无硬件，不安全

——浅谈区块链中的密码机

兴唐通信科技有限公司　姚长远

目录

1

第一部分

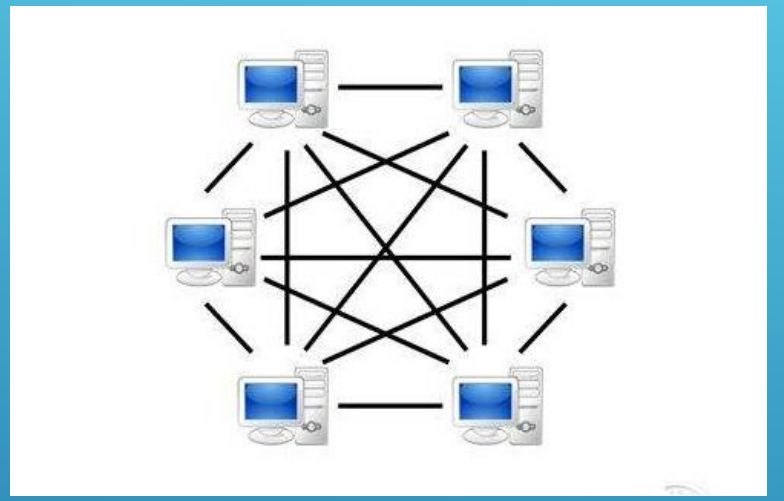
为什么需要密码机

什么是区块链

以一种采用**多方共识**机制来维护的**完整的**、**分布式的**、**不可篡改**的账本数据库

区块链的基石

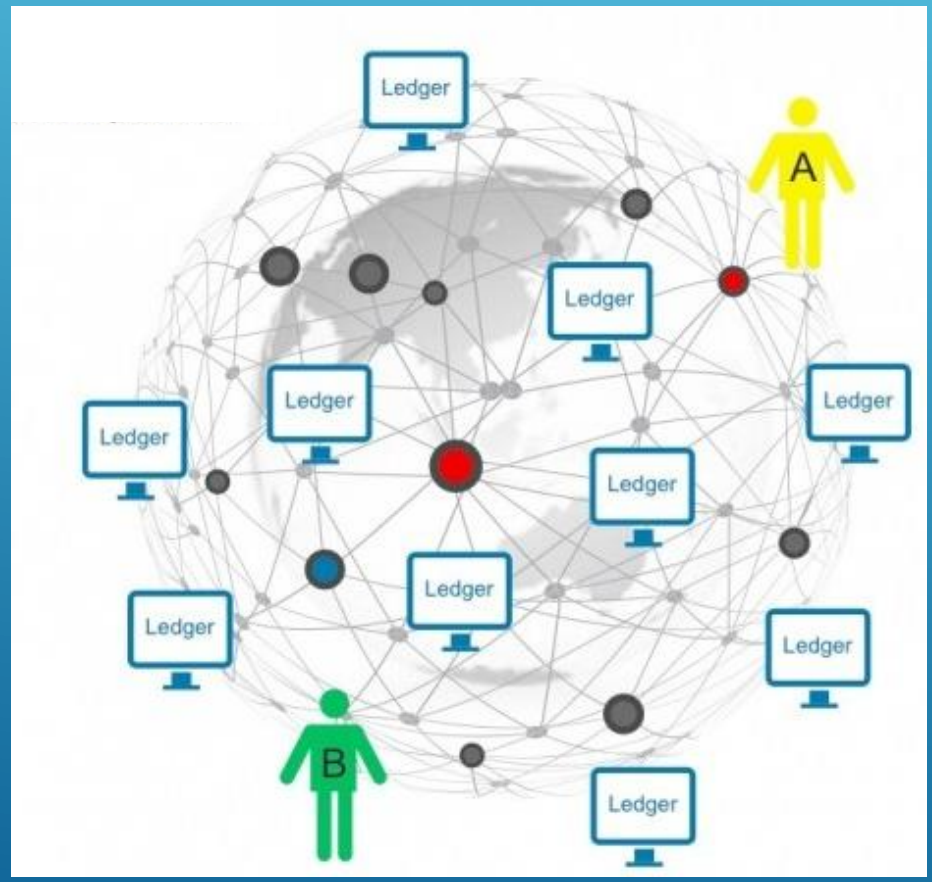
密码学



P2P网络

区块链解决的主要问题

互不信任的实体之间价值传递

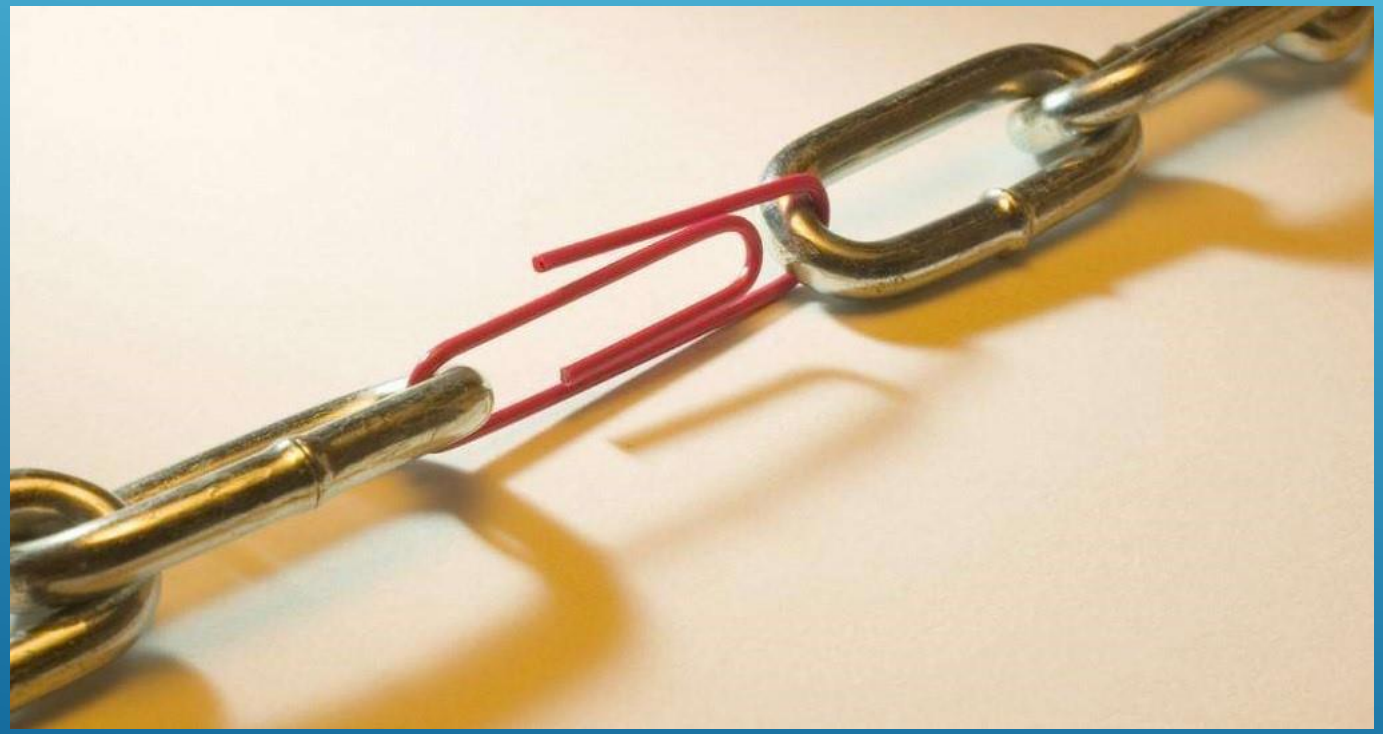


