
# 《区块链技术安全讨论》

| |
|---|
| 安全报告：区块链技术安全讨论 |
| 报告编号：B6-2018-012301 |
| 报告来源：360 网络安全响应中心 |
| 报告作者：360CERT |
| 更新日期：2018 年 1 月 23 日 |

# 目 录

# 0x00 背景介绍

区块链技术是金融科技（Fintech）领域的一项重要技术创新。

作为分布式记账（Distributed Ledger Technology，DLT）平台的核心技术，区块链被认为在金融、征信、物联网、经济贸易结算、资产管理等众多领域都拥有广泛的应用前景。区块链技术自身尚处于快速发展的初级阶段，现有区块链系统在设计和实现中利用了分布式系统、密码学、博弈论、网络协议等诸多学科的知识，为学习原理和实践应用都带来了不小的挑战。

区块链属于一种去中心化的记录技术。参与到系统上的节点，可能不属于同一组织、彼此无需信任；区块链数据由所有节点共同维护，每个参与维护节点都能复制获得一份完整记录的拷贝，由此可以看出区块链技术的特点：

- 维护一条不断增长的链，只可能添加记录，而发生过的记录都不可篡改；
- 去中心化，或者说多中心化，无需集中的控制而能达成共识，实现上尽量分布式；
- 通过密码学的机制来确保交易无法抵赖和破坏，并尽量保护用户信息和记录的隐私性。

虽然单纯从区块链理解，仅仅是一种数据记录技术，或者是一种去中心化的分布式数据库存储技术，但如果和智能合约结合扩展，就能让其提供更多复杂的操作，现在活跃的各个数字货币就是其中一种表现形式。

# 0x01 区块链安全性思考

由于区块链技术的特性，在设计之处就想要从不同维度解决一部分安全问题：

- **Hash 唯一性**

  在 blockchain 中，每一个区块和 Hash 都是以一一对应的，每个 Hash 都是由区块头通过 sha256 计算得到的。 因为区块头中包含了当前区块体的 Hash 和上一个区块的 Hash ,所以如果当前区块内容改变或者上一个区块 Hash 改变，就一定会引起当前区块 Hash 改变。 如果有人修改了一个区块，该区块的 Hash 就变了。为了让后面的区块还能连到它，该人必须同时修改后面所有的区块 ,否则被改掉的区块就脱离区块链了。由于区块计算的算力需求强度很大 ,同时修改多个区块几乎是不可能的。由于这样的联动机制，块链保证了自身的可靠性，数据一旦写入，就无法被篡改。这就像历史一样，发生了就是发生了，从此再无法改变，确保了数据的唯一性。

- **密码学安全性**

  以比特币为例，数字货币采用了非对称加密，所有的数据存储和记录都有数字签名作为凭据，非对称加密保证了支付的可靠性。

- **身份验证**

  在数字货币交易过程中，由一个地址到另一个地址的数据转移都会对其进行验证：

  - 上一笔交易的 Hash(验证货币的由来)
  - 本次交易的双方地址
  - 支付方的公钥
  - 支付方式的私钥生成的数字签名

验证交易是否成功属实会经过如下几步：

- 找到上一笔交易确认货币来源
- 计算对方公钥指纹并与其地址比对，保证公钥的真实性
- 使用公钥解开数字签名，保证私钥真实性

- **去中心化的分布式设计**

针对区块链来说，账本数据全部公开或者部分公开，强调的是账本数据多副本存在，不能存在数据丢失的□险，区块链当前采用的解决方案就是全分布式存储，网络中有许多个全节点，同步所有账本数据（有些同步部分，当然每个数据存储的副本足够多），这样网络中的副本足够多，就可以满足高可用的要求，丢失数据的□险就会低很多。所以建议部署区块链网络时，全节点尽量分散，分散在不同地理位置、不同的基础服务提供商、不同的利益体等。

- **传输安全性**

在传输过程中，数据还未持久化，这部分空中数据会采用HTTP+SSL(也有采用websocket+websocketS)进行处理，从而保证数据在网络传输中防篡改且加密处理。

# 0x02 数字货币安全性思考

## 01 BTC

比特币（Bitcoin，代号 BTC）是一种用去中心化、全球通用、不需第三方机构或个人，基于区块链作为支付技术的电子加密货币。比特币由中本聪于 2009 年

1月3日，基于无国界的对等网络，用共识主动性开源软件发明创立。比特币也是目前知名度与市场总值最高的加密货币。

**比特币区块结构**

| | |
|---|---|
| Magic no | 魔数，值为 0xD9B4BEF9 |
| Blocksize | 区块的大小 |
| Blockheader | 区块头： |
| Version | 记录当前区块的版本信息 |
| hashPrevBlock | 上一个区块的区块头 hash，除了创世块（区块链中的第一个区块）之外都含有该值 |
| hashMerkleRoot | 数据块中交易信息算得的 hash |
| Time | 时间戳 |
| Bits | 目标值 |
| Nonce | 从 0 开始往上增加，相当于一个计数器，记录了为生成当前区块计算 hash 的次数 |
| Transaction counter | 区块中包含的交易数量 |
| transactions | 交易信息 |

