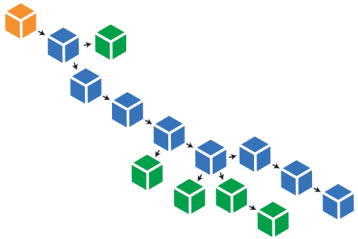
DLT & TEE make IoT to be trust

Lloyd Huang
VP Engineering
2019 June 21

創世・比特幣

數位貨幣及交易

- 挖礦、記帳 - 獎勵機制
- 分散式帳本 - 去中心化
- 不可竄改 - BlockChain



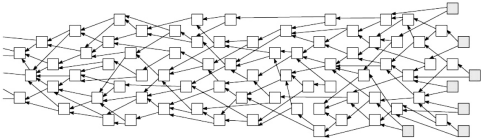
後起新秀 · blockchain 2.0 3.0 ?

智能合約

- 乙太坊
- EOS

DAG Tangle

- IOTA
- TOP



量子危機？

BiiLabs - Blockchain Industry and Innovation Labs

- 存查証・數位公証人
  - 水資源、空氣盒子
  - 保險 (車險、保單)，特殊金融
- 物聯網｜能源交易記錄・數位記帳士
  - 電表-綠能交易
  - 電池 ID
- 新型態資料交易
- 去中心化數位身份・DiD
  - 証書
  - 最小揭露

Application Story: DLT for Water Quality Monitoring

Application	Water quality monitoring
Region	Asia Pacific
Issue	Too much cost carried by the enterprise and lack trust of water quality examination result
DLT Solution	BiiLabs Sentinel Appliance with Alfred API
Benefit	- Lower cost and increasing efficiency for the enterprise - Trust-building among people, government, and enterprise

Application Story: DLT for Air Quality Monitoring

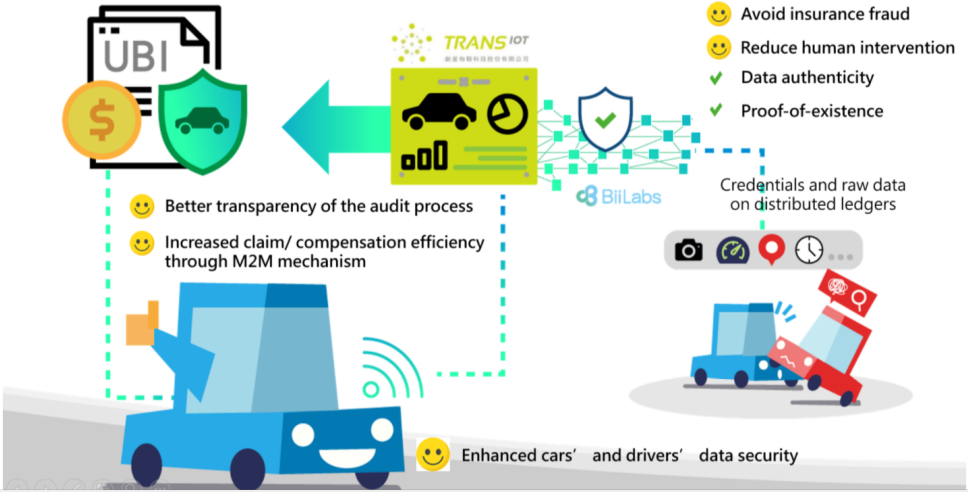
3000+ sensors (**AirBox**) around Taiwan w/ low-level H/W, restricted connectivity and different ownership (typical academic & open source project)

Open Data
airbox.taipei

Migrate AirBox (Low-end H/W like RPi3) to be a end to end solution and put data on the DLT

- Air Box Solution is introduced to over 8 Cities in Taiwan
- The Business Model is ready to shift to other countries, ex. South Korea

