Crypto Hardware
加密硬件

Ethereum Meetup – Shenzhen – July 29th, 2017

Lionello Lunesu 李欧
Enuma Technologies Limited

WeChat微信号：lionello

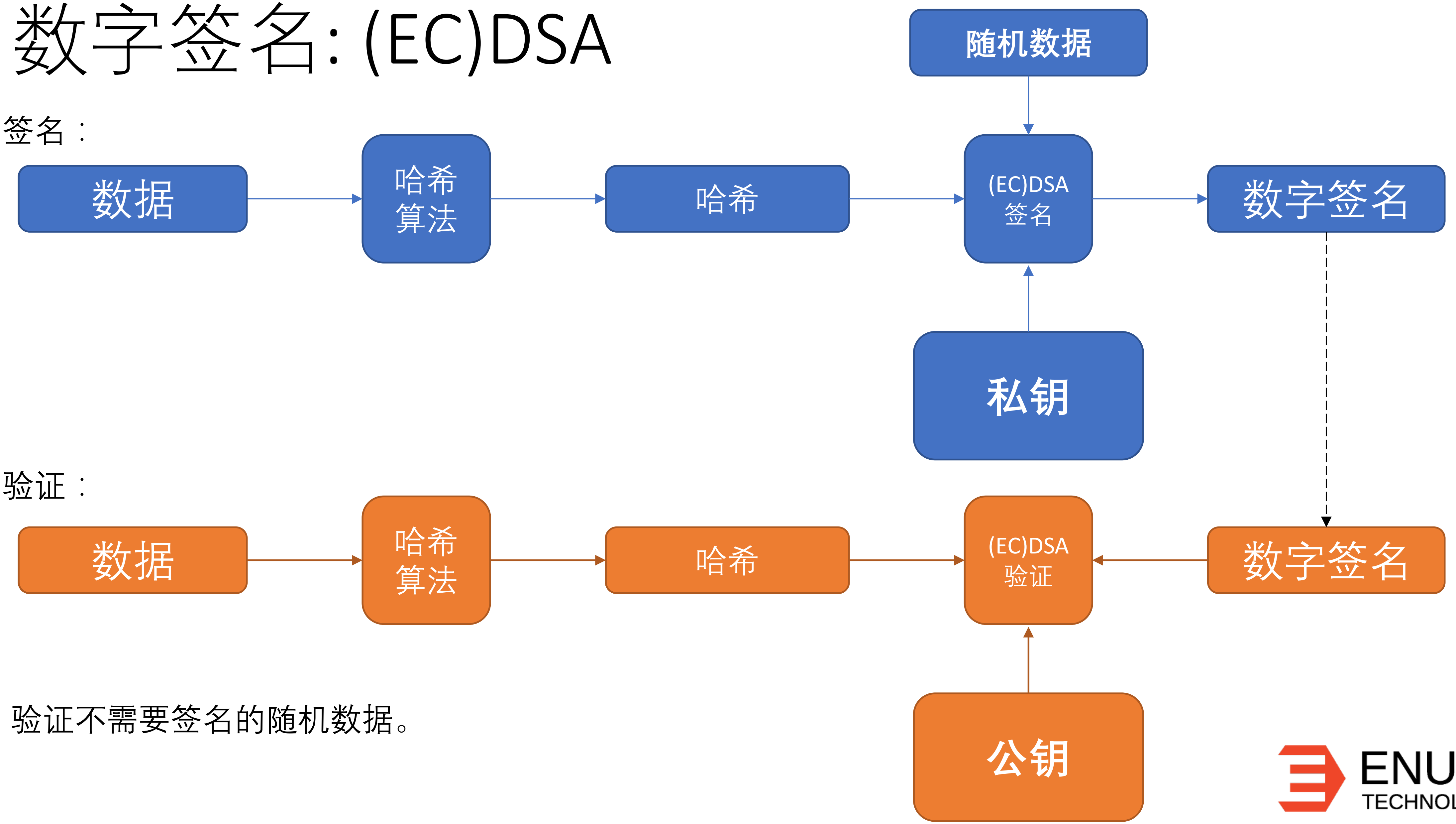
lio@enuma.io

ENUMA
TECHNOLOGIES

数字签名和加密的例子 – Digital Signatures

• SSL证书	SSL certificates (HTTPS)
• 比特币交易	Bitcoin transactions
• 以太坊智能合同	Ethereum smart contracts
• 文件签名	Document signing (PDF)
• 银行卡	Debit/credit card (EMV)
• 消息认证码	Message authentication (Signal/WhatsApp)
• 电子邮件验证标准	DomainKeys Identified Mail (DKIM)
• 公钥加密体系	Public Key Cryptography

