从 2009 年 1 月比特币面世至今近 10 年的时间里，随着它的迅猛发展，各方都看见了基于区块链的代币和“虚拟货币”中
的商机，纷纷投入进来。在投机炒作和不确定的风险之间，“虚拟货币”可谓是走在冰与火的边缘。

当然，火爆的行情吸引了不法者的注意，“虚拟货币”也面临着严重的风险。例如交易所币安被黑客操纵，交易平台 ShapeShift
钱包失窃；钓鱼网站、诈骗与传销事件也层出不穷。

月黑风高，宜割韭菜。雷锋网就在知道创宇发布的《区块链安全风险白皮书第二版报》报告中扒到了一堆奇葩案例。

一、交易市场操纵风险

## 黑客操纵市场

北京时间 3 月 7 日凌晨 1:40，“虚拟货币”交易所币安(Binance)被爆出现故障。

多名用户在论坛发帖称，他们发现自己币安账户中的各种代币、“虚拟货币”被即时交易成 VIA(维尔币)，认为币安疑似遭到黑客攻击。据媒体的报道和分析，这是一场有组织、有预谋的黑客行动。故障源于部分 API 机器人被黑客攻击。

币安立即宣布暂停所有币种的提现。但黑客并没有选择提现，而是利用盗用的账号高价买入 VIA，导致 VIA 被拉爆，涨幅 110 倍。这引发了其它交易所币价的连锁反应，黑客再从其它交易所挂好的空单中渔利，从中获利 1.1 亿美元。

## 交易集团操纵市场

Cloakcoin 是一种较早的山寨币，今年经历了几轮价格飙升。2018 年 7 月1 日在币安上的突然飙升，就是 Big Pump Signal 交易集团操纵所为。Big Pump Signal 公司在他们的电报群里发送消息鼓动参与者们购买，随后 Cloakcoin 价格狂飙。

有研究表示：“在 Cloakcoin 飙升的当天，币安交易所十大比特币交易货币的价格几乎没有变动。”这些发现也证明是交易集团在操纵“虚拟货币”市场。

这种拉高倒货行为，是最古老与典型的市场诈欺手法之一。交易商先透过发放假消息将某种资产价格炒作到一定高点，之后再迅速倒货牟利。这种做法在股 市属于违法，美国证券交易委员会过去常对这类诈骗提起民事诉讼。不过“虚拟货币”市场却因为法规松散，使得相关当局陷入无法可管的窘境。

## 二、交易平台的技术故障

### 比特币因平台技术故障下跌

2017 年 11 月 29 日，比特币交易平台 Coinbase 因技术故障而导致部分用户无法登陆网站进行交易，从而导致市场流动性萎缩，使得卖压释放后，价格快速下跌。比特币创下历史新高 11485 美元后，快速回落近 25%，最低跌至 8595 美元。

因平台故障而错误执行了若干交易指令

在 2017 年 12 月下旬，某“虚拟货币”交易平台因为故障而错误执行了若干交易指令。该交易平台在发现技术错误后，开始单方面逆转指令。本来可以从错误执行中得益的交易商基于平台单方面逆转交易，向新加坡国际商事法庭起诉平台违反合约。

## 三、交易平台“内鬼”风险

### ShapeShift 钱包失窃

2016 年 3 月 14 日，“虚拟货币”交易平台 ShapeShift 的一名员工从自己公司的热钱包中盗走了 315 比特币。ShapeShift 报警并对该名员工提出了民事诉讼。

2016 年 4 月 7 日，在网站迁移过程中，ShapeShift 发现其 3 个钱包已经被黑客攻击，约损失 97 比特币、3600 以太坊和 1900 莱特币。

ShapeShift 团队刊登在 Reddit 上的帖子中写到:我们最初无法确定这种事情是如何发生的。我们已经将网站下线，并假定我们的基础设施和所有的密钥都已经受到了影响。我们在再次发现攻击的 24 小时后在一个全新的主机上重置了所有密钥并建设了全新的基础设施。在重建过程中，我们与黑客建立了联系，他表示几个月前 ShapeShift 的某位员工为他提供了攻击所需的所有信息。在对这

位黑客展开调查并交流后，事情的真相浮出水面:ShapeShift
的某位前雇员出售了攻击需要的能够接入受影响钱包的数据。

ShapeShift 的 CEO Erik Voohees
表示他们已经找回了部分资金，事故中顾客的资金没有被盗取。

## 迪拜某交易所内部员工盗取 80 万个 DHS 代币

迪拜的一个“虚拟货币”交易平台发现他们负责管理交易系统的专家窃取了密钥供他个人使用。

他把在平台上交易的一小部分货币兑换后，进入数据库平台，将虚假信息上传到虚拟账户中，将这些货币转进自己的账户和其他“虚拟货币”交易平台。老板没有理由怀疑这名员工，因为是这位员工自己发明了这个平台还获得了表彰。