Application Story: DLT for UBI



Application Story: DLT for Battery

不同廠商的電池交換？

路邊停車的充電樁？

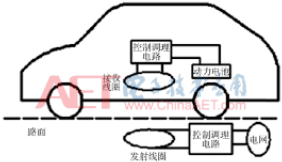


图 1 电动汽车无线充电原理图

等紅燈時無線充電？

- 電動車時時充電與交換的時代，還能用哩程計價嗎？
- 能源交換的生態形成，量大小額的能源交換與計價模式就會出現與成形。

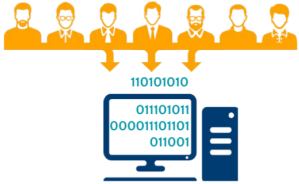
Forces Impacting Security

Challenges in implementing, maintaining, and protecting products and processes

FRAGMENTATION
of Security Offerings

Thousands of security related products from **hundreds** of vendors

INDUSTRIALIZATION
of Hacking



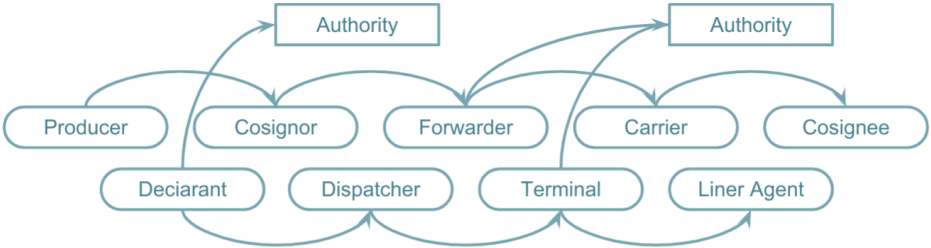
Criminal **sophistication** and evolving intent to get to your **data**

EXPANSION
of Attack Surface

Billions of connected devices and the move to the cloud

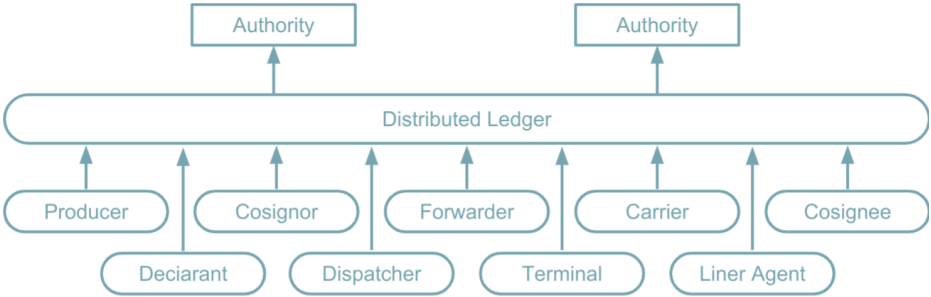
Nowadays

Lack of common pool for trusted computing

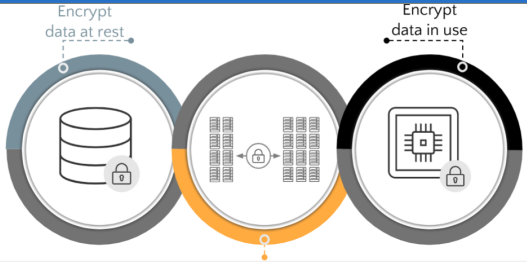


Vision

Build a comprehensive layer for connected devices and user interactions based on Distributed Ledger

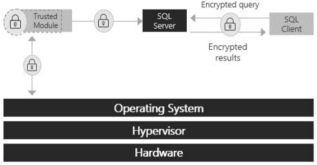


BiiLabs' Trusted Execution Environments

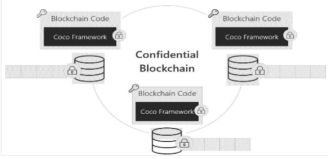


Current Use Cases:

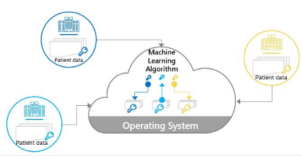
Data Integrity



Blockchain



Data Marketplace



Protecting Data Through its Lifecycle

Existing | New

At rest

Encrypt inactive data when stored in database files, backup files, log files, etc.

In transit

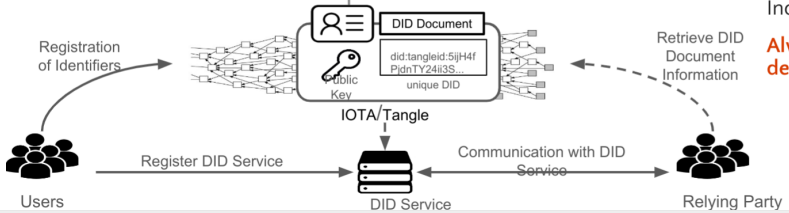
Encrypt data that is flowing between applications and the persistent storage

In use

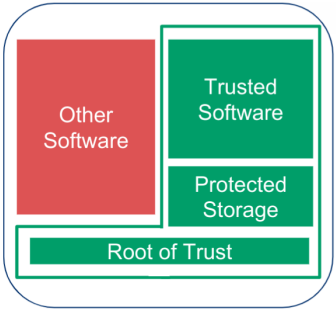
Protect/Encrypt data that is in use during computation

Industry-first solution:

Always Encrypted and decentralized



Can hardware-assisted "trusted computing" help?



