Internet
of Things
World

How to Secure IoT with Blockchain

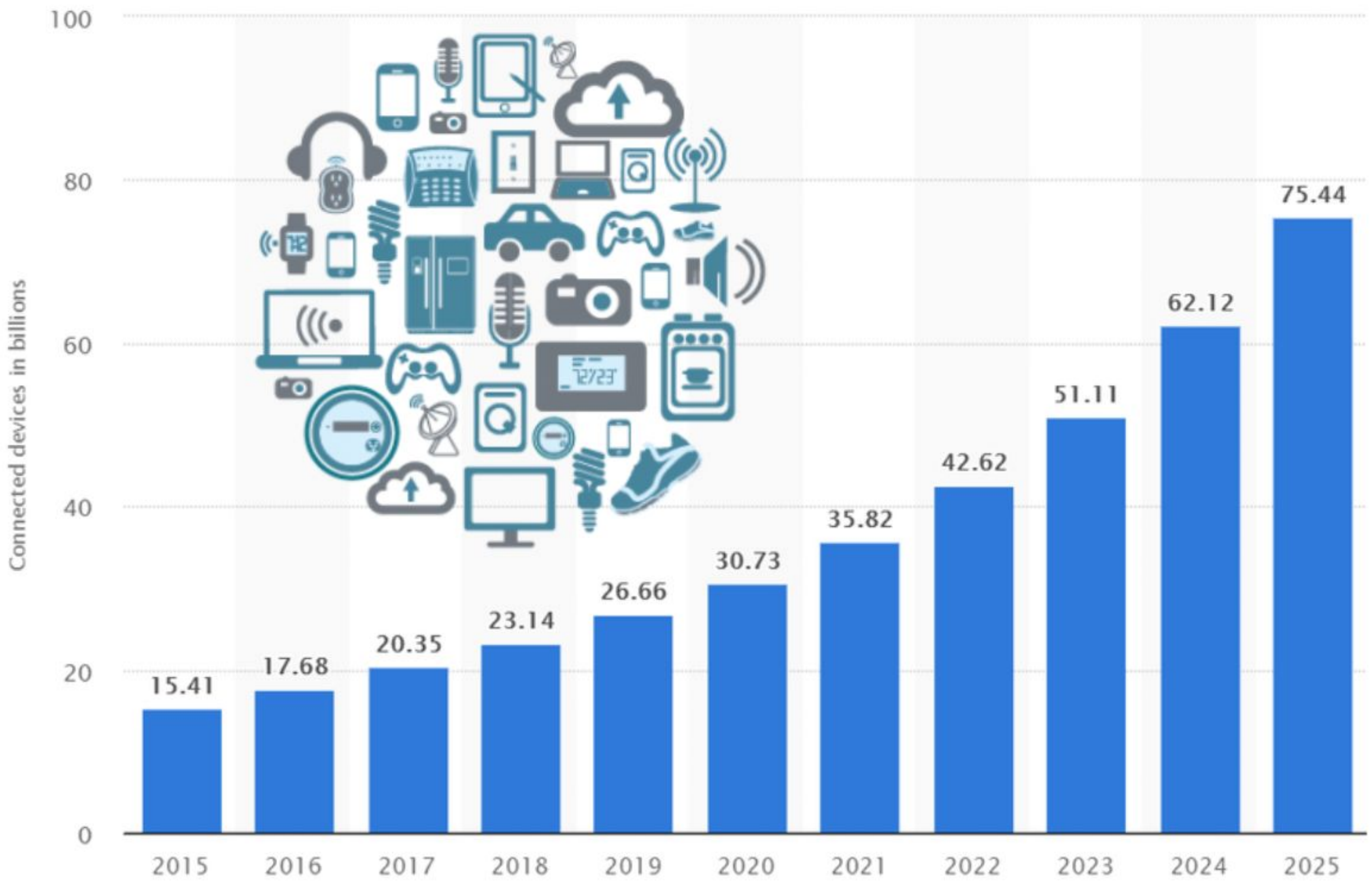
industrial internet®
CONSORTIUM

IoTeX

Xinxin Fan, PhD, CISSP
Head of Cryptography
IoTeX

Internet of Things World

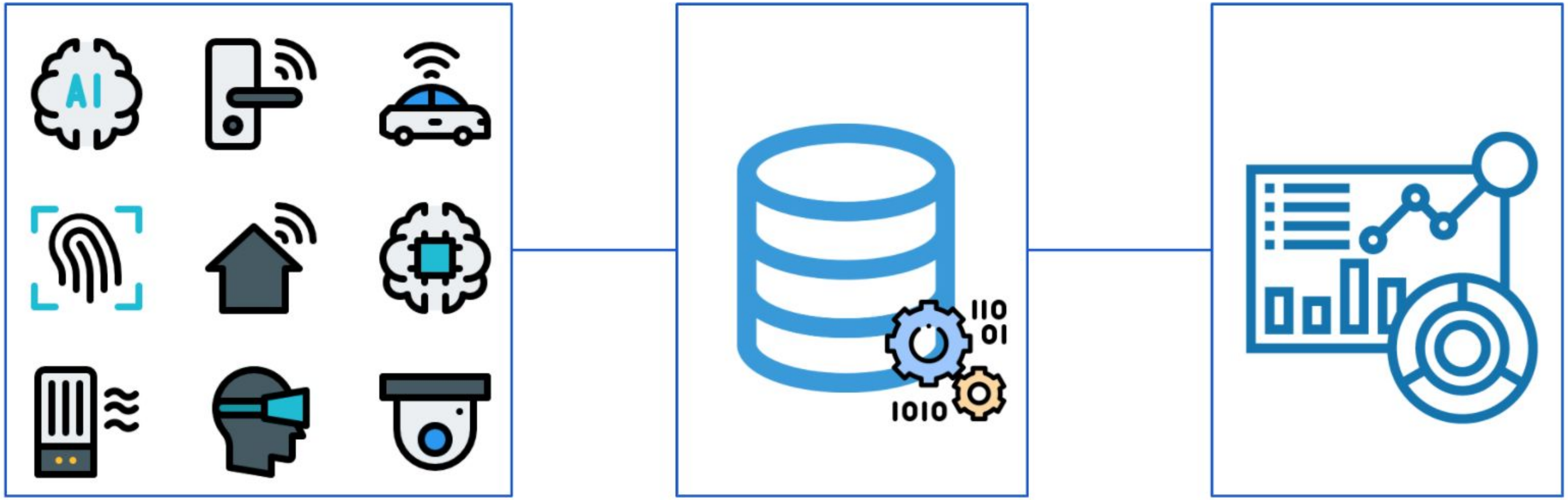
Size of the IoT Market Worldwide



