iot device security conference

A Blockchain Perspective to IoT Device Security

Xinxin Fan, PhD, CISSP
IoTeX
November 15, 2021

Outline

- IoT Device Security Overview
- IoT Device Security: Today
- IoT Device Security: Tomorrow
- IoT Device Security: Future

Device Security - The Key to IoT Success

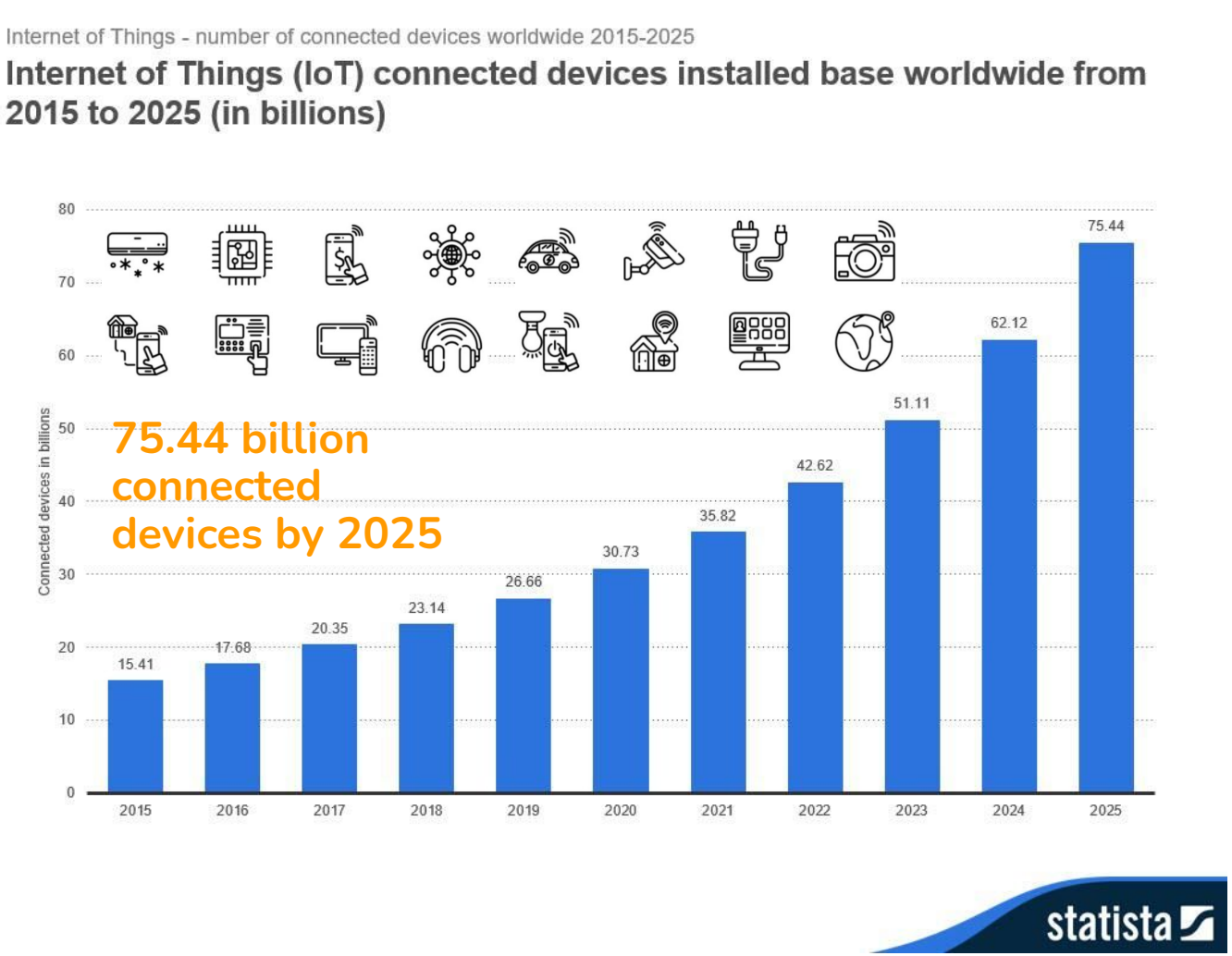
Data Collection & Transmission

Data Ingestion, Storage & Processing

Data Visualization & Analytics

- As a data-driven system, IoT is all about making business decisions based on data collected by smart devices
- The device security and data trustworthiness are essential for the success of IoT

IoT Devices - Smart Yet Flawed



Why are IoT Devices Vulnerable?