**钱包和交易**

比特币钱包的地址就是公钥通过 Base58 算法编码后的一段字符串，使用该算法可以将公钥中的一些不可见字符编码成平时常见的字符。Base58 相对于 Base64 来说消除了非字母或数字的字符，如：“+”和“/”，同时还消除了那些容易产生混淆的字符，如数字 0 和大写字母 O，大写字母 I 和小写字母 l。这一段用作比特币钱包地址的字符串就相当于一个比特币账户。

交易属于比特币中的核心部分，区块链应用到数字货币上也是为提供更安全可靠的交易。交易之前会先确认每一笔笔交易的真实性，如果是真实的，交易记录便会写入到新的区块中去，而一旦加入到区块链中了也就意味着再也不能被撤回和修改。

**交易验证流程大概为：**

1. 验证交易双方的钱包地址，也就是双方的公钥。
2. 支付方的上一笔的交易输出，前面也说到了钱包里面是没有存放你的比特币数量的，而你每一笔交易都会产生交易输出记录到区块链中。通过交易输出可以确认支付方是否能够支付一定数量的比特币。
3. 支付方的私钥生成的数字签名。如果使用支付方的公钥能解开这个数字签名便可以确认支付方的身份是真实的，而不是有人恶意的使用当前的支付方的钱包地址在做交易。

一旦这些信息都能得到确认便可以将交易信息写入到新的区块中去，完成交易。受比特币区块大小的限制（目前的为 1MB，一笔交易信息大概需要 500 多字节），一个区块最多只能包含 2000 多笔的交易。因为区块链中记录了所有的交易信息，所以每个比特币钱包的交易记录和币的数量都是可以被查到的，但是只要没有对外公开承认钱包地址是属于你的，也不会有人知道一个钱包地址的真实拥有者。 还有一种交易叫做 coinbase 交易，当矿工挖到一个新的区块时，他会获得挖矿奖励。挖矿奖励就是通过 coinbase 交易拿到手的，也一样是需要把交易信息添加到新的区块中去，但是 coinbase 交易不需要引用之前的交易输出。

**安全问题**

比特币基于区块链，具有去中心化结构，用户通过一个公开的地址和密钥来宣示所有权。某种程度上，谁掌握了这个密钥，谁就实质性地拥有了对应地址中的比特币资产。而区块链的防篡改特征，是指比特币的交易记录不可篡改，

而非密钥不会丢失。同时，也正因为区块链不可篡改，密钥一旦丢失，也意味着不可能通过修改区块链记录来拿回比特币。

因此针对比特币的盗币事件屡有发生，主要是通过下面三个手段：

1. 交易平台监守自盗
2. 交易所遭受黑客攻击
3. 用户交易账户被盗

交易平台监守自盗可以向平台索回，但是黑客攻击导致的盗币，很难被追回。因为黑客一旦盗取比特币，接下来便会通过混币等手段进行洗白，除非有国家力量强力介入，否则追回的可能性仅仅停留在理论层面。

## 02 ETH

以太币（Ether，代号 ETH）为以太坊区块链上的代币，可在许多加密货币的外汇市场上交易，它也是以太坊上用来支付交易手续费和运算服务的媒介。以太坊（Ethereum）是一个开源的有智能合约功能的公共区块链平台。通过其专用加密货币以太币提供去中心化的虚拟机（称为“以太虚拟机”Ethereum Virtual Machine）来处理点对点合约。

**智能合约**

以太坊与比特币最大的一个区别——提供了一个功能更强大的合约编程环境。如果说比特币的功能只是数字货币本身，那么在以太坊上，用户还可以编写智能合约应用程序，直接将区块链技术的发展带入到 2.0 时代。


以太坊中的智能合约是运行在虚拟机上的，也就是通常说的 EVM（Ethereum Virtual Machine，以太坊虚拟机）。这是一个智能合约的沙盒，合约存储在以太坊的区块链上，并被编译为以太坊虚拟机字节码，通过虚拟机来运行智能合约。由于这个中间层的存在，以太坊也实现了多种语言的合约代码编译，网络中的每个以太坊节点运行 EVM 实现并执行相同的指令。如果说比特币是二维世界的话，那么以太坊就是三维世界，可以实现无数个不同的二维世界。

**安全问题**

ETH 最大的特点就是智能合约，而智能合约漏洞也就导致了 ETH 的安全问题。2016 年黑客通过 The Dao，利用智能合约中的漏洞，成功盗取 360 万以太币。THE DAO 持有近 15%的以太币总数，因此这次事件对以太坊网络及其加密币都产生了负面影响。

The DAO 事件发生后，以太坊创始人Vitalik Buterin 提议修改以太坊代码，对以太坊区块链实施硬分叉，将黑客盗取资金的交易记录回滚，得到了社区大部分