Deployed IoT devices projected to be 75.44 billion by 2025

statista

Data-Driven IoT System



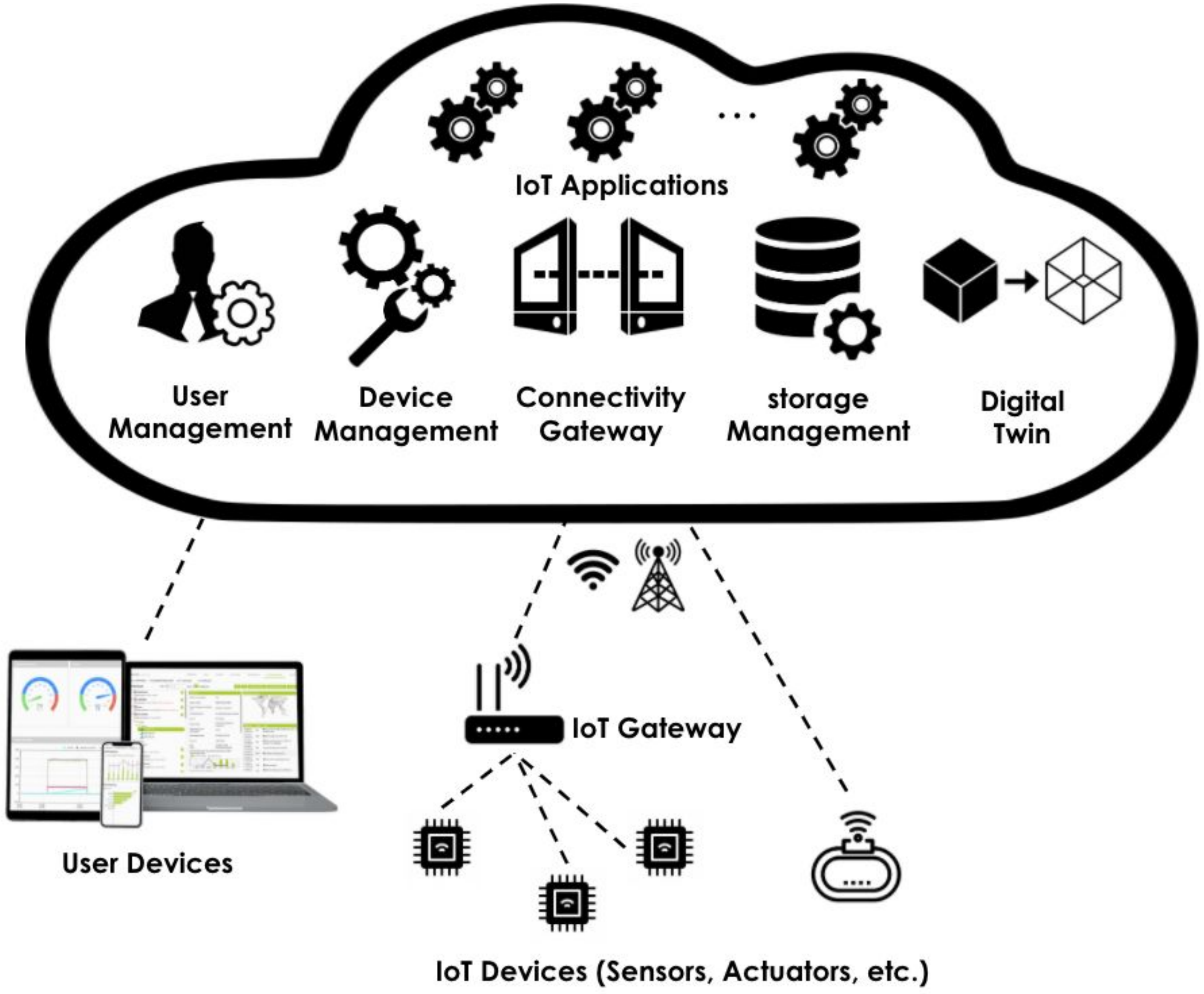
Data Collection & Transmission

Data Ingestion, Storage & Processing

Data Visualization & Analytics

IoT is all about making business decisions based on data collected by smart devices!