Business Aspects

- High volume and low cost
- Time-to-market pressure
- Specialized skills
- Steep learning curve
- User security awareness

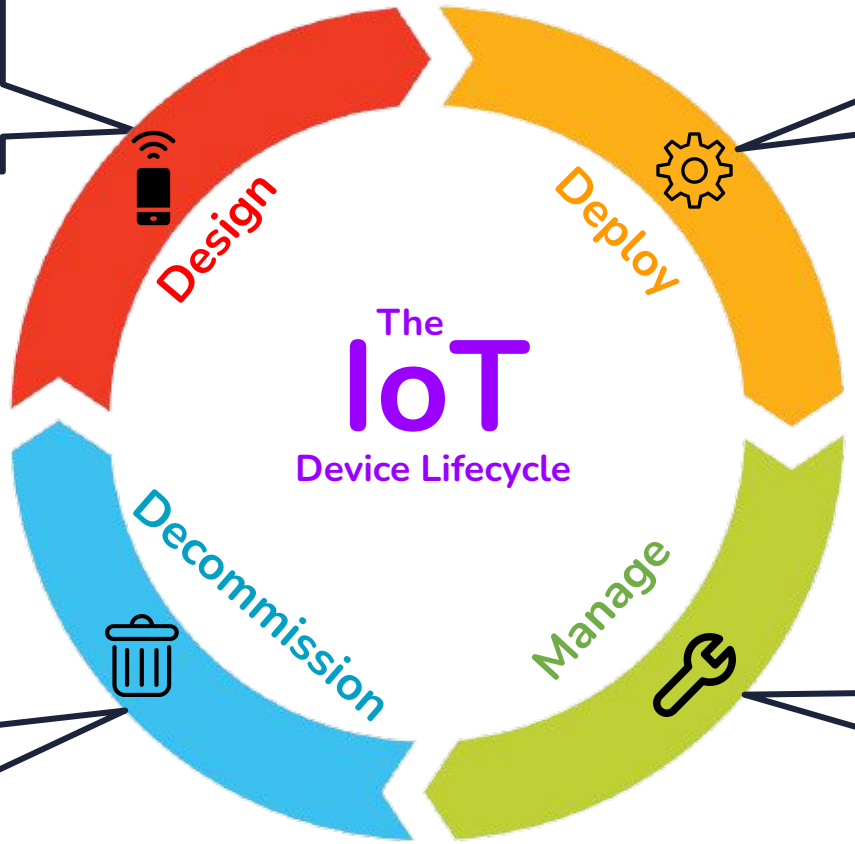
Technical Aspects

- Limited computational capabilities, memory footprint, and storage
- Heterogeneous transmission technologies
- Supply chain attacks
- Complex device lifecycle