Hardware support for

- Isolated execution
- Protected storage: Sealing
- Ability to report status to a remote verifier: Attestation

Trusted Execution Environment (TEE)

Cryptocard s

https://www.ibm.com/security/cryptocard/

Trusted Platform Modules

https://www.infineon.com/tpm

ARM TrustZone

arm

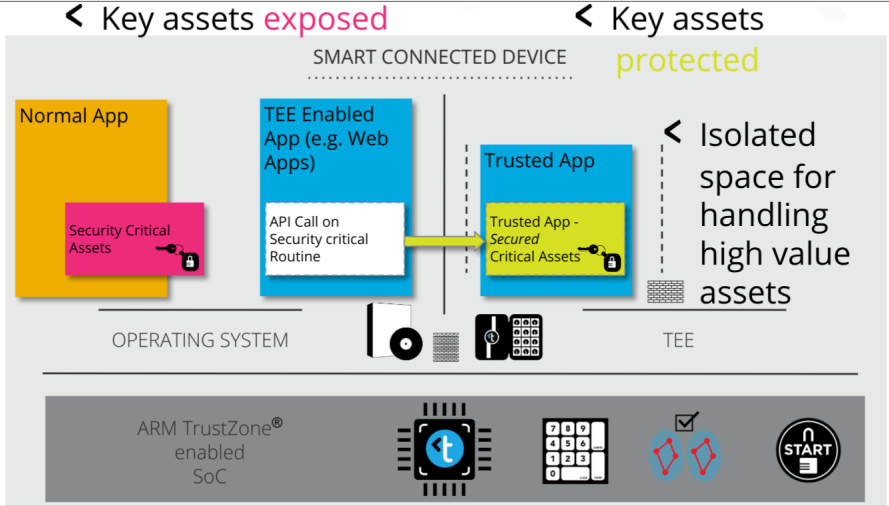
https://www.arm.com/products/security-on-arm/trustzone