矿工的支持，但也遭到了少数人的强烈反对。最终坚持不同意回滚的少数矿工们将他们挖出的区块链命名为 Ethereum Classic（以太坊经典，简称 ETC），导致了以太坊社区的分裂。在虚拟货币历史上，这是第一次，也可能唯一一次由于安全问题导致的区块链分叉事件。

无独有偶 2017 年 7 月 19 日，多重签名钱包 Parity1.5 及以上版本出现安全漏洞,15 万个 ETH 被盗,共价值 3000 万美元。

两次被盗事件都是因为智能合约中的漏洞。让我们看到，虚拟货币的安全不仅仅是平台和个人，区块链上的应用，也是我们应该关注的内容。

## 03 XMR

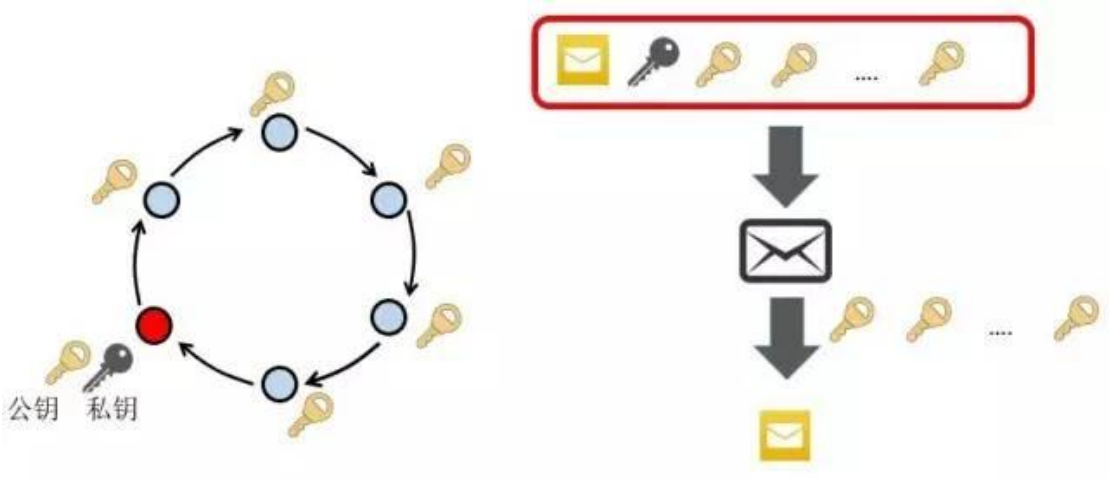
门罗币（Monero，代号 XMR）是一个创建于 2014 年 4月开源加密货币，它着重于隐私、分权和可扩展性。与自比特币衍生的许多加密货币不同，Monero 基于 CryptoNote 协议，并在区块链模糊化方面有显著的算法差异。

**隐蔽地址**

隐蔽地址是为了解决输入输出地址关联性的问题。每当发送者要给接收者发送一笔金额的时候，他会首先通过接收者的地址（每次都重新生成），利用椭圆曲线加密算出一个一次性的公钥。然后发送者将这个公钥连同一个附加信息发送到区块链上，接收方可以根据自己的私钥来检测每个交易块，从而确定发送方是否已经发送了这笔金额。当接收方要使用这笔金额时，可以根据自己的私钥以及交易信息计算出来一个签名私钥，用这个私钥对交易进行签名即可。

**环签名**

隐蔽地址虽然能保证接收者地址每次都变化，从而让外部攻击者看不出地址关联性，但并不能保证发送者与接收者之间的匿名性。因此门罗币提出了一个环签名的方案——事实上，在古代就已经有类似的思想了：如图 5 所示，联名上书的时候，上书人的名字可以写成一个环形，由于环中各个名字的地位看上去彼此相等，因此外界很难猜测发起人是谁。这就是环签名。




除了交易地址，交易金额也会暴露部分隐私。门罗币还提供了一种叫做环状保密交易（RingCT）的技术来同时隐藏交易地址以及交易金额。这项技术正在逐步部署来达到真正的匿名。这项技术采用了多层连接自发匿名组签名（Multi-layered Linkable Spontaneous Anonymous Group signature）的协议。

**安全问题**

比特币交易私密性方面做的不太好，关于货币隐私的两个基本属性：

1. 不可链接性（Unlinkability）：无法证明两个交易是发送给同一个人的，也就是无法知道交易的接收者是谁。

2. 不可追踪性（Untraceability）：无法知道交易的发送者是谁。

比特币交易要发送地址信息，很明显不符合之上的要求。门罗币通过隐蔽地址来保证不可链接性，通过环签名来保证不可追踪性，从而给用户的交易信息提供了很好的隐私性。另一方面，比特币挖矿主要依赖于大量专业化的专用集成电路（ASIC）。它的算法在 ASIC 上的运行速度远超于在标准家庭电脑或者笔记本电脑上运行。相比之下，门罗币的挖矿算法要精良得多。它并不依赖于 ASIC，使用任何 CPU 或 GPU 都可以完成，这就意味着门罗币具有更低的挖掘门槛。