Securing IoT Devices - A Lifecycle Approach

- Device Provisioning
- Identity Generation

- Network Onboarding
- Application Onboarding



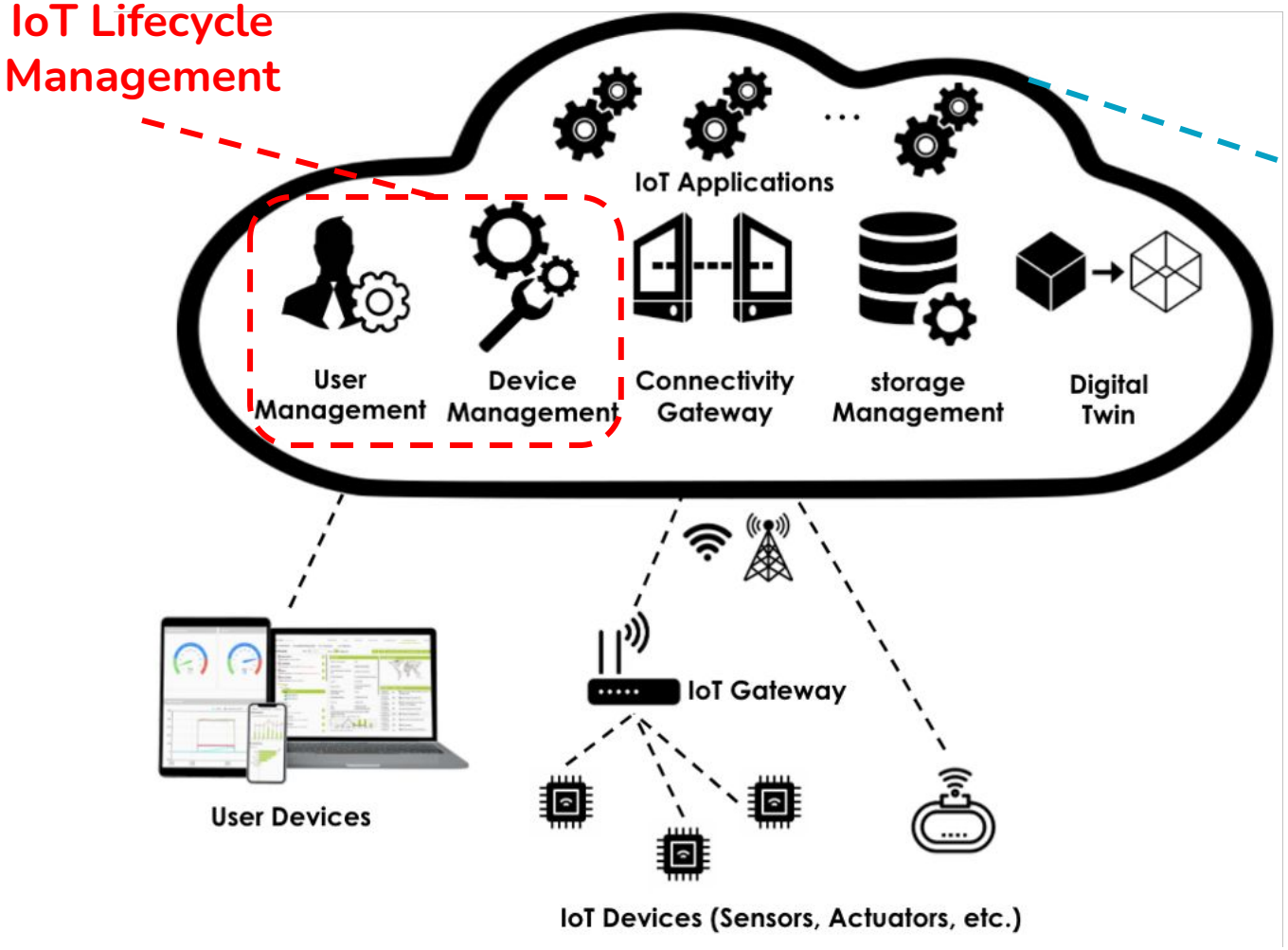
- Device Decommission
- Credential Revocation

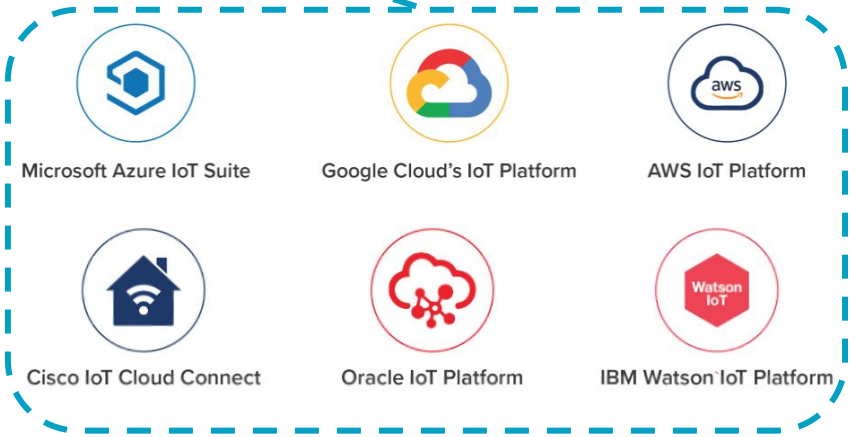
- Over-the-air Update
- Ownership Transfer