Cloud-Centric IoT System Architecture



IoT Security Challenges

Device Security

- Secure Hardware
- Secure OS

Communication Security

- Secure Link

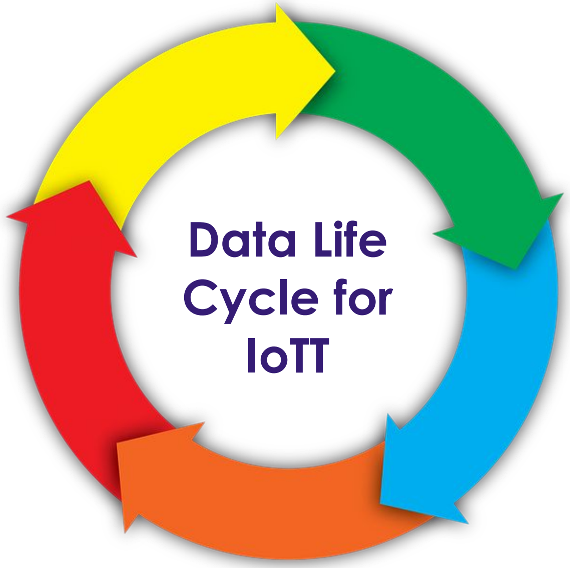
Cloud Security

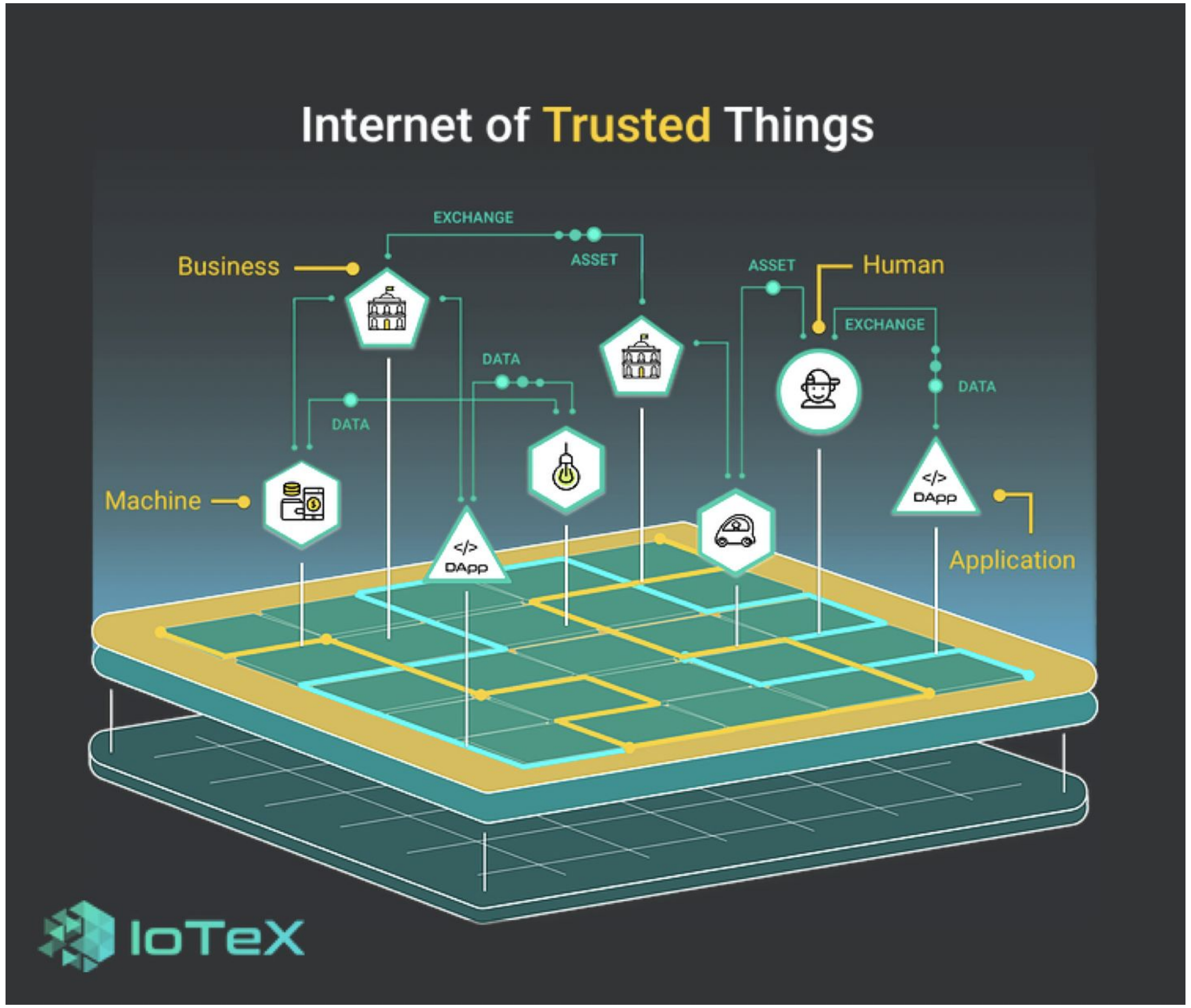
- Identity & Access Management
- Data Encryption
- Device Authentication
- Data Authorization
- DDoS Resilience
- Device Management

Data Trustworthiness in IoT Systems

Internet of Trusted Things (IoTT)

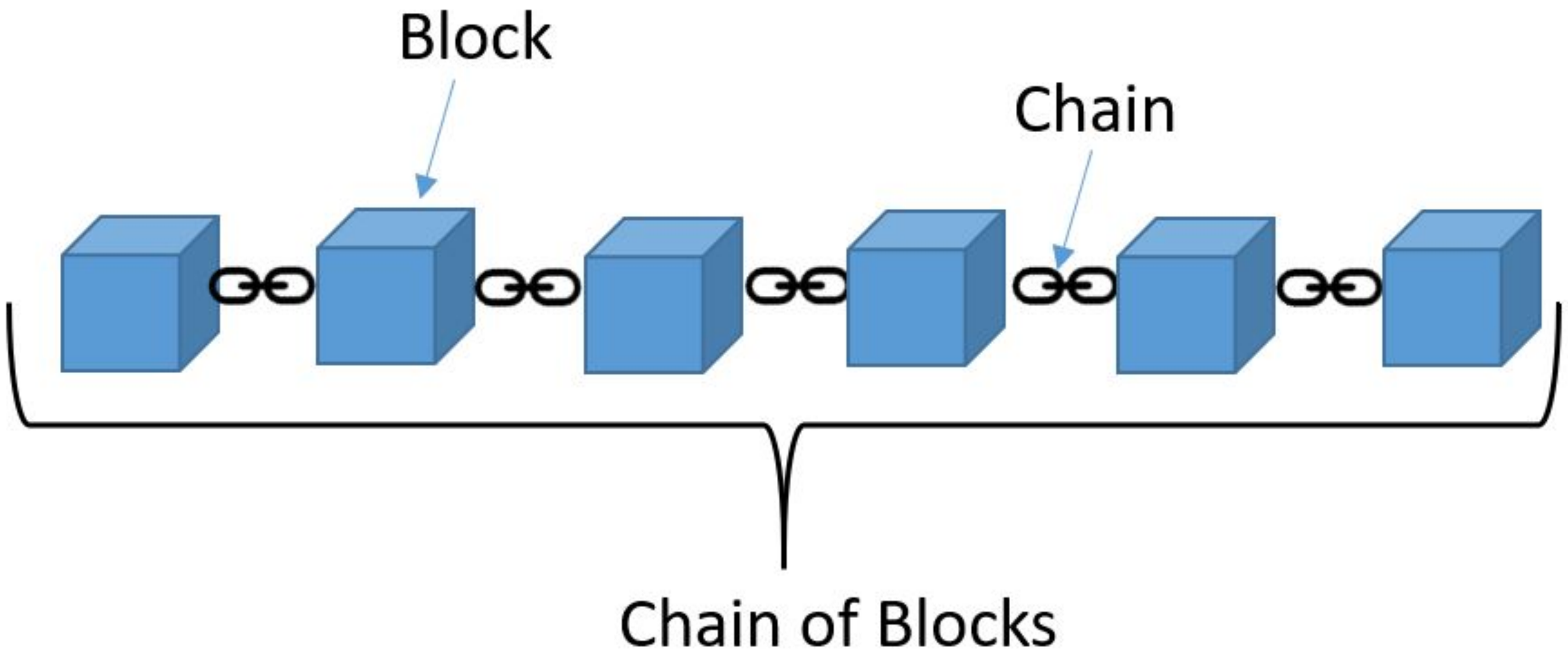
- Data collection
- Data in transit
- Data at rest
- Data processing
- Data retention





Blockchain in a Nutshell

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company or government).

