



ISC 互联网安全大会



360 互联网安全中心



数字钱包安全浅析

马臣云 信任度科技CEO

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China



360 技术

IT大咖说
知识共享平台

目录

CONTENTS



ISC 互联网安全大会



360 互联网安全中心

一、安全事件频发

二、数字货币钱包的基本原理

三、常见数字货币钱包及安全风险分析

四、硬件钱包基本原理和安全风险

五、移动钱包如何提升安全性

六、钱包私钥备份与恢复

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China



IT大咖说
知识共享平台

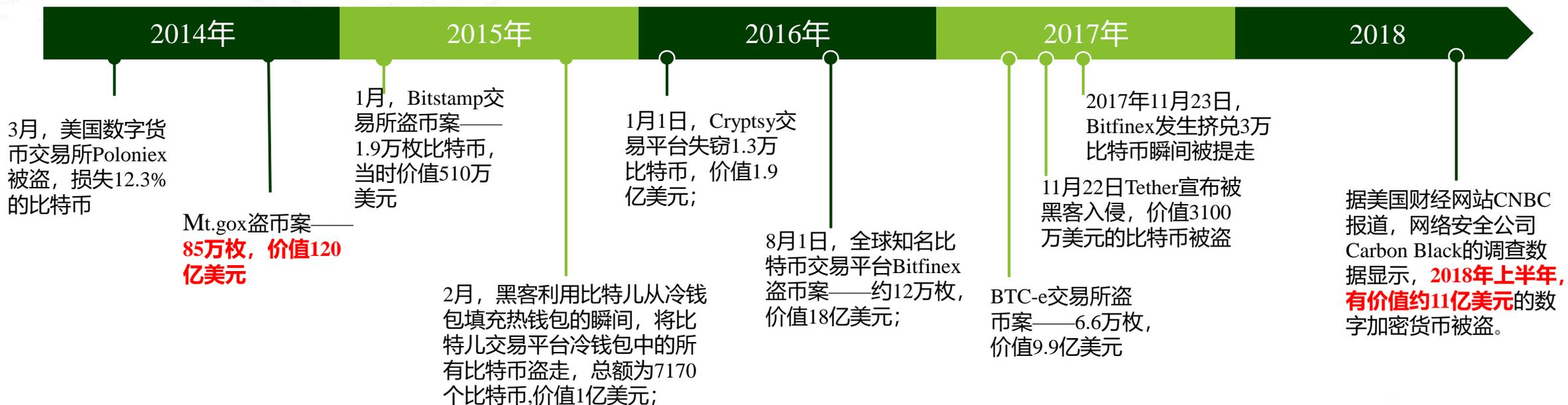
数字货币安全事件频发



ISC 互联网安全大会



360 互联网安全中心



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

➤ 数字货币是黑客的饕餮盛宴



ISC 互联网安全大会



360 互联网安全中心

高收益

直接变现

低风险



360 技术

IT 大咖说

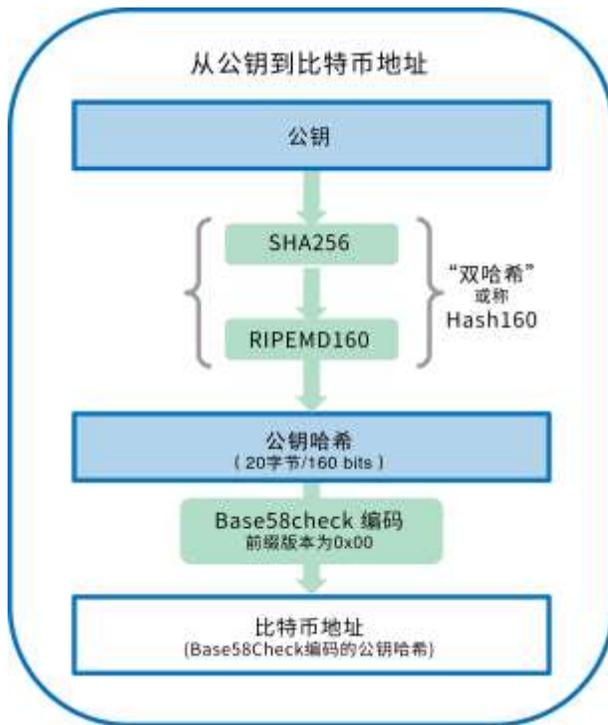
知识共享平台

SECURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

➤ 数字钱包基本原理（比特币为例）

比特币的所有权是通过数字密钥、比特币地址和数字签名来确立的。数字密钥由用户生成并存储于数字钱包中，也称为比特币钱包。钱包中包含成对的私钥和公钥。用户用这些私钥来签名交易，从而证明它们拥有交易的输出（其中的比特币）。而通过公钥生成的比特币地址，用于收款。