IoT Device Security: Today

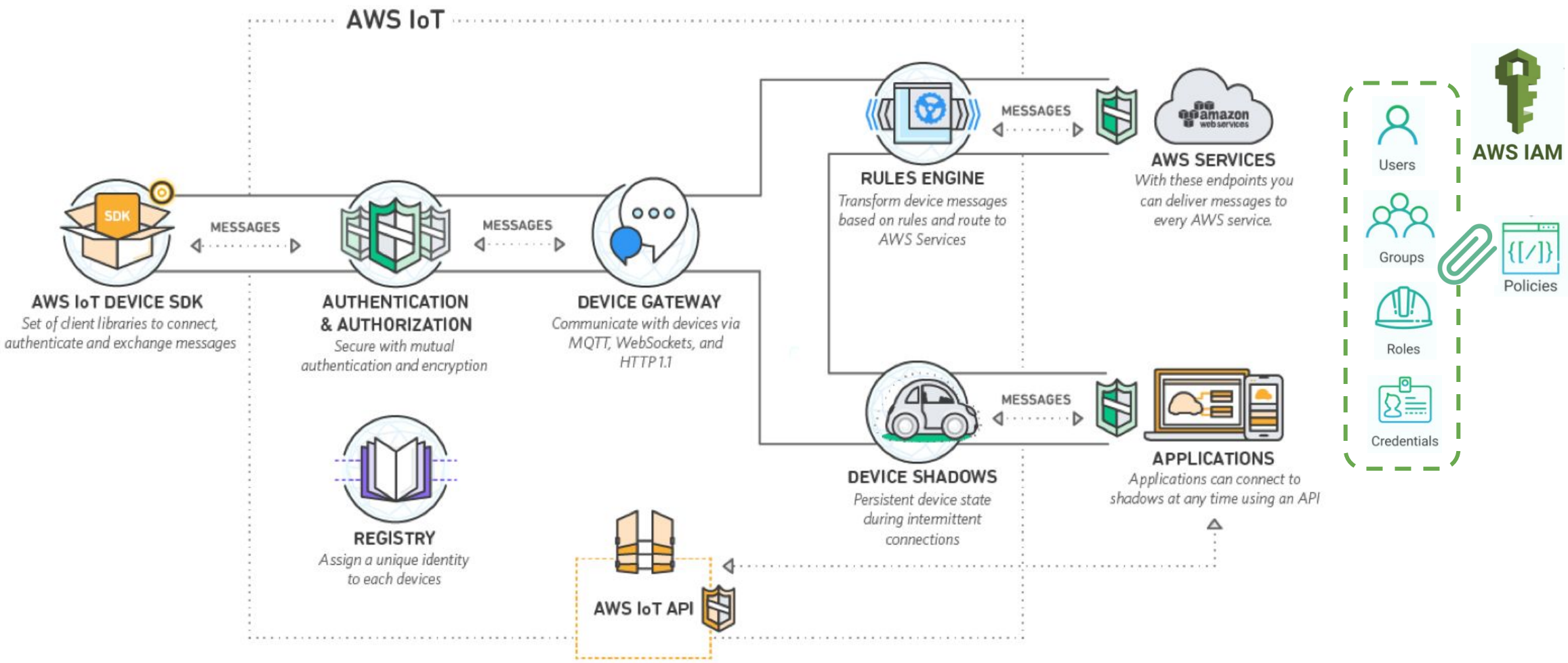
Centralized Approach

Cloud-Native IoT System Architecture





User and Device Management in AWS

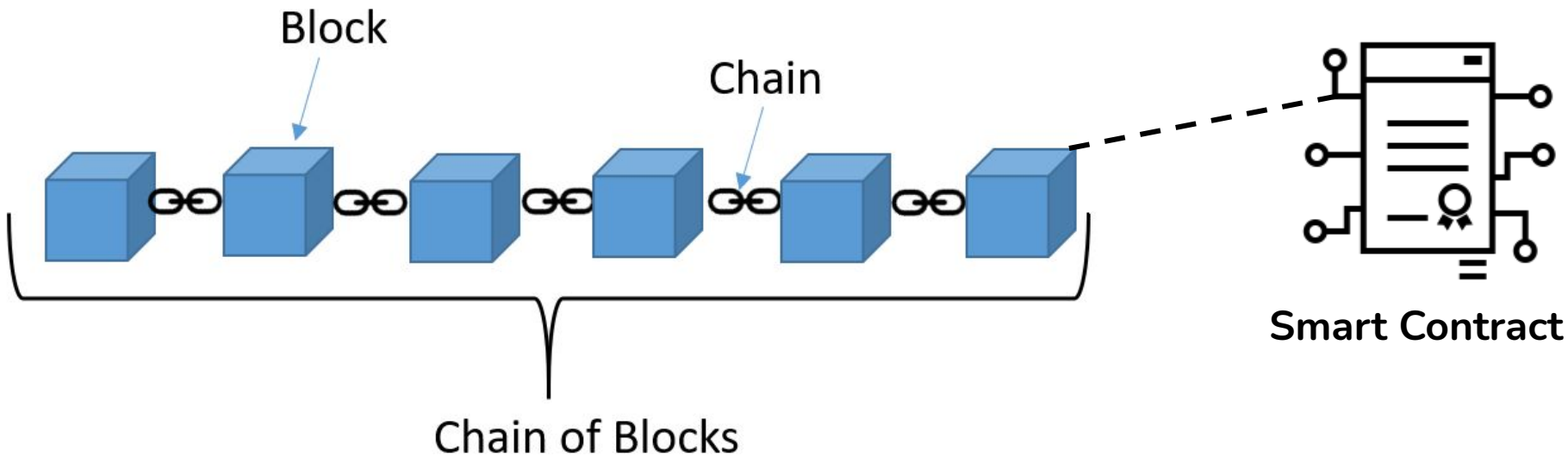


IoT Device Security: Tomorrow

Hybrid Approach

Blockchain and Smart Contract

- A blockchain is a collaborative, tamper-resistant ledger that maintains transactional records