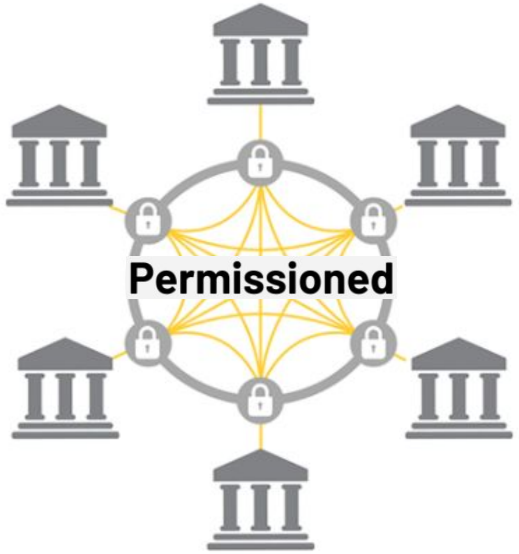


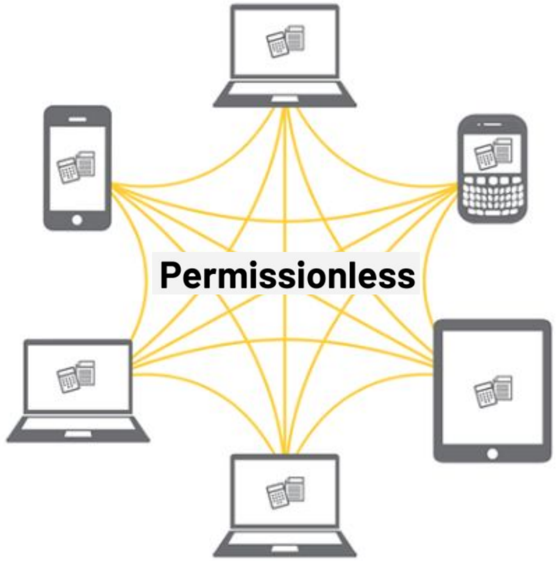
NIST
National Institute of Standards and Technology

Permissionless vs. Permissioned Blockchains

Permissionless blockchain

- Anyone can join the network
- Anyone can read the ledger data and validate transactions
- Ledgers replicate the high degree of trust





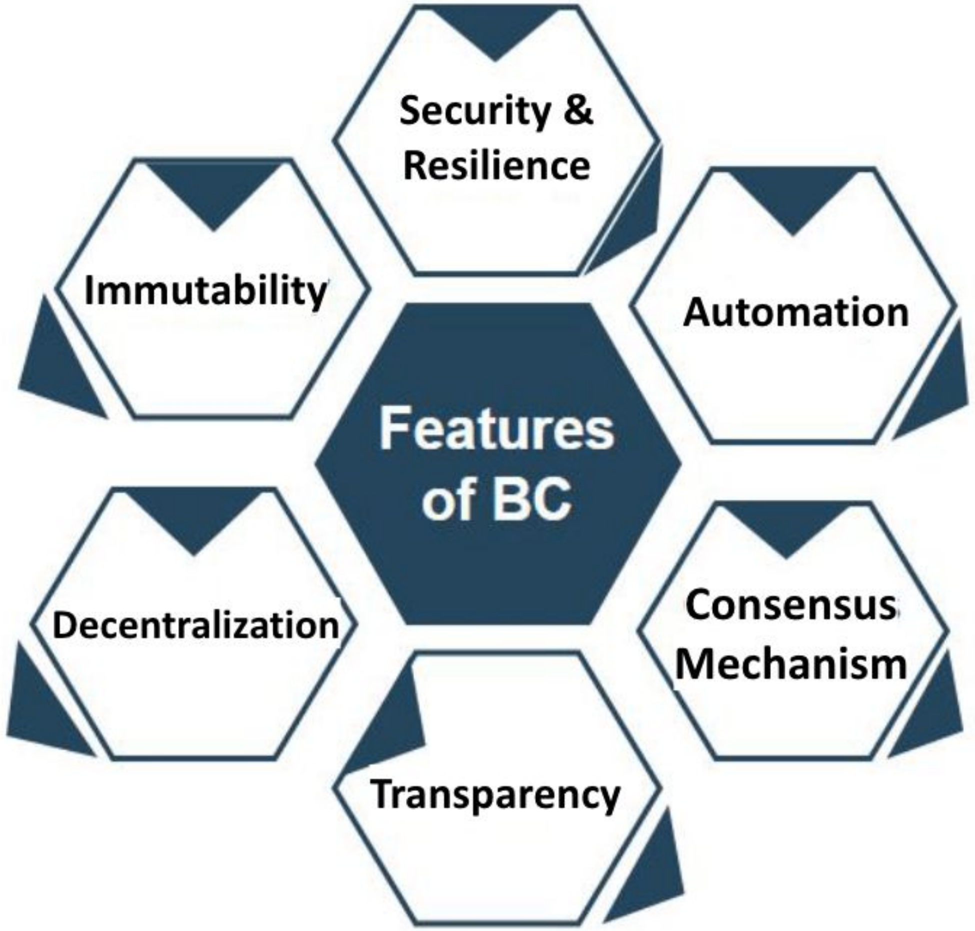
Permissioned blockchain

- Formed by a set of known transacting parties
- Validation is controlled by a selected set of nodes
- Ledgers replicate the high degree of transparency and accountability

Internet of Things World

Salient Properties of Blockchains

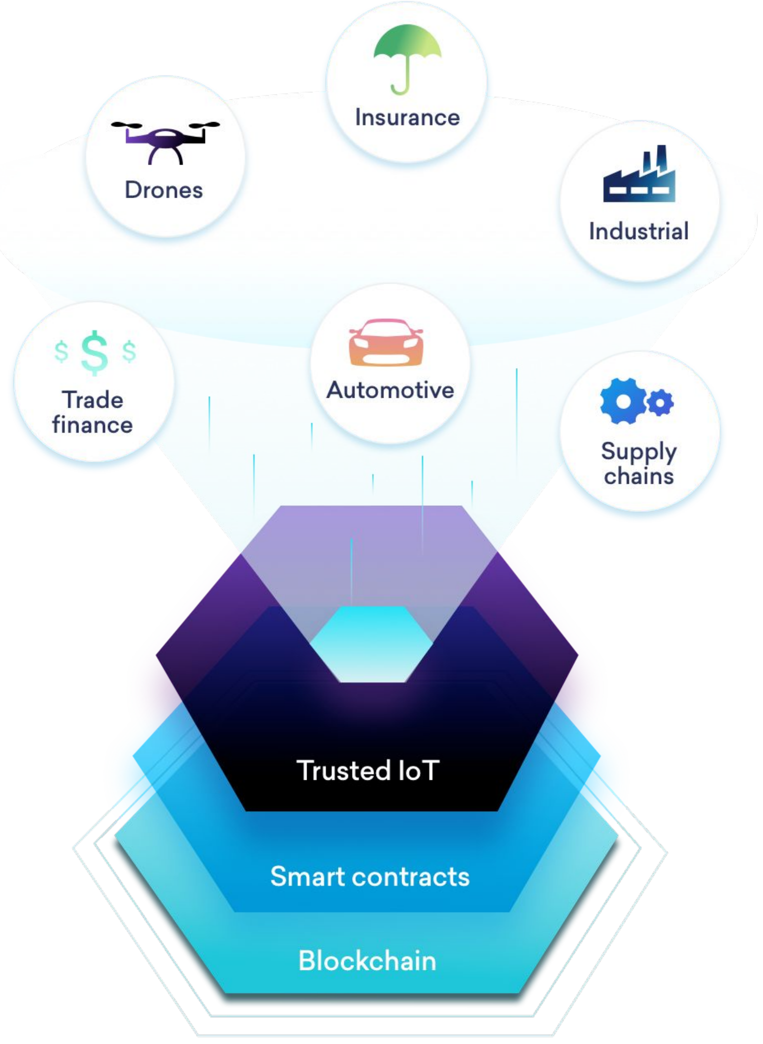
- **Decentralization**: Remove the ‘single-point-of-failure’ embodied in a trusted central authority
- **Immutability**: Use cryptographic hashes
- **Transparency**: Provide a fully auditable and valid ledger of transactions
- **Security and Resilience**: Use public-key cryptography and digital signatures to prove ownership of data and allows the ownership to be transferred
- **Automation**: Streamline complex business processes that involve multiple intermediaries using smart contracts



