Trusted IoT Alliance (TIoTA) Reference Architecture

Introduction

The Trusted IoT Alliance (TIoTA) reference architecture is a synthesis of more than four years of experience with integrations between blockchain and the Internet of Things (IoT).

TIoTA Reference Architecture Overview

The TIoTA reference architecture consists of three layers, namely the asset layer, the IoT cloud layer and the blockchain layer, as illustrated in Figure 1.

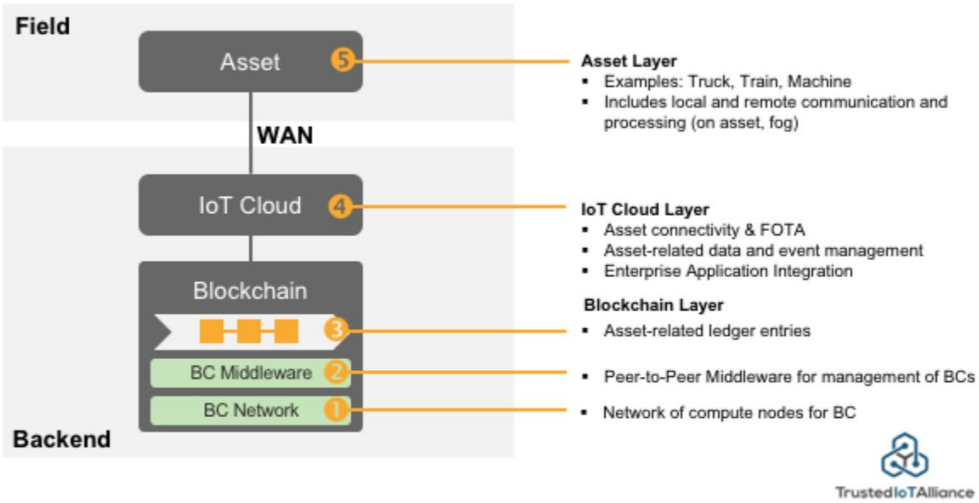


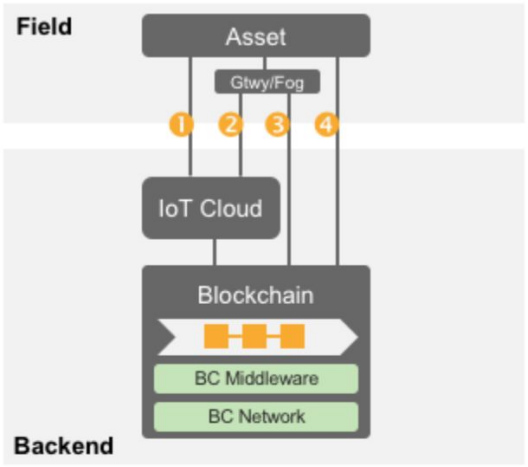
Figure 1. The TIoTA Reference Architecture

- *Asset Layer*: The asset layer represents a variety of physical assets in the field that are connected to IoT devices. Those smart devices capture the physical properties of the associated assets and take specific actions if needed. The asset layer involves various IoT devices/gateways and wireless communication techniques.
- *IoT Cloud Layer*: The IoT cloud layer contains a complete set of components for connecting, processing, storing and analyzing asset-related data both at the edge and in the cloud. The core functionalities provided by the IoT cloud layer include device identity management, device connectivity management, device data storage, device data analytics, device control and automation, business integration, etc.
- *Blockchain Layer*: The blockchain layer is comprised of the following three sub-layers:
    - *Blockchain Network*: The blockchain network is comprised of all the nodes that provide CPU, storage and network for supporting blockchain operations.

- *Blockchain Middleware*: The blockchain middleware deals with peer-to-peer communications and performs consensus mechanisms to produce blocks.
- *Blockchain Application*: The blockchain application maintains users' accounts and records all the transactions and blocks related to the assets.

TIoTA Reference Architecture Integration Patterns

The TIoTA reference architecture focuses on four primary integration patterns, as shown in Figure 2.



	a.) W-Only	b.) R-Only	c.) RW
1: Asset-to-Cloud-to-BC			
2: Gtwy-to-Cloud-to-BC			
3: Gtwy-to-BC			
4: Direct			

Examples

- 1a: IoT Cloud manages all asset data, selectively writes critical data / events to BC
- 1b: Cloud reads other asset`s data for validation, e.g. for pairing of two assets
- 2a: Track & Trace beacons send critical event to gateway (e.g. via BLE), gateway forwards event to IoT Cloud, data is evaluated and stored in BC
- 4a: On-asset intelligence is executing BC logic and communication directly

TrustedIoTAlliance

Figure 2. The TIoTA Reference Architecture Integration Patterns

Integration Pattern I: Asset → IoT Cloud → Blockchain

This pattern focuses on the IoT devices (e.g., those built from single board computers) that have Wi-Fi and/or cellular connectivities and are able to directly communicate with the IoT cloud using various IoT data protocols (e.g., MQTT). In this pattern, the IoT cloud manages all the asset data and the blockchain serves as the data integrity layer and/or intra-organizational data plane across multiple IoT clouds in the reference architecture. Moreover, the IoT cloud chooses which data and events will be stored in the blockchain.