- The transactional records are grouped into blocks
- A block is connected to the previous one by including a unique identifier that is based on the previous block's data
- A smart contract represents a piece of code that is stored, verified and executed on a blockchain



Why does Blockchain Matter for IoT Device Security?

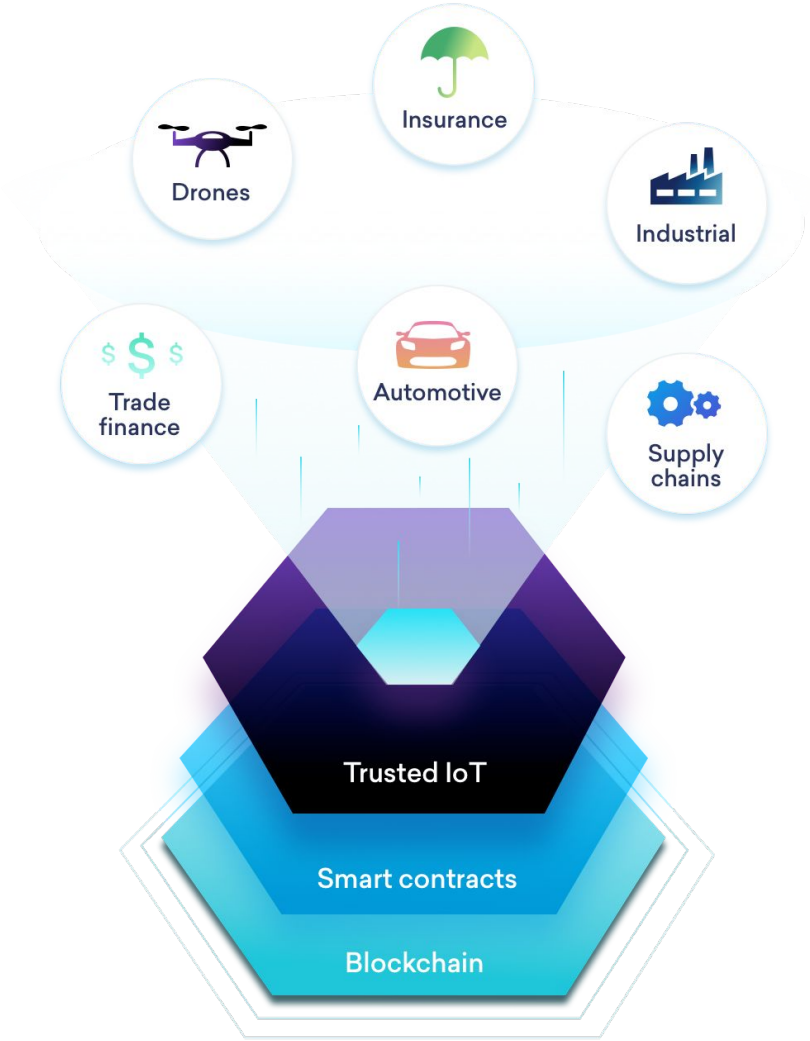
Remove single point of failure (decentralization)

