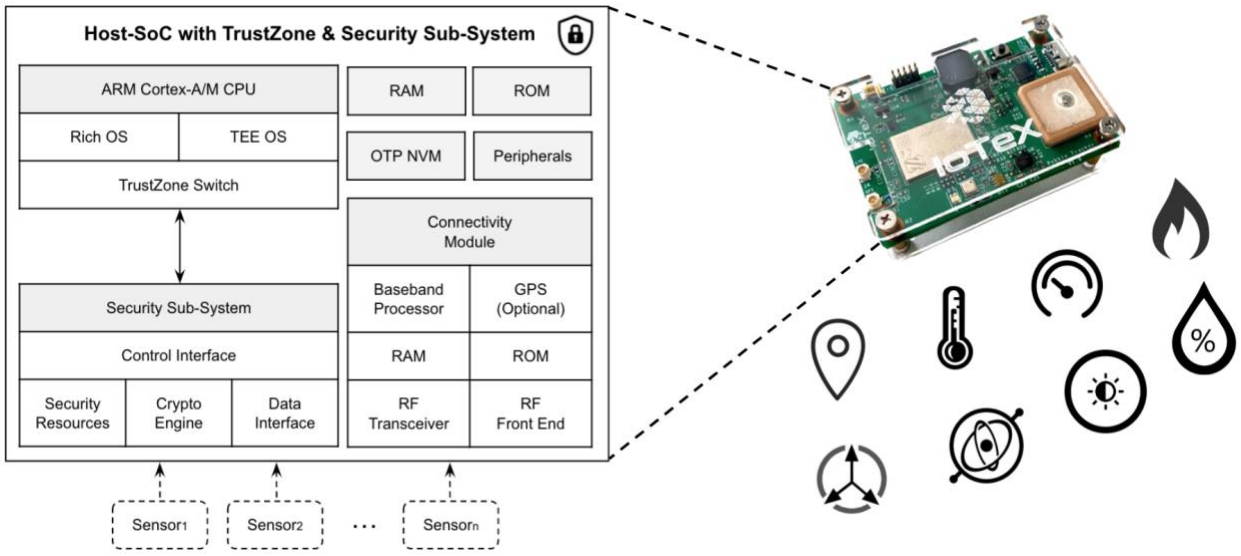


Figure 1-1. *A secure edge device for asset tracking*

Essentially, a secure edge device leverages an Arm TrustZone-enabled microcontroller coupled with a security sub-system to realize strong software isolation and data integrity protection. A more detailed discussion about securing edge devices can be found in IIC's IIoT Distributed Computing in the Edge white paper. An instantiation of a secure edge device, Pebble Tracker (shown on the right side of Figure 1-1), has become available for building secure asset-tracking applications.

1.2 Consortium Blockchain

According to NIST, blockchains are tamper-evident and tamper-resistant digital ledgers implemented without a central repository (i.e. distributed) and usually without a central authority (i.e. a bank, company or government). There are three main types of blockchain systems: public, private and consortium blockchains. A consortium blockchain (e.g., the IoTeX Patheon), which aims to facilitate collaboration among enterprises, is a permissioned platform governed by multiple organizations. A consensus protocol implemented in blockchain ensures that nodes agree on a unique order in which blocks are appended.[2]

Unlike conventional ERP solutions that mainly focus on bridging two siloed enterprise systems, blockchain systems enable (mutually) untrusted parties to conduct business and serve as the single source of truth regarding the collaborative business process. Moreover, blockchain

[2] *https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp*

systems are able to replace trust intermediaries (e.g., notaries, escrows) by so-called smart contracts, which are forms of code distributed on the blockchain that will be automatically executed under certain conditions without human intervention. Smart contracts simplify trust establishment and improve operational efficiency significantly.

Decentralization, immutability, transparency, security, resiliency and smart contracts are a promising infrastructure for documenting business interactions among stakeholders in complex supply-chain applications. For a more general discussion about distributed ledgers and their potential use cases, the interested reader is referred to the Distributed Ledgers in IIoT white paper.

