Hitcon Badge 2018

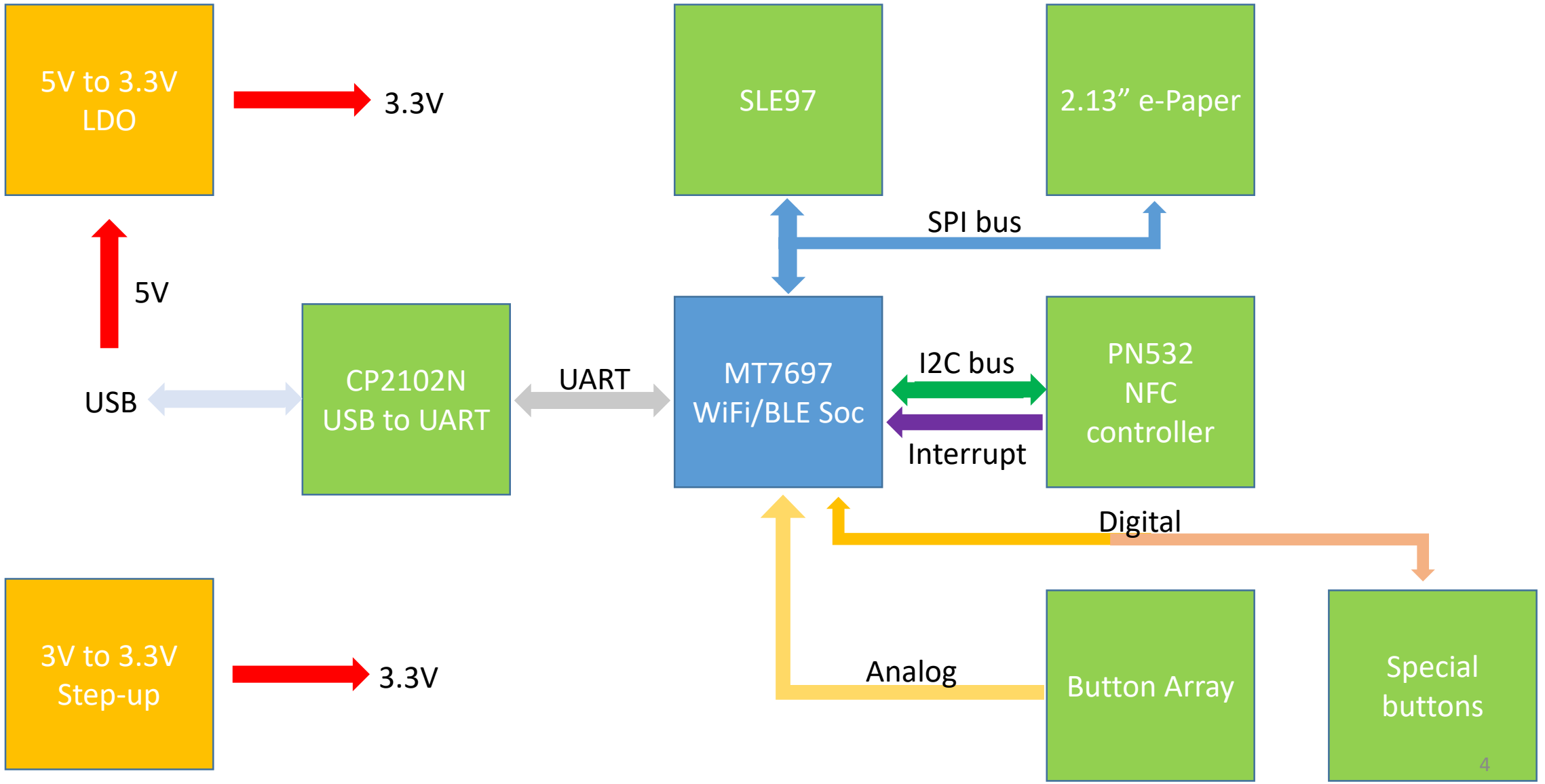
MEDIATEK 黃偉峻 MEDIATEK 李倫銓

Guidline

- Hardware overview
- Subsystems
- ETH Transaction
- HD Wallet - BIP32,39,44
- Secure Element with Wallet
- Manufacture
- Documents

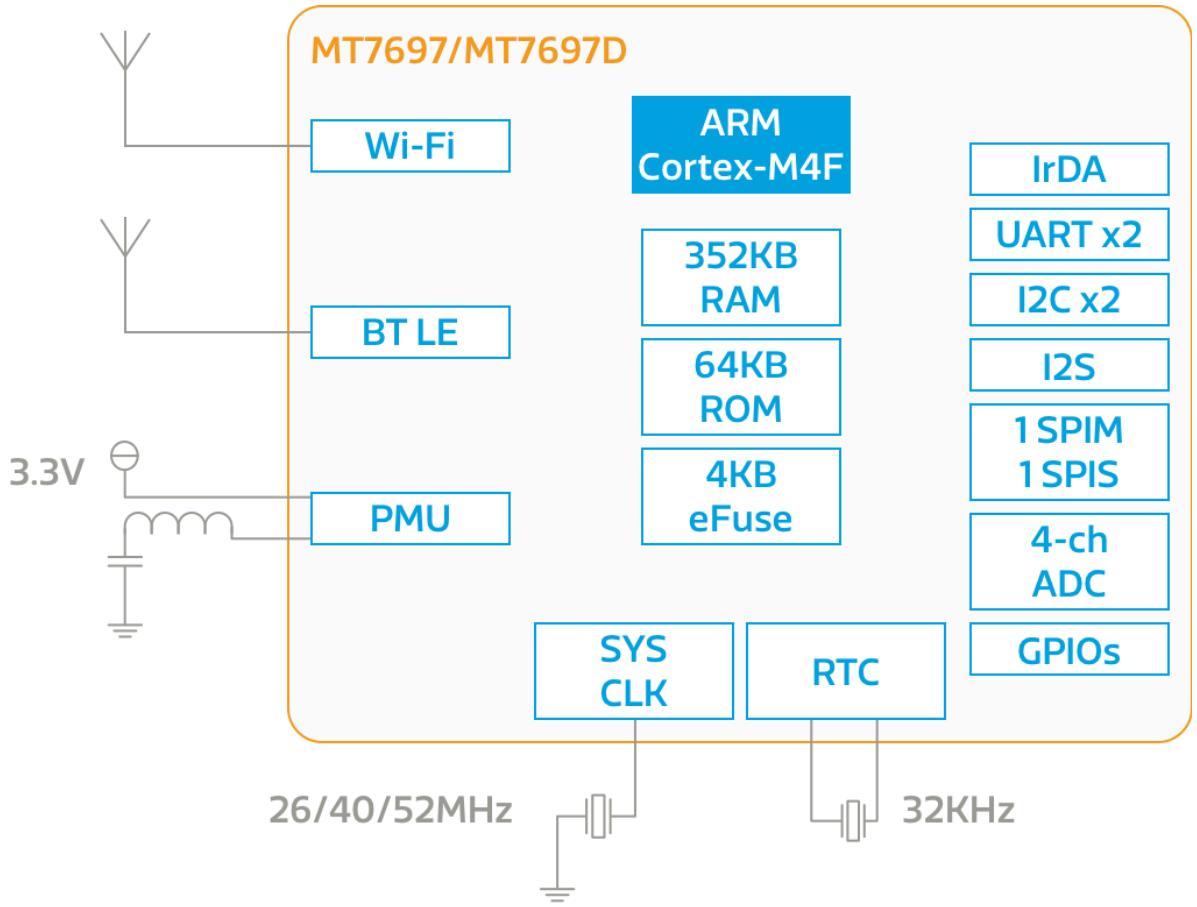
Hitcon Badge 2018

Hardware Diagram



MT7697

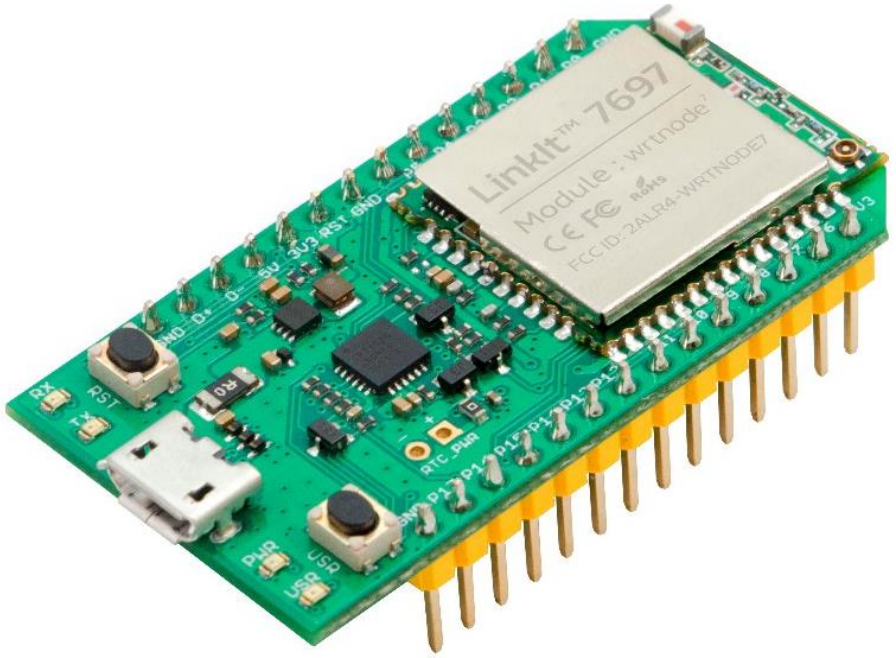
- 192 MHz Cortex-M4F
- WiFi 802.11b/g/n & BLE SoC
- 352KB Ram / External SPI flash
- 64KB Bootloader Rom
- UART/SPI/I2C
- Crypto-engine



Linkit 7697

- Arduino Support
- Wrtnode’s module with 4MB Flash
- MTK Official Support Platform
- With Auto-Switch to load Firmware
- Arduino IDE Setup:

https://docs.labs.mediatek.com/resource/linkit7697-arduino/en/environment-setup/setup-arduino-ide



Hitcon Badge‘s Arduino Package

官方的版本有幾個狀況需要修改，所以直接Fork一版出來

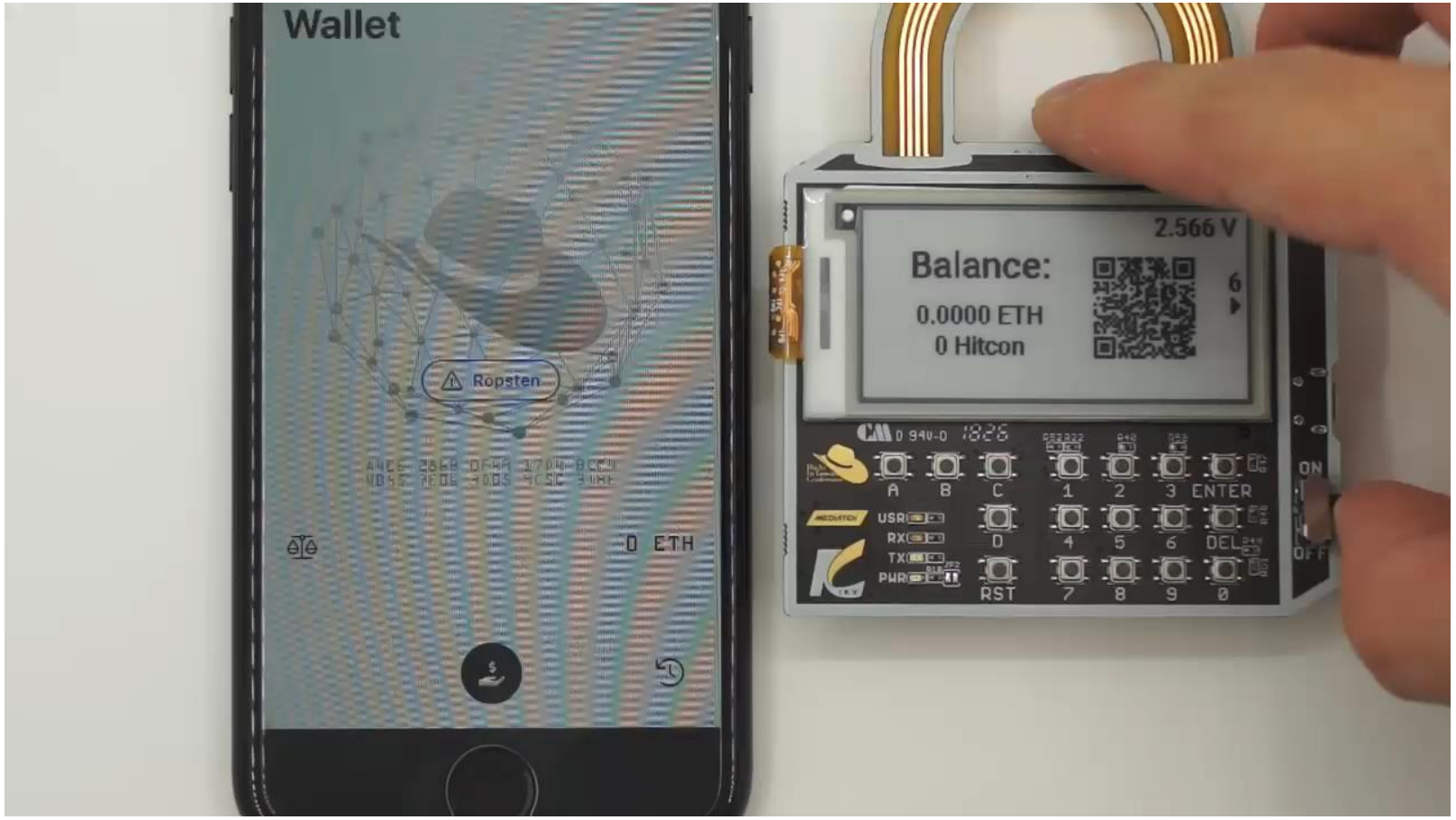
Package:https://raw.githubusercontent.com/will127534/HITCON-Badge-2018/master/Software/Arduino_packages/package_hitcon_badge_index.json

修正改的內容:

1. ~~RTOS Tickless Sleep~~ 移除了，多虧Android的Active Scanning
2. BLE MTU Size
3. Analog Read和Sleep的Bug
4. 關閉Wifi
5. 加入Secure Element+電子紙的Library