Ensure data integrity (immutability)

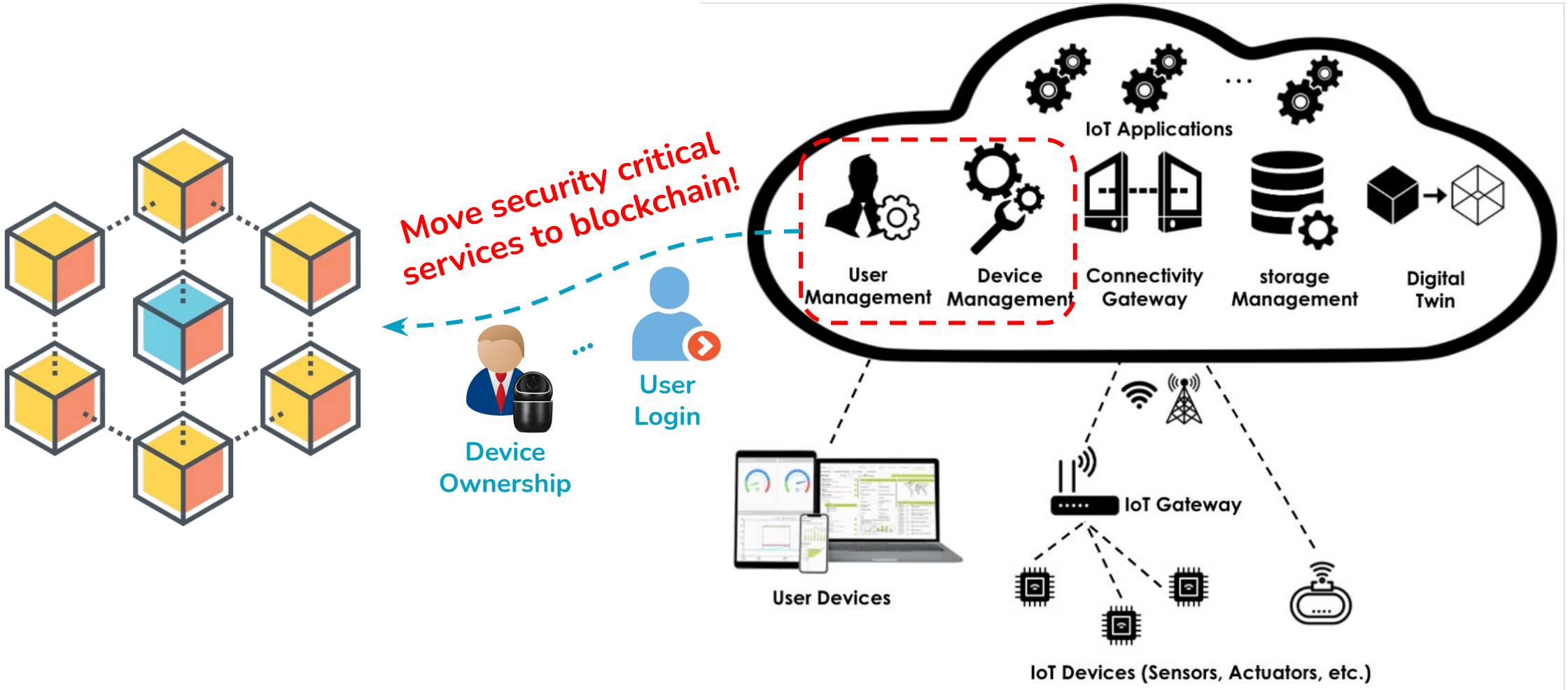
Track status of connected devices (Transparency)