数字签名: (EC)DSA



验证不需要签名的随机数据。

比特币交易里的数字签名 – Bitcoin Transaction

```
000:  0100000001ac18fa31f68e5597d4d1580ec1bdea10be30a39d10dddfd41360b3
020:  f7bbc40fac000000006a47304402206d3e58f553c0605c3a663d6baa7258cd53
040:  6f3c50f4aac96c361695f82ab2017d022003ad05075cff6be0185d4dcc7581a6
060:  0634de35a33585f009ab2f0d1beb9ccbd801210374b22e7dd641b4d24c483023
080:  a275fc808c813fe89f8cb4a9c97ef0f3431afb37ffffffff0202000000000000
0A0:  001976a914a24d41cca0b9baba81ce4f43747d97e24846ca6088acee3dcd1d00
0C0:  0000001976a91444635889ad4ba11e76c14d347867c48dba4069b388ac000000
0E0:  00
```

A 256-bit ECDSA signature consists of two 256-bit DER-encoded integers.

以太坊交易里的数字签名 – Ethereum Transaction

```
000:  f86d21850ba43b7400832fefd89454450450e24286143a35686ad77a7c851ada
020:  01a0880de0b6b3a7640000801ba0c36fdbf8043a64a6096ee81da4de7f04def4
040:  77b9a3210a18967fad07f72112b2a04aedfd1d9d9085256373b40ef02bc3da0a
060:  95054f40075de340086c9512707b29
```

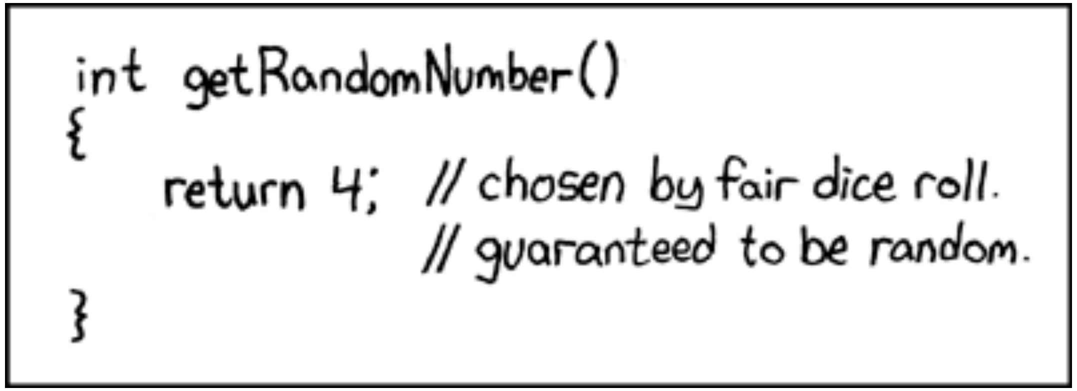
A 256-bit ECDSA signature consists of two 256-bit RLP-encoded integers.

加密软件的入侵 – Software Vulnerabilities

- 随机攻击
  - PS3
  - 安卓比特币钱包
- 产生私钥的问题
  - BIP032漏洞
  - Trezor v1边信道攻击
- 私钥侵扰
  - 私钥复制 Cloning
  - Cross-VM窥探
  - “Row hammer” 攻击

- Random Number Generation
  - PS3
  - Android Bitcoin Wallet
- Private Key Generation
  - BIP032 vulnerability
  - Trezor v1 side-channel attack
- Private Key Vulnerability
  - Private Key Cloning
  - Cross-VM Snooping
  - “Row hammer” attack

PS3随机攻击 – PS3 “Random Number” Hack



```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

© xkcd 221

加密硬件 – Crypto Hardware

- iOS Secure Enclave (iOS9以上)
- ARM Trusted Execution Environment (Android M以上)
- iNTEL SGX
- Atmel ECC crypto element
- Infineon Security controller
- NXP Secure authentication microcontroller
- FPGA-based
- SafeNet Luna SA (Amazon CloudHSM)
- Thales nShield (Azure Key Vault)

在iOS使用加密硬件 – iOS Secure Enclave

```
var dict: [String: AnyObject] = [
    String(kSecAttrKeyType) : kSecAttrKeyTypeEC,
    String(kSecAttrKeySizeInBits) : 256 as AnyObject
]

