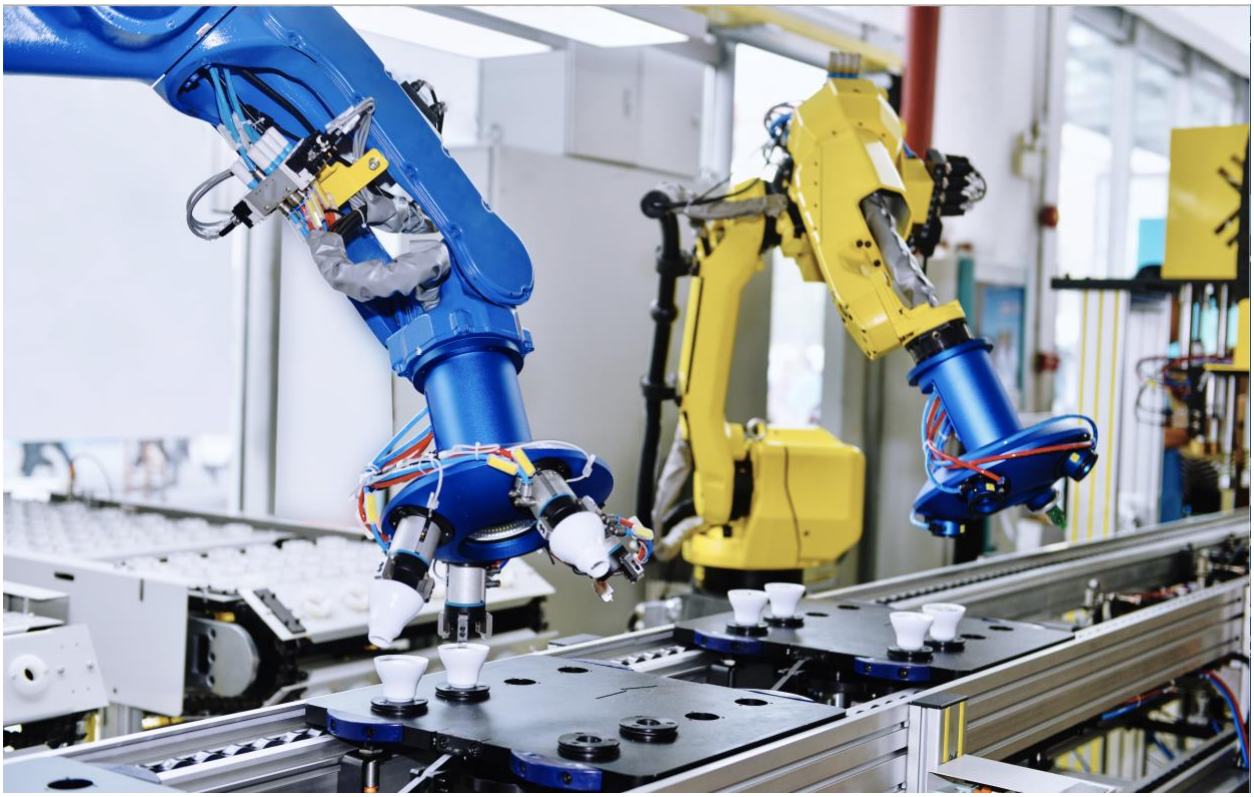


Decentralized Identity for Edge Computing

An Industrial Internet Consortium Tech Brief

2020-09-18

industrial internet CONSORTIUM

Table of Contents

THE IDENTITY ON EDGE

The explosion of networked smart devices, ranging from home appliances to medical devices to consumer electronics, is shaping our lives and disrupting traditional businesses at a staggering rate during the past few years. According to Gartner, connected devices across all technologies will reach 20 billion by 2020. This means that identity and access management (IAM) services need to identify billions of IoT devices and millions of potential users uniquely.

Unfortunately, legacy IAM systems are not able to fulfil this requirement, largely because they focus extensively on identifying people, rather than identifying smart devices of internet of things (IoT) systems.