Waveshare 2.13” Black and White e-paper

- GDE0213B1 - Support Partial Update – takes only 0.2s

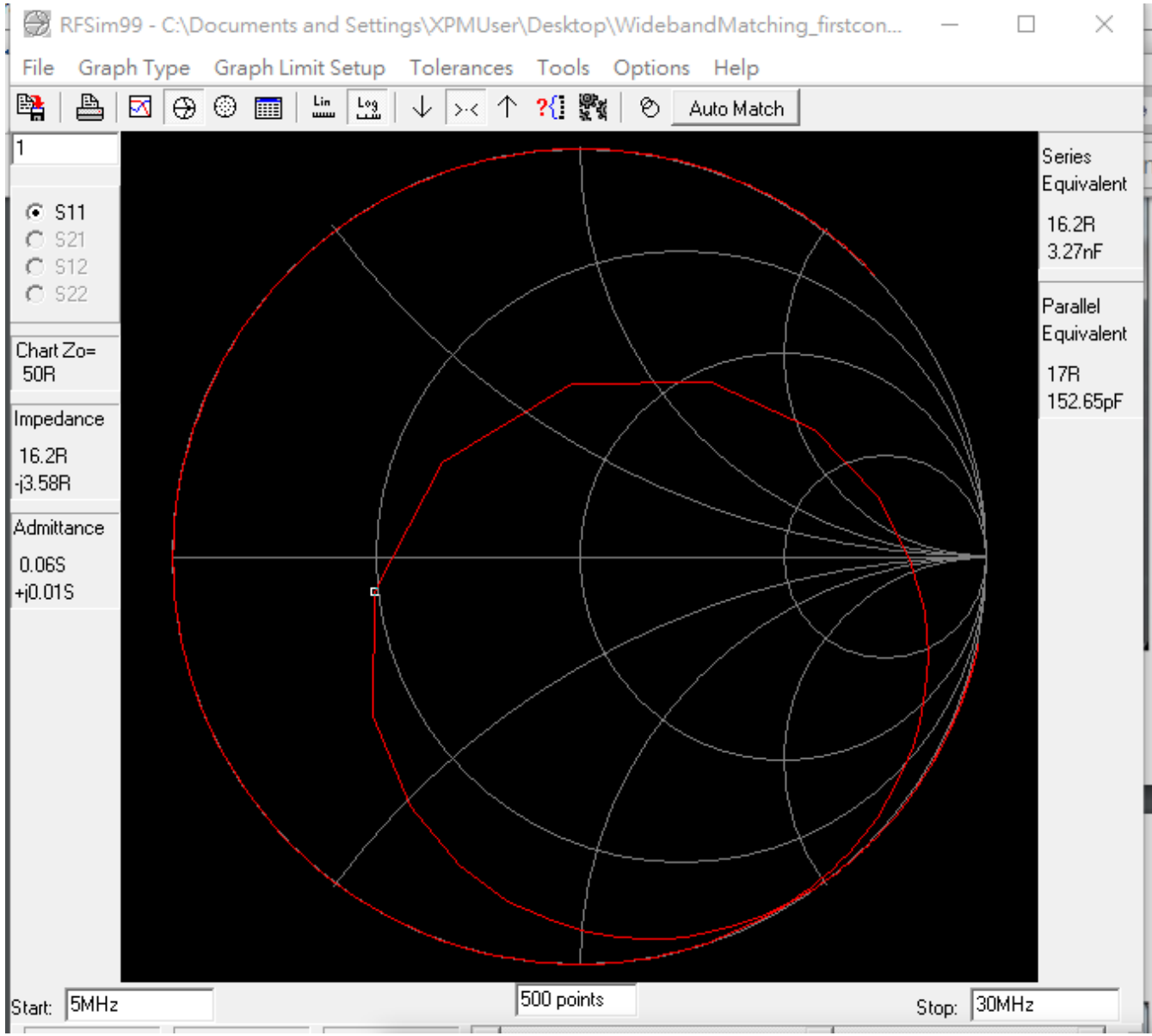


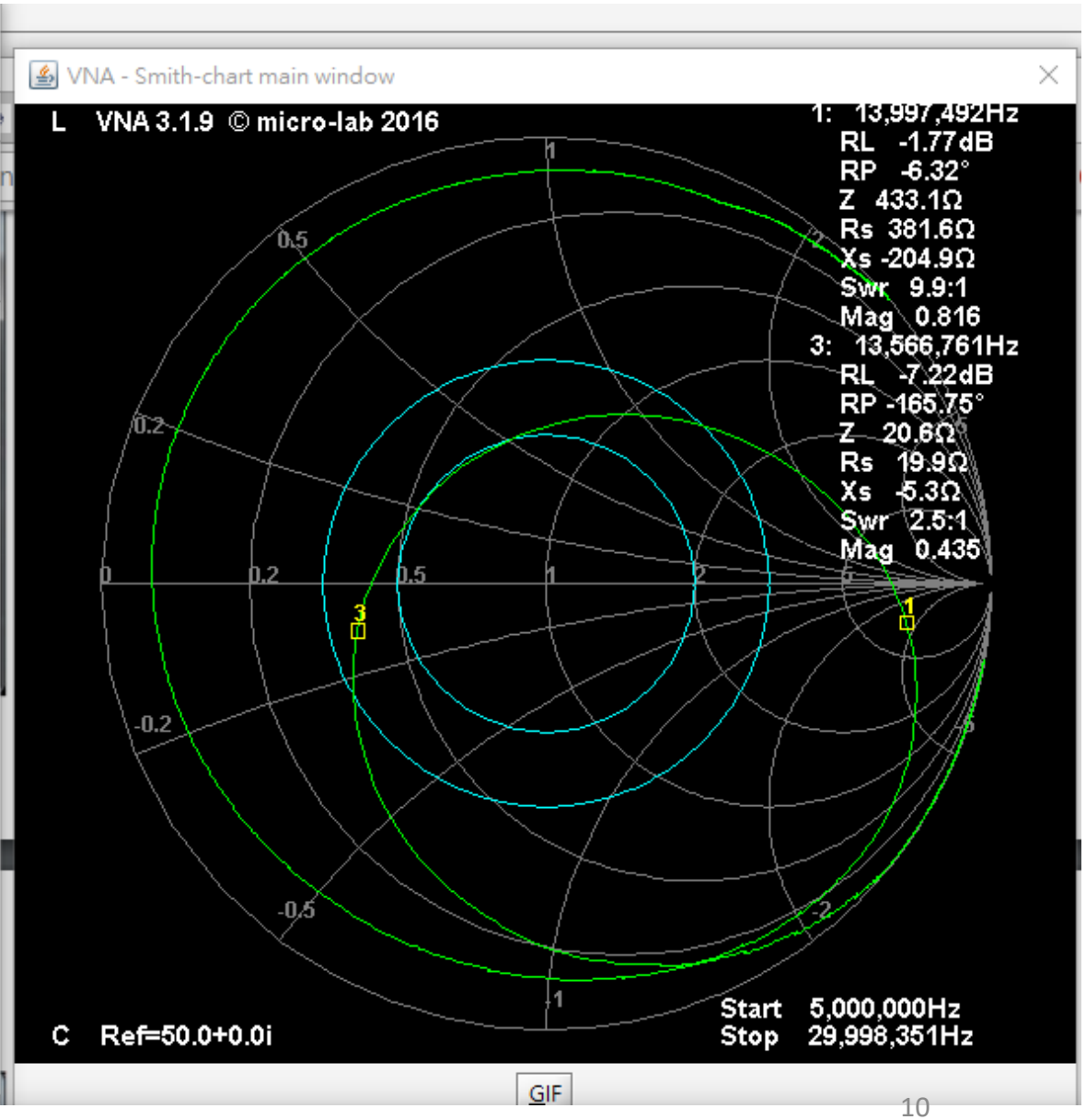
PN532 – NFC controller

- Not used, 時間來不及
- 天線形狀比較特殊，電路需要調整阻抗匹配

Simulated

Real

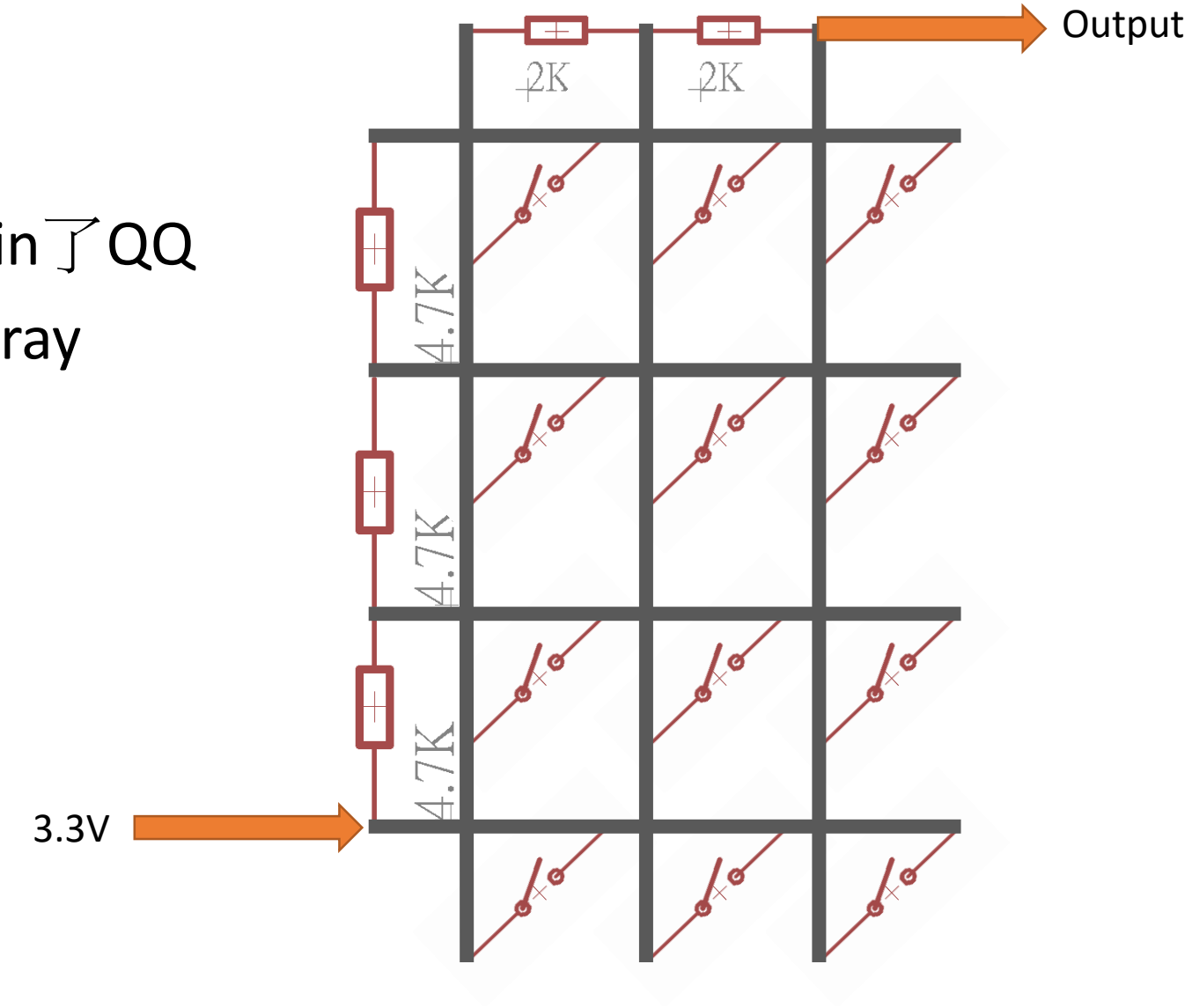




PN532 – NFC controller

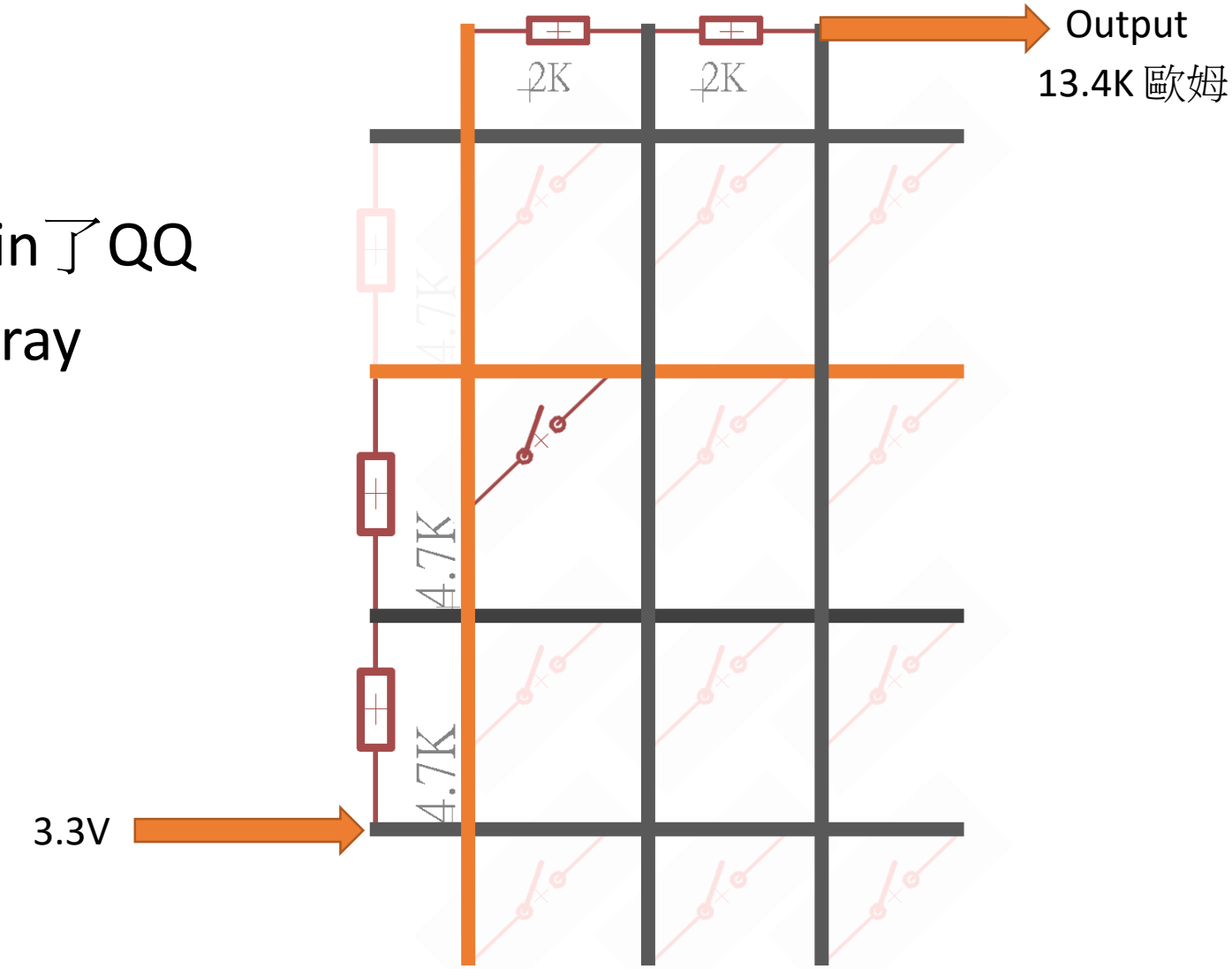
Button Array

- MT7697沒有多的Digital pin了QQ
- Solution: Analog Button Array



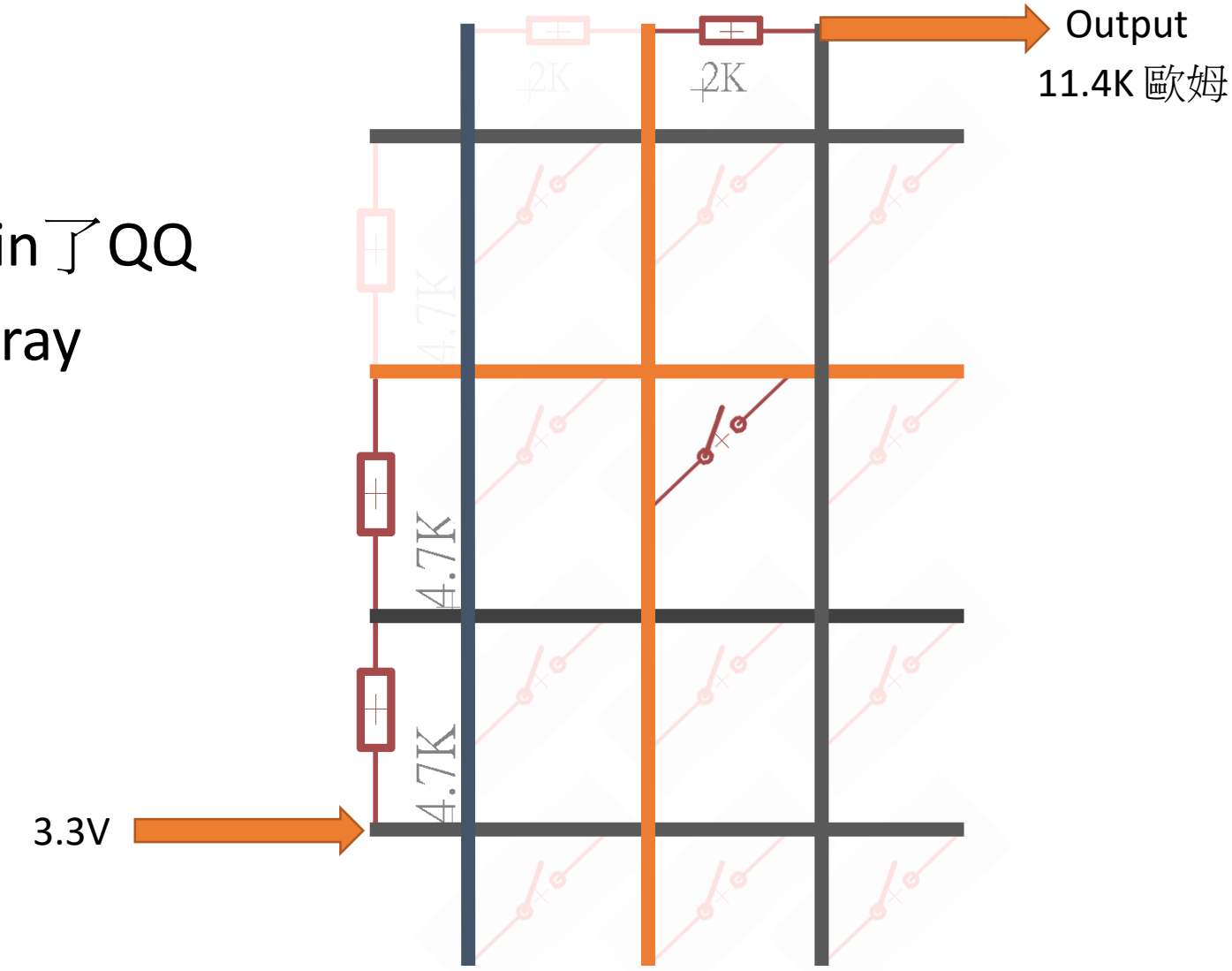
Button Array

- MT7697沒有多的Digital pin了QQ
- Solution: Analog Button Array



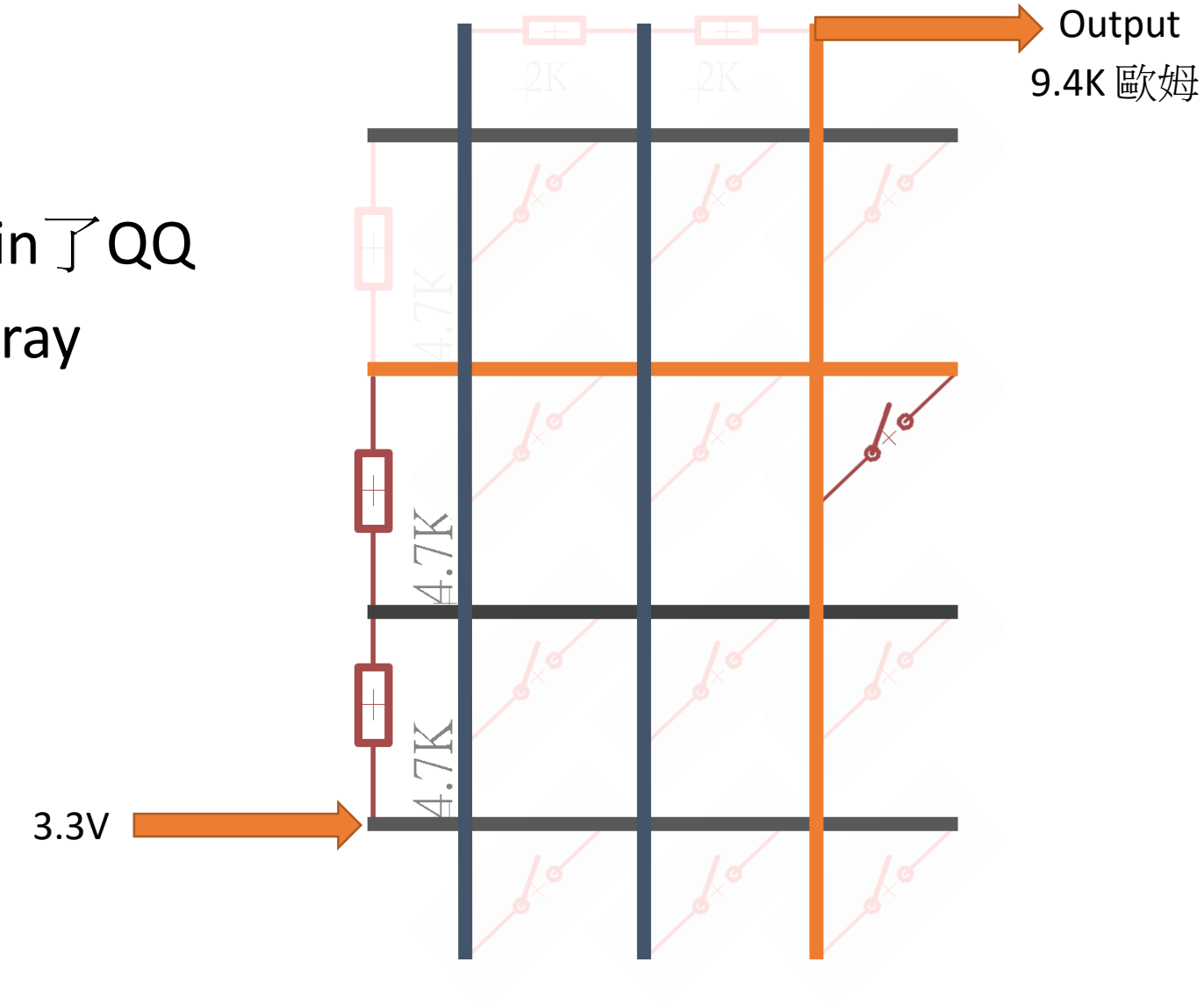
Button Array

- MT7697沒有多的Digital pin了QQ
- Solution: Analog Button Array



Button Array

- MT7697沒有多的Digital pin了QQ
- Solution: Analog Button Array



Button Array

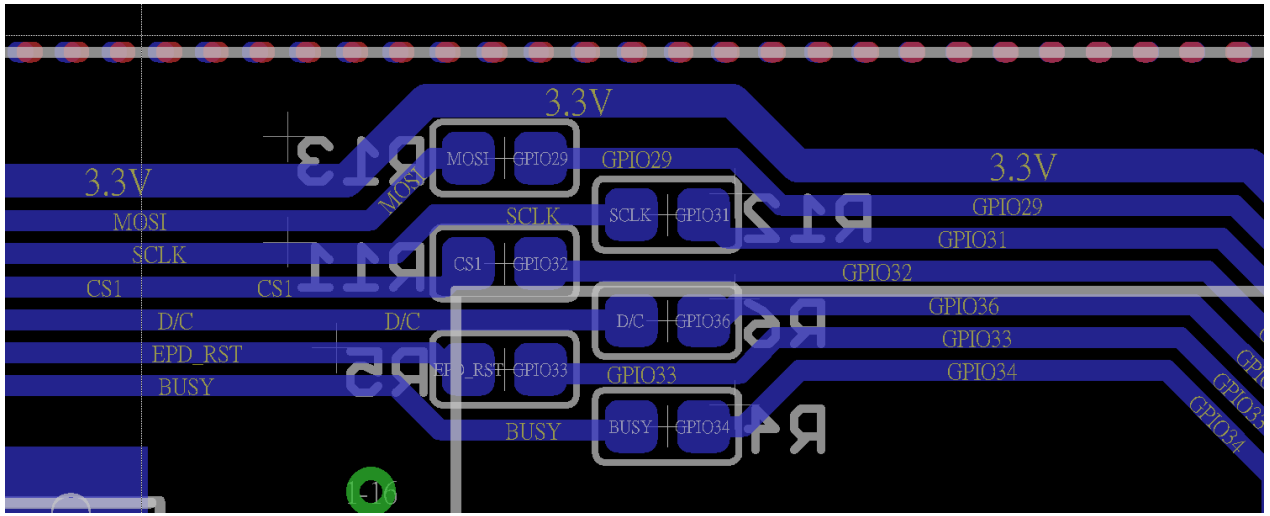
- 需要精確的電壓和電阻
- 但是Badge上面有兩個供電，電壓升壓和USB降壓

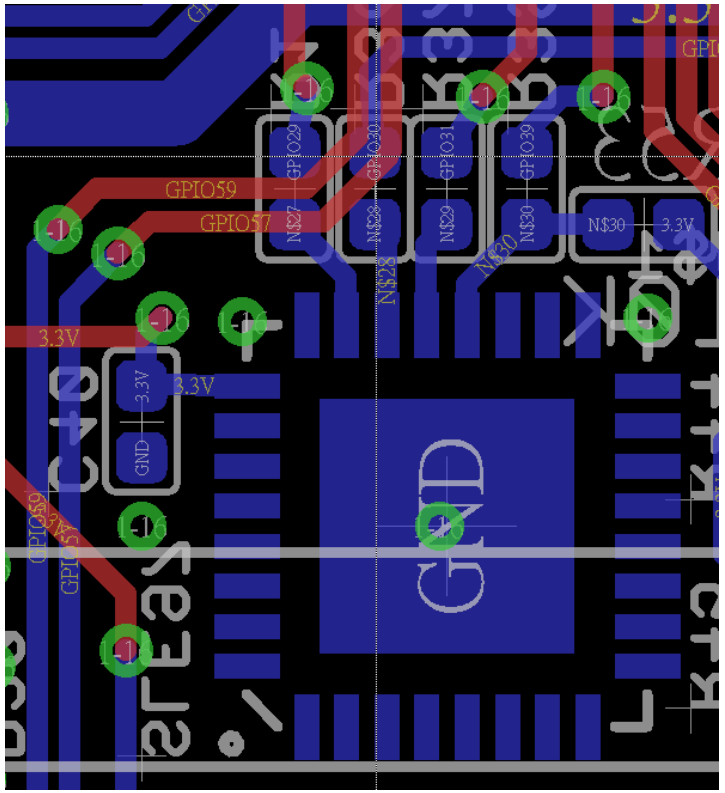
➔透過使用者一定會按到的按鈕自動校正電壓

Button ENTER + Button 6, 這兩個按下去之後會校正輸入的電壓

Misc.