系统安全吗？

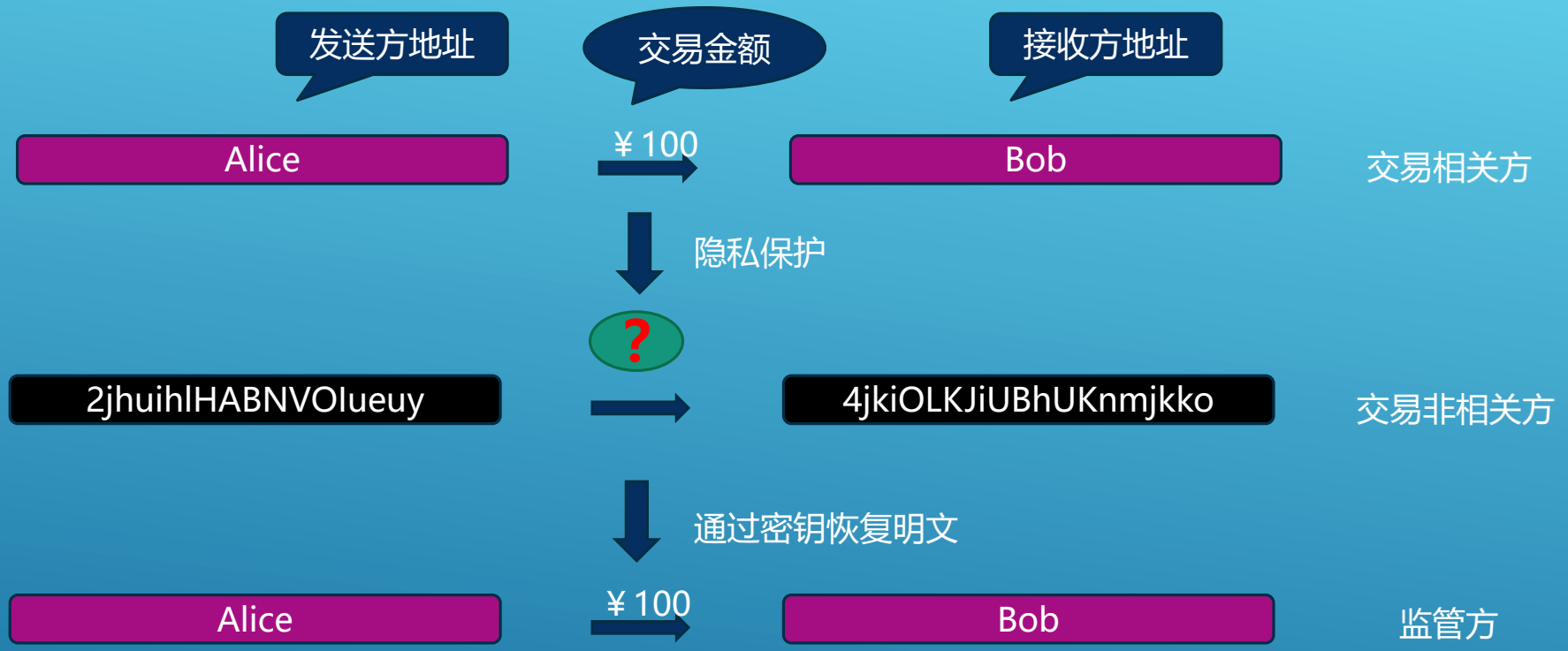
- 经过实践检验系统是安全的

区块链安全方面存在的问题

- 隐私保护和监管
- 密钥安全



隐私保护和监管


发送方地址
交易金额
接收方地址
Alice
￥100
Bob
交易相关方
隐私保护
?
2jhuihlHABNVOIueuy
4jkiOLKJiUBhUKnmjkko
交易非相关方
通过密钥恢复明文
Alice
￥100
Bob
监管方

公有链上隐私面临的威胁

- 公开账本模式带来严重的隐私保护隐患
  - 链上数据分析
  - 交易地址分析
  - 实体确认

区块链隐私泄露实例			
实体ID	地址数目	累计BTC	交易数目
A	78251	2886650	246012
Mt.Gox	156722	2206170	477526
C	13289	941013	77525
D	12520	867996	48347
E	191	692864	1353
F	12	660000	23
Instawallet	134	633606	92593
Deepbit	2	452929	814044
M	9	442000	10
N	128	432161	137