门罗币的这些特性，使其成为黑产挖矿的不二之选。过去的一段时间，出现了许多以门罗币挖矿为目的的网络攻击事件。

### 04 小结

在以太坊这种平台区块链上，如果运行智能合约，应用程序出现漏洞，同样也会威胁其上的数字资产。以太坊解决了比特币的单应用的局限，使得区块链像一个操作系统，开发者可以在其上搭建自己的“应用”。门罗币降低了挖矿的门槛，同时又满足了交易私密性需求。这些特性都符合黑产的需要，过去的一段时间，以门罗币挖矿为目的的网络攻击事件时有发生。

## 0x03 交易平台安全性思考

随着区块链技术的迅速发展,使得虚拟货币渐渐走入的大众的视线。随之而来的就是大量的虚拟币交易平台。虚拟货币交易平台就是为用户提供虚拟货币与虚拟货币之间兑换的平台，部分平台还提供人民币与虚拟货币的 p2p 兑换服务。现在交易平台平均每天的交易额都是数以亿计 ,然而交易平台背后的经营者能力与

平台的自身的安全性并没有很好的保障。从 14 年至今据不完全统计，单纯由于交易所安全性导致的直接损失就达到了 1.8 亿美元之多。

**2014 年 7 月**

数字货币交易所 Cryptsy 声称平台已资不抵债
**13,000 BTC 以及 300,000 LTC**

**2014 年 8 月**

比特儿(Bter.com) 比特币交易平台被盗
**5000 万 NXT**

**2016 年 3 月**

比特币交易所 BitQuick 遭网络攻击
数字货币交易服务所 ShapeShift 被黑之后宣布下线
**盗走了 315 比特币**

**2016 年 6 月**

香港数字货币交易所 Gatecoin 资金被盗后下线
**消息称损失达 200 万美元**

DAO 被黑 逾 5000 万美元以太币被盗 拖累比特币跌 10%
**以太币（ETH）市场价格瞬间缩水**
**从记录高位 21.50 美元跌至 15.28 美元，跌幅逾 23%。**

**2016 年 8 月**

Bitfinex 遭黑客攻击 比特币价格应声大跌 25%
**目前被盗的比特币总数为 119756 个，总价值约为 7500 万美元**
**受此消息影响，全球比特币价格应声下跌 25%。**

**2017 年 9 月**

黑客盗走了 15 万枚以太币 数字钱包多重签名存漏洞
**Edgeless Casino，Swarm City 和 Aeternity 三家知名平台受到了攻击**
**确认损失了至少 4.5 万枚以太币，Aeternity 则证实该平台被盗走了 8.2 万枚以太币**

**2017 年 12 月**

USDT 发行方 Tether 遭受黑客攻击
**盗走了价值约 3100 万美元的 USDT 代币**
韩国比特币交易所 Youbite
**造成的损失相当于平台内总资产的 17%**

| 时间 | 相关平台 | 货币类型 | 造成损失 |
| --- | --- | --- | --- |
| 2014.08 | Bter.com | NXT | 200 |
| 2016.01 | Cryptsy | BTC\LTC | 415 |
| 2016.04 | ShapeShift | BTC | 23 |
| 2016.05 | Gatecoin | ETH | 200 |
| 2016.07 | Kraken | BTC | 285 |
| 2016.08 | Bitfinex | BTC | 7500 |
| 2017.07 | Edgeless Casino<br>Swarm City<br>Aeternity | BTC\ETH | 3260 |
| 2017.12 | Tether | USDT | 3095 |
| 2017.12 | Youbite | BTC | 4000 |
| 2017.12 | liqui | BTC | 60 |

随着虚拟币的水涨船高，交易所就成了黑客们的首要目标，据统计入侵一家交易所给黑客带来的直接利益大约 1000 万美元左右，然而交易所的安全性参差不齐和各个国家对这类平台基本都暂时没有好的管控策略，这给黑客带来了很大的便利，同时也直接威胁着用户的资金安全。

# 01 平台被黑事件回顾

- **比特儿(Bter.com) 比特币交易平台被盗事件**

  2014-08-15

  事件简介：

比特儿是一家中国的山寨币交易所。NXT 等山寨币都在上面交易。

由于 POS 币的钱包必须上线运行才能获取利息。因此 NXT 钱包必须在线运行，给了入侵的机会。POS 币不能冷钱包保存，暴露出 POS 的重大安全隐患。黑客盗走 NXT 后与平台方通过交易留言进行了谈判：