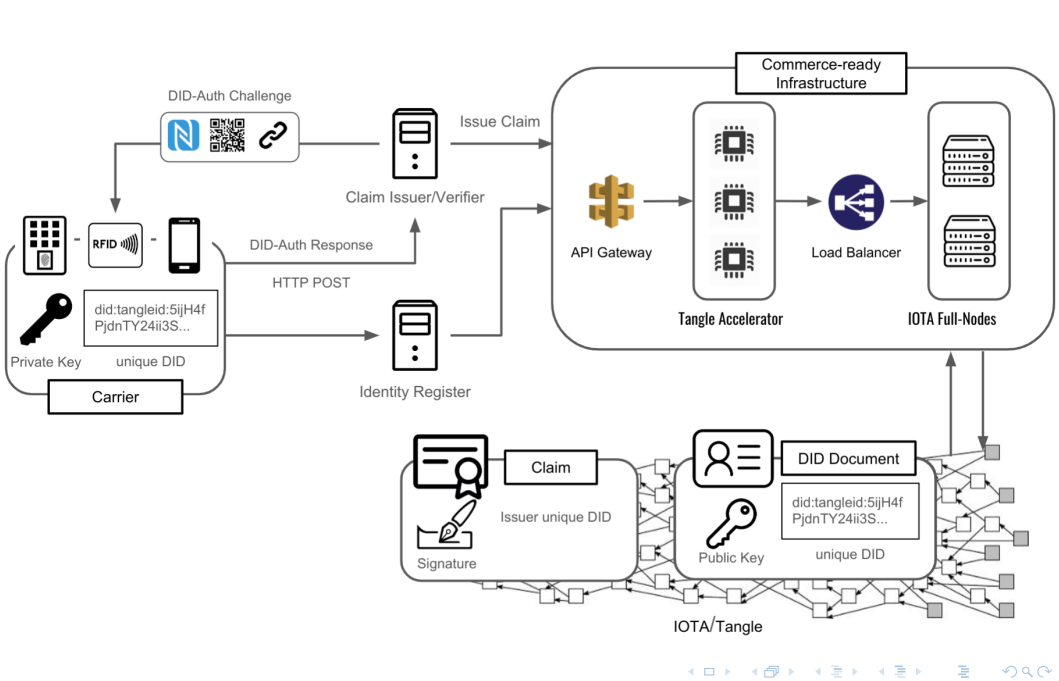
Intel Software Guard Extensions

intel

https://software.intel.com/en-us/sgx

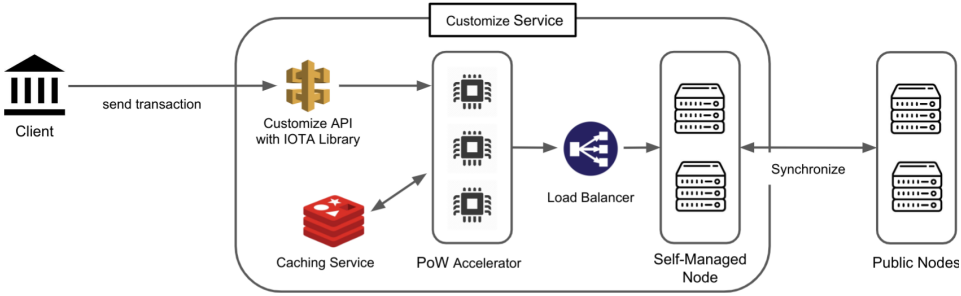
Why use a TEE?


Key assets exposed
Key assets protected
SMART CONNECTED DEVICE
Normal App
Security Critical Assets
TEE Enabled App (e.g. Web Apps)
API Call on Security critical Routine
Trusted App
Trusted App - Secured Critical Assets
Isolated space for handling high value assets
OPERATING SYSTEM
TEE
ARM TrustZone® enabled SoC
START

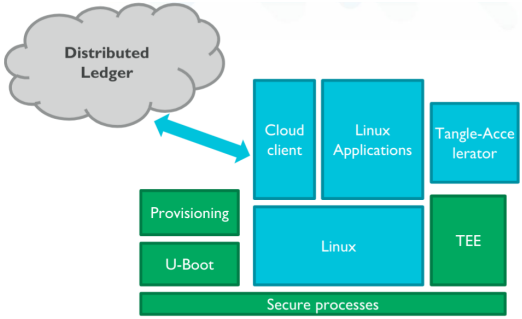

DID-Auth Challenge
Issue Claim
Commerce-ready Infrastructure
Claim Issuer/Verifier
RFID
DID-Auth Response
HTTP POST
API Gateway
Load Balancer
Tangle Accelerator
IOTA Full-Nodes
did:tangleid:5ijH4f
PjdnTY24ii3S...
Private Key
unique DID
Carrier
Identity Register
Claim
Issuer unique DID
Signature
DID Document
did:tangleid:5ijH4f
PjdnTY24ii3S...
Public Key
unique DID
IOTA/Tangle

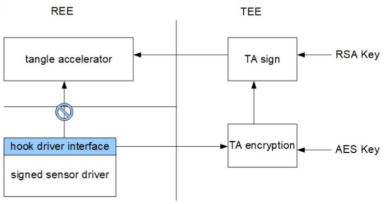
Unique Backbone

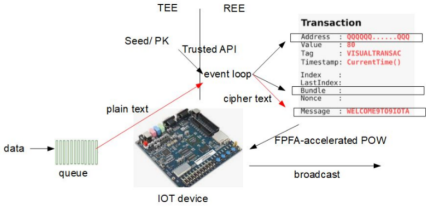
scalability and high availability(HA) with cost-efficient infrastructure



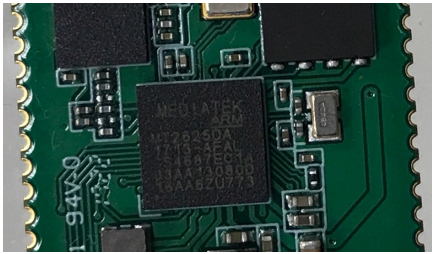
Distributed Ledger + TEE







NB-IoT



- CPU ARM Cortex-M4 with FPU and MPU
- RAM 4MB PSRAM
- Flash 4MB NOR
- Wireless NB-IoT
- ID e-SIM
- OS FreeRTOS
- Protocol MQTT
- DLT (Distributed Ledger Technology)

Enabling the Trusted Economy

BiiLabs

Dedicated to Blockchain Innovation to the Industries

#BiiLabsrocks

#BiiLabsrocks

#BiiLabsrocks