Integration Pattern II: Asset → Gateway/Fog → IoT Cloud → Blockchain

This pattern covers the resource-constrained IoT devices (e.g., sensors, RFIDs, smart meters, etc.) that can only connect to an IoT gateway via low-power wireless communication protocols (e.g., ZigBee, Z-Wave, LoRa, etc.), which then forwards the collected data to the IoT cloud. The blockchain plays the same role as that in the integration pattern I.

Integration Pattern III: Asset → Gateway/Fog → Blockchain

This pattern aims for the emerging computing paradigms such as edge/fog computing, where the IoT gateways and edge/fog nodes directly handle the connection, storage, processing and analysis in a distributed manner. In this pattern, the blockchain replaces the centralized IoT

cloud for controlling and managing IoT devices, gateways and edge/fog nodes to realize various asset-related core functionalities.

Integration Pattern IV: Asset → Blockchain

This pattern mainly targets machine-to-machine communication and payment scenarios, where the IoT devices, which are equipped with Wi-Fi/cellular modules, need to run either a light client or full node to communicate with others in a decentralized manner. Smart contracts are extensively utilized to define the interaction rules and policies between IoT devices. The IoT devices monitor the specific events on the blockchain and take actions accordingly.

TIoTA Trusted Asset Lifecycle

To ensure the end-to-end security for the IoT applications, the TIoTA reference architecture defines a complete three-phase lifecycle management mechanism for the trusted assets, as illustrated in Figure 3.

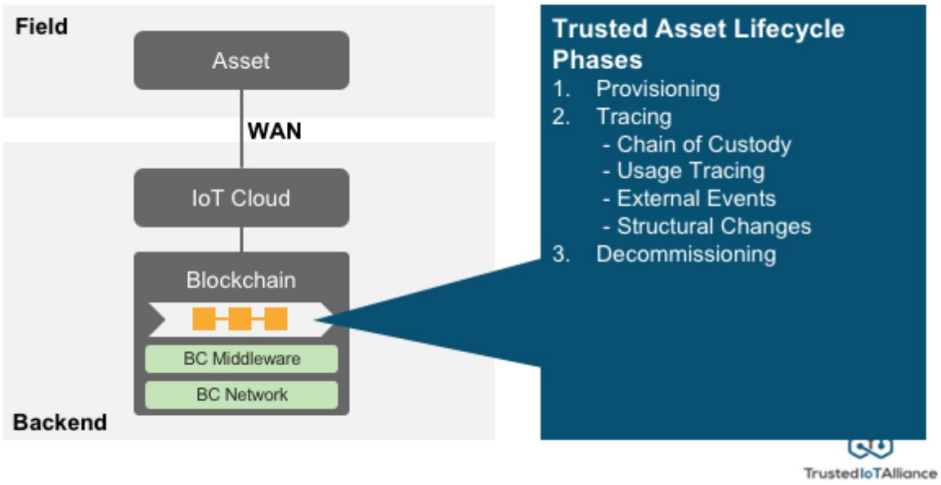


Figure 3. The TIoTA Three-Phase Trusted Asset Lifecycle

Phase I: Provisioning

In this phase, the IoT devices are provisioned in a secure manufacturing environment with cryptographic materials (e.g. cryptographic keys, digital certificates (optional), etc.). The cryptographic materials should be kept in a tamper-resistant storage and only accessible by the on-board security engine and trusted execution environment (TEE). The provisioned secure IoT devices are then associated with the physical assets and deployed in the field. Once the IoT devices complete authentication with the IoT cloud, it registers those devices on the blockchain with a smart contract, thereby enabling a blockchain-based device management.

Phase II: Tracing

In this phase, the IoT device continuously reports data (i.e., physical properties of the associated assets such as temperature, humidity, location, etc.) to the IoT cloud, which then

selectively stores the critical data and events to the blockchain. By tracing the transactions on the blockchain, one can determine the state transitions of the physical assets, including but not limited to the chain of custody, usage frequency, external events, structure changes, etc. By analyzing the state transitions on the blockchain, one can gain valuable insight into the assets.