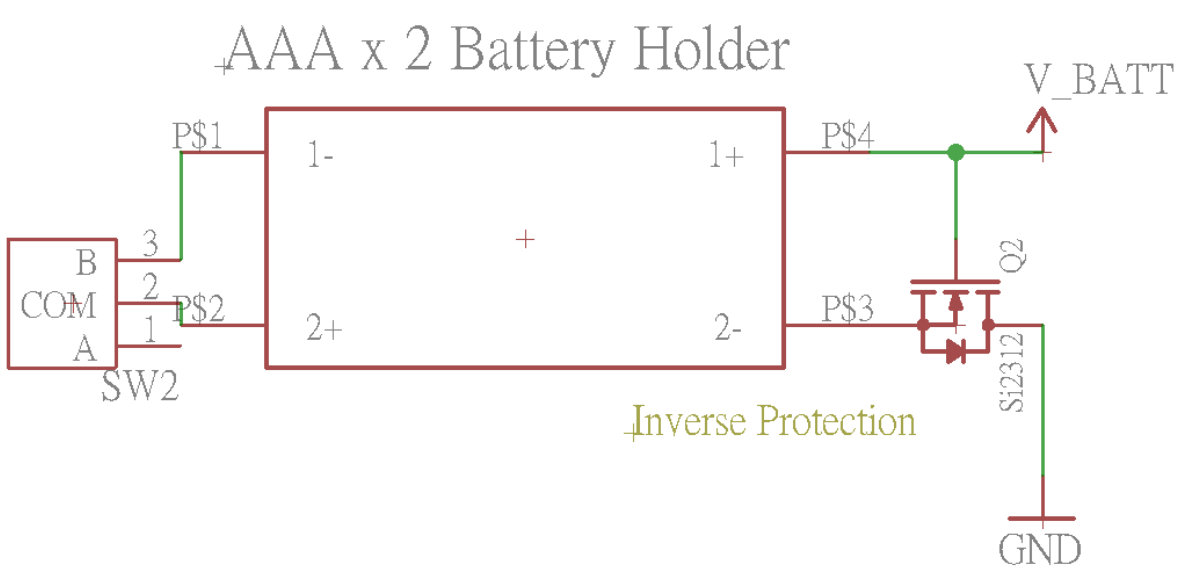
- 多數Interface都是以1K或者0歐姆電阻串接，方便斷開

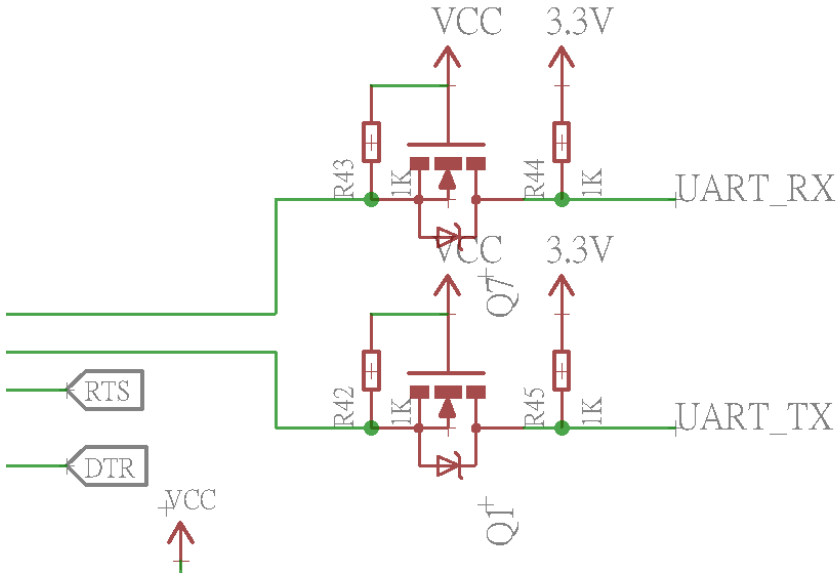




Misc.

- 正面的Power LED燈預設斷路以減少耗電量
- USB 轉 UART 和其他供電有做隔離，避免CP2102N消耗電池
- Battery有做防反接的保護



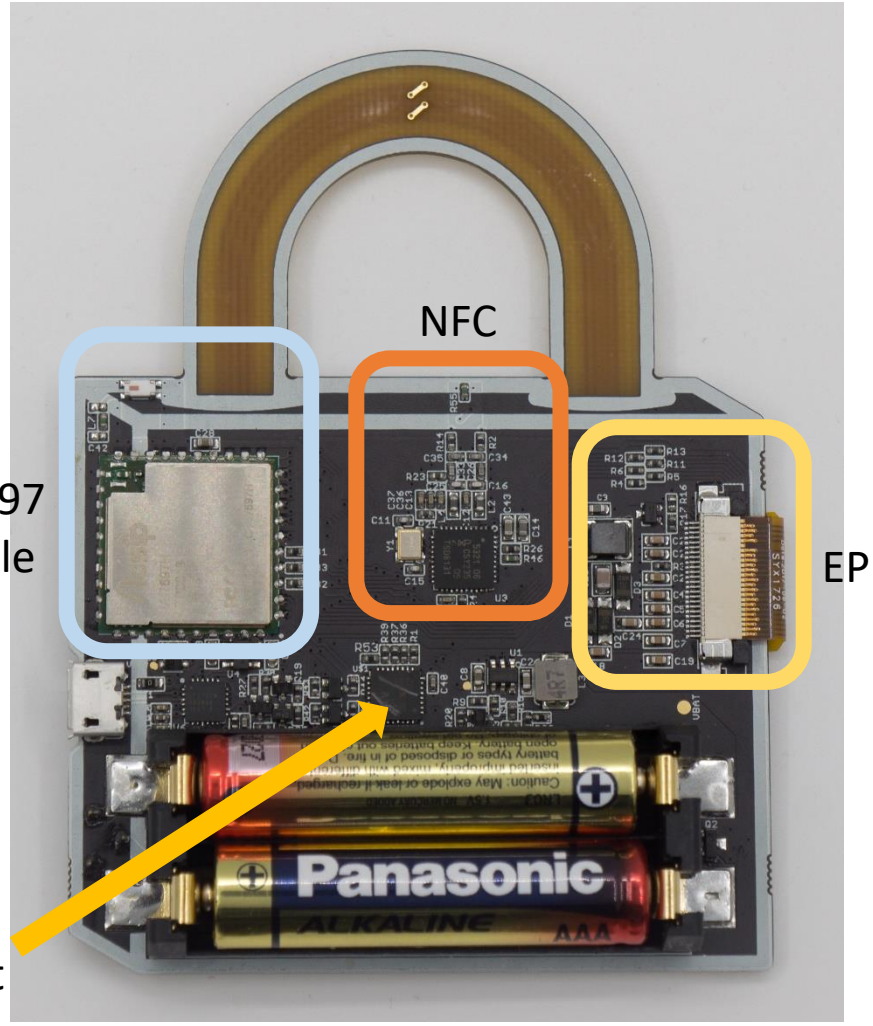


Secure Element

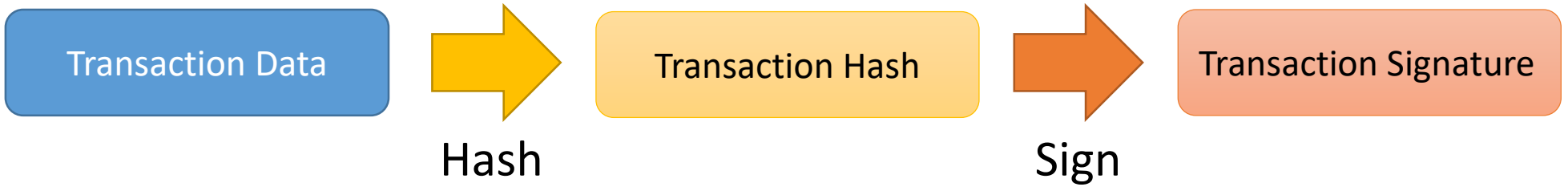
- SLE97 – From Infineon, Software from IKV
- ARM® SecurCore™ SC300™
- Crypto processor
- ISO 7816 interface
- SPI interface

CC EAL5+ high !

Hitcon Badge 2018 Hardware overview

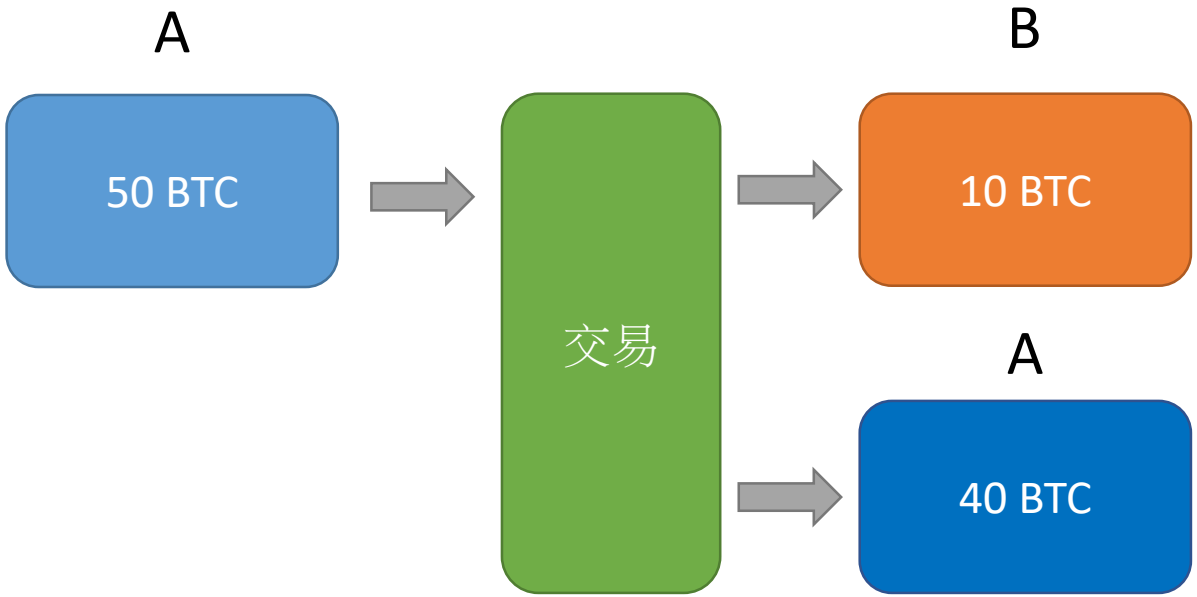


Wallet – Cryptocurrency



Wallet – Cryptocurrency: BTC

- 對比特幣來說，每一筆交易完成後，餘額會匯到新的錢包

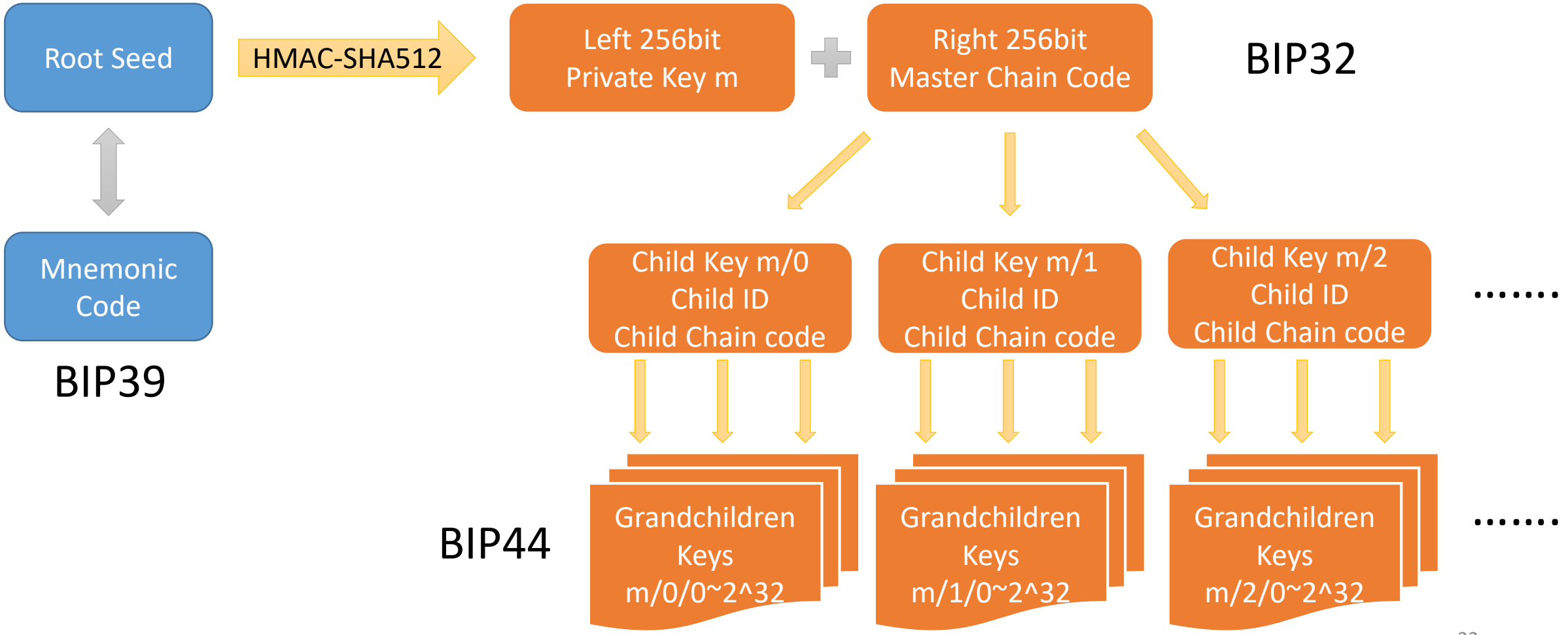


錢包需要管理一堆Private Key

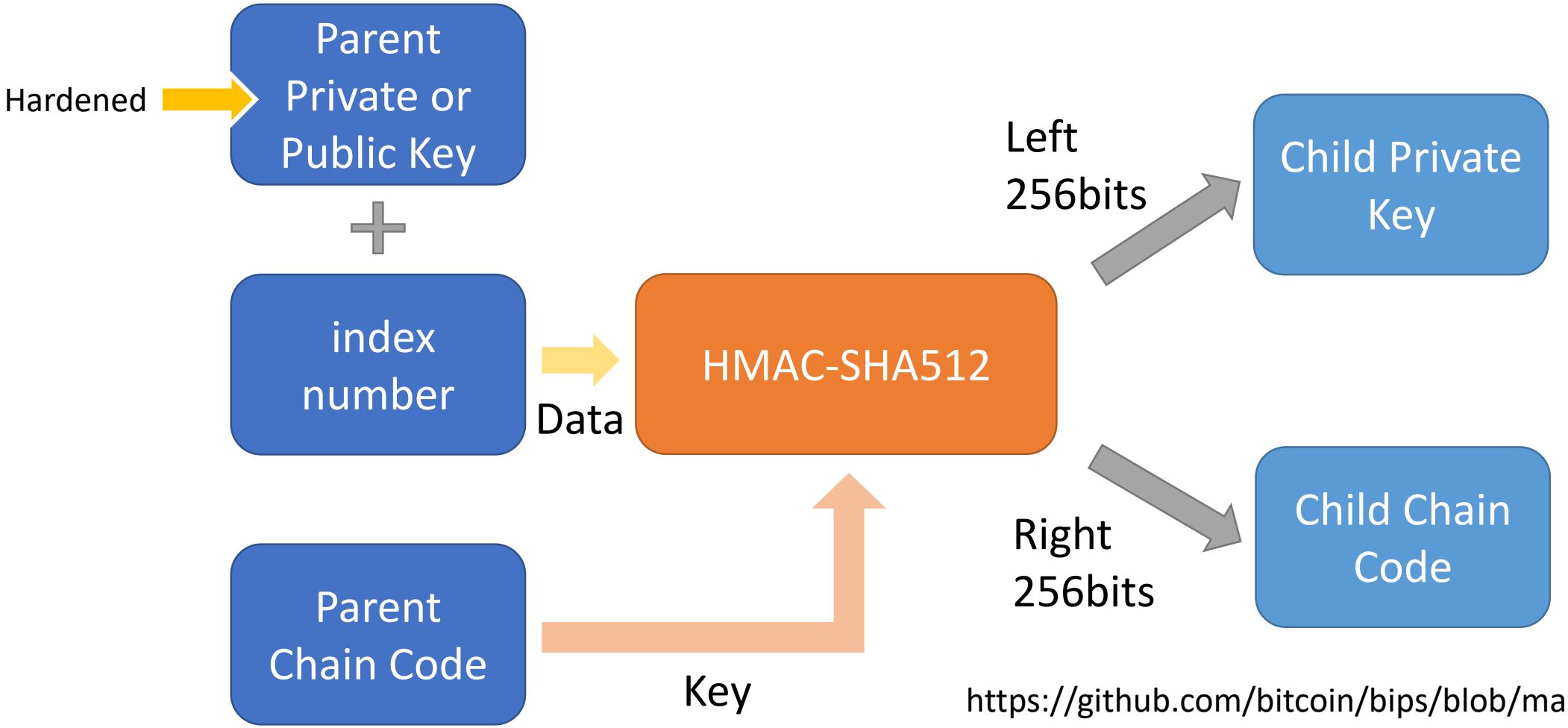
➔Private Key 管理問題

Solution: Deterministic Wallet

HD Wallet – BIP32,39,44 Overview



Child key derivation

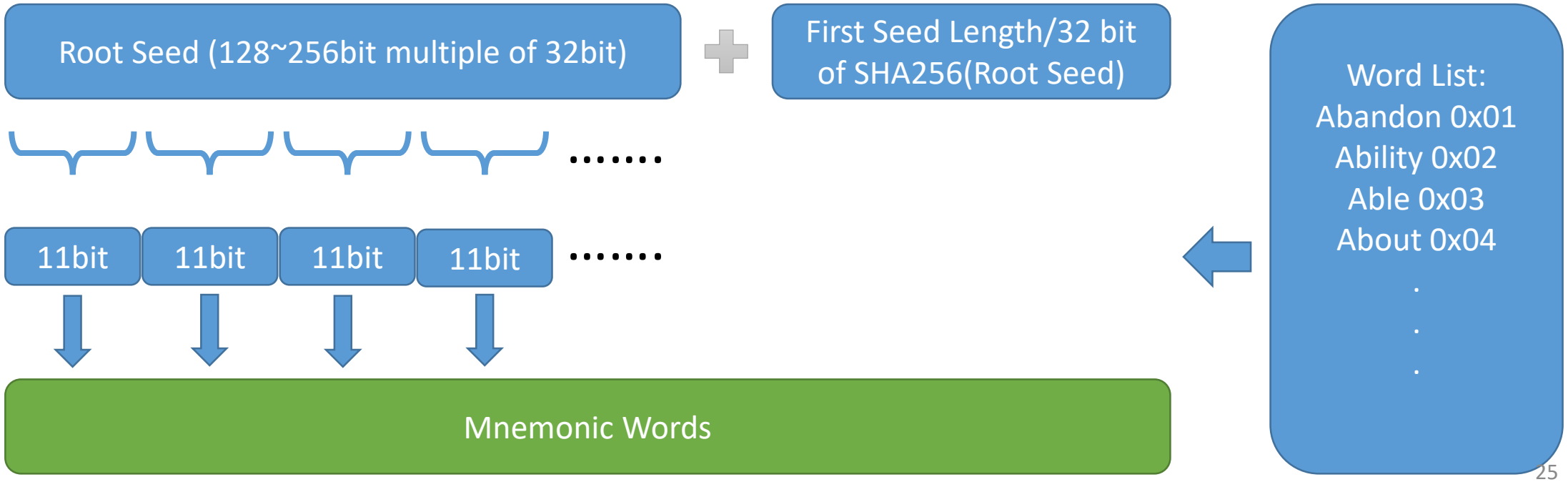


https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

BIP39 - Mnemonic Code

https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

- 由於Root Seed 不方便人類抄寫，所以透過2048個字的組合定義一個Coding 方式
- 2048個字➔ 每個字代表11byte



BIP39 - Mnemonic Code

https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

Root Seed Length	Checksum Length	Total Length	Word Length
128 Bits	4 Bits	132 Bits	12 Words
160 Bits	5 Bits	165 Bits	15 Words
192 Bits	6 Bits	198 Bits	18 Words
224 Bits	7 Bits	231 Bits	21 Words
256 Bits	8 Bits	264 Bits	24 Words