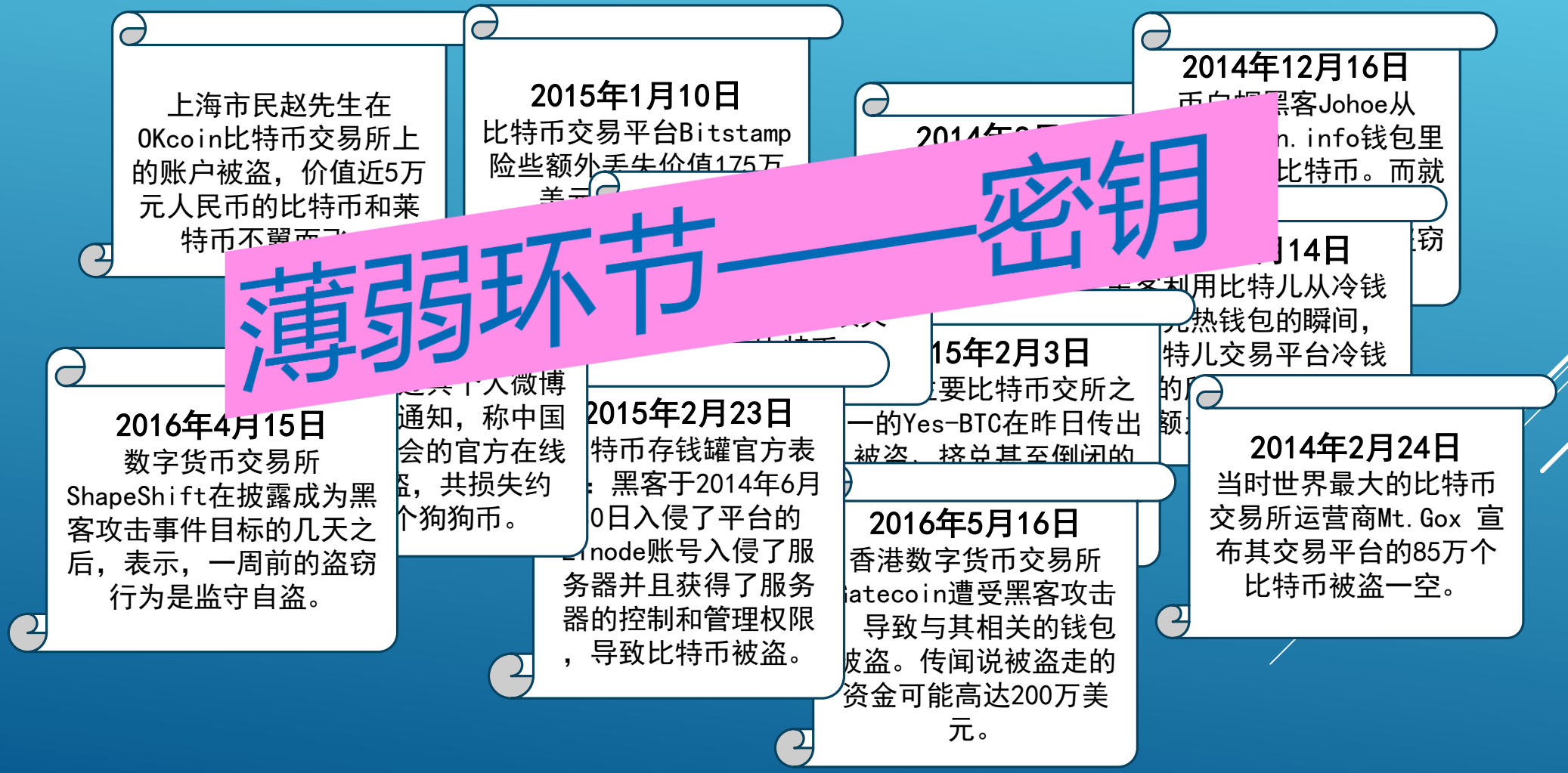
公有链上的方案

- 门罗币
  - 环签名
  - 同态加密
- 零币
  - 零知识证明

可能的解决方案

- 新的算法
  - 隐私保护算法
    - 环签名
    - 同态密码
    - 非交互零知识证明
  - 监管算法
    - 多方秘密共享
    - 群签名
    - 关联环签名
    - 可撤销匿名环签名