1.3 Standardized Supply Chain Data Format

A uniform language that enables automatic and seamless data processing across a variety of IT systems is essential; a standardized data format should be employed to resolve interoperability issues in multi-party supply chains. For example, the Electronic Product Code Information Services (EPCIS) is a global *GS1* standard that enables supply chain stakeholders to share transactional information about the movement and status of physical objects as they travel throughout the supply chain. Each EPCIS transaction contains key data elements that describe attributes (i.e. "What", "When", "Where" and "Why") of an event that happens to an item within a supply chain. With a standard like EPCIS in place, data from one stakeholder is transformed into a standard-compliant output that can then be easily processed by other stakeholders in the supply chain.

2 AuthTrail: A Trusted and Transparent Asset Tracking Framework

A typical multi-party asset tracking application involves shippers, receivers and a freight-carrier network with multiple stakeholders (e.g., manufacturer, distributor, provider, carrier) that have mutual obligations to deliver assets in time. Unfortunately, the traditional asset-tracking solutions have posed a multitude of concerns due to the lack of trustworthy and transparent information across the supply chain. The Covid-19 pandemic has further exposed the fragility of the current supply chains and highlighted the need for improving the existing supply chain infrastructure through digital transformation. To tackle the industry-wide challenges for global supply chains, we describe a trusted and transparent asset tracking framework called AuthTrail. The proposed framework establishes a trusted data-sharing fabric for streamlining workflow and increasing supply chain visibility among all the stakeholders.

As shown in Figure 2-1, AuthTrail leverages a consortium blockchain to store and exchange all the information related to freight contracts, real-time locations, climatic conditions, transportation and handling of physical assets, thereby creating a single source of truth available to all stakeholders in the system and eliminating potential issues like late reconciliation, improper handling of assets, etc. Moreover, secure edge devices ensure trustworthiness of the data

collection for the status of the attached physical assets. In particular, trusted real-time IoT data will be fed into smart contracts, which specify the service-level agreements (SLAs) negotiated among stakeholders, for evaluation periodically and the penalty settlement will be triggered automatically in the event that an SLA is breached. Finally, to create the chain of custody when assets are moving in the supply chain, AuthTrail requires the stakeholders to record standardized EPCIS events on the blockchain whenever the status of assets changes.

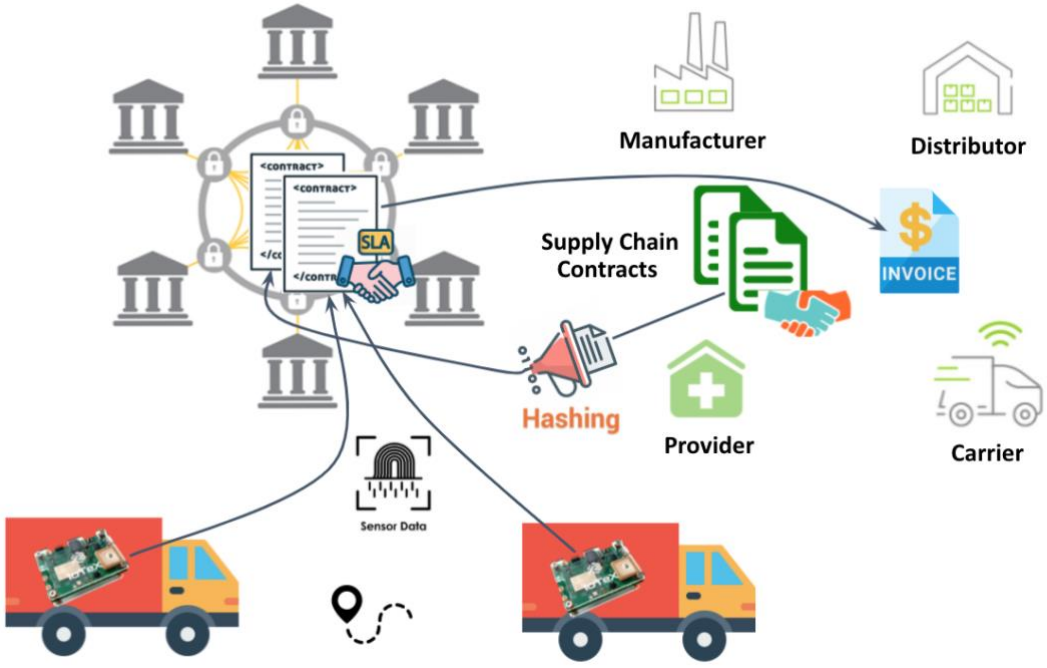


Figure 2-1. *A high-level system architecture for AuthTrail*

The AuthTrail framework has these major steps:

*Asset tracking stakeholders onboarding***.** A consortium blockchain is provisioned and an administrator sends invitations to stakeholders of the freight-carrier network for joining the system. Upon creating an account and logging in the system, each stakeholder generates a decentralized identifier (DID) and stores the corresponding DID document on the blockchain.