Badge預設值

BIP 44 – Meaningful structure

m / purpose' / coin_type' / account' / change / address_index

- Purpose ➔ 固定 44’
- Coin type
  - Bitcoin ➔ 0’
  - Eth ➔ 60’
- Account
- Change
  - 0 for External chain ➔收款/付款用
  - 1 for internal chain ➔ 內部處裡用
- Address index
- Badge預設: m/44’/60’/0’/0/0

Tool:https://coinomi.com/recovery-phrase-tool.html

BIP 44 – Meaningful structure

m / purpose' / coin_type' / account' / change / address_index

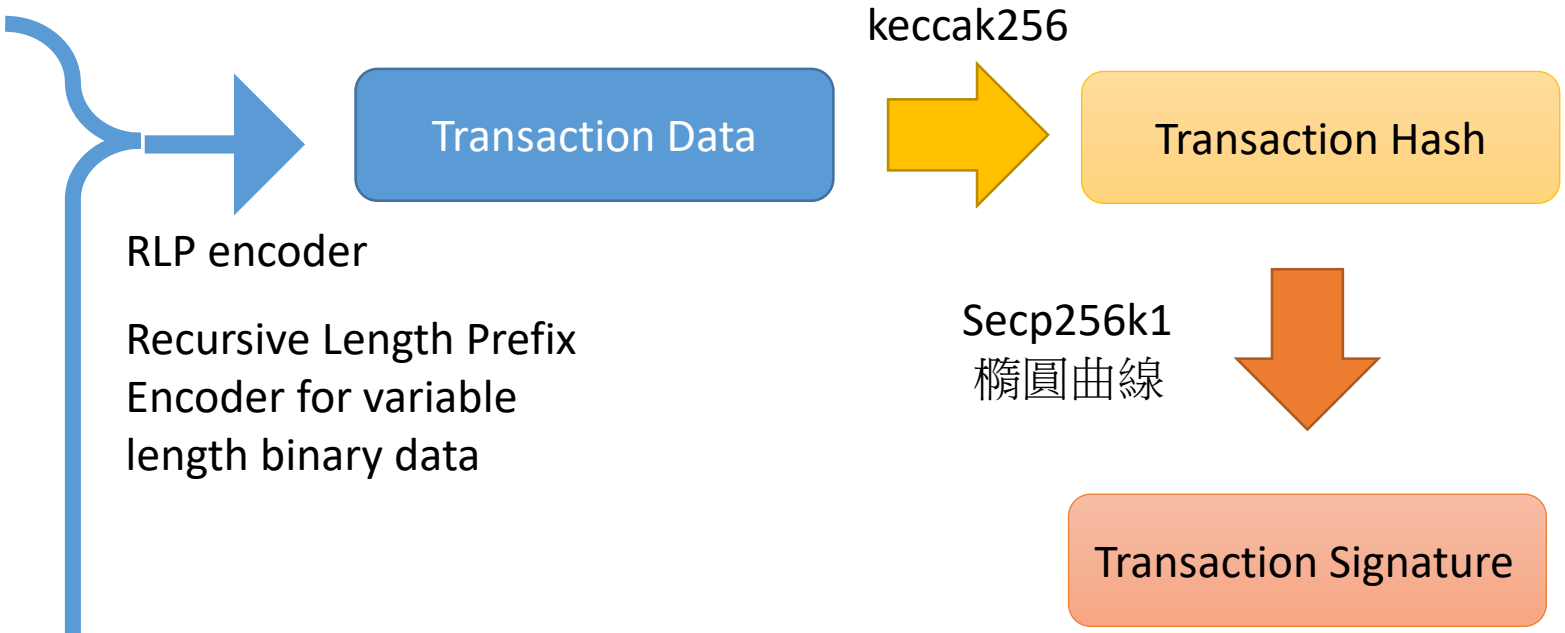
Hardened key

- Purpose ➔ 固定 44’
- Coin type
  - Bitcoin ➔ 0’
  - Eth ➔ 60’
- Account
- Change
  - 0 for External chain
  - 1 for internal chain
- Address index
- Badge預設: m/44’/60’/0’/0/0

Tool:https://coinomi.com/recovery-phrase-tool.html

乙太幣交易

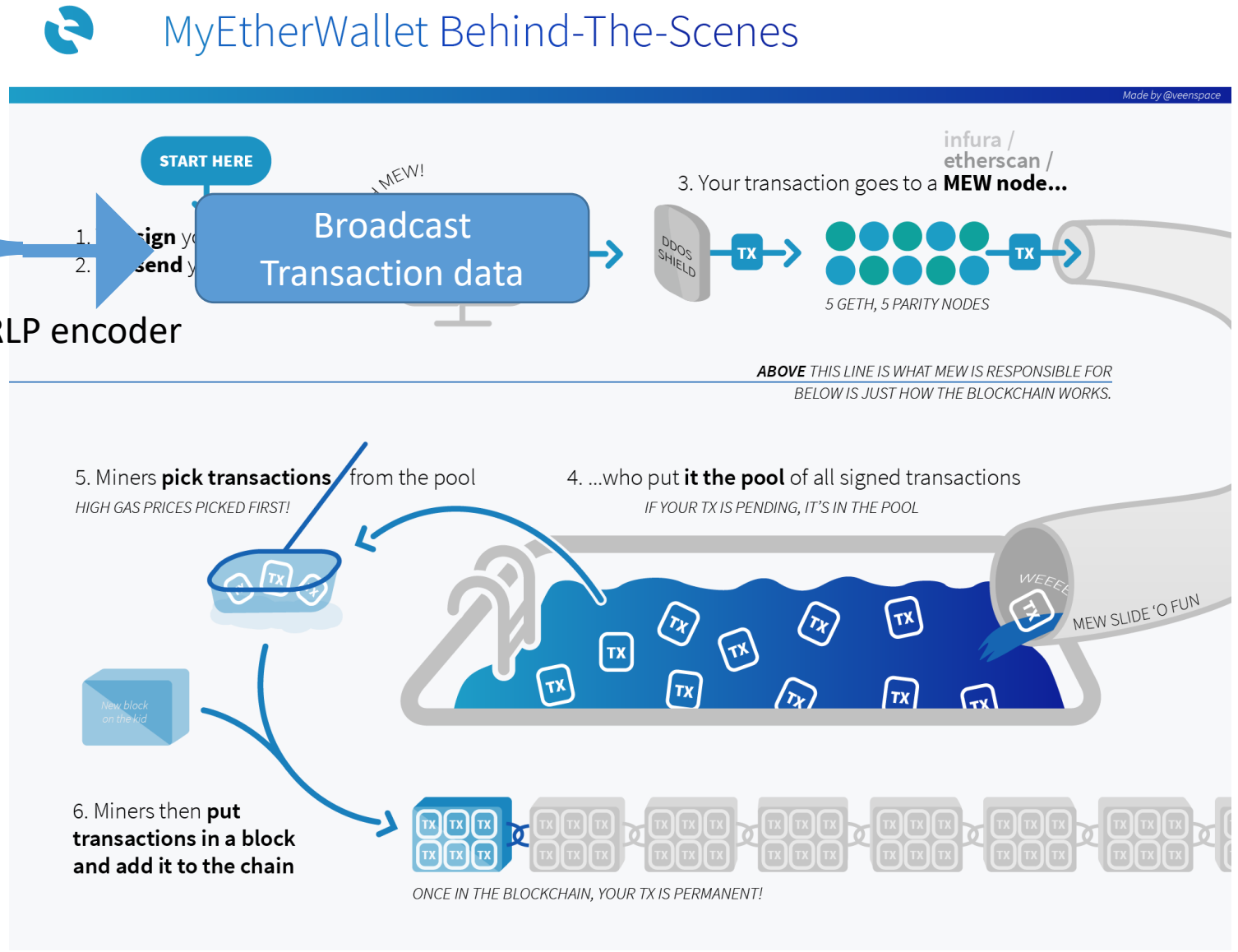
- To Who
  - 交易對方的Address
  - 20byte
- How much
  - 金額 單位為wei
  - Uint256_t
- Gas Price
  - 手續費 單位為wei
  - Uint256_t
- Gas Limit
  - 運算數量
  - Uint256_t
- Nonce
  - 交易筆數
- Data



乙太幣交易

- To Who
  - 交易對方的Address
  - 20byte
- How much
  - 金額 單位為wei
  - Uint256_t
- Gas Price
  - 手續費 單位為wei
  - Uint256_t
- Gas Limit
  - 運算數量
  - Uint256_t
- Nonce
  - 交易筆數
- Data
- Transaction Signature

RLP encoder



https://steemit.com/ethereum/@n-ur/behind-the-scene-on-how-myetherwallet-works-simple-illustration

Smart Contract : Program on ETH

- Smart Contract: 類似一種部屬在乙太幣網路的一段程式碼
- 藉由交易來傳遞/運算資料

- 一旦交易的對象是Smart Contract，Data會傳遞到對應的程式執行

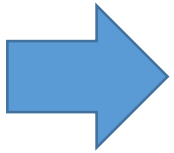
ERC20 – define Interface (Application Binary Interface)

- TotalSupply
- BalanceOf (address _owner)
- transfer(address _to, uint256 _value)
- transferFrom(address _from, address _to, uint256 _value)
- approve(address _spender, uint256 _value)
- allowance (address *_owner*, address *_spender*)

怎麼交易ERC20?

- 對於錢包來說，ERC20只是帶有Data的交易
- 能夠塞Data就代表能支援ERC20，只是不一定有辦法顯示相對應的交易資料

- To Who
- How much
- Gas Price
- Gas Limit
- Nonce
- Data



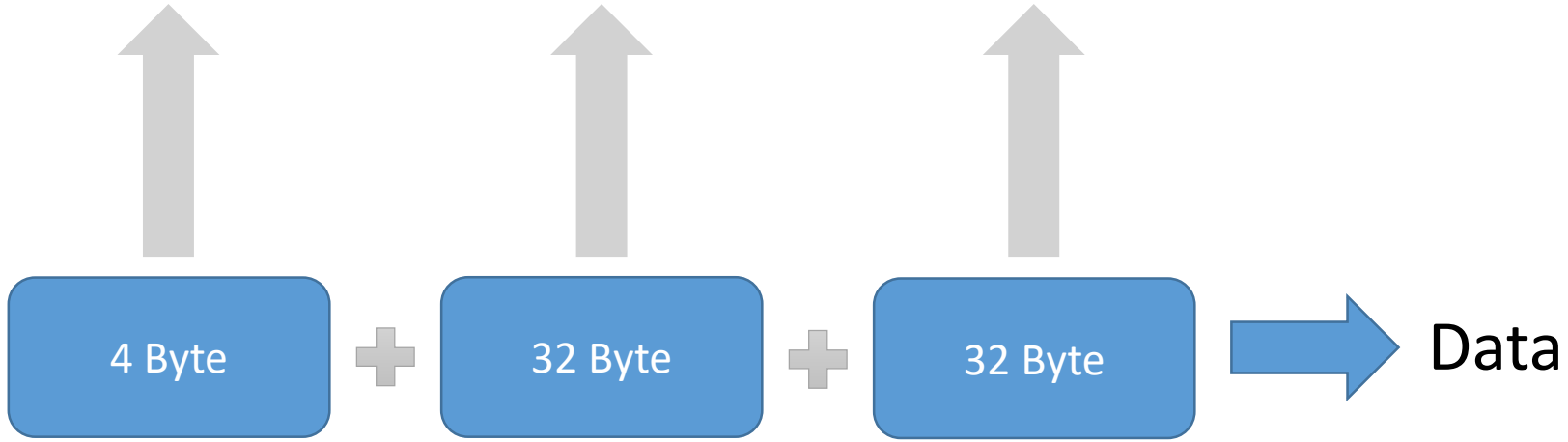
- Contract Address
- ~~How much~~ meaning less
- Gas Price
- Gas Limit
- Nonce
- Data

- Contract Method
- Contract Data

ERC20 Data format

- Contract Method – 4 Byte ➔ Hashed Application Binary Interface
- Contract Data – Depend on function
- EX:

transfer(address _to, uint256 _value)



Detail: https://github.com/ethereum/wiki/wiki/Ethereum-Contract-ABI

ERC20 Data format

- Example: 要轉 1 個 Hitcon Token給我的話
- transfer(0x4bf5193805a4fd033b84b5bb700bf2a2aaae6a7d, 0xDE0B6B3A7640000)
- “transfer(address,uint256)” ➔SHA3➔ a9059cbb2ab09eb219583f4a59a5d0623ade346d962bcd4e46b11da047c9049b
- Address ➔ Append to 32Bytes

  0x0000000000000000000000004bf5193805a4fd033b84b5bb700bf2a2aaae6a7d
- Value ➔ Append to 32Bytes
  0x0000000000000000000000000000000000000000000000000de0b6b3a7640000

➔Data:0xa9059cbb0000000000000000000000004bf5193805a4fd033b84b5bb700bf2a2aaae6a7d0000000000000000000000000000000000000000000000000de0b6b3a7640000

Secure Element – Why?

雖然錢包可以透過軟體實作，但是容易造成Master Key被偷

➔冷錢包，透過一個專門的硬體去存放/使用Master Key

- 但是即使是冷錢包，實作方式主要分成兩類
  - MCU　Ex:TREZOR
  - Secure Element + MCU　Ex:Ledger Wallet

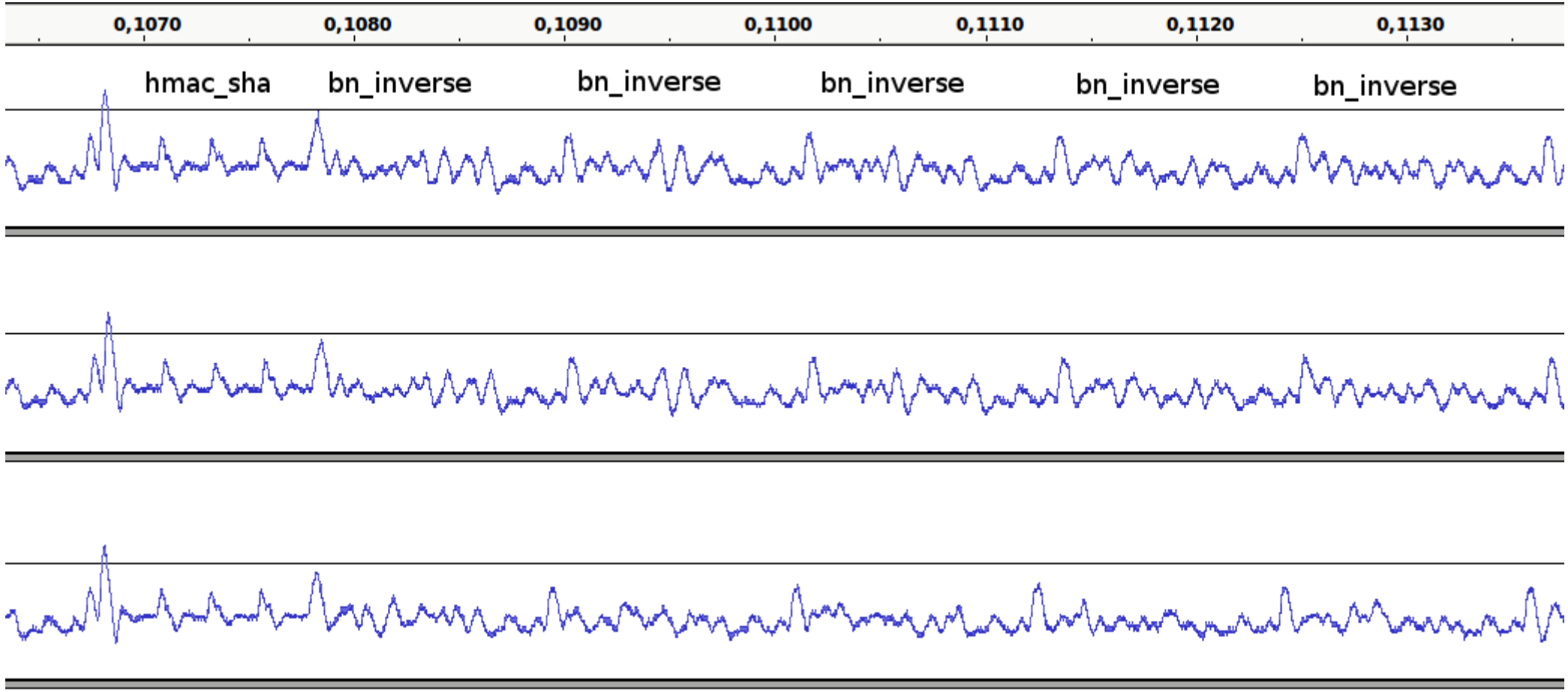
Secure Element – Why?

TREZOR ➔ 透過MCU實作

通常絕大多數的MCU都難以抵抗Side-channel攻擊，所以較為容易被破解

Ex: https://jochen-hoenicke.de/trezor-power-analysis/ P.S 已經Fix了

Secure Element – Why?



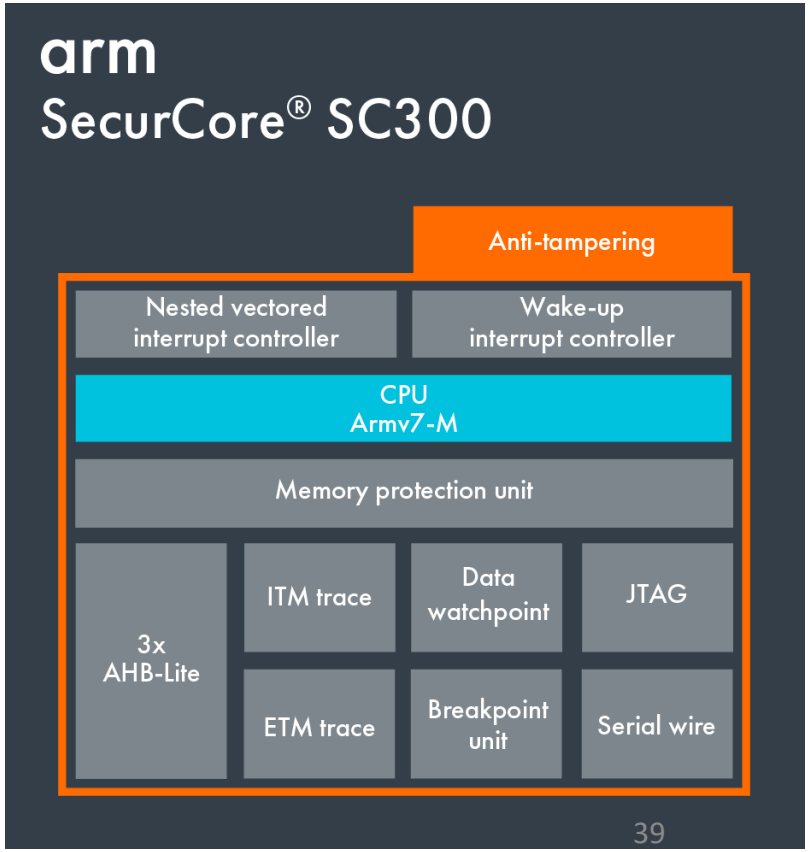
https://jochen-hoenicke.de/trezor-power-analysis/

Secure Element – Why?