比特币和各类代币丢失和被盗事件层出不穷



密钥安全

- 区块链上存储的是资产，密钥是资产所有权的唯一证明

密钥面临的威胁

生成安全

随机数生成


```
{
"address":"f9f5f85afa5e7a3e75493b0073616ffc96cf1c8a",
"crypto":
{"cipher":"aes-128-ctr",
"ciphertext":"83fc001fe018c8181e25e6a14356779ed277432bd8c8de2b668a1823d55d4967",
"cipherparams":{"iv":"1e78c34e34e9d9ad55121d329ad4a8b5"},
"kdf":"scrypt",
  "kdfparams": {
      "dklen": 32,
      "n": 262144,
      "p": 1,
      "r": 8,
      "salt": "1f602c6d43778c8e874c654da83b07893f6db1529c08af1d11d49f8df848a7c9"
    },
"mac":"09d9b506bd112291c5ddc2a916d14d3a12b9f8e0eaac81f82cf05a8b21e49592"
},
"id":"b2716d06-14fc-4b29-b18b-48b07bb95591",
"version":3
}
```

硬件密码设备才能保证安全

密钥安全只用软件难以保证，需要使用硬件密码设备保证安全

密码机：在**密钥**作用下，实现明-密变换或者密-明变换的装置

形态：芯片（SE）、usb key、无线key、桌面型密码机、机架式密码机等

广义概念：包括密码机、密码方案、配套设施

硬件钱包

Trezor

Ledger Nano、Ledger Nano S、
Ledger Blue

KeepKey

CoolWallet