| | | | |
|---|---|---|---|
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | 100 btc, than we're talking. otherwise, let it do the rollback. | 2014-08-15 11:12:27 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | left what? I don't need your lousy 10BTC | 2014-08-15 11:11:38 |
| NXT-LSC3-VB9T-2W3V-BH7FB | NXT-8WJ7-8A2H-MBYN-3W9K4 | 1 BTC sent. Now it's your turn to return the NXT and we will give the left. | 2014-08-15 11:09:50 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | good luck ;) | 2014-08-15 11:07:57 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | lol. than i leak your all md5 passwords. 10btc you kidding me ? | 2014-08-15 11:07:24 |
| NXT-LSC3-VB9T-2W3V-BH7FB | NXT-8WJ7-8A2H-MBYN-3W9K4 | send all NXT back to NXT-R3V3-2S79-F3ZM-BVXKZ or the stolen address now. Leave a BTC address for 10BTC. You can go with what you have otherwise, a rollback will happen in minutes and we are going to take all our power and publish a huge bounty to take you down. We promise. | 2014-08-15 11:05:58 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | btc purse | 2014-08-15 10:59:59 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | 13UZjKkhHWyTmQ4mx28WT5Wj1zw4pEByZw | 2014-08-15 10:59:44 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | Okay, so I'll send everything back right now, if I get compensated. | 2014-08-15 10:58:33 |
| NXT-LSC3-VB9T-2W3V-BH7FB | NXT-8WJ7-8A2H-MBYN-3W9K4 | return all the NXT back to NXT-R3V3-2S79-F3ZM-BVXKZ, otherwise we are going to take all our power and a huge bounty to hunt you down . be smart | 2014-08-15 10:58:22 |
| NXT-LSC3-VB9T-2W3V-BH7FB | NXT-8WJ7-8A2H-MBYN-3W9K4 | contact bter for BTC otherwise action will be taken soon | 2014-08-15 10:51:48 |

并要求平台方支付 BTC 作为赎金换回 NXT

| | | | |
|---|---|---|---|
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | Deal is off. Good night. | 2014-08-15 12:23:45 |
| NXT-QT7P-HWS6-SABB-G59H8 | NXT-LSC3-VB9T-2W3V-BH7FB | Once the dust has settled, I highly encourage you to publish the hacker's attack vector to the other exchanges, if they may be affected by the exploit. | 2014-08-15 12:21:14 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | So, what taking so long? Send me the next batch already. I'm going to leave soon. It's already 2 hours of negotiation, it took me 1 hour to clean your whole exchanger. BTC 500+ I'm not going to sit here, and wait 2 more hours for you to decide to send the lousy 10 BTC. | 2014-08-15 12:17:39 |
| NXT-LSC3-VB9T-2W3V-BH7FB | NXT-8WJ7-8A2H-MBYN-3W9K4 | send the left first and we will send you the left BTC. We are an exchange, we do it publicly and we keep our promise. Otherwise, we can do 20 by 20 to speed it up. | 2014-08-15 12:08:43 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | This is taking too long. I dont have all night. | 2014-08-15 11:59:03 |
| NXT-WTTE-PRGM-DHMP-EZCL3 | NXT-8WJ7-8A2H-MBYN-3W9K4 | Thanks for negotiating. You did the right thing! | 2014-08-15 11:57:32 |
| NXT-KMVR-BH6Q-J8HM-BLELV | NXT-PGF9-SHUV-NLB2-8SJK3 | Repaying the 3 NXT I got from your faucet to get started with NXT. Thank you. | 2014-08-15 11:54:53 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | first batch sent | 2014-08-15 11:54:22 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | okay. moment. | 2014-08-15 11:52:42 |
| NXT-LSC3-VB9T-2W3V-BH7FB | NXT-8WJ7-8A2H-MBYN-3W9K4 | considering all our users and the NXT community, we will cover all the users' loss and we will take your 100 BTC offer. 1+9 BTC has already sent to you. Now send NXT back to NXT-R3V3-2S79-F3ZM-BVXKZ (11513376607016028001) | 2014-08-15 11:45:40 |
| NXT-8WJ7-8A2H-MBYN-3W9K4 | NXT-LSC3-VB9T-2W3V-BH7FB | No. 100 BTC. Send me 10 BTC, I send you some NXT until we finish our deal. I don't mind waiting for rollback. I'm just sorry that whole NXT community will have to suffer because your lack of competence. | 2014-08-15 11:37:30 |
| NXT-QT7P-HWS6-SABB-G59H8 | NXT-8WJ7-8A2H-MBYN-3W9K4 | There's a lot of talk about a rollback. You're going to lose that NXT in any case. I suggest sending it back to BTER. Who knows - they may pay you for finding the vulnerability, and then you at least get something! | 2014-08-15 11:33:29 |
| NXT-LSC3-VB9T-2W3V-BH7FB | NXT-8WJ7-8A2H-MBYN-3W9K4 | 1 of 50 BTC sent. Now send the NXT back the the stolen account. | 2014-08-15 11:21:47 |
| NXT-F9YV-VFNJ-X534-7J66B | NXT-LSC3-VB9T-2W3V-BH7FB | Don't try to play with the hacker, give him at least 100btc. There will be no rollback without the support of the community. | 2014-08-15 11:20:11 |
| NXT-ELEB-XT6G-L475-HXRFX | NXT-8WJ7-8A2H-MBYN-3W9K4 | The NXT Forgers are going to do a rollback. You can save all of us the hassle and return the stolen NXT. Either way, there'll be nothing for you anyway, or of you for that matter. | 2014-08-15 11:16:33 |