*Freight contracts negotiation and archiving***.** All the freight contracts (e.g., broker carrier agreements, load tenders, rate conformations, bill of lading) are negotiated offline among stakeholders and the hashes of the digital versions of those freight contracts are committed to the blockchain for secure logging and auditing purposes. In particular, service-level agreements between stakeholders are written into smart contracts and deployed on the blockchain.

Secure edge device onboarding. Once a secure edge device is powered on for the first time, it generates a private/public key pair within the secure hardware and registers the public key on

the blockchain via a decentralized secure device onboarding process. The registered public key is then used to perform the on-chain sensor data verification by the smart contracts.

*Real-time asset tracking***.** When an asset is being moved by the freight carrier network, the secure edge device captures its real-time status (e.g., location, temperature, humidity) and signs it using the private key. Based on the location of the asset, the signed asset status is then sent to a specific smart contract for the SLA validation.

*Automatic penalty settlement***.** In the case that an SLA is breached, a special event is emitted on the blockchain by the smart contract. Once the event is captured by the corresponding stakeholders' enterprise networks, the penalties will be automatically settled among stakeholders involved in the SLA.

*Chain-of-custody creation***.** The stakeholders send transactions to the blockchain when the asset is in their custody. Each transaction encapsulates a standardized EPCIS event describing what has happened to the asset. All the EPCIS events, which are recorded on the blockchain and shared among all the stakeholders, establish the chain of custody of the asset in the supply chain.

3 BUSINESS OPPORTUNITIES

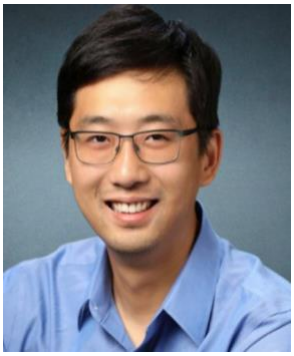
The unique combination of secure edge devices, consortium blockchain, and standardized supply chain format is revolutionary in its ability to create trust among stakeholders in supply chain applications. In addition, the increasing need to eliminate intermediaries and automate supply chain operations are expected to provide tremendous growth opportunities for blockchain empowered asset tracking solutions. The AuthTrail framework has been dedicatedly designed to meet the needs of the supply chain market, including, but not limited to, asset provenance, cost reduction, workflow automation, and restoration of consumer confidence.

4 ABOUT THE AUTHORS

The views expressed in this IIC Technical Brief are the contributing authors' views and do not necessarily represent the views of their respective employers nor those of the Industry IoT Consortium.

Dr. Fan is responsible for directing the IoTeX's strategy and product roadmaps as well as developing the core technologies and IP portfolio. Before joining IoTeX, he was a senior research scientist of Security and Privacy Group at Bosch Research Technology Center North America, where he defined and conducted innovative research on security and privacy for Internet of Things, machine-to-machine communication, cloud computing and data mining. He is an inventor with 17 patent filings for innovative information security and privacy-enhancing technologies.

Dr. Fan received his Ph.D. degree in Electrical and Computer Engineering from the University of Waterloo.



Dr. Chai founded IoTeX in 2017 to focus on the building of auto-scalable and privacy-centric blockchain infrastructure that is designed and optimized for Internet-of-Things (IoT). Previously, he worked at Google as senior software engineer leading many security initiatives for its technical infrastructure. He was also the founding engineer of Google Cloud Load Balancer, which now serves thousands of cloud services with 1+ million queries per second. Prior to that, he was the head of cryptography R&D at Uber, leading the research and development of credential storage system, authentication system, risk management and in-house cryptographic tools. Dr. Chai received his Ph.D. degree in Engineering from the University of Waterloo.

5 COPYRIGHT