BWallet

数字货币指纹硬件钱包

更安全高效的设备

- 对于个人用户，硬件钱包基本能够保护密钥（资产）的安全性

- 对于企业用户、联盟链中的验证节点等，需要更安全高效的硬件密码设备

2

第二部分

需要什么样的密码机

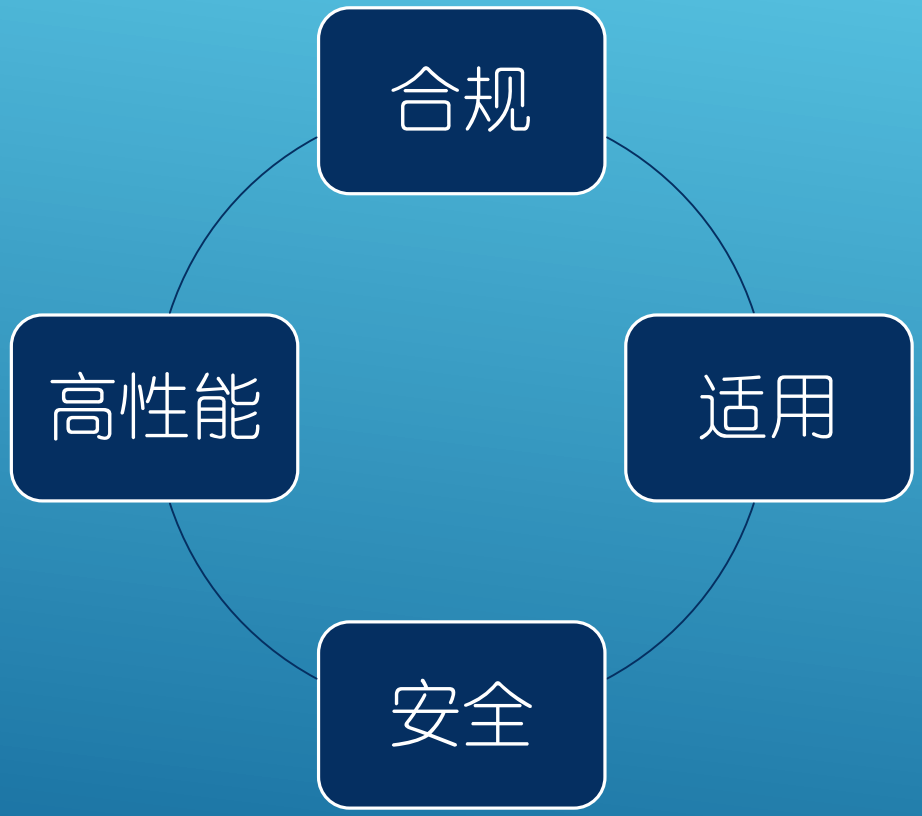
1 合规

2 适用

3 安全

4 高效

区块链密码机的新需求



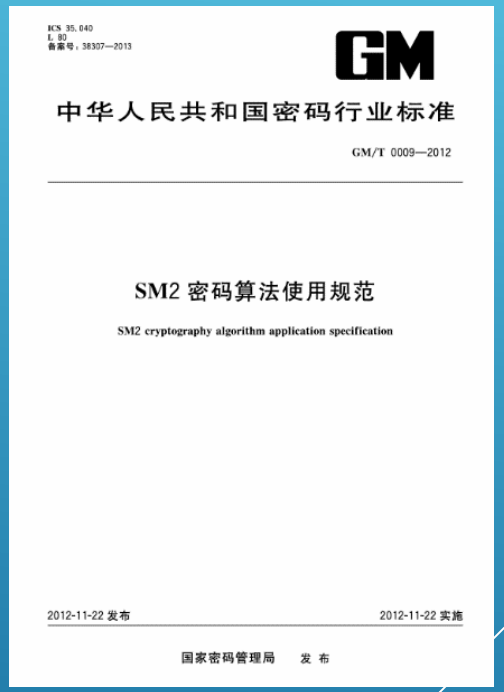
合规性

- 重要信息系统密码国产化要求

适用性

- 算法模式不同

不适用



ICS 35.040
L 80
备案号：38307—2013

GM

中华人民共和国密码行业标准

GM/T 0009—2012

SM2 密码算法使用规范

SM2 cryptography algorithm application specification

2012-11-22 发布　　2012-11-22 实施

国家密码管理局　发布

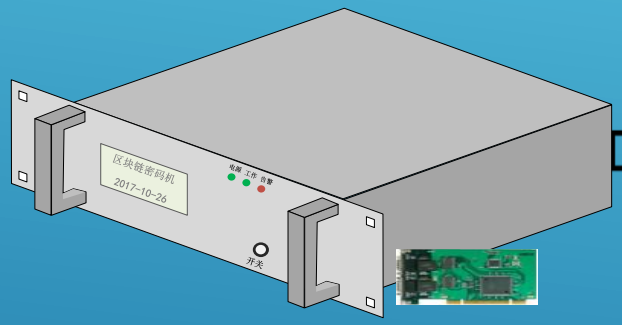
新的业务需求

- 隐私保护
  - 账户余额
  - 交易方
  - 交易金额
- 监管

新的功能实现

- 新的算法需求
  - 隐私保护算法
    - 环签名
    - 同态密码
    - 非交互零知识证明
  - 监管算法
    - 多方秘密共享
    - 群签名
    - 关联环签名
    - 可撤销匿名环签名

角色的转变



安全性

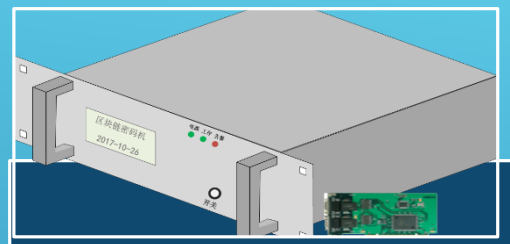
■ 什么是信息安全

ISO 17799中定义安全包括：

- **保密性**：确保只有被授权的人才可以访问信息；
- **完整性**：确保信息和信息处理方法的及时性、准确性和完整性；
- **可用性**：确保在需要时，被授权的用户可以访问信息和相关的资产