In an increasingly connected world, managing device and user identities as well as the relationships among various entities faces significant challenges:

1. Due to the lack of IAM standards for IoT, manufactures have to use proprietary approaches for naming and identifying their devices, which results in IoT application silos, and hinders interoperability among connected devices from different manufactures.
2. An IoT system needs to go through a series of stages during its lifetime, which further complicates integration of IAM capabilities into the operational lifecycle of IoT devices.
3. Last but not least, there exists a multitude of protocols and standards for various IoT devices and applications. A lack of a common operating and security framework has posed some serious concerns for device manufacturers and consumers. As a result, there is a strong need for introducing a new IAM framework that is able to adapt to the proliferation of connected devices in the coming years.

ABOUT THIS TECH BRIEF

This Tech Brief provides an overview of emerging concepts such as *decentralized identifiers (DIDs)* and *verifiable credentials (VCs),* and it describes how to create a unified, interoperable and tamper-proof device identity registry on top of the blockchain by introducing DIDs and VCs into the lifecycle of IoT devices, thereby breaking IoT application silos and unlocking the potential of IoT on a global scale. Learn more about our ongoing Edge initiatives at *https://iiconsortium.org*.

Related presentation from IIC: "*Decentralized Identity for Edge Computing*," from the IIC's Edge Computing Task Group meeting 2020-04-23. (YouTube video.)

OVERVIEW OF EMERGING CONCEPTS

DECENTRALIZED IDENTIFIER

A decentralized identifier (DID) is a new type of identifier that is globally unique, resolvable with high availability and cryptographically verifiable. A DID comprises three components separated by colons, as shown below:

$$\underbrace{\text{did}}_{\text{Scheme}} : \underbrace{\text{method}}_{\text{Method}} : \underbrace{\text{123456789abcdefghij,}}_{\text{Method-Specific Identifier}}$$

where the scheme, did, is fixed for all DIDs. The method describes how DIDs work with a specific blockchain and the DID Method Registry of the World Wide Web Consortium (W3C) summarizes the DID method specifications currently in development. The method-specific identifier is an alphanumeric string that is guaranteed to be unique within the context of the DID method. To discover what a DID means, the DID method outlines the way to resolve a DID to the associate DID document.

A DID document is a JSON-LD document containing six optional components, as illustrated in Figure 1. “id” denotes the DID, “publickey” a list of public keys, “authentication” a list of protocols for verifying the control of the DID and delegated capabilities, “service” a set of service endpoints for interacting with the entity that the DID identifies, “created/updated” a timestamp that indicated when the DID document was created or updated and “proof” a digital signature for verifying the integrity of the DID document.


```
{
 "@context": "https://w3id.org/did/v1",
 "id": "did:io:123456789abcdefghij",
 "publicKey": [{
  "id": "did:io:123456789abcdefghij#keys-1",
  "type": "RsaVerificationKey2018",
  "controller": "did:io:123456789abcdefghij",
  "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
 }],
 "authentication": [{
  "type": "RsaSignatureAuthentication2018",
  "publicKey": "did:io:123456789abcdefghi#keys-1"
 }],
 "service": [{
  "id": "did:io:123456789abcdefghij;exam_svc",
  "type": "ExampleService",
  "serviceEndpoint": "https://example.com/endpoint/1576358"
 }],
 "created": "2019-02-08T15:23:42Z",
 "proof": {
  "type": "LinkedDataSignature2015",
  "created": "2019-02-08T15:12:30Z",
  "creator": "did:io:8uQhQMGzWxR8vw5P3UWH1ja#keys-1",
  "signatureValue": "QNB13Y7Q9...1tzjn4w=="
 }
}
```