Phase III: Decommissioning

In this phase, the IoT devices need to be decommissioned for various reasons (e.g., replacement) from the existing IoT applications. In this case, the decommission event should be recorded on the blockchain and the decommissioned devices should be marked as “inactive” on the device registry, which enable the IoT applications to adapt to this change accordingly.

In the three-phase trusted asset lifecycle, the blockchain keeps track of the state transitions of the IoT devices and the associated physical assets, thereby offering an authenticated audit trail for the lifecycle of the physical assets.

TIoTA Smart Contract Integration Patterns

Smart contracts play an important role in the TIoTA reference architecture to enable the decentralized interactions among IoT devices. The most common event-triggered smart contract integration pattern in shown in Figure 4.

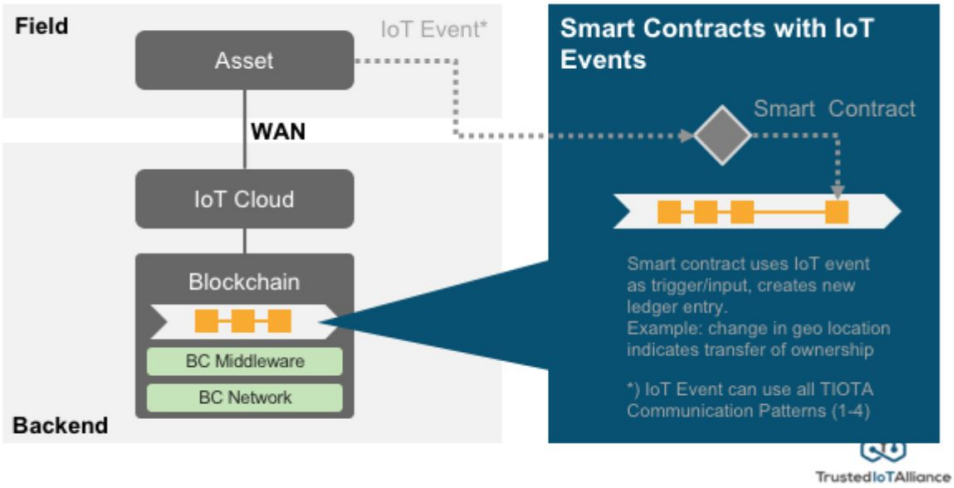


Figure 4. The TIoTA Event-Triggered Smart Contract Integration Pattern

In this pattern, the critical IoT events (e.g., change in geo location, temperature beyond the threshold, etc.) trigger the execution of the smart contract on the blockchain, which causes the state change of the IoT devices and may incur further actions to be taken on the device side. Note that the critical IoT events can be injected into the blockchain via the four TIoTA communication patterns defined in the previous section.

Besides the common event-triggered smart contract integration pattern, the TIoTA reference architecture also covers the cross-chain communications via smart contracts, as demonstrated in Figure 5.

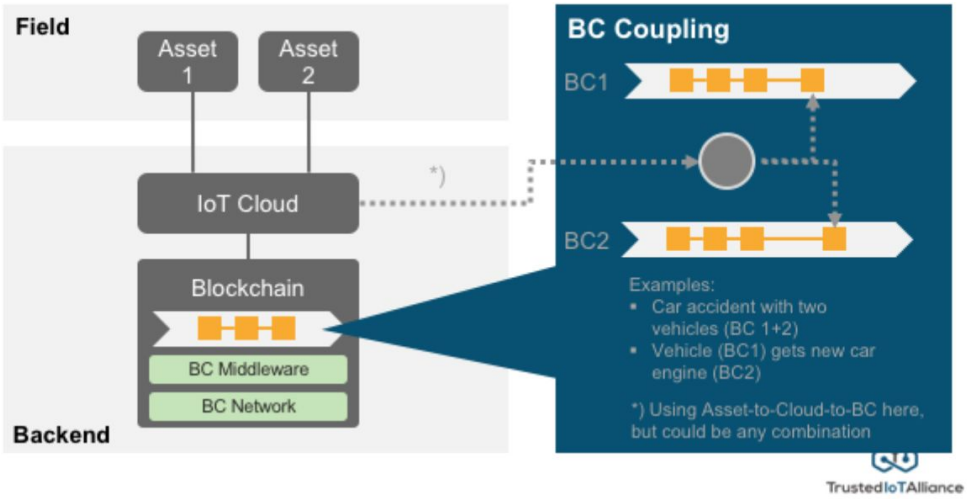


Figure 5. The TIoTA Cross-Chain Communication Smart Contract Integration Pattern

In this pattern, the IoT cloud, which is running either light clients or full nodes for two blockchains, is able to monitor transactions on both chains. Smart contracts deployed on one blockchain can be triggered to execute by the events on the other blockchain, thanks to the bridging node running on the IoT cloud.