Authenticate users and devices (Security & Resilience)

Build trust among IoT processes (Smart Contract)

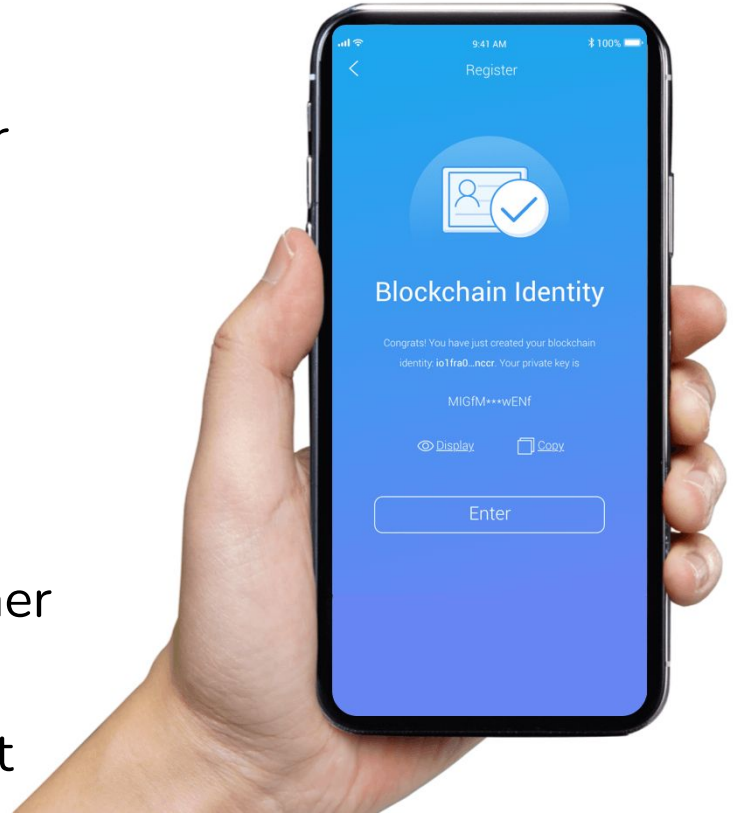


Blockchain-Enhanced IoT System Architecture



One-Click, Passwordless User Authentication with Blockchain

- A blockchain wallet is generated on the mobile app
- The blockchain address is passed to the IoT cloud for user account registration
- Each user account contain a blockchain address and a random challenge
- The mobile app signs the random challenge to complete login after the user's confirmation
- A JWT is issued to the user to access cloud storage or other cloud services
- The random challenge is updated after each login attempt