Figure 1. An Example of a DID Document

VERIFIABLE CREDENTIAL

A verifiable credential (VC) is a tamper-evident credential that has authorship that can be cryptographically verified. VCs attest identity attributes of subjects and the exchange of VCs builds up trust among DID-identified peers. In particular, issuers of VCs determine which claims are contained in the credentials, whereas verifiers make their own decisions regarding the trustworthiness of the received credentials. A VC is also a JSON-LD document as shown in Figure 2. “id” denotes the DID of the VC, “type” is the type of the VC, “issuer” is the DID of the credential issuer, “issued” indicates the date that the VC was issued, “claim” is a list of identity attributes attested by the issuer and lastly, the “proof” comprises a digital signature for verifying the validity of the credential.


```
{
  "@context": "https://w3id.org/credentials/v1",
  "id": "did:io:WRfXPg8dantKVubE3HX8pw/credentials/1",
  "type": ["Credential", "NameCredential"],
  "issuer": "did:io:WRfXPg8dantKVubE3HX8pw",
  "issued": "2019-07-01",
  "claim": {
      "id": "did:btcr:x6lj-wzvr-qqrv-m80w",
      "name": "John Doe",
      "address": "..."
   },
  "proof": {
     "type": "RsaSignature2018",
     "created": "2019-06-25T21:19:15Z",
     "creator": "did:io:WRfXPg8dantKVubE3HX8pw#key-1",
     "nonce": "c0ae1c8e-c7e7-469f-b252-86e6a0e7387e",
     "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCneO4Jugez
      8RwDg/+MCRVpjOboDoe4SxxKjkCOvKiCHGDvc4krqi6Z1n0
      UfqzxGfmatCuFibcC1wpsPRdW+gGsutPTLzvueMWmFhw
      YmfIFpbBu95t501+rSLHIEuujM/+PXr9Cky6Ed+W3JT24=
   }
}
```


Figure 2. An Example of a Verifiable Credential

DIAM-IOT: A DECENTRALIZED IAM FRAMEWORK FOR IOT

Consider a global-scale IoT ecosystem that contains a large number of device manufacturers, billions of IoT devices and millions of users. In such an ecosystem, a variety of IoT systems that feature proprietary IAM solutions and different communication standards coexist, thereby creating application silos and preventing the vision of interoperability. To address these challenges, a new decentralized IAM (DIAM) framework for IoT called DIAM-IoT is proposed to

connect IoT application silos and facilitate user-centric data sharing in a decentralized manner, as illustrated in Figure 3.

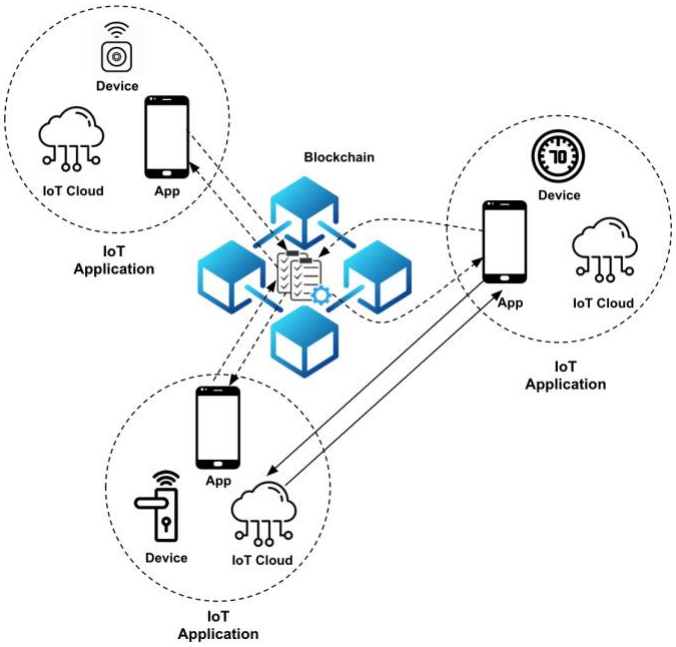


Figure 3. A High-Level System Architecture of DIAM-IoT

DIAM-IoT introduces DIDs and VCs into the lifecycle of IoT devices without significantly changing the existing system workflows and leverages distributed ledger and smart contracts to manage device manufactures and DIDs. After IoT devices are sold to consumers, it is up to the consumers to decide whether they would like to share their device data with others. If data sharing is not an option, consumers just use their IoT system as usual. Otherwise, they receive VCs during the device binding process and register device DIDs by invoking manufacture-managed smart contracts.

Furthermore, consumers manage data access with their own smart contracts on the blockchain that act as the service endpoints and ensure fairness of the data sharing process. The salient feature of DIAM-IoT is that device owners have full control over how their device data is being accessed. In the following subsections we present the detailed design of DIAM-IoT.