数字钱包

- 私钥的容器
- 密钥对和钱包地址生成
- 交易签名
- 收款

比特币钱包一般分为**在线钱包**、**本地钱包**、**离线钱包**等几种类型。

● 本地钱包

本地钱包即桌面程序，运行在用户本地操作系统，密钥在本地生成（保存在名为“wallet.dat”的文件中），并由口令等因素加密。比如，Bitcoin-Qt（官方客户端，基于C++/Qt，全平台）、MultiBit（全平台，轻钱包，官方推荐）、Electrum（著名轻钱包）、Armory（基于Python，含有诸多特性的轻钱包）。

● 离线钱包

离线钱包有时也被称之为“冷存储”。离线钱包即在一个不联网的电脑中，使用本地钱包软件生成私钥，在不联网的情况下对交易签名，通过U盘等存储介质把交易内容拷贝到联网的电脑中再广播该交易。

● 在线钱包

在线钱包一般是在线的网站提供的钱包服务，私钥由网站托管，用户通过口令或其他认证手段登录网站，从而获取私钥的操作权限。比如BlockChain.info、Inputs.io等。

常见的比特币钱包安全风险分析



ISC 互联网安全大会



360 互联网安全中心



360 技术

IT大咖说

知识共享平台

SECURITY

WEB INTERNET
INFORMATION LEAK
TECHNOLOGY
IDENTITY SECURITY
IDENTITY AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

➤ 私钥保护攻击模型和安全需求



ISC 互联网安全大会



360 互联网安全中心

| 攻击模型 | 安全需求 |
|-------------------|--|
| 一、以恢复用户密钥为目的的攻击 | 具有较强的抗密钥恢复攻击的能力，保证密钥的存储以及运算中的安全 |
| 二、以非法调用用户密钥为目的的攻击 | 具有对用户进行认证的能力，保证密钥的调用安全，防止假冒用户身份 |
| 三、以绕过认证机制为目的的攻击 | 具有一定的抗逆向工程以及抗调试与篡改的能力，防止恶意程序或攻击者绕过用户身份认证机制直接调用密钥 |
| 四、以篡改交易内容为目的的攻击 | 防止交易地址和金额被恶意篡改，用户没有发现 |



360 技术

IT 大咖说

知识共享平台

SECURITY

IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China

私钥的生成

私钥自身的质量取决于产生私钥的随机数的质量；伪随机和真随机

私钥的存储

当前区块链的私钥一般都是软实现进行存储的，以文件形式保存到终端或服务器数据库中，使用口令作为认证手段。容易被黑客或内鬼复制、窃取、暴力破解，安全风险极高

私钥的使用

私钥计算软实现，加载私钥到内存，通过CPU完成计算，计算过程私钥以明文的形式在内存和CPU中出现，容易被攻击程序获取



私钥在硬件内生成，私钥不出硬件；

通过PIN码认证，**设备+PIN形成双因素认证；**

内置显示屏和物理按钮，检查确认交易，**防止远程劫持；**

在银行领域，称这种有屏幕和按键的U盾为**二代U盾**，反之为**一代U盾**。



图为Ledger Nano S

主流硬件钱包



ISC 互联网安全大会



360 互联网安全中心



TREZOR



Keep Key



Coin Pass BLE (国产)