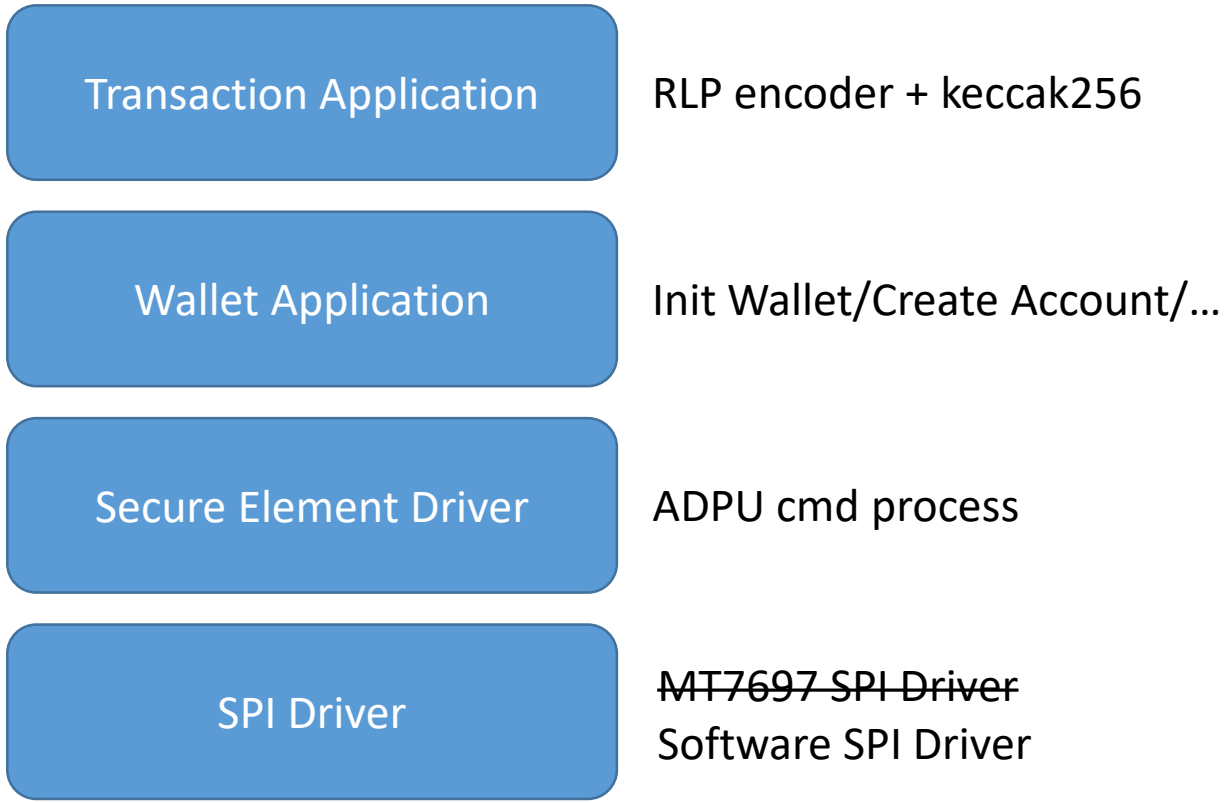
而Secure Element最主要的目的就在於如何防止Side-channel

IC廠商會加上不同的Anti-tampering方法

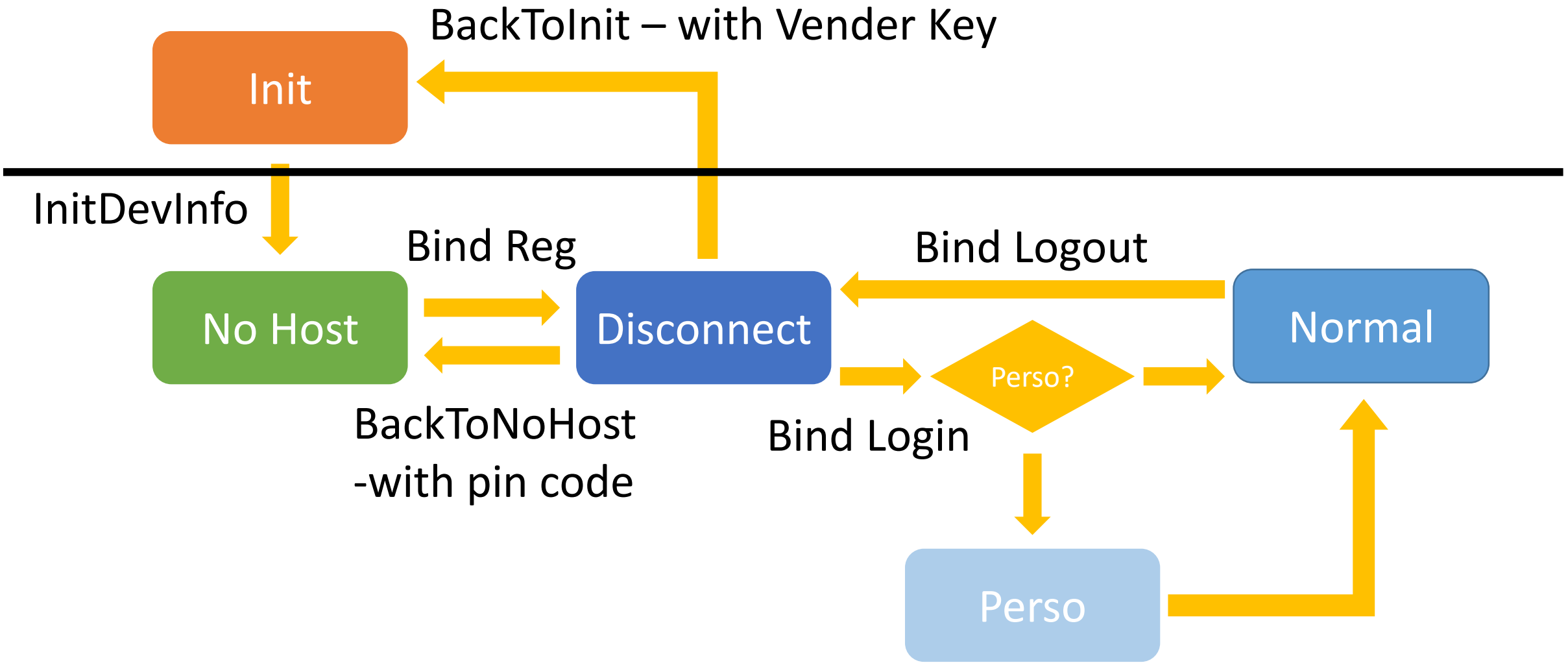
常見於信用卡/SIM卡等晶片上



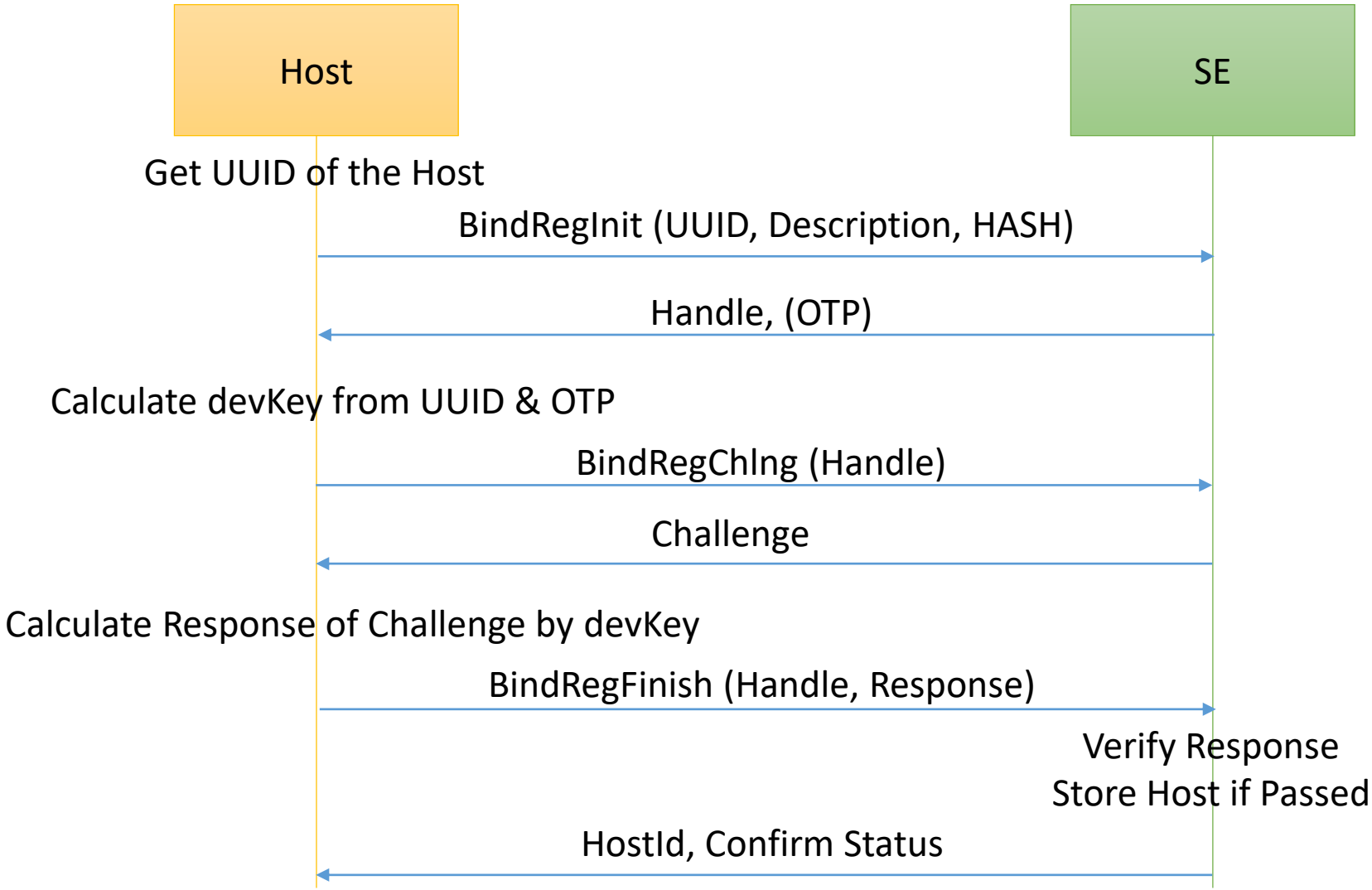
Secure Element - Usage



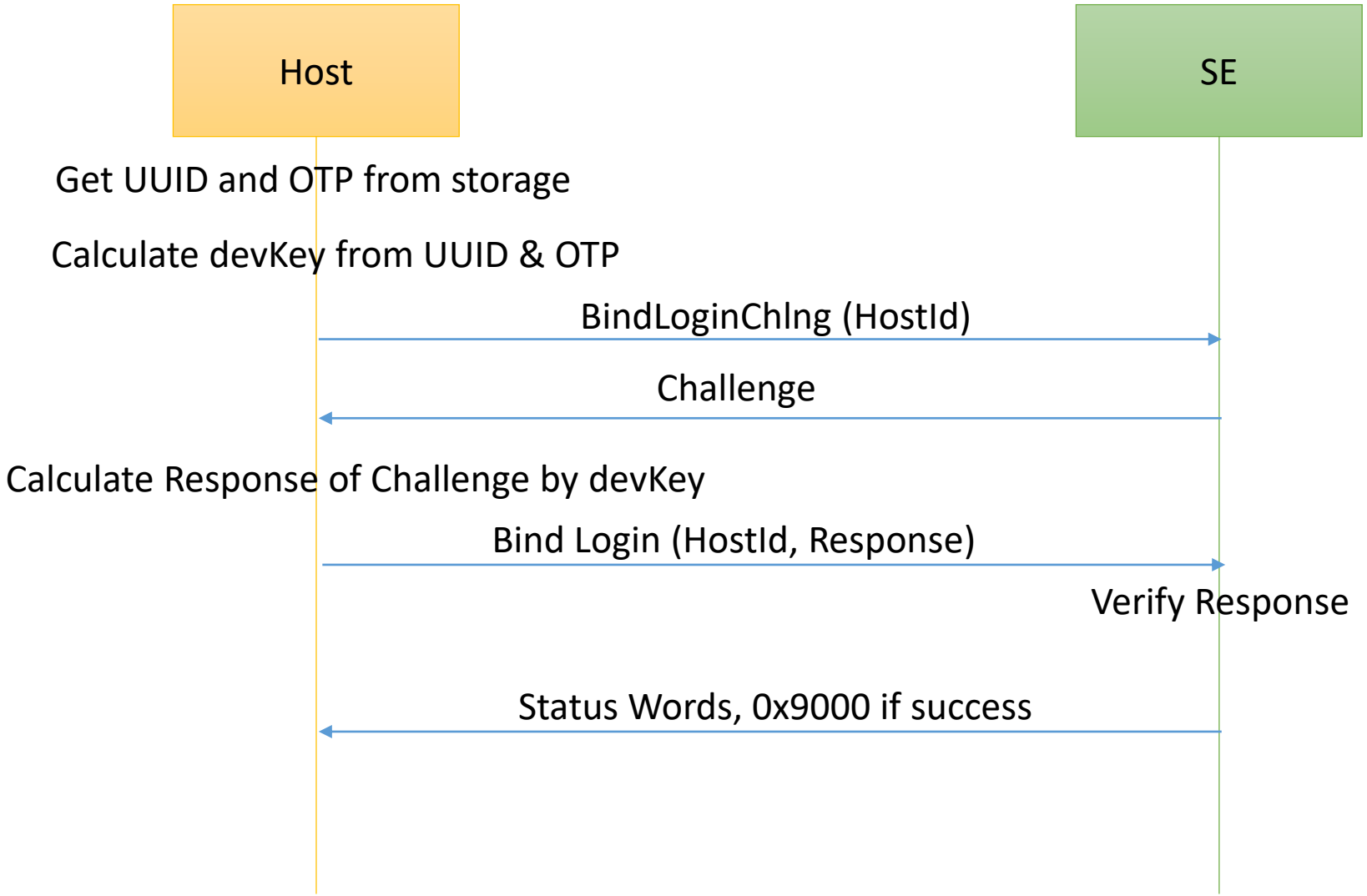
Secure Element - State



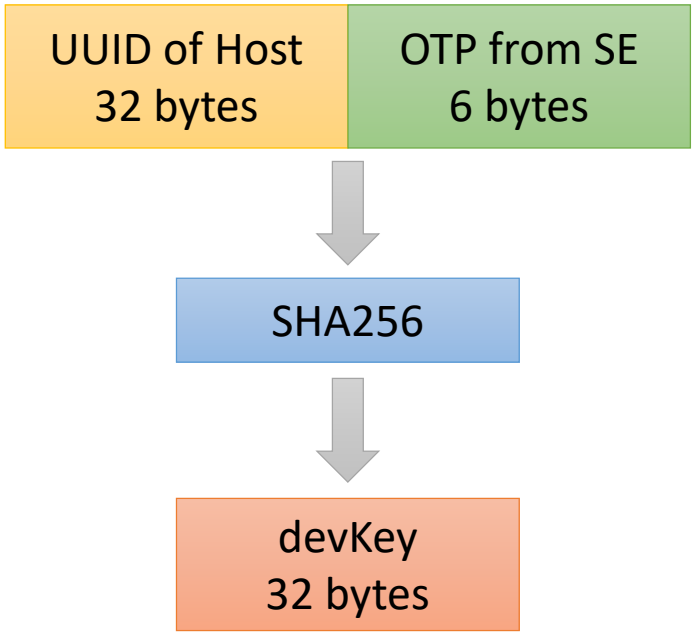
Host Registration



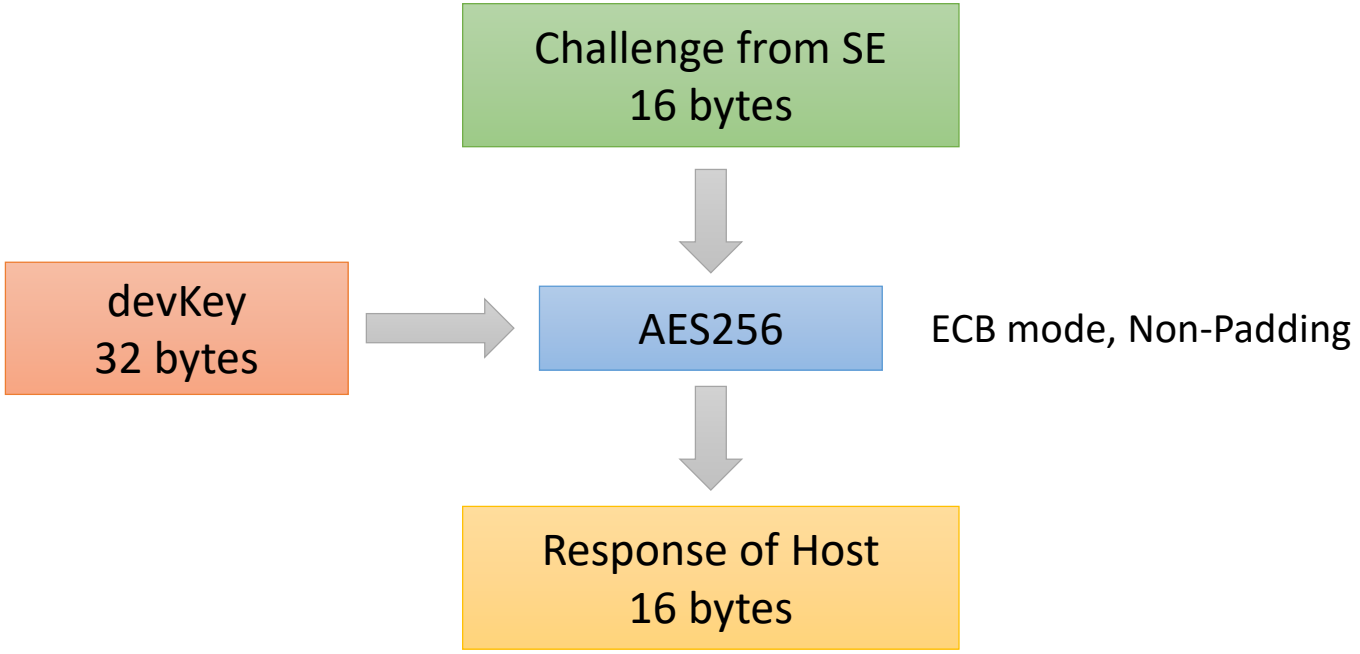
Host Login


Host
SE
Get UUID and OTP from storage
Calculate devKey from UUID & OTP
BindLoginChlng (HostId)
Challenge
Calculate Response of Challenge by devKey
Bind Login (HostId, Response)
Verify Response
Status Words, 0x9000 if success