The DIAM-IoT framework consists of the following major steps:

- *IoT manufacturer onboarding.* DIAM-IoT uses a two-layer approach for managing DIDs of IoT devices with smart contracts. While a master smart contract maintains a registry of IoT manufacturers, each manufacturer manages its own device registry with a manufacturer smart contract. From a consumer perspective, the manufacturer handles the DID operations for its own IoT devices, whereas the master smart contract deals with the DID resolution for all other devices.

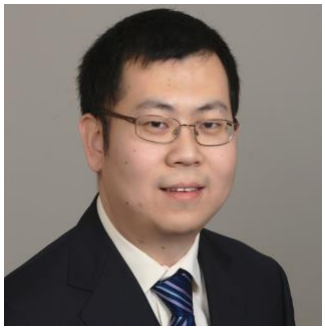
- *User account registration.* A cryptocurrency wallet is created for a user interacting with the blockchain. The IoT cloud needs to verify that both the user account (e.g. an email address) and the blockchain address belong to the same user. At the end of user registration, the IoT cloud binds the user account with its blockchain address and public key.
- *Device binding and verifiable credential generation.* To register a DID for an IoT device on the blockchain, a user needs to obtain a VC from the IoT cloud which binds the device DID and its owner's DID. This confirms the device ownership and allows only the device owner to register the DID for its IoT device on the blockchain. In DIAM-IoT, a VC is generated by the IoT cloud after a device binding is performed successfully.
- *Device DID registration.* Before registering a DID for the IoT device on the blockchain, the device owner first deploys a service smart contract, which serves as the endpoint for interacting with the IoT data service and ensures the fair payment and timely dissemination of IoT data. In DIAM-IoT, a DID document is stored off-chain and only its hash value is kept on-chain for maintaining consistency with the off-chain record. The DID document is signed by the device owner and contains service-related information such as device owner, device metadata, service endpoints, among others. Upon completing the storage of the DID document, the device owner initiates the device DID registration by invoking the manufacturer smart contract.
- *Decentralized and user-centric data authorization.* The decentralized and user-centric data authorization enables device owners to realize fine-grained access control on data collected by their IoT devices. A data requester needs to first resolve the IoT device's DID of a device owner by invoking the master smart contract and extracting the address of the corresponding service smart contract. The data requester then requests data access by interacting with the device owner's service smart contract. Once the data access request is granted by the device owner, the data requester is able to retrieve data using the access token issued by the device owner.

BUSINESS OPPORTUNITIES

DIDs and VCs enable the existing IoT solutions across their own application domains and facilitate the value exchange among various IoT applications. As a result, IoT systems that integrate the DIAM-IoT framework are able to interact with each other seamlessly in a global-scale ecosystem. In particular, IoT solution providers are able to build powerful decentralized applications by incorporating data from other IoT systems. From the perspective of consumers, the DIAM-IoT framework allows them to have full control of their IoT devices and data, thereby giving consumers the peace of mind they deserve.

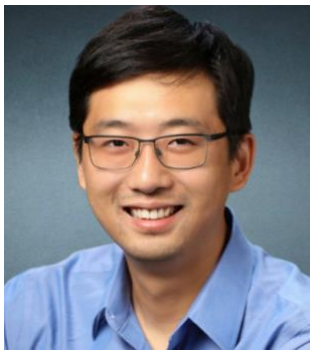
About the Authors

The views expressed in the IIC Technical Brief on Edge are the contributing authors' views and do not necessarily represent the views of their respective employers nor those of the Industrial Internet Consortium.



Dr. Xinxin Fan, Head of Cryptography, IoTeX

Dr. Fan is responsible for directing the company'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 16 patent filings for innovative information security and privacy-enhancing technologies. Dr. Fan received his Ph.D. in Electrical and Computer Engineering from the University of Waterloo.



Dr. Raullen (Qi) Chai, CEO, IoTeX

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.

About IoTeX

Founded as an open source platform in 2017, IoTeX is building the **Internet of Trusted Things**, where all physical and virtual "things"—*humans, machines, businesses and DApps*—can exchange information and value at a global scale. By serving as a decentralized trust fabric for IoT, IoTeX will empower the future decentralized economy by "connecting the physical world, block by block". During the past few years, IoTeX has amassed considerable expertise and experience in IoT security and privacy and is actively collaborating with other IIC members to address a wide range of industry challenges.

COPYRIGHT