360 技术

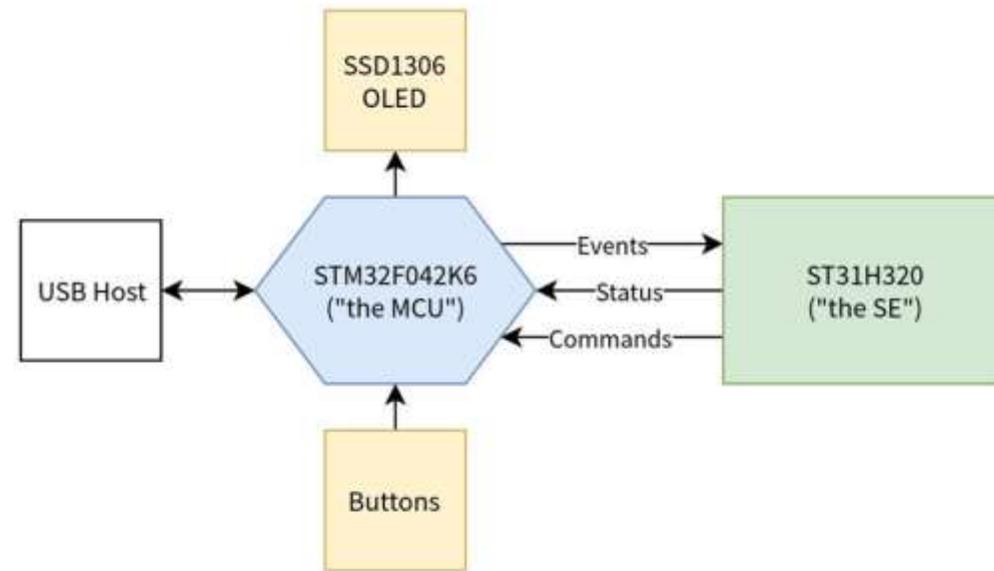
IT 大咖说

知识共享平台

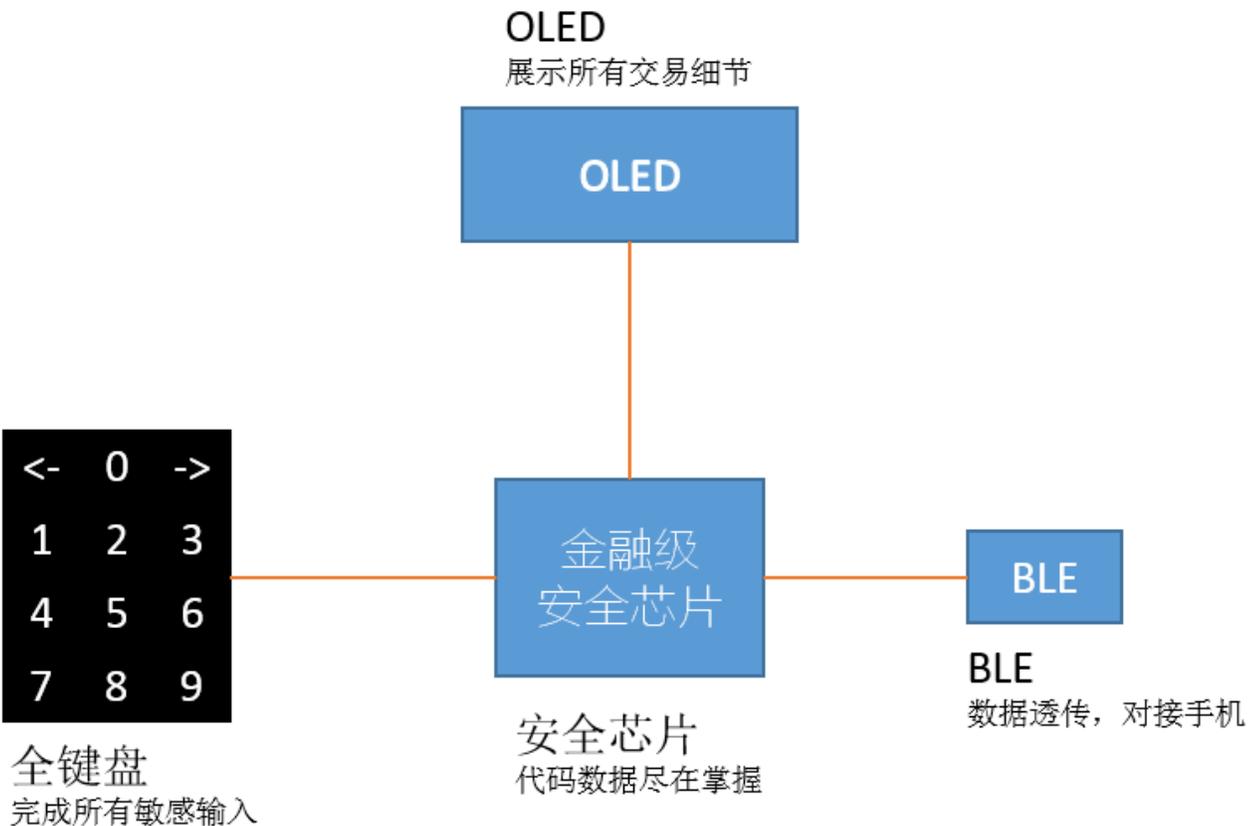
CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

硬件就安全吗?