最初，公司意识到“虚拟货币”交易有出入，并且与系统中的记录并不相符。 但由于他们的安全系统有漏洞存在，整个团队都在使用管理员账户访问网站，他们无法找到罪犯。涉事员工慢慢地积累了转移的金额，并在他的个人电脑上暴露了更多的细节。犯案者共盗取了 80 万个 DHS 代币(约合 20 万美元)。

印度比特币交易所被“黑”

2018 年 4 月，印度“虚拟货币”交易所 Coinsecure 被盗 438 个比特币， 价值 350 万美元，疑似内部人员所为。该交易所于 4 月 13 日暂停交易，与警方合作进行相关调查。

该公司在声明中称:他们的比特币基金看起来被转移到了一个不受他们控制的地址，并且承认系统并未受到网络攻击，该交易所将自掏腰包赔偿客户。

该公司创始人及首席执行官 Mohit Kalra 告知当地媒体，他怀疑是交易所首席安全官 Amitabh Saxena 监守自盗，他是唯一具有该交易所主要钱包私人密钥的高层。

Kalra 说:“私人密钥应该不会暴露于网络。这看来像是内部犯罪。我们已将这一怀疑告知了网络调查部门，并联系了专家追寻黑客源头和丢失的比特币。”他还补充道:“由于私有密钥由 Amitabh Saxena 保管，我们感觉他与此事有关。他的护照应该被扣留以防止他逃往海外。”

# 四、诈骗风险

## 庞氏骗局

一家名为 Bitconnect 的平台曾发行一种名为 BCC 的平台币，要求其用户将手里的 BTC 兑换成 BCC，而且平台承诺会给予他们天价的回报，此外，该平台 还推出一项服务，用户可以将自己的“虚拟货币”借给公司，公司会给用户巨额回报。但实际上 BCC 在之后从 200 多美元直线下跌至 37 美元。

平台长期被认为是庞氏骗局，最后在 2018 年 1 月宣布关停。据称 BitConnect 的创始人 Divyesh Darji 于 2018 年 8 月在迪拜被捕。

## 五行币骗局

五行币是 5000 元一个的硬币，据称实体币后面附带了会迅速升值的 5000“虚拟货币”，一年可以赚至少四百万。五行币的运营主体是一家名为“云数贸联盟”的没有注册地址的网站，创始人是张健(真名宋密秋)。按照推介人员的说法，“五行币”是限量版，总共发行 5 亿个，将来会全面替代纸币，并称“五行币是中国唯一的‘虚拟货币’”,同时对创始人进行大肆吹捧。

五行币的奖励注册制度除分级发展下线获得奖励外，还有一种“静态收益”，也就是说等着全球买入“五行币”的人增多，价格上涨，可以获得分红，这个分红可以选择再投资“五行币”。

五行币很早就被立案，但在 2017 年 6 月，宋密秋才被从印度尼西亚缉捕回国。

## ICO 骗局

越南一家名为“现代科技”(Modern Tech)的公司运营的两起 ICO——Pincoin 和 iFan，总共欺骗了 32,000 名参与者，共计 6.6 亿美元。这家公司在胡志明市设置了办公室，4 月 8 日，在该公司拒绝处理现金提款后，一些参与者在空置的办公室外抗议。胡志明市政府已下令警方调查这起诈骗案。这一骗局被认为是 ICO 历史上最大的骗局。

两个 ICO 都被归类为多层次的营销骗局。iFan 为一个名人宣传社交媒体平台，向粉丝宣传他们的内容。Pincoin 项目声称正在建立一个在线平台，包括广告网络、拍卖和投资门户以及基于区块链技术的 P2P 市场，投资回报率高达 40%。

钓鱼网站+虚假的钱包地址欺诈

支付服务公司 CoinDash 在 2017 年夏季的时候进行了 ICO，但是很快就不得不终止了这个项目，因为接收用户以太坊的地址遭到了恶意篡改。

CoinDash 在这个黑客篡改地址事件之前募集了折合 730 万美元的资金，但是随着这次事件发生资金流向不知所踪。公司关停了这个项目，并要求参与者停止将以太坊发送至该网站，同时承诺向这些参与者发放“虚拟货币”CDT 作为补偿。

但是仍有一部分参与者对 CoinDash 表示支持，并继续将以太坊发送至这个地址，这就使得被盗取的资金从 700 万美元上升至 1000 万美元。

## 五、不安全的钱包

根据 2018 年 5 月《数字货币钱包安全白皮书》发布的数据，市场上近20多款主流数字钱包中，有八成存在安全隐患。“核心代码未加固、不检测系统运行环境、允许截屏录屏、APP 存在伪造漏洞、未检测弱口令”成为当前“虚拟货币”软件钱包所面临的主要问题。

不仅是软件钱包，硬件钱包也面临着安全问题。

L 品牌硬件钱包加密芯片不完善，存在设计缺陷；T 品牌硬件钱包完全开源容易被恶意用户攻击；C 品牌硬件用手机改装而成，操作系统采用某种智能手机解决方案，而这种智能手机方案本身是存在漏洞的。硬件系统太复杂，有BUG风险；手机随时触网，有病毒风险。