#if !((arch(i386) || arch(x86_64)) && os(iOS) && !NO_SE)
    dict[String(kSecAttrTokenID)] = kSecAttrTokenIDSecureEnclave
#endif

let result = SecKeyGeneratePair(dict as CFDictionary, &publicKey, &privateKey)
```

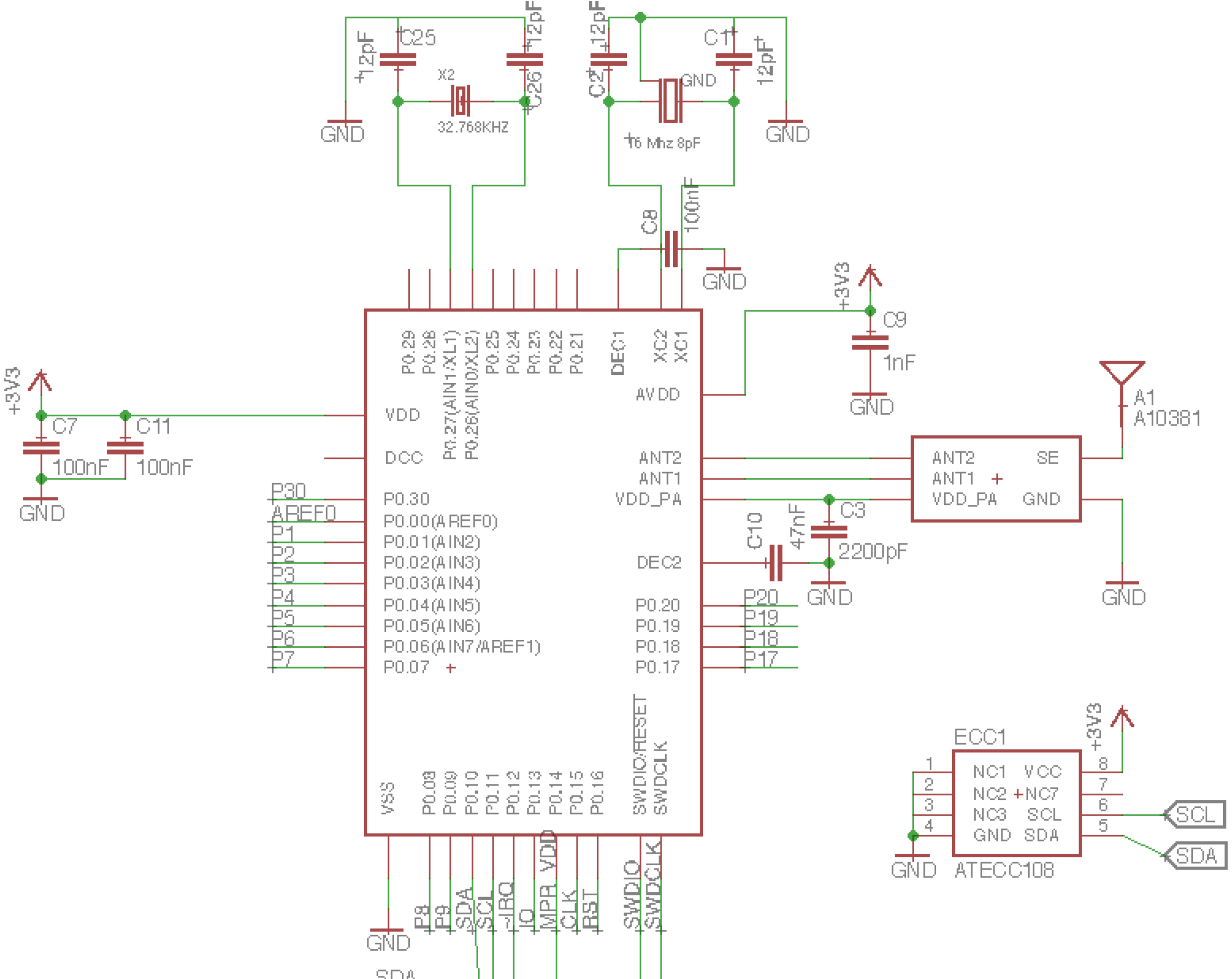
在安卓使用加密硬件 – Android TrustZone

```
KeyPairGenerator keyPairGenerator =
    KeyPairGenerator.getInstance(KeyProperties.KEY_ALGORITHM_EC,
                                 "AndroidKeyStore");

KeyGenParameterSpec.Builder builder =
    new KeyGenParameterSpec.Builder("some key alias",
                                    KeyProperties.PURPOSE_SIGN);

keyPairGenerator.initialize(
    builder
        .setAlgorithmParameterSpec(new ECGenParameterSpec("secp256r1"))
        .setDigests(KeyProperties.DIGEST_SHA256, KeyProperties.DIGEST_NONE)
        .build());