安全性

传统密码机



- 机密性
- 完整性
- 可用性

区块链密码机

- 机密性
- 完整性
- 可用性

性能要求

- 算法复杂
- 交易量高

3

第三部分

如何实现

1 系统化设计

2 工程实现

3 测评验证

如何实现

系统安全设计

- 密码方案设计
- 密钥安全（生成、存储、备份、恢复）
- 可靠性设计
- 维修性设计
- 可测试性设计

工程实现

- 硬件：
  - 基于成熟产品，新研高性能算法单元
- 操作系统：
  - 定制系统
  - 可信运行控制
- 应用程序：
  - 异构冗余
  - 存储冗余备份

检验测评

- 方案评审
- 第三方测评

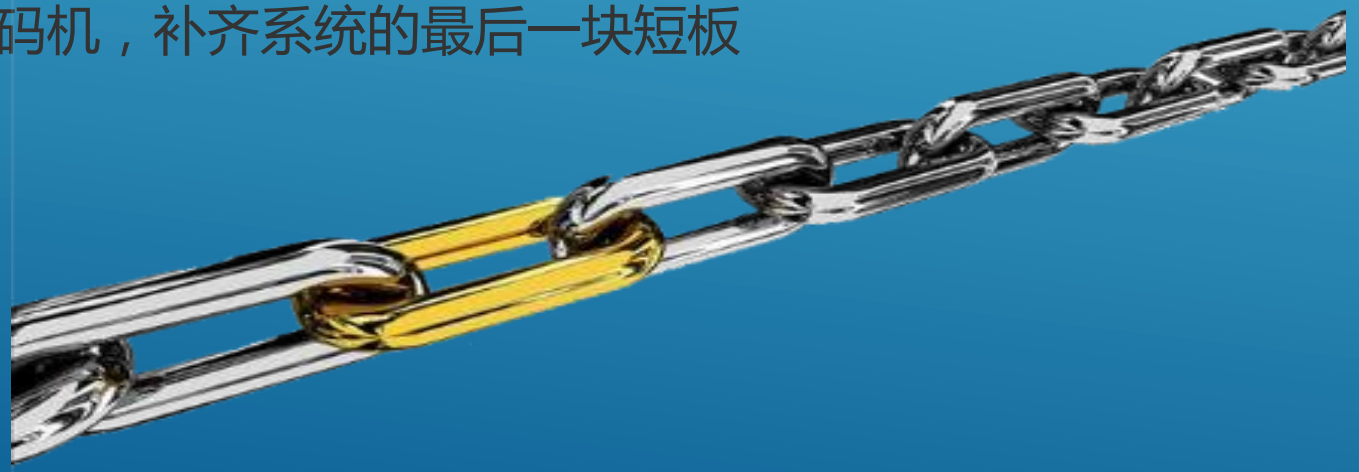
4

第四部分

总结

总结

- 区块链中需要解决的安全问题是监管下的隐私保护和密钥安全问题，通过密码机可以解决这些问题
- 区块链的密码算法需要符合国家相关规定。密码机在区块链中要支持新的算法、新的模式以及可控匿名等新的功能要求；在保证机密性和完整性的前提下要保证可用性；区块链密码机需要更高的性能。
- 在系统设计、工程实现、检验测评方面努力，可以实现安全的区块链密码机，补齐系统的最后一块短板



公司简介

- 兴唐通信科技有限公司是专为我国重要领域提供保密通信与信息安全保障的高科技中央企业，是ITU-T SG17 网络安全组的中国代表团团长单位。长期从事密码基础理论、密码算法、密码芯片、系列密码设备及密码应用系统的研究和开发，为我国金融、公安、电力等关键信息基础设施提供密码安全保障，是我国二代证数字信息密码防伪系统的总体设计与研制建设单位，获得国家科技进步一等奖2项。正牵头承担科技部“电子货币新算法与新原理研究”项目
- 希望研用单位合作发挥各自优势，一起推动行业的发展

谢谢！