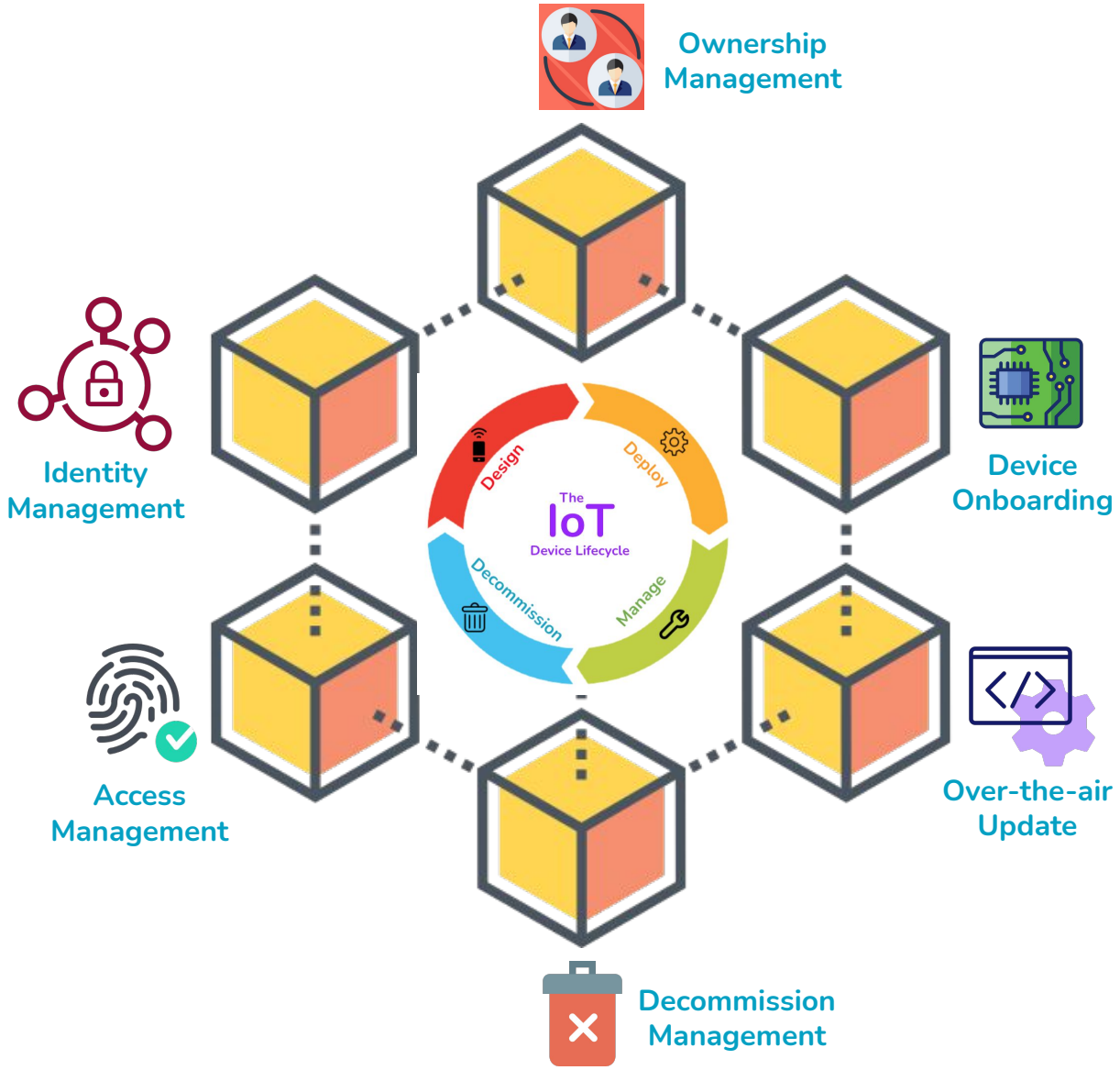
Device Ownership Protection with Blockchain

- A blockchain wallet is generated on a device during the manufacturing process
- An ownership management smart contract is deployed on the blockchain by the device manufacturer
- The owner sends his/her blockchain address to the device during the device binding process
- The device binds its blockchain address with its owner's one via digital signature
- The ownership management smart contract is invoked to validate and update the device ownership
- The blockchain holds the ground truth regarding device ownership

IoT Device Security: Future

Decentralized Approach

Blockchain-Orchestrated Device Lifecycle Management



Advantages

- High level security and resilience
- End-to-end trust from design to end-of-life
- Unified identity management
- Fine-grained access control
- Interoperability
- .....

IEEE P2958 Standards Project - Project Overview

- The Project Authorization Request (PAR) https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8651
- Project Scope: Define a decentralized IAM framework for IoT based on the emerging concepts such as decentralized identifiers (DIDs) and verifiable credentials (VCs)
- Working Group: Identity of Things Working Group (BOG/CAG/IDOTWG)

IEEE SA STANDARDS ASSOCIATION | IEEE P2958 – Identity of Things Working Group

IEEE P2958 Standards Project - Project Goal

- Integrate DIDs and VCs into the lifecycle of IoT devices
- Specify a suite of decentralized IoT security protocols:
  - Device identity Generation
  - Device onboarding
  - Device authentication
  - Data authorization & access control
  - ……
- Enable organizations and other solution providers to build blockchain-based DIAM-as-a-Service products

DIAM-as-a-Service

iot device security conference

Xinxin Fan

Head of Cryptography

IoTeX

IoTeX
xinxin@iotex.io
https://www.iotex.io/

LET'S BUILD DECENTRALIZED FUTURE TOGETHER!