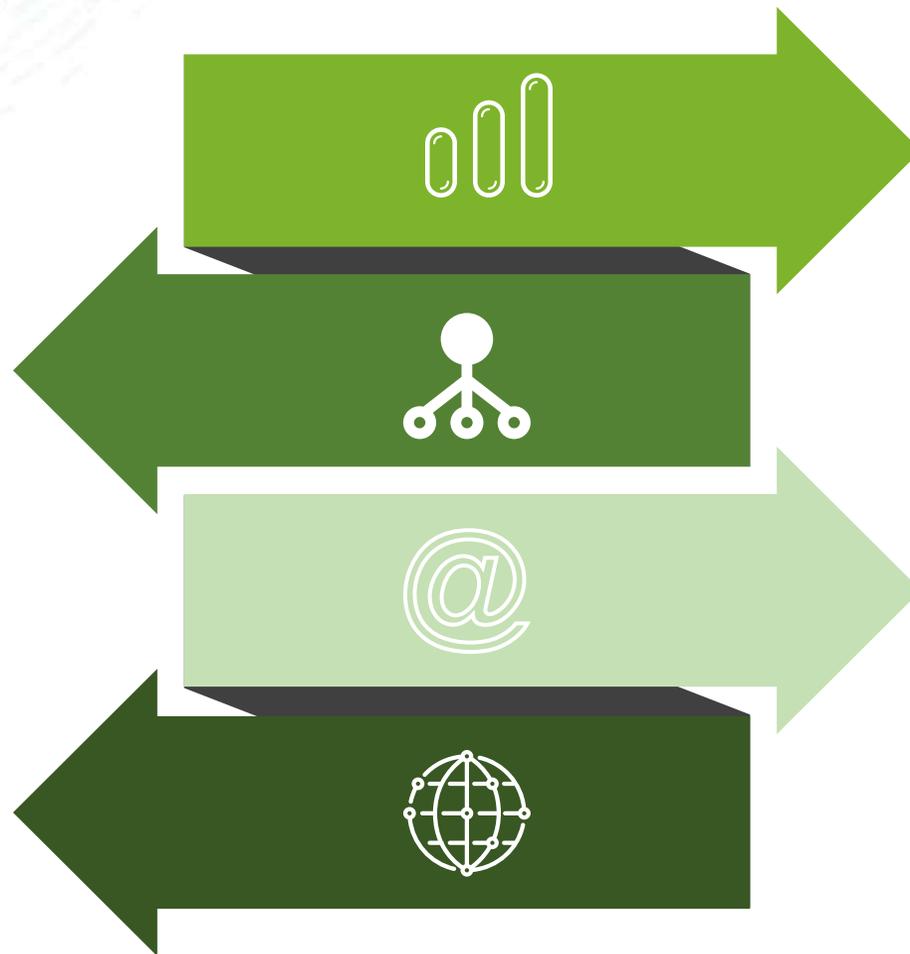
Ledger钱包的技术框架



全部由安全芯片主控 代码和数据（私钥）不分离

几个比较垃圾的设计:

- 口令托管, 在线钱包
- 本地私钥存储, 明文
- 本地私钥存储, 加密, 但密钥是写死在代码中



几个有益的做法:

- TEE/SE中生成和存储密钥
- APP移动安全 (安装包抗篡改、内存安全、反调试)
- 开发流程安全

► 使用第三方移动终端密码模块



密码技术为根，创新算法保护密钥

SM2国密算法，多方协同密文计算，密钥永远不会明文出现，让黑客无从下手；

硬件级保护

TEE、SE、云密码机等硬件级别保护

生物特征识别技术

支持指纹的安全认证，生物特征和密码技术融合

移动安全加固

移动端采取了防逆向、防篡改、防调试、防窃取等多种措施，防止恶意程序或攻击者绕过用户身份认证机制。

设备绑定

手机硬件信息参与密钥计算，复制到其他手机无法解密；

信任度手机盾

国密认证二级，媲美U盾

银行卡检测中心认证，金融级别安全

公安部安全测试报告



IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

传统银行

卡\U盾、口令丢失，只需要出示身份证即可找回



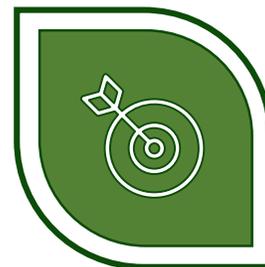
数字货币

私钥即资产，私钥即全部，私钥丢失等于资产灭失



如果是简单的私钥文件备份或者助记词备份，那么备份文件就成为攻击点

门限算法、分散存储；比如3/5门限，密钥分解成5份，任意3份或以上可恢复密钥；



1份自己保存（离线U盘）
其他4份保存到第三方权威机构；

重型资产也可以托管到银行保管箱



ISC 互联网安全大会



360 互联网安全中心

样稿

THANKS

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing · China



360 技术

IT 大咖说
知识共享平台