Device Key (devKey) Derivation

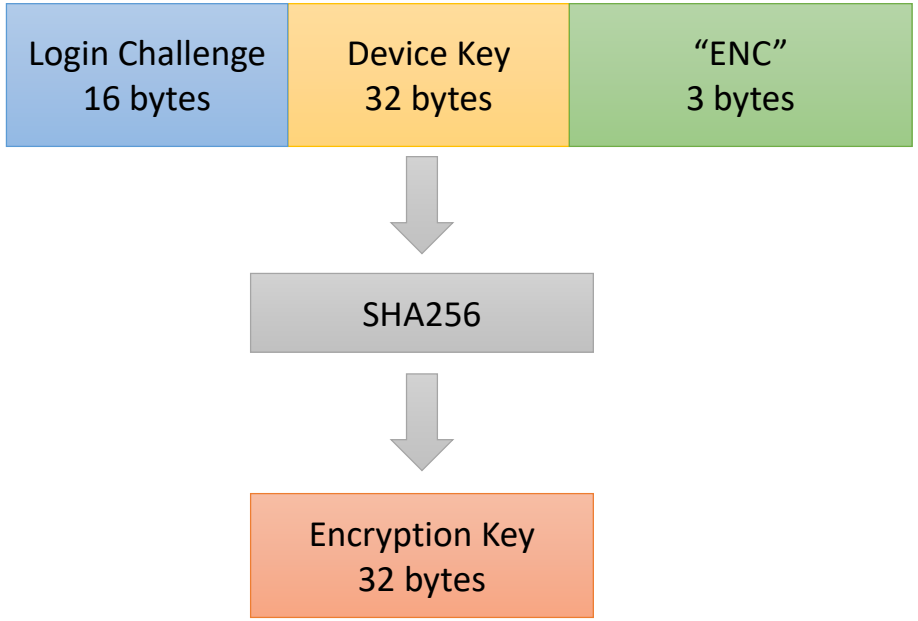


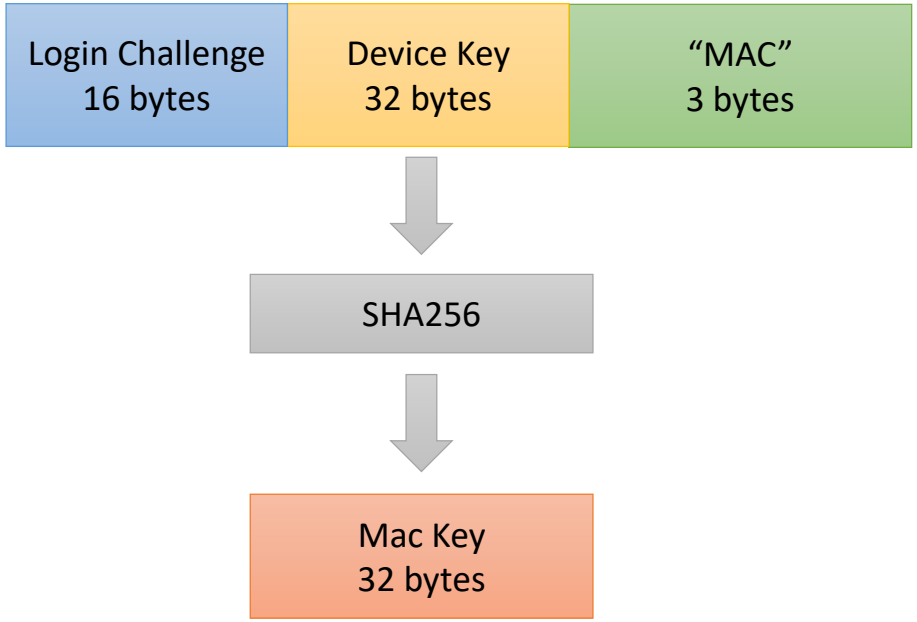
Challenge and Response



Encrypt Key and MAC Key

- Encryption Key
  - Used for Data Encryption after Login
- Mac Key
  - Used for Data HMAC-SHA256





https://en.wikipedia.org/wiki/Hash-based_message_authentication_code

HDW Management

- Secure Element Handles BIP32 Path
  - m/BIP44/coin/Account/Change/Address
  - Badge預設: m/44'/60'/0'/0/0

- Secure Element Holds up to 5 accounts
  - External Address Pointer of each account (update to 2^{128} addresses)
  - Internal Address Pointer of each account (update to 2^{128} addresses)

Cmd line Management

- QueryAccountKey: Query Public Key for a specific Account/Key_ID
  Usage: QueryAccountKey [account] [key_id]

- CreateAccount: Create a New Account for a specific cointype/account_id
  Usage: CreateAccount [cointype] [account_id] [Name]

- QueryAccountInfo: Query a specific Account Info
  Usage: QueryAccountInfo [account_id]

- CreateNextAddr: Generate a new key for a Specific Account
  Usage: CreateNextAddr [account_id]

- Account ID:0~4

Cmd line Management

- SEState: Query Secure Element State
- BindReg: Bind Register
- BindLogin: Bind Login
- BindLogout: Bind Logout
- BackToNoHost: Back to NoHost state
- BackToInit: Back to Init State
- InitDevInfo: InitDeviceInfo and confirm
- PINAuth: Auth Pin Code
- InitWallet: Initialize Wallet from Mnemonic Words
- QueryWalletInfo: Query Wallet Info
- QueryAllAccount: Query All Account Info
- QueryAccountKey: Query Public Key for a specific Account/Key_ID
- CreateAccount: Create a New Account for a specific cointype/account_id
- QueryAccountInfo: Query a specific Account Info
- CreateNextAddr: Generate a new key for a Specific Account
- Transaction: Generate a new Raw Transaction

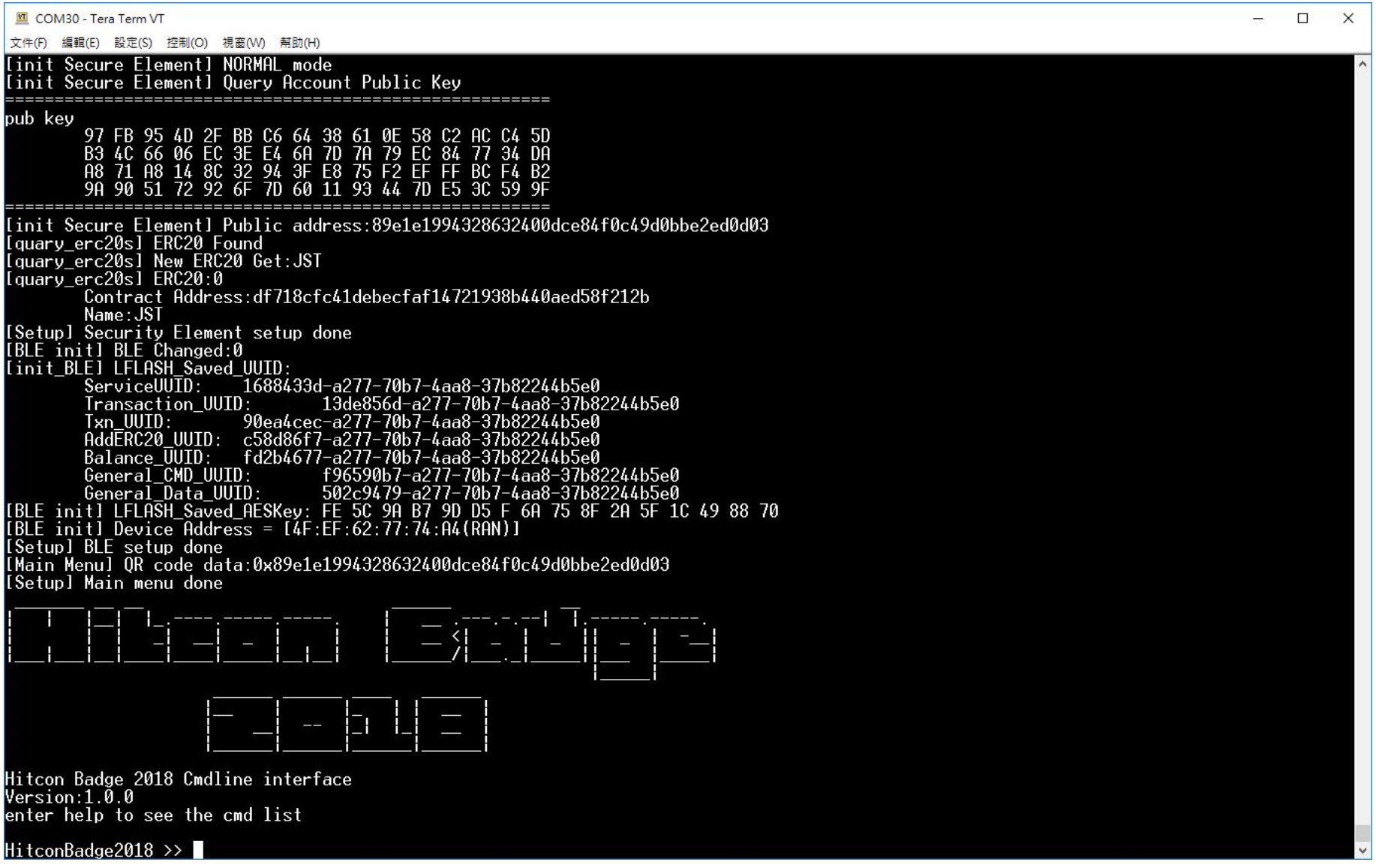
- Misc.
- Voltage: Read Battery Voltage
- ReinitBLE: Re-init BLE
- AddVcard: Adding a Vcard
- ResetHitconTokenDisplay: Reset Hitcon Token counter

Cmd line Usage

- USB to UART IC: CP2102N
- Driver: Linux & Windows & Mac https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers
  - Mac OSX 10.11 up: Apple Blocked kernel extension.
  - https://stackoverflow.com/questions/47109036/cp2102-device-is-not-listed-in-dev-on-macos-10-13 (Note: Answer 2)

- Setting:115200 8N1

Cmd line Usage



HDW Management

```
HitconBadge2018 >> QueryAllAccount
=======================================================
ACCOUNT ID
        00 00 00 00
=======================================================
=======================================================
ACCOUNT PURPOSE
        2C 00 00 80
=======================================================
=======================================================
ACCOUNT COINTYPE
        3C 00 00 80
=======================================================
=======================================================
ACCOUNT BALANCE
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=======================================================

Error at 90 00

=======================================================
ADPU rx buf
        02 00 66 37 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00 00 00 00
=======================================================
Error code:37==>Wrong HDW account ID
Query End!
hdw_query_all_account_info Success!!

HitconBadge2018 >>
```

- Account Purpose: 2C 00 00 00 ➔ 44
- Account Cointype: 3C 00 00 00 ➔ 60
- Little endian

HDW Management

```
HitconBadge2018 >> QueryAccountKey 0 0
Query account id: 0 Key_id:0
=====================================================
pub key
        09 8D 57 72 F8 60 47 FF 77 69 C7 48 47 28 1C B1
        72 F0 AD B5 48 68 5D 25 C6 11 BB 08 91 D2 7F EB
        AD B7 96 28 EB 28 75 46 D7 22 DB 3D FF 04 15 55
        79 32 57 FA 62 35 75 AE 21 CD FA ED 87 AB 9D B5
=====================================================
ETH Address:a4ee286b0f4917d4bcf44b557e063db59c5c31be
QueryAccountKey Success!!

HitconBadge2018 >> QueryAccountKey 0 1
Query account id: 0 Key_id:1
=====================================================
pub key
        04 95 13 C5 14 8F 1C 44 3D 27 31 64 02 48 BD 4E
        DD 83 12 6A 97 D8 E9 F6 C3 23 BC 91 91 CD 95 C9
        90 DE 81 44 7A 3C EB 71 5E 92 E5 BC BA E8 B6 2E
        B1 B4 ED D9 6A 11 F2 97 74 68 FC 0D 77 E9 3A A2
=====================================================
ETH Address:058dbd9e05323ff82c1ae4a28e66c067974e17eb
QueryAccountKey Success!!
```

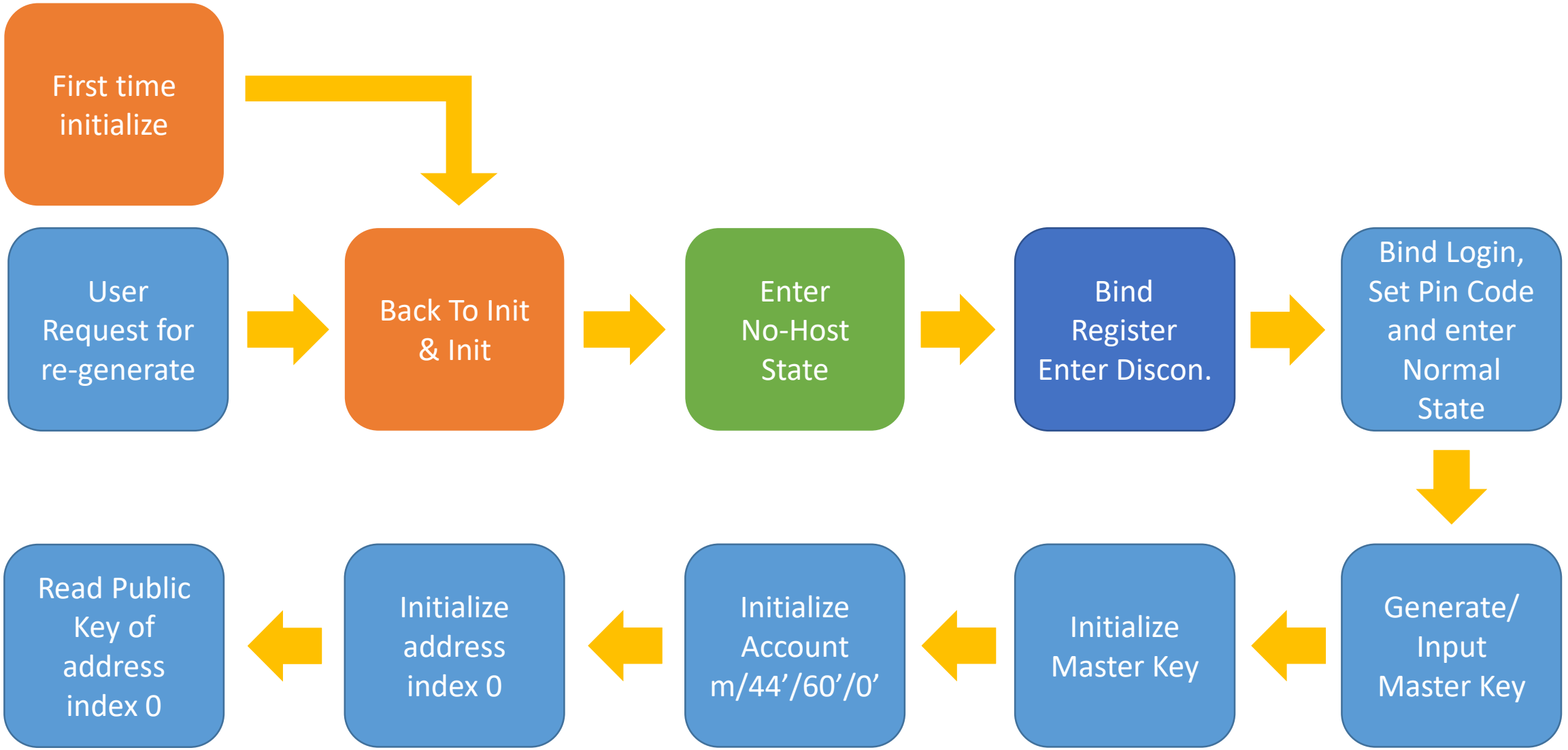
Derived Addresses

Note these addreses are derived from the **BIP32 Extended Key**

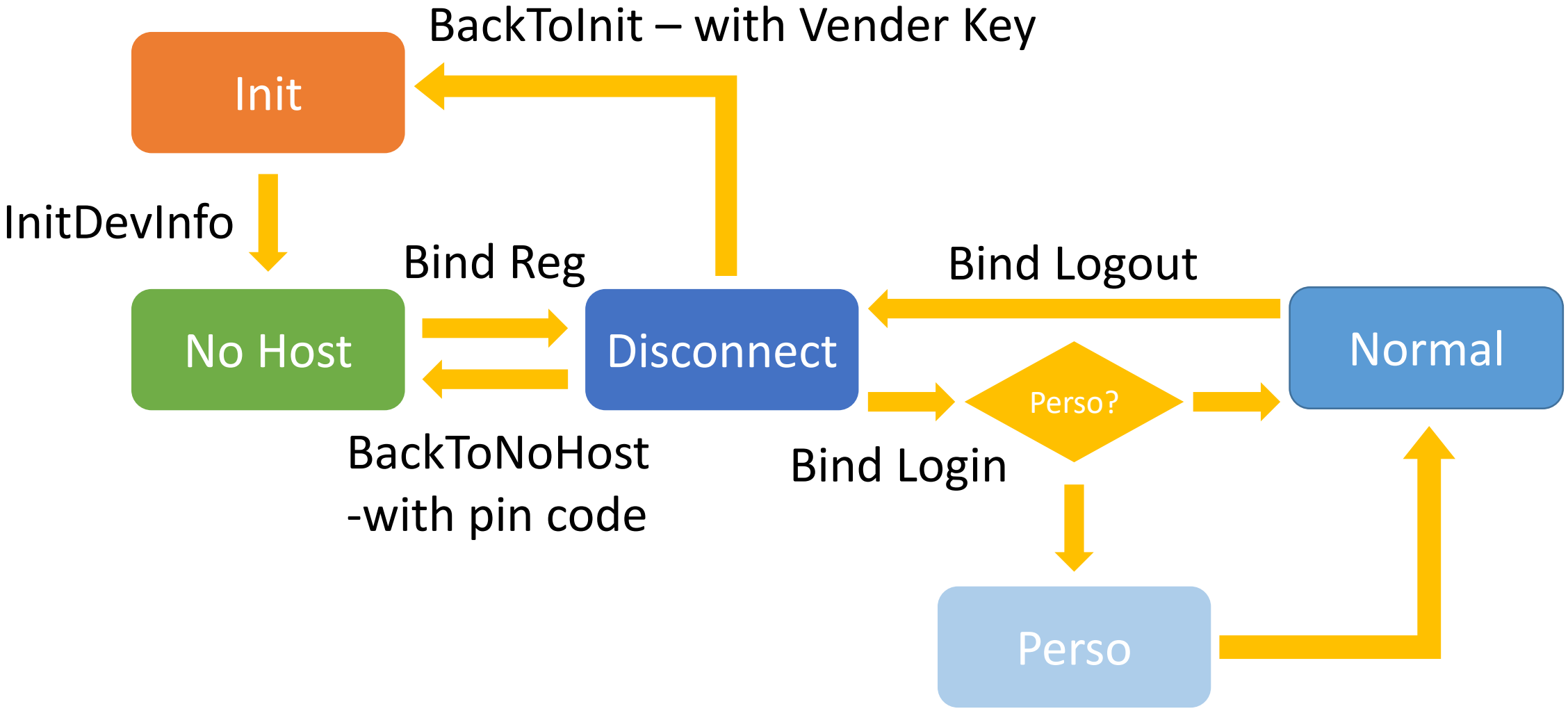
Path Toggle	Address Toggle	Public Key To
m/44'/60'/0'/0/0	0xA4eE286b0F4917D4bcF44B557E063dB59C5C31bE	0x03098d5772f8
m/44'/60'/0'/0/1	0x058dBD9e05323fF82c1aE4A28E66C067974e17eB	0x02049513c514
m/44'/60'/0'/0/2	0x2DF0B5033f9eB763B3f1a5d05b272122A7b32900	0x0355feda333ca
m/44'/60'/0'/0/3	0x4308f77C4365f8CdBb55B1c67FA23A674be83b1b	0x026e87073f7d4
m/44'/60'/0'/0/4	0xf92DE49a114E3A152D6eb0E9AeC8eBA0591B036d	0x039aa1d6e844