KeyPair keyPair = keyPairGenerator.generateKeyPair();
```

在Azure平台使用加密硬件 – Azure HW Keys

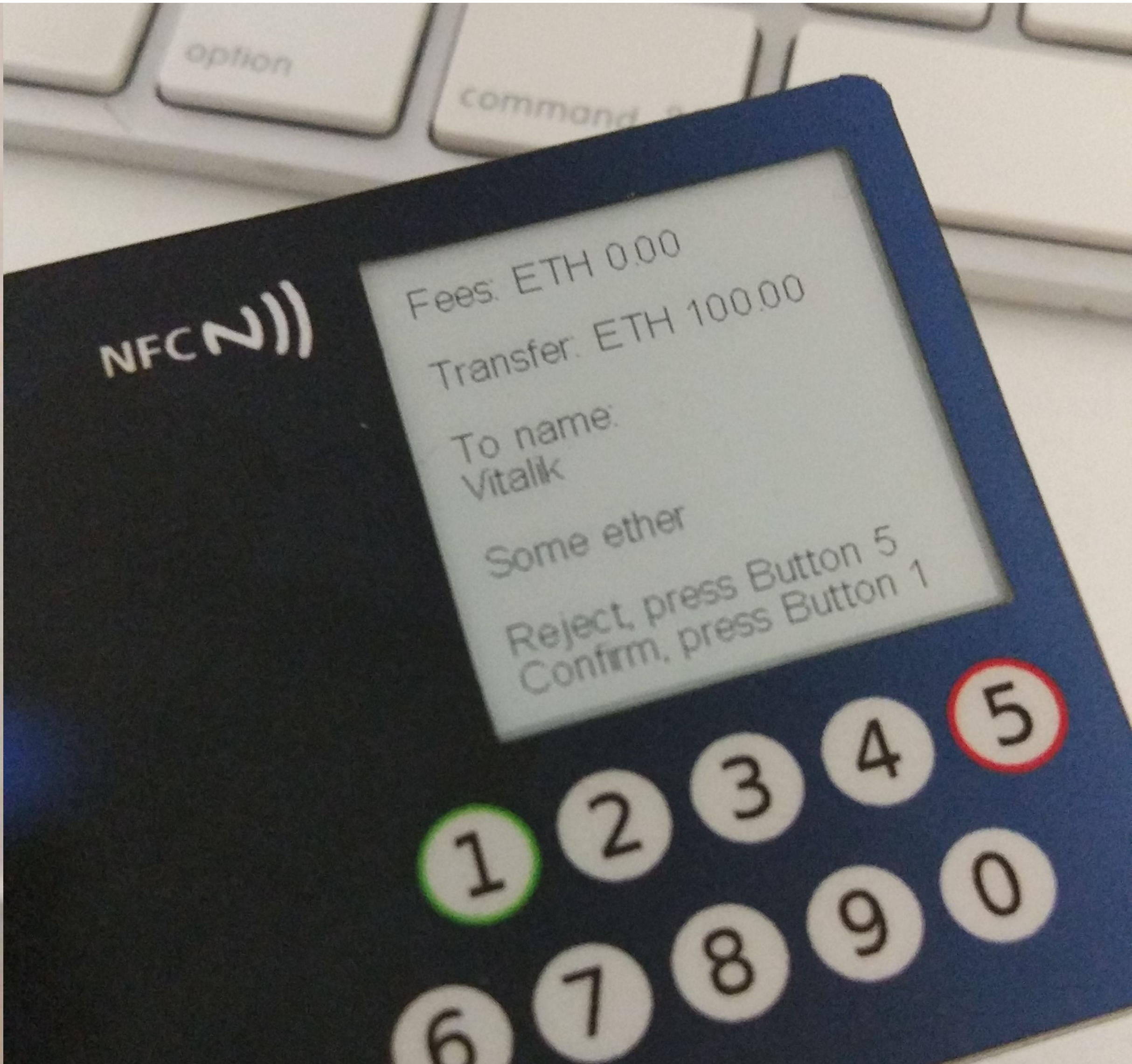
```
npm install azure -g

azure keyvault create my-vault --resource-group free-hk --location eastasia --sku premium

azure keyvault key create --vault-name my-vault --key-name MyKey --destination HSM
```

在物联网使用加密硬件 – IoT Crypto HW



ENUMA
TECHNOLOGIES

以太坊信用卡 – Ethereum HW Key



Fees: ETH 0.00
Transfer: ETH 100.00
To name:
Vitalik

Some ether

Reject, press Button 5
Confirm, press Button 1

加密硬件的限制 – Limitations of Crypto HW

- 钥匙限制
  - 一般≤256位EC
  - ≤2048位RSA
- 演算法限制
  - EC, SHA, ECDHE, RSA?
- ECC椭圆曲线限制
  - Secp256r1
  - 一般不支持Secp256k1 ☹

- Private Key Limitations
  - ≤256 bits EC
  - ≤2048 bits RSA
- Limited algorithms
  - EC, SHA, ECDHE, RSA?
- ECC Curve limitations
  - Secp256r1
  - but usually no Secp256k1 ☹

谢谢！ Thank you!

- 问题？Q?

WeChat微信号：lionello

lio@enuma.io

ENUMA
TECHNOLOGIES