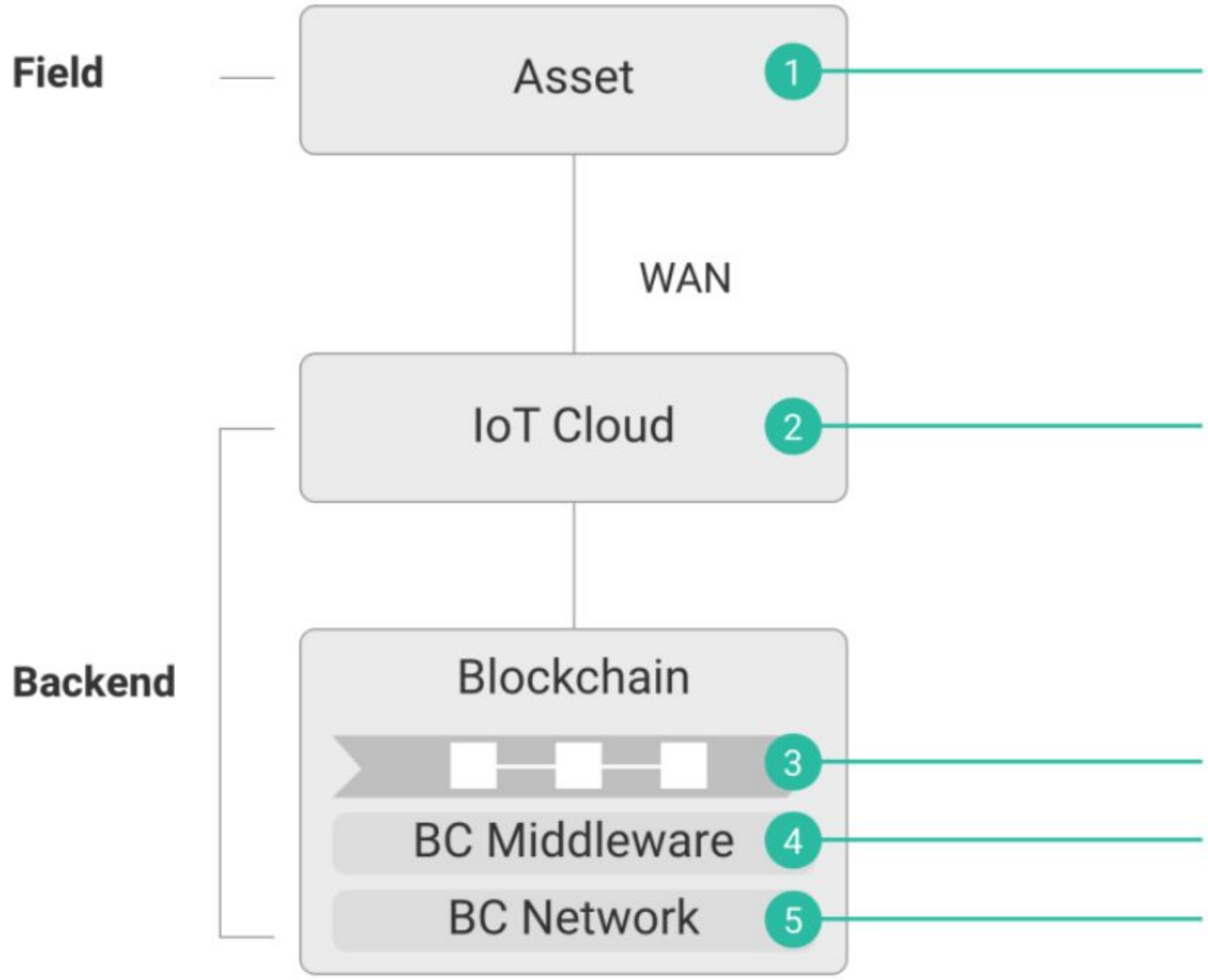
Internet of Things World

Security Implications for IoT Applications

- 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 & IoT Reference Architecture



Asset Layer

- Examples: Truck, Train, Machine
- Includes local and remote communication and processing (on asset, fog)