Tool:https://coinomi.com/recovery-phrase-tool.html

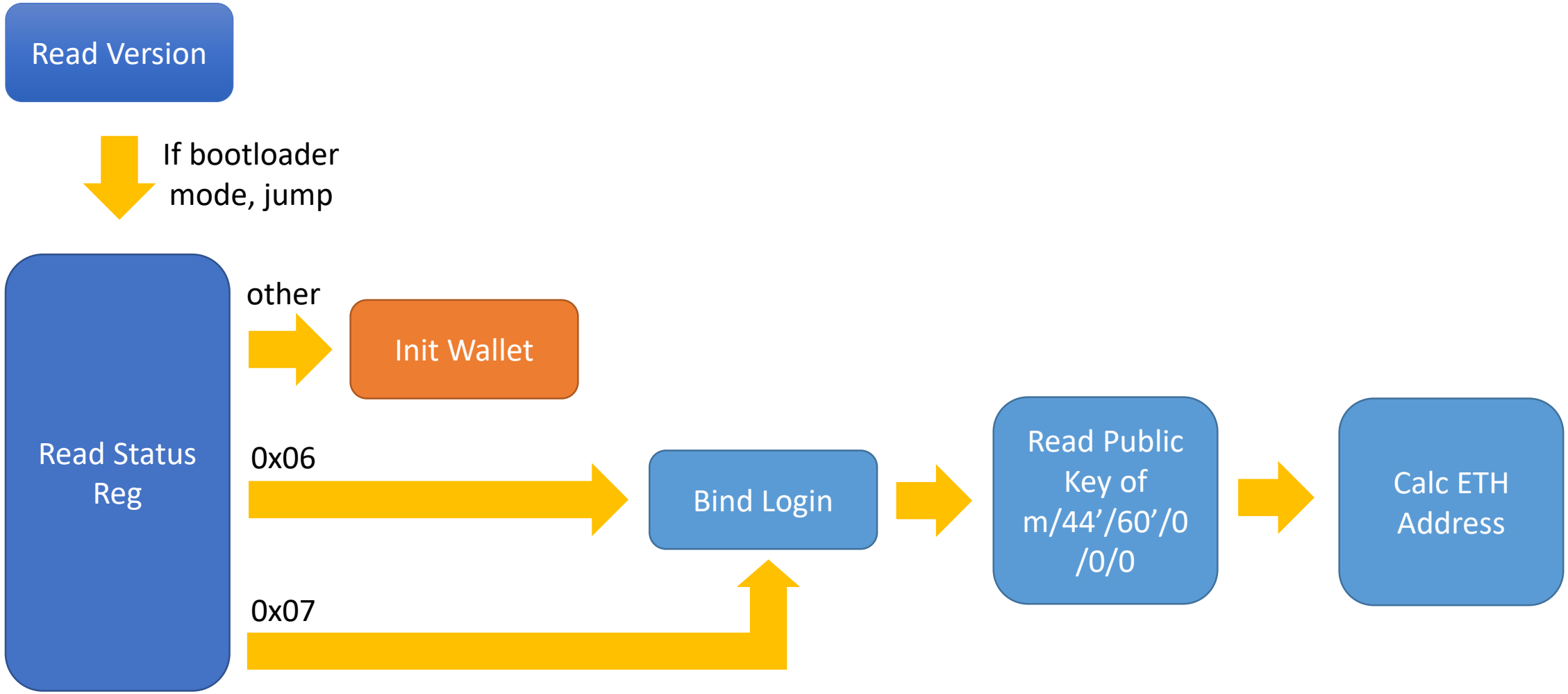
Badge initialize + re-generate wallet



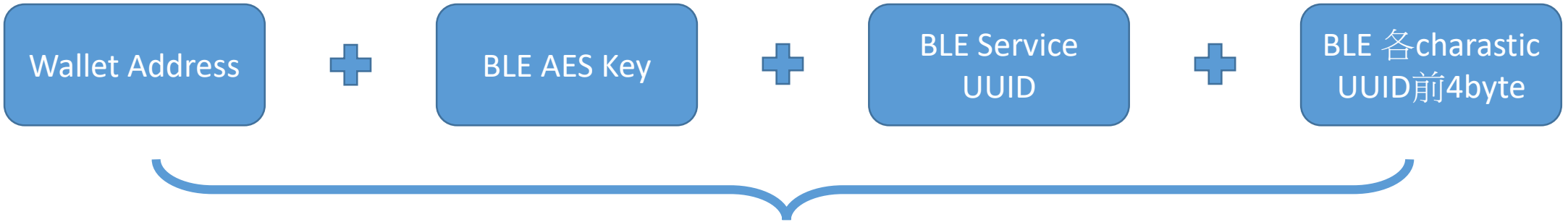
Secure Element - State



Badge startup wallet



Hitcon Badge 2018 – BLE Initialize + Re-paring



初始化的時候，
Badge會將生成好的Public Address和BLE Key打包成一個網址顯示在QR Code上面

QR-Code

格式:
Hitcon://pair?v=版本數
&a=錢包Address
&k=AES Key
&s=ServiceUUID
&c=Characteristic前四個Byte[6]

Example:
hitcon://pair?
v=18&
a=808c2257d778e5f1340d9325116f5a7273b33f5d&
k=09626aa096254e8a8ce871bfd7b8895c&
s=1cbfbb33-ffc7-c966-77f9-311c6ba9e425&
c=26ccce12e2c66a0b72c50cca509dbfc1275074f57e7c5668

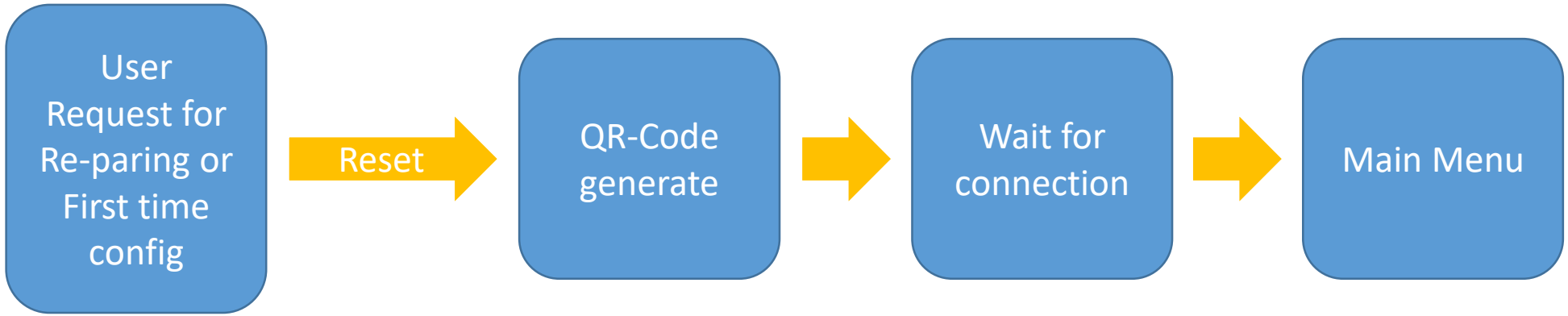
Hitcon Badge 2018 – BLE UUIDs

為了避免濫發交易訊息，UUID是綁定時隨機產生的
QR Code會寫Characteristic UUID的前4個Byte，後面的UUID與Service相同
QR code的Characteristic順序如下:

Transaction, Txn, AddERC20, Balance, General Purpose Cmd, General Purpose Data

EX:
[init_BLE] LFLASH_Saved_UUID:
ServiceUUID: 8b15cb6c-0dfd-553a-9302-3cdcded12f56
Transaction_UUID: bbf16eb7-0dfd-553a-9302-3cdcded12f56
Txn_UUID: d754e76e-0dfd-553a-9302-3cdcded12f56
AddERC20_UUID: 448821bb-0dfd-553a-9302-3cdcded12f56
Balance_UUID: 19aceb1f-0dfd-553a-9302-3cdcded12f56
General_CMD_UUID: 8a2c0cd1-0dfd-553a-9302-3cdcded12f56
General_Data_UUID: 4ff47ce6-0dfd-553a-9302-3cdcded12f56

Hitcon Badge 2018 – BLE Initialize + Re-paring

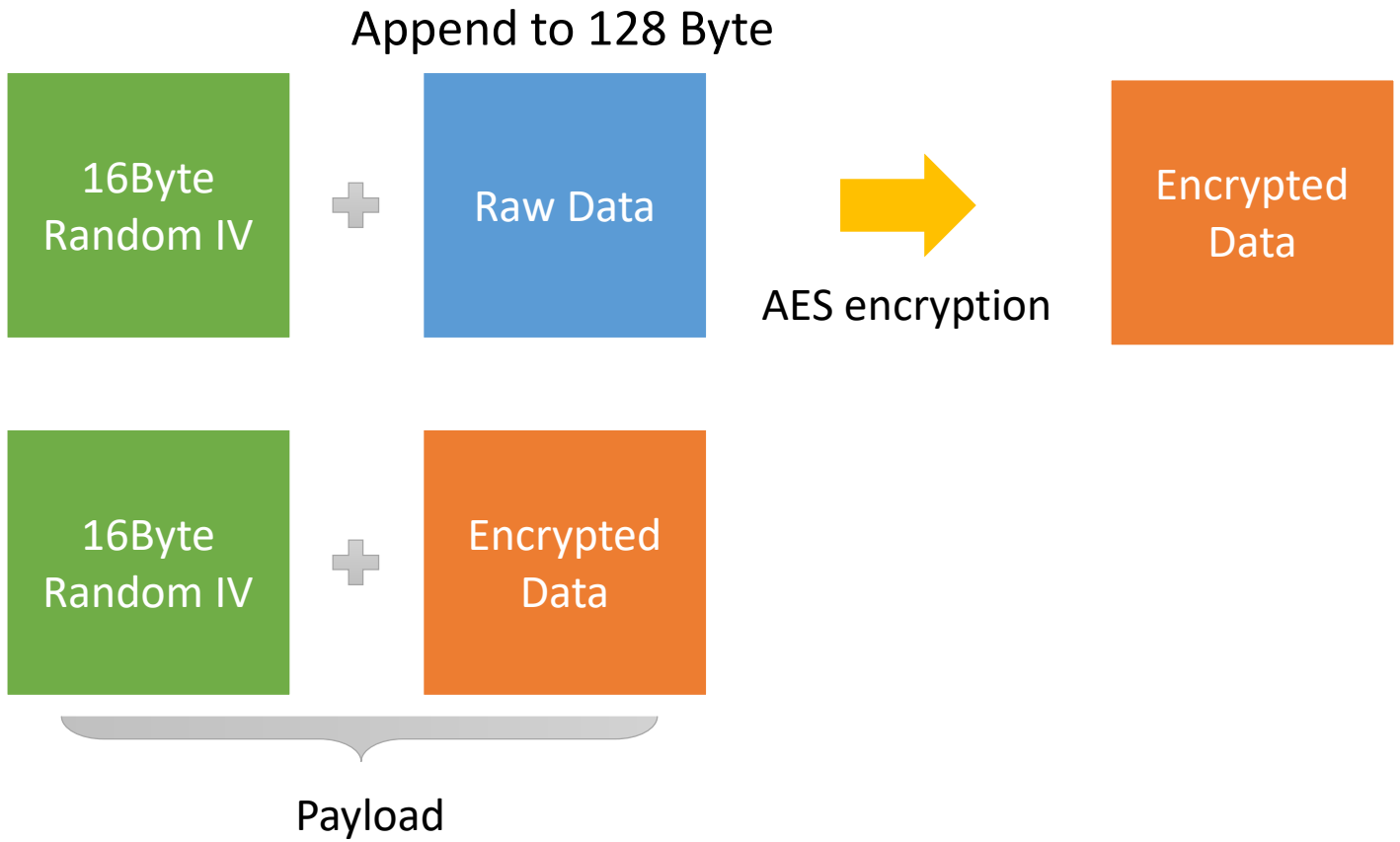


MT7697沒辦法 on-flight 修改BLE，
所以必須Reset一次

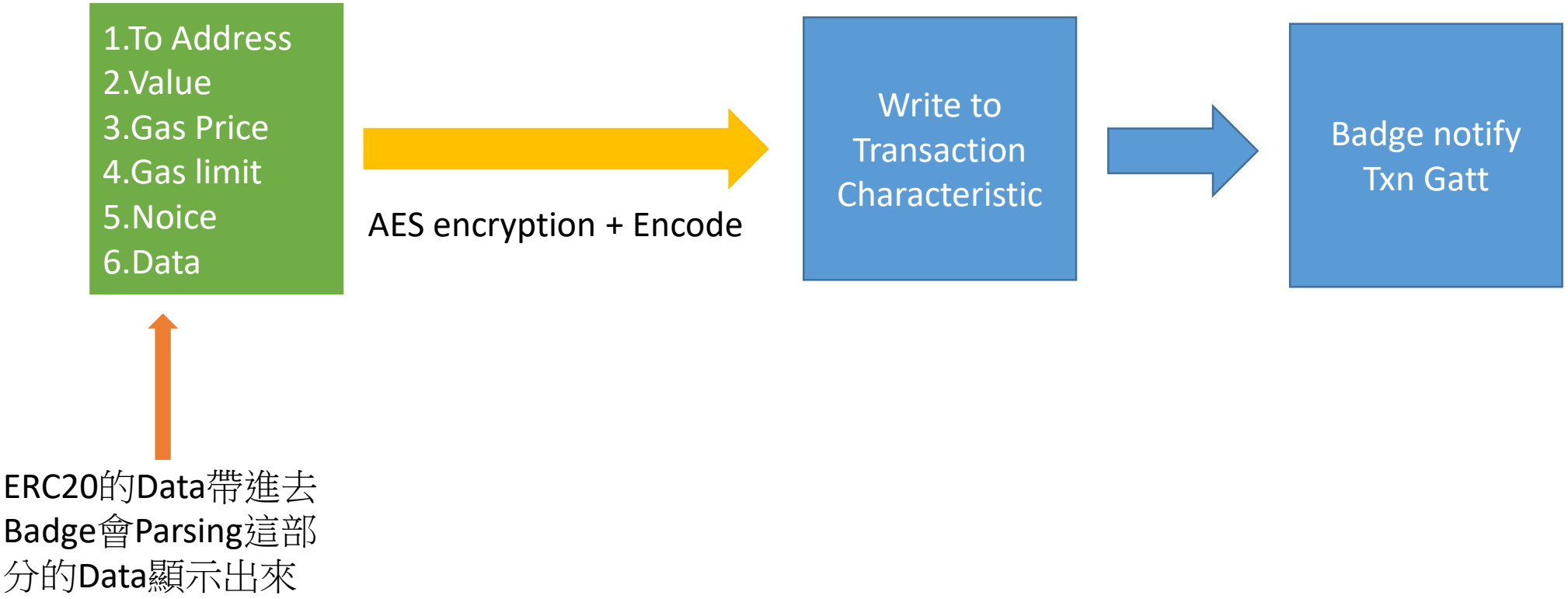
AES encryption + Encoding

Encoding Format:

Header1(uint8_t)	length1(uint8_t)	Data1[len]
Header2(uint8_t)	length2(uint8_t)	Data2[len]
Header3(uint8_t)	length3(uint8_t)	Data3[len]



Transaction



Update Balance or ERC20 Balance

Encoding Format:

0x01	0x14	ADDRESS
0x02	0x08	Value(Double)

Badge 並不會知道Balance是否正確!

Apple, Why....

6/12 Update

感謝@CW Cai支援

3.1.5 (b) Cryptocurrencies:

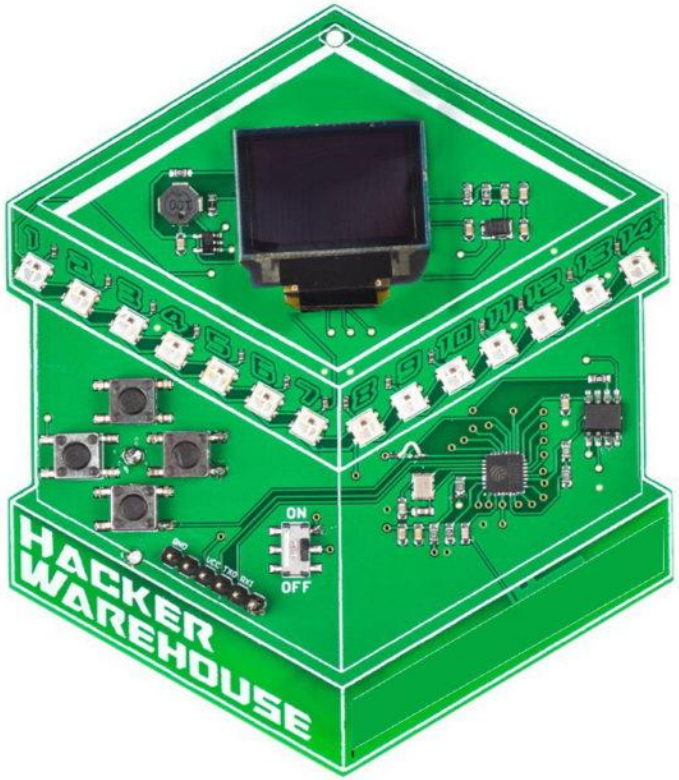
- (i) Wallets: Apps may facilitate virtual currency storage, provided they are offered by developers enrolled as an organization.
- (ii) Mining: Apps may not mine for cryptocurrencies unless the processing is performed off device (e.g. cloud-based mining).
- (iii) Exchanges: Apps may facilitate transactions or transmissions of cryptocurrency on an approved exchange, provided they are offered by the exchange itself.
- (iv) Initial Coin Offerings: Apps facilitating Initial Coin Offerings ("ICOs"), cryptocurrency futures trading, and other crypto-securities or quasi-securities trading must come from established banks, securities firms, futures commission merchants ("FCM"), or other approved financial institutions and must comply with all applicable law.
- (v) Cryptocurrency apps may not offer currency for completing tasks, such as downloading other apps, encouraging other users to download, posting to social networks, etc.

Prototypes


HitconBadge
2018
OFF
ON
SW1
0.00 V
Balance:
0.0000 ETH
[A]:SET
Address:
VUSB
TX
RX
3V3
SCL SDA
RST
PWR
LED1
GND
BUTTON1
BUTTON2
BUTTON3