最终平台支付了 110 个 BTC，却未能完全赎回 NXT，只能要求社区回滚 NXT 的交易区块。

本次比特儿被黑是历史上第一次完全公开展现的网络犯罪 ,暴露出交易平台和数字货币在当时没有监管野蛮生长的严肃问题。

- **以太币组织 The DAO 被黑事件**

  2016-06

  事件简介：

  以太币的去中心化组织 The Dao 被黑，价值逾 5000 万美元的以太币外溢出 DAO 的钱包。以太币（ETH）市场价格瞬间缩水，从记录高位 21.50 美元跌至 15.28 美元，跌幅逾 23%。

  在此前的智能合约写法中，有三个严重漏洞，黑客也正是利用这几个漏洞攻击 The DAO 窃取以太币。

- **fallback 函数调用**

向合约地址发送币有两种写法：

```
address addr = 地址;
if (!addr.call.value(20 ether)()) {
    throw;
}
```

```
address addr = 地址;
if (!addr.send(20 ether)) {
    throw;
}
```

二者都是发送 20 个 ether，都是一个新的 message call，不同的是这两个调用的 gasli mit 不一样。send()给予 0 的 gas( 相当于 **call.gas(0).value()()**)，而 **call.value()()**给予全部( 当前剩余 )的 gas。当我们调用某个智能合约时，如果指定的函数找不到 ,或者根本就没指定调用哪个函数( 如发送 ether )时，fallback 函数就会被调用。

当通过 **addr.call.value()()**的方式发送 ether，和 send()一样，fallback 函数会被调用，但是传递给 fallback 函数可用的气是当前剩余的所有 gas，如果精心设计一个 fallback 就能影响到系统，如写 storage，重新调用新的智能合约等等。

- **递归调用**

一段用户从智能合约中取款的代码如下：

```
function withdrawBalance() {
    amountToWithdraw = userBalances[msg.sender];
    if ( amountToWithdraw > 0) {
    if (!(msg.sender.call.value(amountToWithdraw)())) {
        throw;
    }
    userBalances[msg.sender] = 0;
}
}
```

如果付款方的合约账户中有 1000 个 ether，而取款方有 10 个 ether，此处就有严重的递归调用问题，取款方可以将 1000 个 ether 全部取走。

- **调用深度限制**

合约可以通过 message call 调用其他智能合约， 被调用的合约继续通过 message call 在调用其他合约，这样的嵌套调用深度限制为 1024。

```
function sendether() {
    address addr = 地址;
    addr.send(20 ether);
    var thesendok = true;
}
```

如果攻击者制造以上的 1023 个嵌套调用，之后再调用 **sendether()**，就可以让 **add.send(20 ether)**失效，而其他执行成功：

```
function hack() {
    var count = 0;
    while (count < 1023) {
        this.hack();
        count++;
    }
    if (count == 1023) {
        thecallingaddr.call("sendether");
    }
}
```

在 DAO 的代码中：

```
function splitDAO(uint _proposalID, address _newCurator) noEther onlyTokenhol
ders returns(bool _success) {
    ...
    uint fundsToBeMoved = (balances[msg.sender] * p.splitData[0].splitBalance) /
 p.splitData[0].totalSupply;
    if (p.splitData[0].newDAO.createTokenProxy.value(fundsToBeMoved)(msg.send
er) == false) throw;
    ...
    withdrawRewardFor(msg.sender);
    totalSupply -= balances[msg.sender];
    balances[msg.sender] = 0;
    paidOut[msg.sender] = 0;
    return true;
}
```

当合约执行到 **withdrawRewardFor(msg.sender);** 进入到函数

**withdrawRewardFor 判断**

```
function withdrawRewardFor(address _account) noEther internal returns(bool _success) {
    ...
    if(!rewardAccount.payOut(_account, reward)) //漏洞代码
    throw;
    ...
}
```

payOut 定义如下:

```
function payOut(address _recipient, uint _amount) returns(bool) {
    ...
    if(_recipient.call.value(_amount)) //漏洞代码
    PayOut(_recipient, _amount);
    return true;
} else {
    return false;
}
}
```

和此前的举例类似，DAO 通过 **addr.call.value()()**发送以太币而没有选择 **send()**从而黑客只需要创建 fallback 再次调用 **splitDAO()**即可转移多份以太币，PoC 如下:

```
p.splitData[0].newDAO.createTokenProxy.value(fundsToBeMoved)(msg.sender)
```