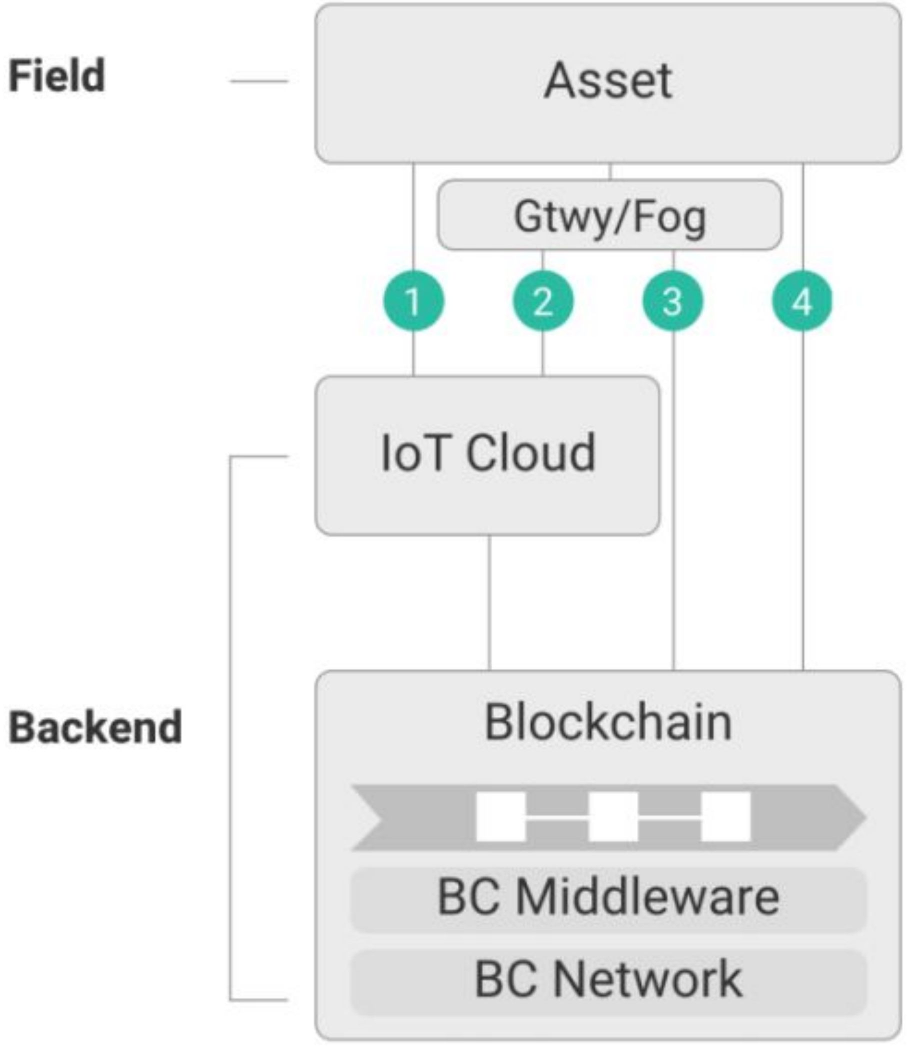
IoT Cloud Layer

- Asset connectivity & FOTA
- Asset-related data and event management
- Enterprise Application Integration

Blockchain Layer

- Asset-related ledger entries
- Peer-to-Peer Middleware for management of BCs
- Network of compute nodes for BC

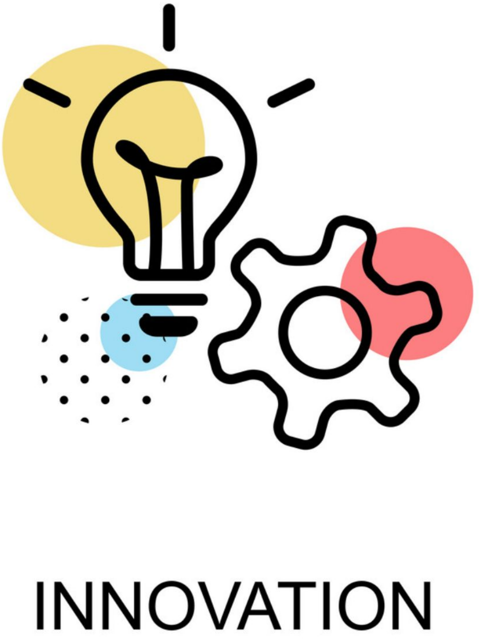
Four Blockchain & IoT Integration Patterns



1. **Asset → IoT Cloud → Blockchain**
2. **Asset → Gateway/Fog → IoT Cloud → Blockchain**
3. **Asset → Gateway/Fog → Blockchain**
4. **Asset → Blockchain**

https://hub.iiconsortium.org/portal/IndividualContribution/5db03a83f7679b000f0e762f

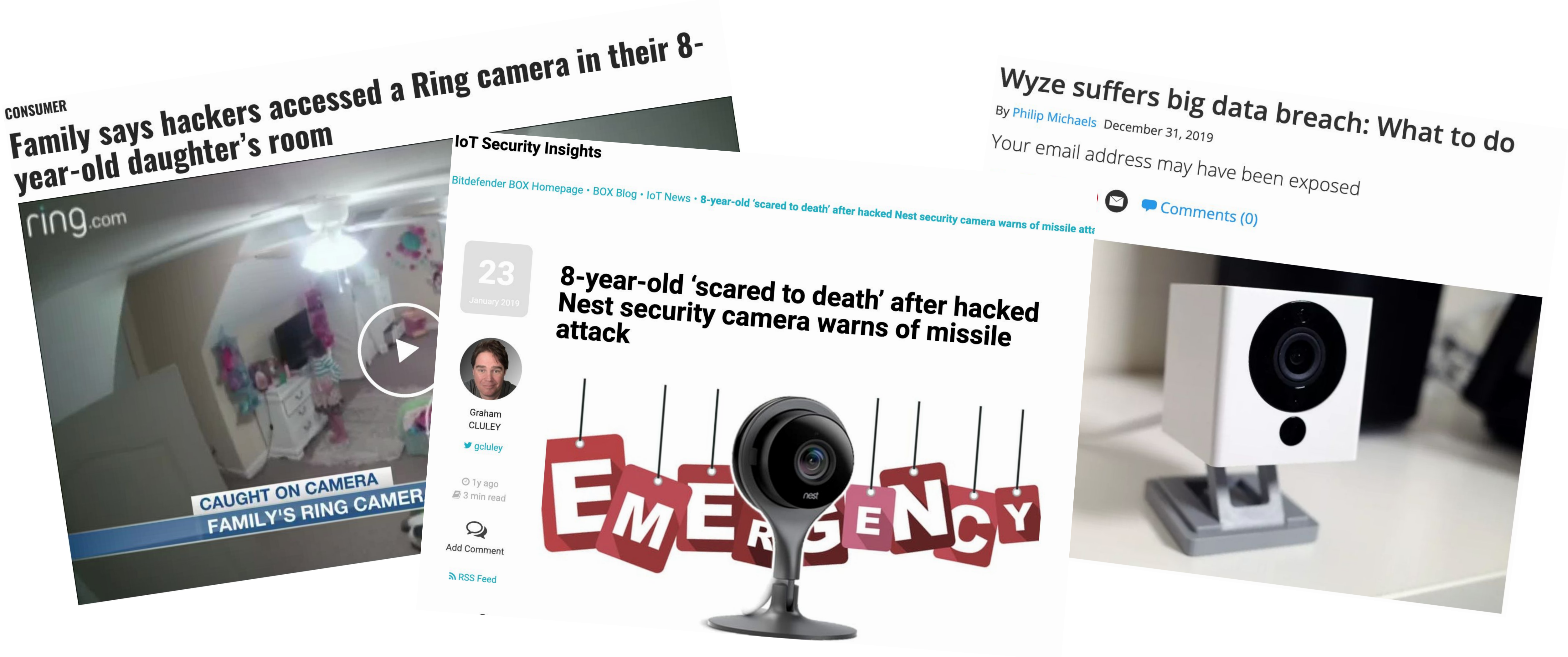
Case Study - When Home IP Camera Meets Blockchain



Can we enhance the security of home IP camera systems using blockchain?