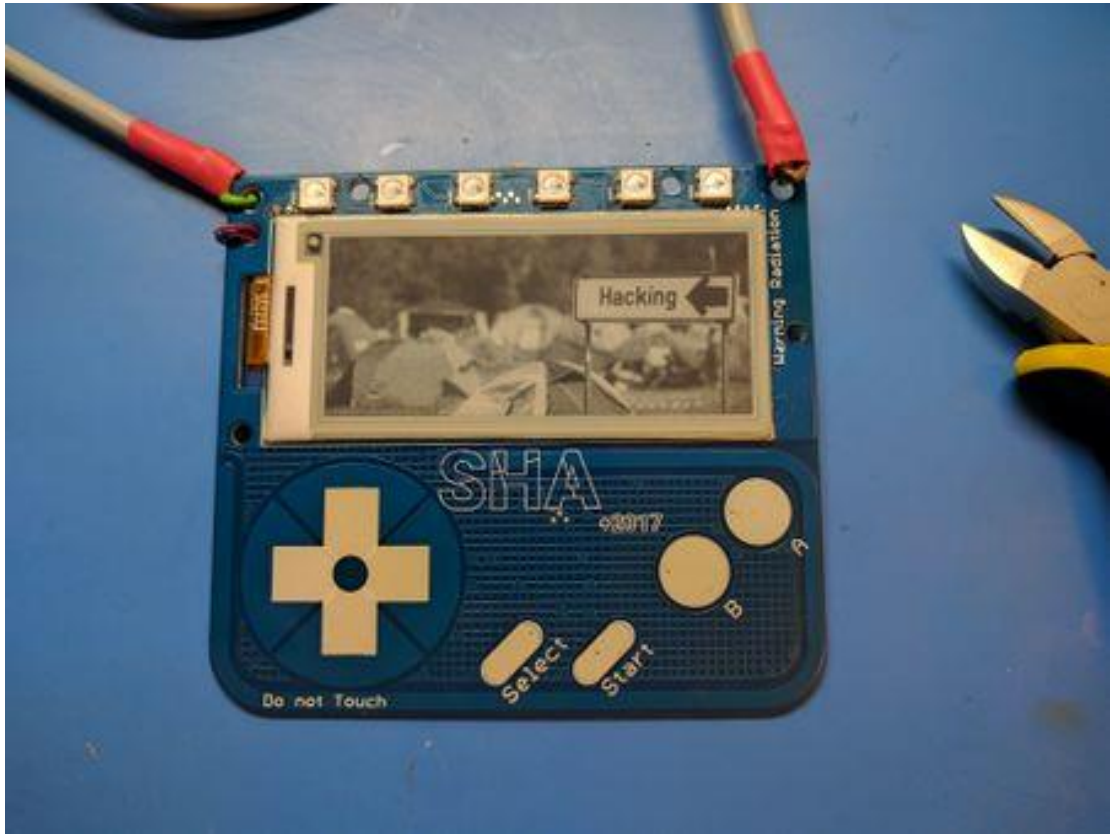
靈感來源

Hacker Warehouse Electronic Badge



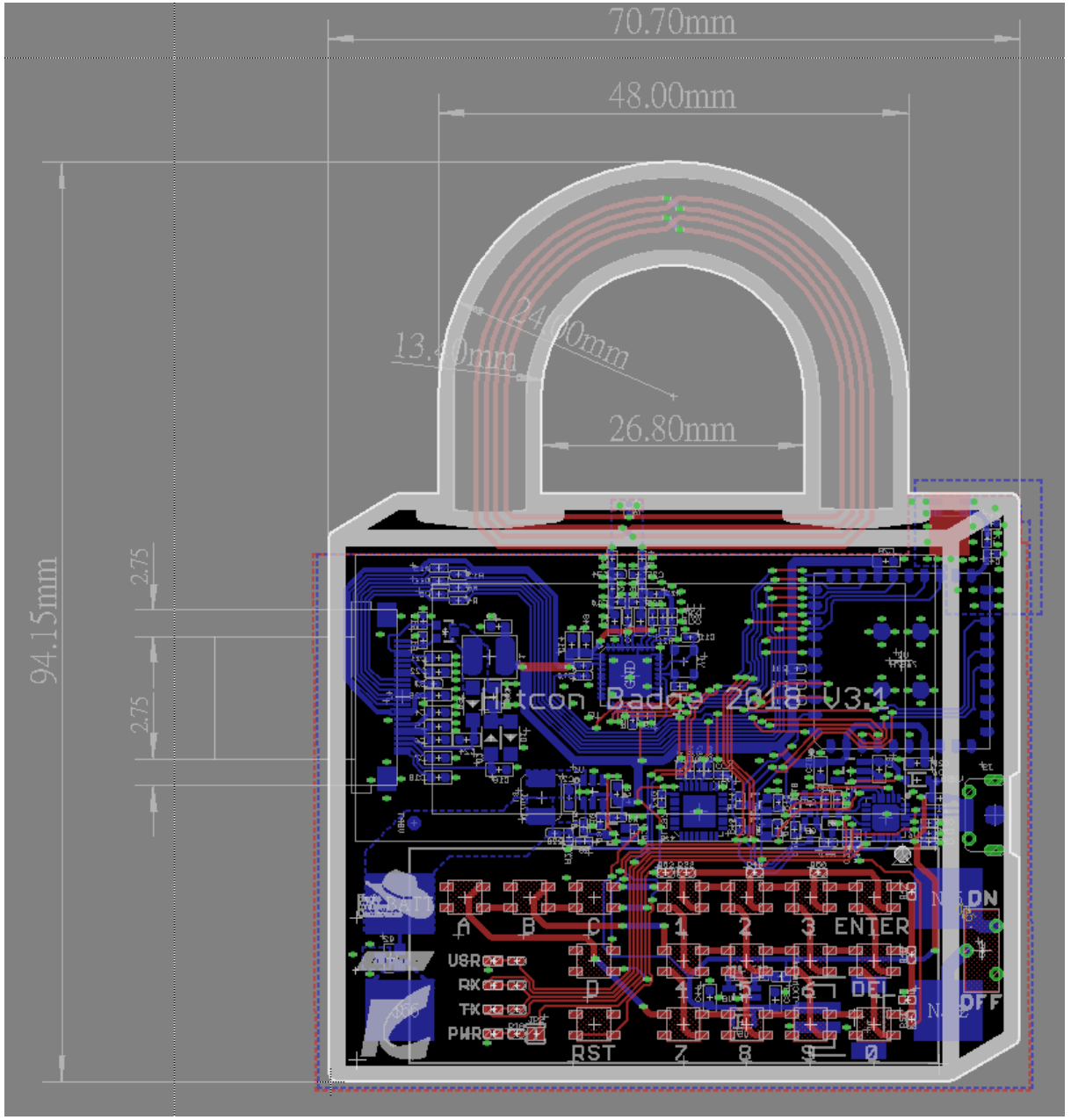
https://hackerwarehouse.com/product/hacker-warehouse-electronic-badge/

SHACamp 2017 badge



https://wiki.sha2017.org/w/Projects:Badge

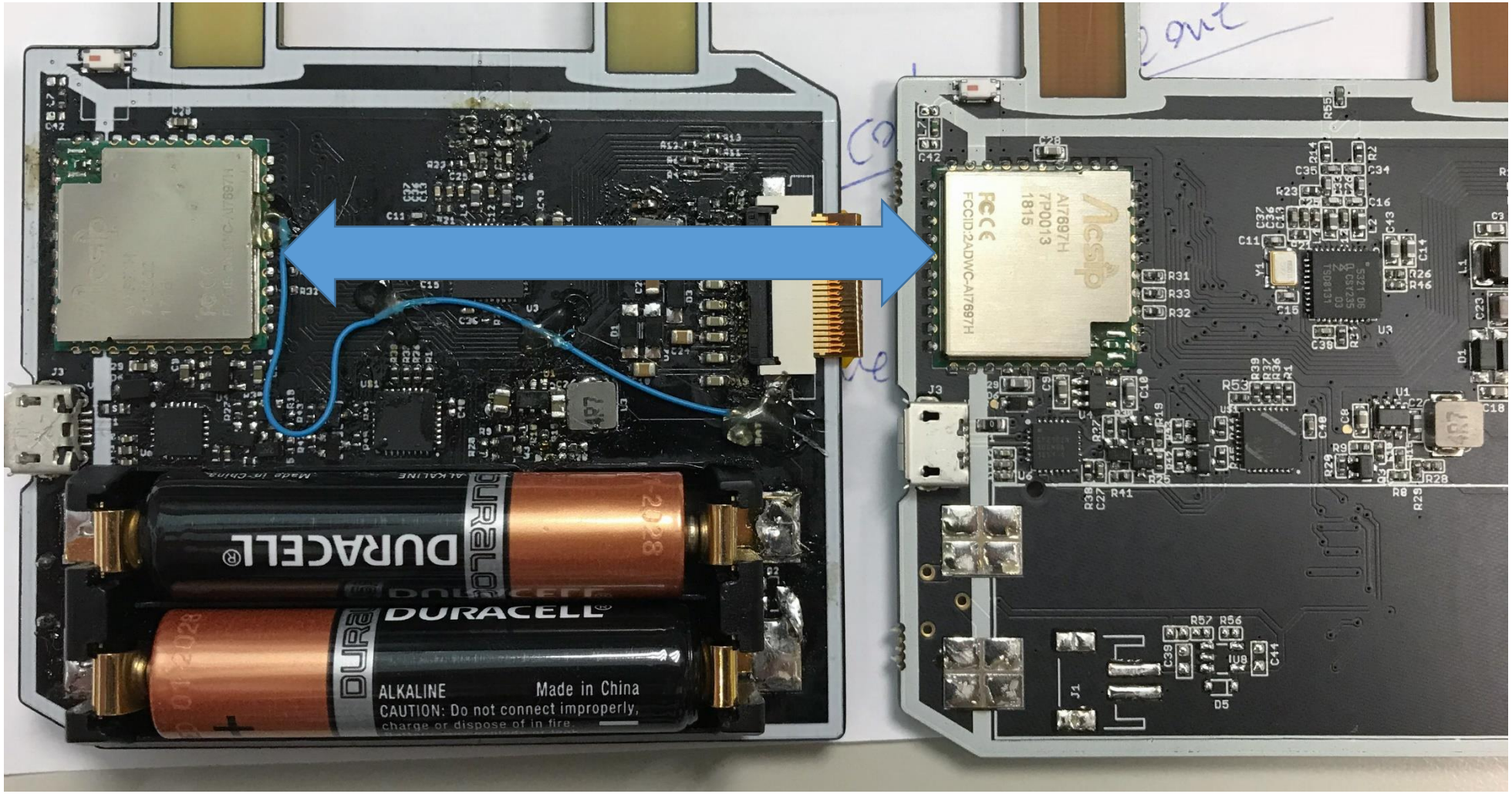
Prototypes


70.70mm
48.00mm
94.15mm
26.80mm
2.75
2.75
Hitcon Badge 2018 V3.1
A
B
C
1
2
3
ENTER
USR
RX
TX
PWR
RST
7
8
9
0
DEL
ON
OFF

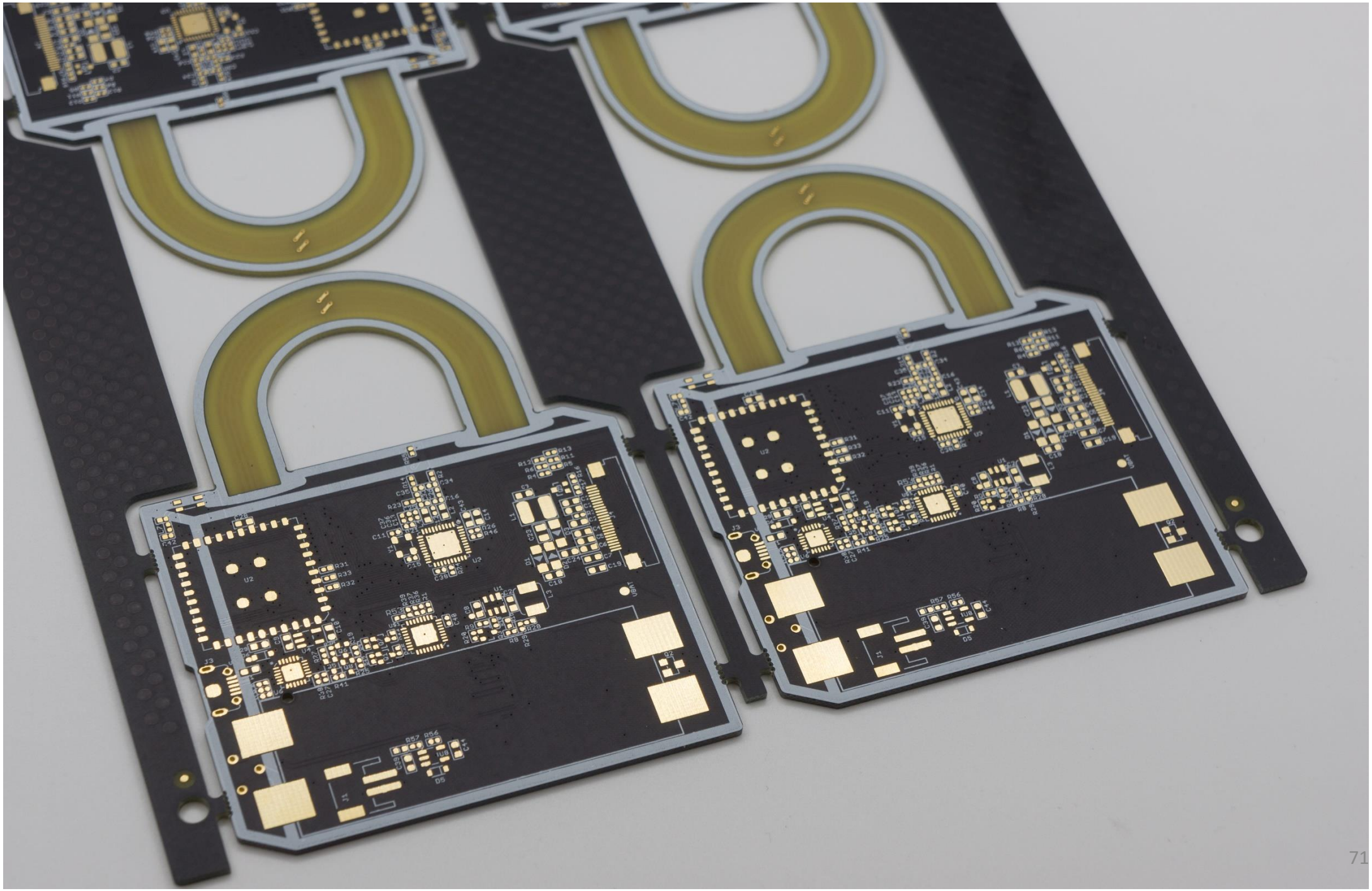
後記 - Prototypes

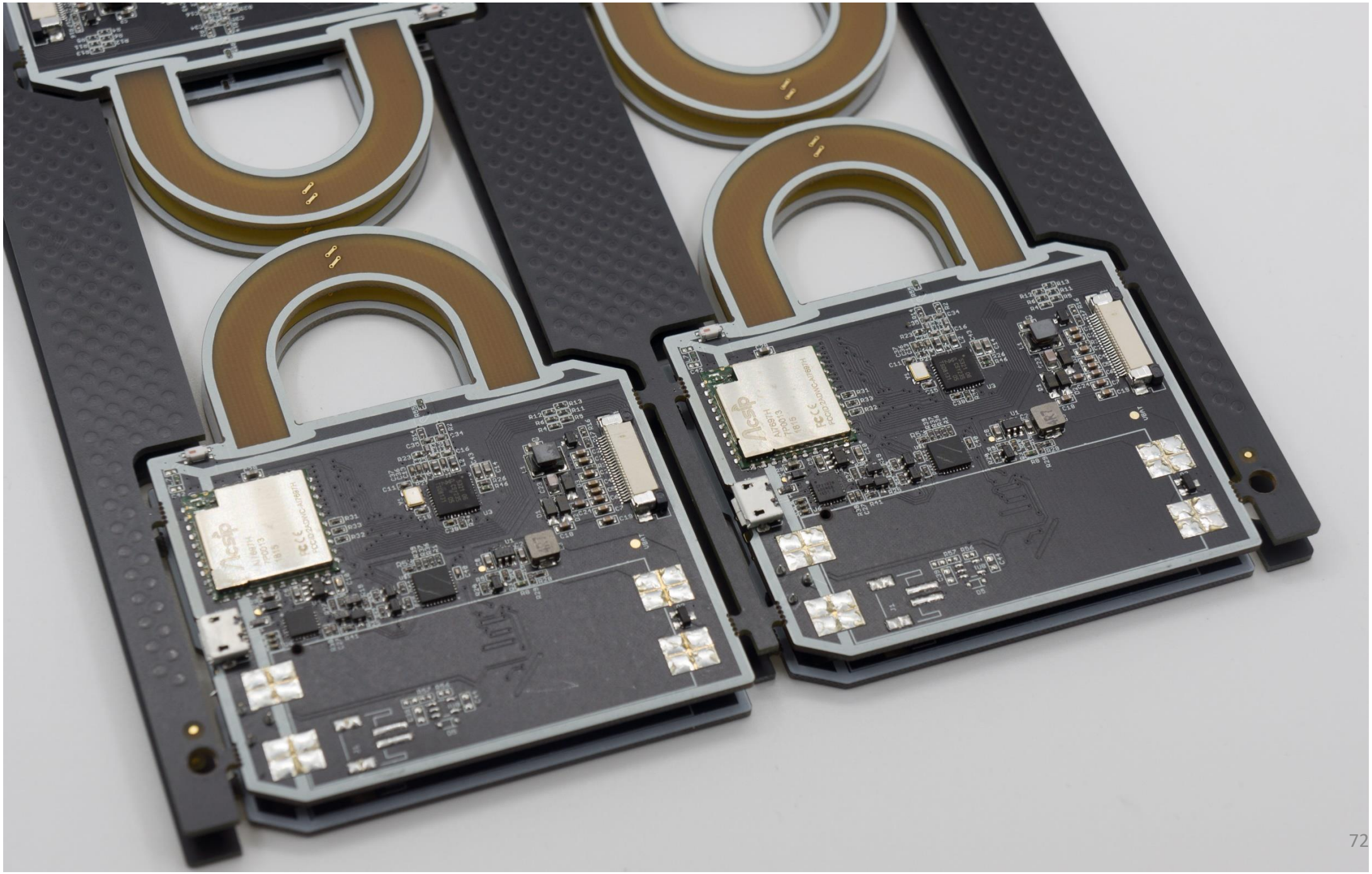
後記 – 生産線

後記 – 生產線


DURACELL
DURACELL
ALKALINE
Made in China
CAUTION: Do not connect improperly,
charge or dispose of in fire.
FCC ID:2ADWC-AI7697H
AI7697H
7P0013
1815

後記 – 生產線



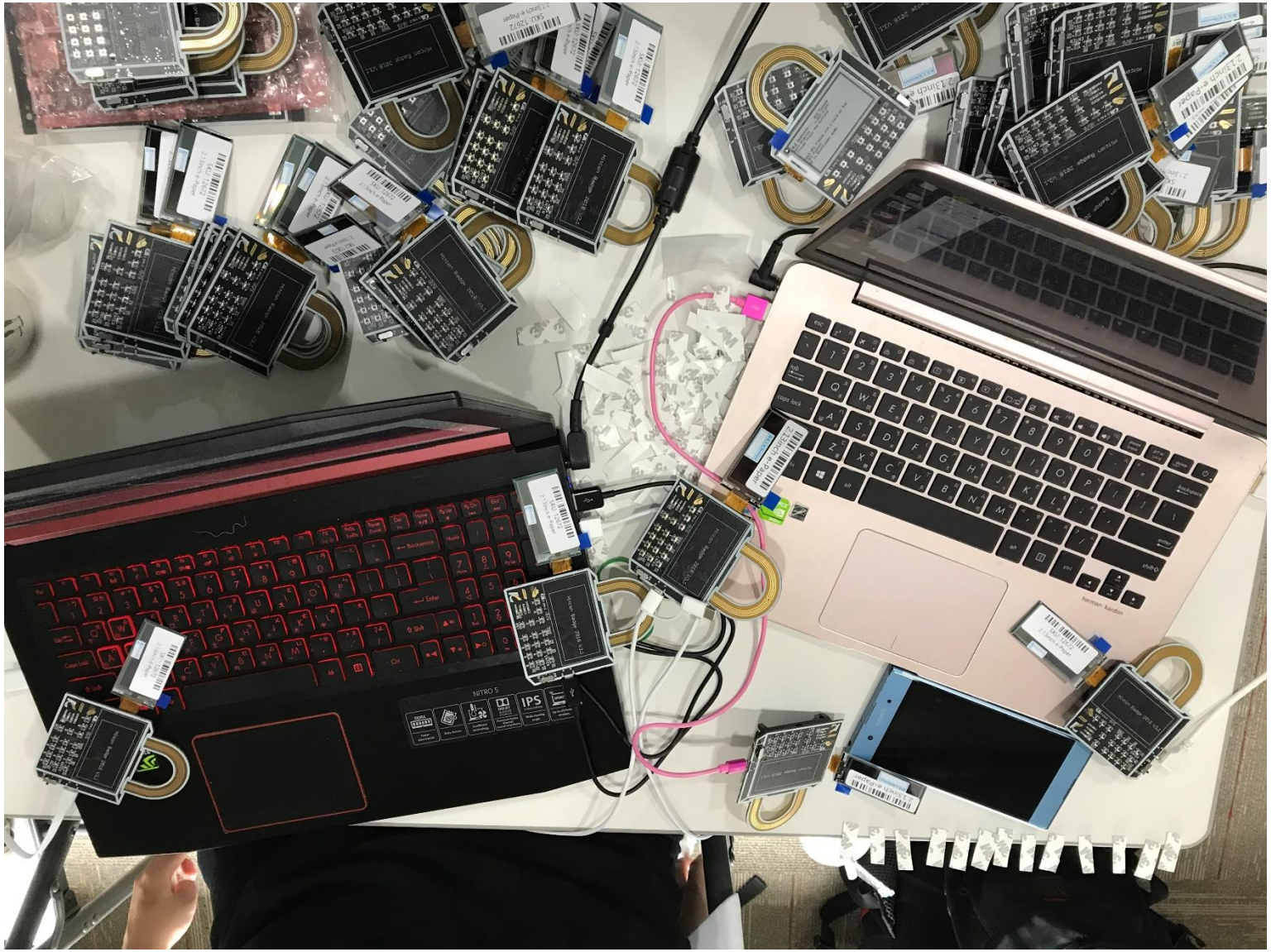



BLM
1.5V
"AAA"
1.5V

後記 – 生產線

後記 – 生產線- Team Work

後記 – 生產線- Team Work



後記 – 生產線- Team Work

感謝廠商

銓安智慧科技

www.ikv-tech.com

邁特電子

www.might.com.tw

資料

- Hardware 和 Badge Software 都是 Open-Sourced
- Github: https://github.com/will127534/HITCON-Badge-2018/
- Android: https://github.com/johnny5581/HitconWalletJava
  - Big Thanks to @Nagi @WizTonE @Aaron Luo for the Android App
- Hitcon Badge 2018 Arduino Boards support package:

https://raw.githubusercontent.com/will127534/HITCON-Badge-2018/master/Software/Arduino_packages/package_hitcon_badge_index.json

- Linkit 7697: https://labs.mediatek.com/zh-tw/chipset/MT7697