The DAO 事件给整个以太坊社区带来了重大影响，也导致了之后的硬分叉和 ETC(以太经典)的剥离。

- **Bitfinex 遭黑客攻击事件**

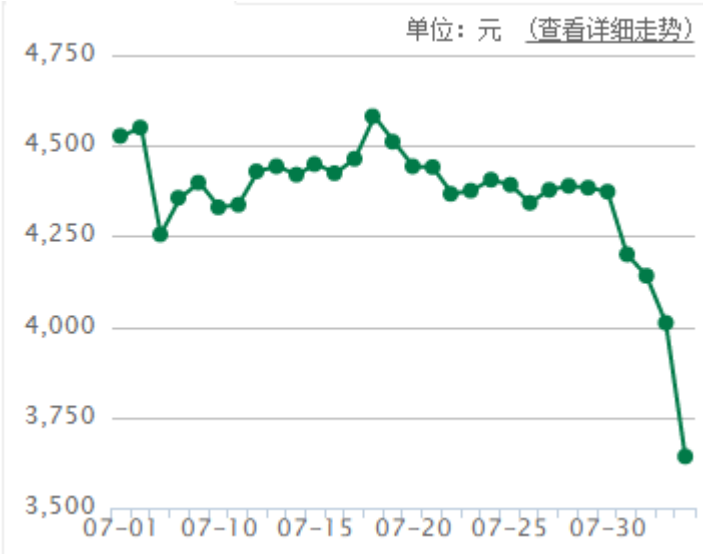
2016-08

**事件简介：**

Bitfinex 是交易比特币、ether 和莱特币等数字货币的最大交易所之一。

根据 Bitfinex 在 8 月 2 日凌晨发布的公告，该交易所在发现了一个安全漏洞后便停止了交易。发布在官网上的声明表示：


Bitfinex 负责社区和产品开发的主管塔克特(Zane Tackett)证实，119,756 个比特币遭窃，该公司已经知道相关系统是如何被入侵的。以周二的价格计算，失窃比特币价值约 6,500 万美元，受此消息影响，全球比特币价格应声下跌 25%。




随后 Bitfinex 官网发布公告称这次损失将由平台上所有用户共同承担 ,这将导致每位用户的账户平均损失 36%

对于类似比特币这样的数字货币，由于是通过数学算法挖矿形成，与实体质地的纸币不同 ,这些数字货币交易的安全性就完全体现在交易所的风险控制能力以及防黑客能力上。

- **Parity 多重签名钱包被盗事件**

2017-07

**事件简介：**

Parity 是一款多重签名钱包，是目前使用最广泛的以太坊钱包之一，创始人兼 CTO 是以太坊前 CTO 黄皮书作者 Gavin Woods。

7 月 19 日，Parity 发布安全警报，警告其钱包软件 1. 5 版本及之后的版本存在一个漏洞。据该公司的报告，确认有 150，000ETH(大约价值 3000 万美元)被盗。据 Parity 所说，漏洞是由一种叫做 wallet.sol 的多重签名合约出现 bug 导致。后来，白帽黑客找回了大约 377,000 受影响的 ETH。

Severity: Critical

Product affected: Parity Wallet

Affected implementations: Parity 1.5 or later

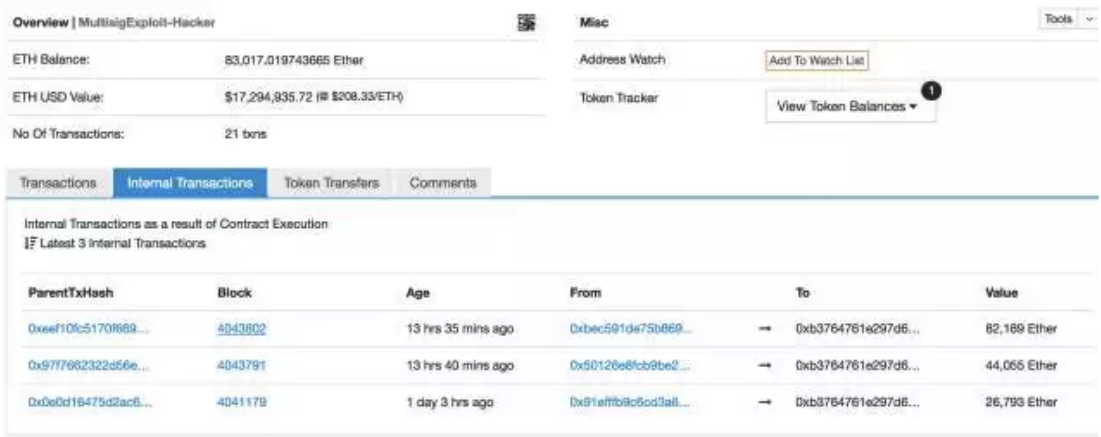
Summary: A vulnerability in Parity Wallet's variant of the standard multi-sig contract has been found.

Affected users: Any user with assets in a multi-sig wallet created in Parity Wallet prior to 19/07/17 23:14:56 CEST.

Mitigation steps: Immediately move assets contained in the multi-sig wallet to a secure address.

UPDATE (20/07/17, 00:26 CEST): Future multi-sig wallets created by versions of Parity are secure (Fix in the code is https://github.com/paritytech/parity/pull/6103 and the newly registered code is https://etherscan.io/tx/0x5f0846ccef8946d47f85715b7eea8fb69d3a9b9ef2d2b8abcf83983fb8d94f5f).