Internet of Things World

Security of Home IP Cameras



CONSUMER

Family says hackers accessed a Ring camera in their 8-year-old daughter's room

IoT Security Insights

Bitdefender BOX Homepage • BOX Blog • IoT News • 8-year-old 'scared to death' after hacked Nest security camera warns of missile atta

23 January 2019

Graham CLULEY

gcluley

1y ago

3 min read

Add Comment

RSS Feed

8-year-old 'scared to death' after hacked Nest security camera warns of missile attack

Wyze suffers big data breach: What to do

By Philip Michaels December 31, 2019

Your email address may have been exposed

Comments (0)

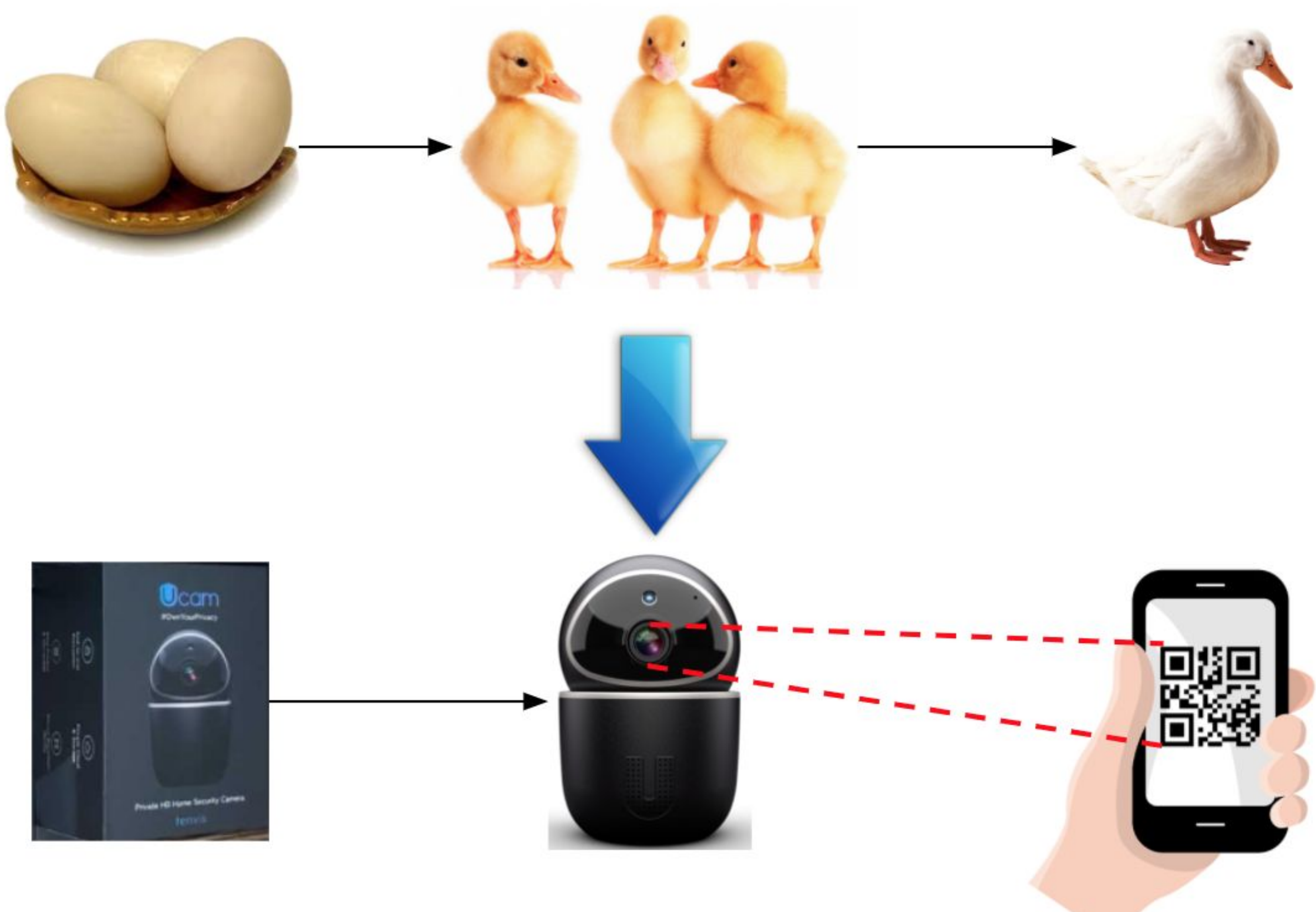
Major Security Concerns

- Username/password-based logins
  - Poor/leaked password w/o MFA
  - Buggy IAM systems
- Database breaches
  - Password leakage
  - Ownership compromise
- Insecure device binding
  - Ownership compromise
- Data integrity of local/cloud storage
  - Insert, delete, modify video clips