本次攻击造成了以太币价格的震荡，Coindesk 的数据显示，事件曝光后以太币价格一度从 235 美元下跌至 196 美元左右。此次事件主要是由于合约代码不严谨导致的。我们可以从区块浏览器看到黑客的资金地址




可以看到，一共盗取了 153,037 个 ETH，受到影响的合约代码均为 Parity 的创始人 Gavin Wood 写的 Multi-Sig 库代码。通过分析代码可以确定核心问题在于越权的函数调用，合约接口必须精心设计和明确定义访问权限，或者更进一步说，合约的设计必须符合某种成熟的模式，或者标准，合约代码部署前最好交由专业的机构进行评审。否则，一个不起眼的代码就会让你丢掉所有的钱。

- **USDT 发行方 Tether 遭受黑客攻击事件**

2017-12

**事件简介：**

Tether 公司是 USDT 代币的发行公司——USDT 是一种与美元挂钩的加密货币，如今正在被交易所广泛用于进行交易。该公司在公告中声称其系统遭受攻击，已经导致价值 3000 万美元的 USDT 代币被盗。

> *"$30,950,010 USDT was removed from the Tether Treasury wallet on Nov. 19, 2017 and sent to an unauthorized bitcoin address. As Tether is the issuer of the USDT managed asset, we will not redeem any of the stolen tokens, and we are in the process of attempting token recovery to prevent them from entering the broader ecosystem."*

被盗的代币不会再赎回，但 Tether 公司表示他们正在试图恢复令牌，以确保这些交易所不再交易或引入这些被盗的资金，不让这些资金回到加密货币经济。此次被黑事件后，比特币的价格下降了 5.4%，是 11 月 13 日以来的最高纪录。然而，Tether 被盗声明一出，国外社区有用户认为，该地址中被盗的 3000 万美元只是 Tether 掩耳盗铃的第一步。实际面临的兑付危机远远不止 3000 万美元。此次事件不仅单纯的一次虚拟币被盗事件同时导致了 Tether 的信任危机。

- **Youbite 交易所被入侵事件**

2017-12-19

**事件简介：**

12 月 19 日，韩国数字货币交易所 Youbite 宣布在当天下午 4 时（北京时间 3 时）左右，交易平台受到黑客入侵，造成的损失相当于平台内总资产的 17%。 这家平台是韩国一家市场份额较小的数字货币交易平台，在今年 4 月，这家平台

也曾经遭受过黑客攻击，损失了近 4000 个比特币。


Youbit 表示，在 4 月份遭遇黑客攻击之后，其加强了安全策略，将其余 83%的交易所资金都安全地存放在冷钱包里。尽管如此，运营该交易所的公司 Yaipan 还是于本周二申请了破产，并停止了平台交易。公告显示，该交易所将所有客户的资产价值减记至市场价值的 75%，客户可立即提取这部分资产。该公司表示，将在破产程序结束时偿还剩余的资金，届时将提出保险索赔并出售公司的经营权。

## 02 小结

虚拟币的火热，直接搅动着金融市场与科技市场，也面临着各种安全问题。现在各个国家也开始对区块链市场与虚拟币市场相继出台政策与治理方案，对交易所也开始纳入管控范围，韩国前段时间对其国家 7 家大型交易所进行了安全测试均被成功入侵，但每个交易所每天交易量是数以亿计的。可见这类安全问题不是个例，作为虚拟币交易平台，是否有资质有能力保护在线虚拟货币啊安全性成为

一个值得考究的问题，虚拟币已经渐渐的从网络进入到现实世界中，然而这个过程的进步同样带来了很大的隐患，这也促使着政府企业以及个人对交易平台以及虚拟币本身更加的慎重选择与投入。

## 0x04 区块链在安全行业的应用

区块链社区非常活跃，人们经常认为，这项技术不仅有效地推动了虚拟货币的发展，而且还加强了现有的安全解决方案，从区块链角度解决了一些安全问题。列举几个区块链技术的安全用途：

- **更安全的认证机制**

  根据区块链技术的特性，设备可以以对等的方式识别和交互，而不需要第三方权威。伴随着双重身份验证，伪造数字安全证书成为不可能，使得网络结构具有更好的安全性。比如应用到密码验证服务，物联网设备认证。

- **更安全的数据保护**

  在基于区块链的系统中，存储的元数据分散在分布式账本中，不能在一个集中点收集，篡改或者删除。其中的数据，具有更好的完整性，可靠性以及不可抵赖性。可以应用到公共数据存储场景，比如产权记录，金融记录。

- **更安全的基础设施**

  利用区块链分布式特性，可以提供一种分散式平台，通过这种系统，可以访问和利用共享的带宽，这种方式远优于带宽有限的单服务器集中模型。去中心化的平台可以降低 DDoS 成功的□险，更好的保护基础设施。比如网站，DNS 解析服务等。