Passwordless User Authentication

- 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

Blockchain-Based Ownership Management

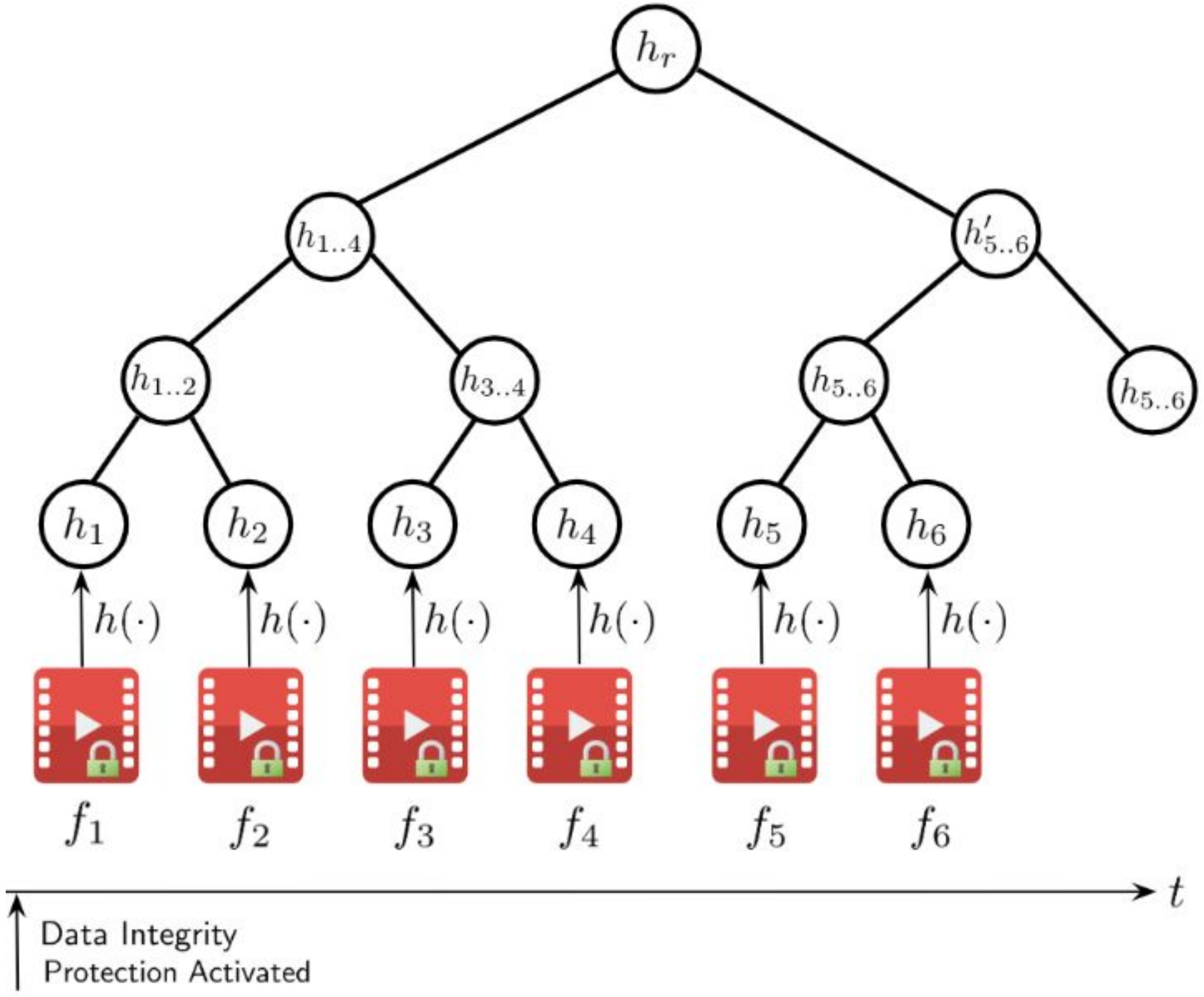


Resurrecting Duckling Security Model

- Device binding is conducted using the resurrecting duckling security model
- The camera associates its blockchain address with its owner’s one and invokes the ownership management smart contract on the blockchain
- Each device reset will restart the device binding process
- The blockchain serves as the ground truth regarding device ownership

Blockchain-Based Data Integrity Protection

- The user enables the data integrity feature on the mobile app and specify the time period in days for checkpoint commitments.
- The camera builds a Merkle tree dynamically for video clips received during the user-specified time period
- The camera invokes the checkpoint management smart contract for integrity checkpoint commitments.
- The user is able to verify data integrity of video clips retrieved from the SD card or cloud storage with the Merkle root.



Design Methodology Highlight

- Username/password based login is replaced by passwordless login using blockchain wallet
- Device ownership is managed by a smart contract in blockchain
- Data integrity of local/cloud storage is ensured by retrieving the Merkle root from blockchain

CES INNOVATION AWARDS 2020 HONOREE

CES Innovation Award for Cybersecurity & Personal Privacy

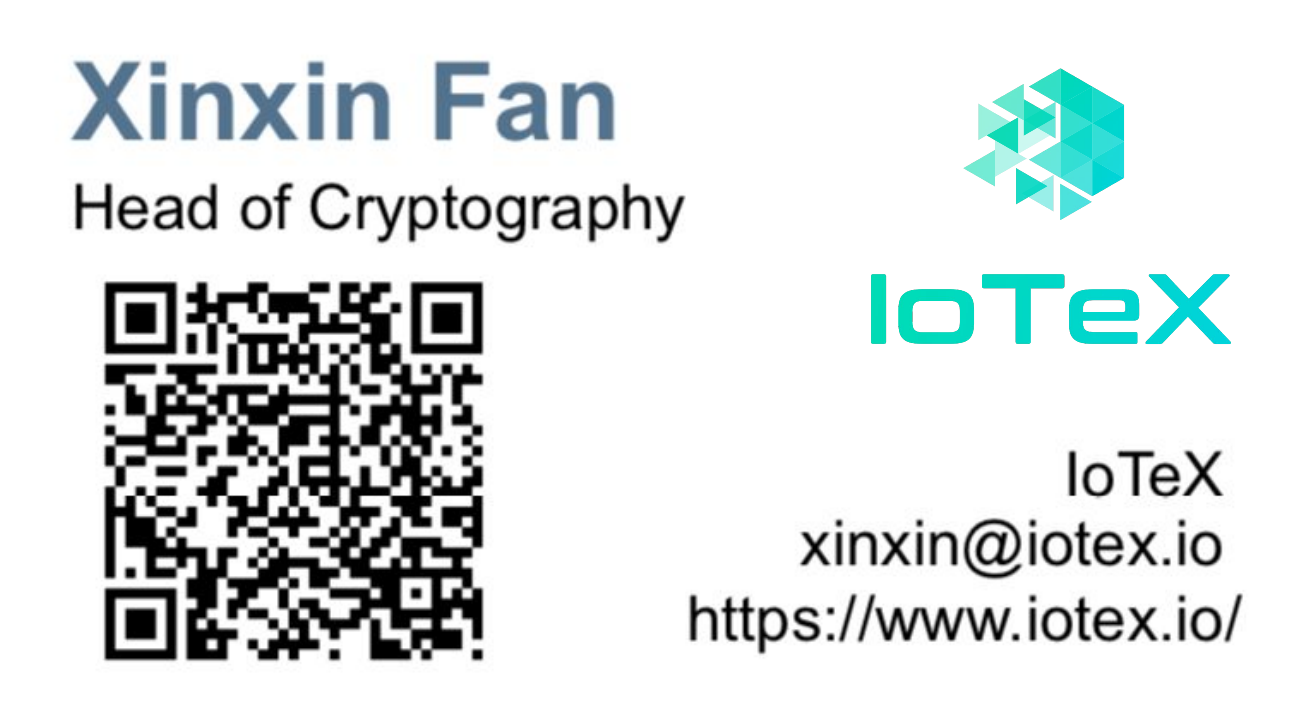
tenvis

Built in partnership with leading security camera manufacturer

Ucam

Powered by IoTeX

Internet of Things World



Xinxin Fan

Head of Cryptography

IoTeX

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

industrial internet®
CONSORTIUM