知道创宇

走在 冰与火 边缘的“虚拟货币”

知道创宇区块链安全风险白皮书 第二版

KNOWNSEC.COM

目录

开篇

区块链技术始于比特币的出现。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。

一方面，“虚拟货币”的价格探底回升。在经历了年初的峰值、第三季度的低谷后，2018 年 9 月 30 日，全球“虚拟货币”总市值已经达到约 2223 亿美元，其中比特币约 1141 亿美元。BitMEX、Binance 交易所的单日交易额能高于 10 亿美元。如今，相关交易平台已经遍地开花，著名的交易平台有 BitMEX、OKEX、火币等；各种相关业务和衍生产品也层出不穷，如 Coinbase 推出的“虚拟货币”指数基金。

另一方面，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；此外钓鱼网站、诈骗与传销事件也层出不穷。在 2018 年 8 月，中国互联网金融举报信息平台将“代币发行融资”列入举报范围，举报内容包括了“虚拟货币”的兑换、买卖、定价、中介、承保及其他使用“币”的名称开展的非法金融活动。

尽管目前在国内非法，“虚拟货币”行业的各种安全风险依然值得我们注意和研究，为以后的监管道路做好铺垫。如何规避、控制这些安全威胁，将是我们接下来所要重点探讨的。

1 全球“虚拟货币”现状分析

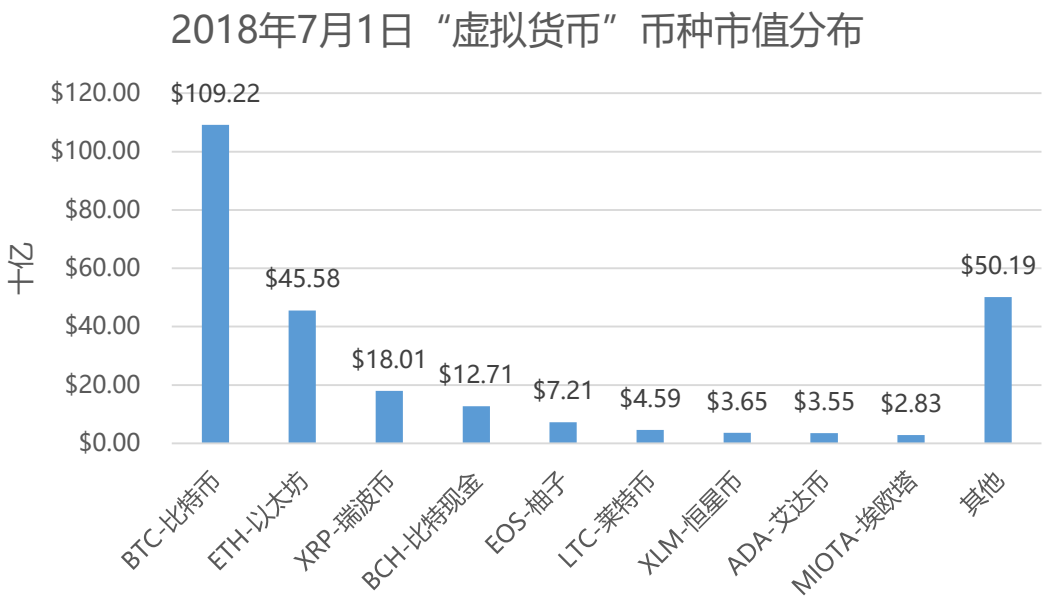
1.1 全球“虚拟货币”总市值变动

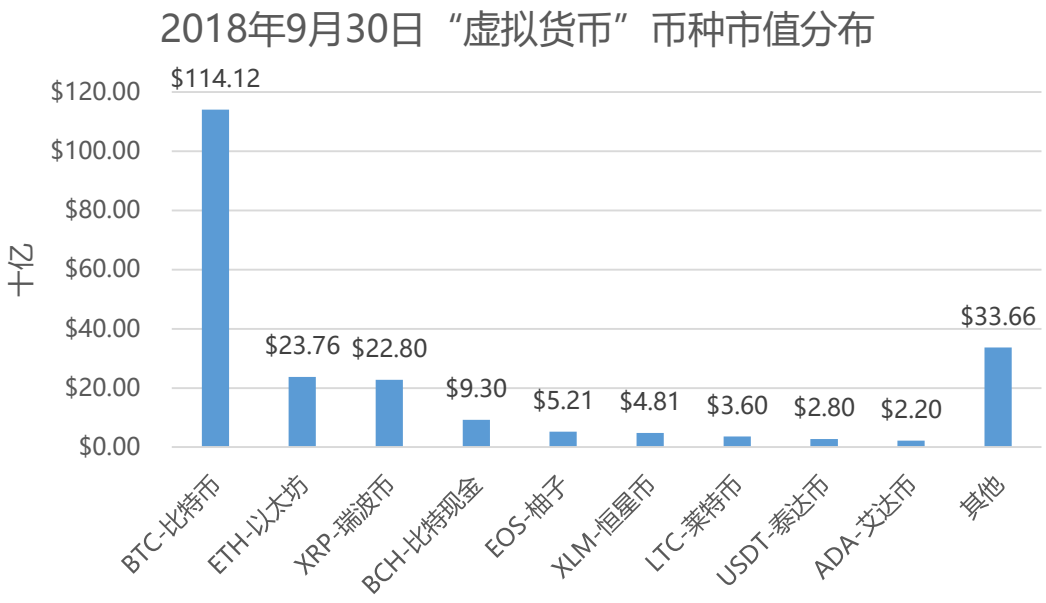
2017 年火爆的“虚拟货币”市场如今持续熊市，让参与者们很痛苦。我们通过图示和虚拟分析一下全球“虚拟货币”总市值的走向。下图表示 2018 年 7 月 1 日和 2018 年 9 月 30 日全球“虚拟货币”的总市值。

（全球“虚拟货币”总市值变动数据 图片来源：coinmarketcap.com @2018.09.30）

在 2018 年 7 月 1 日时全球“虚拟货币”市值为 257,538,000,000 美元。而到了三个月后的 9 月 30 日，全球“虚拟货币”市值为 222,260,621,623 美元，市值是 7 月 1 日的 86%，是 2018 年 1 月 1 日总市值的 37%。在这三个月期间，全球“虚拟货币”市值持续 5 月以来的低迷，总体依然呈下跌趋势，但与前几个月相比，下跌速度有所减缓。同时成交量也不高，由此可以看出在熊市，参与者都在保持观望态度。

1.2 “虚拟货币”币种市值分布





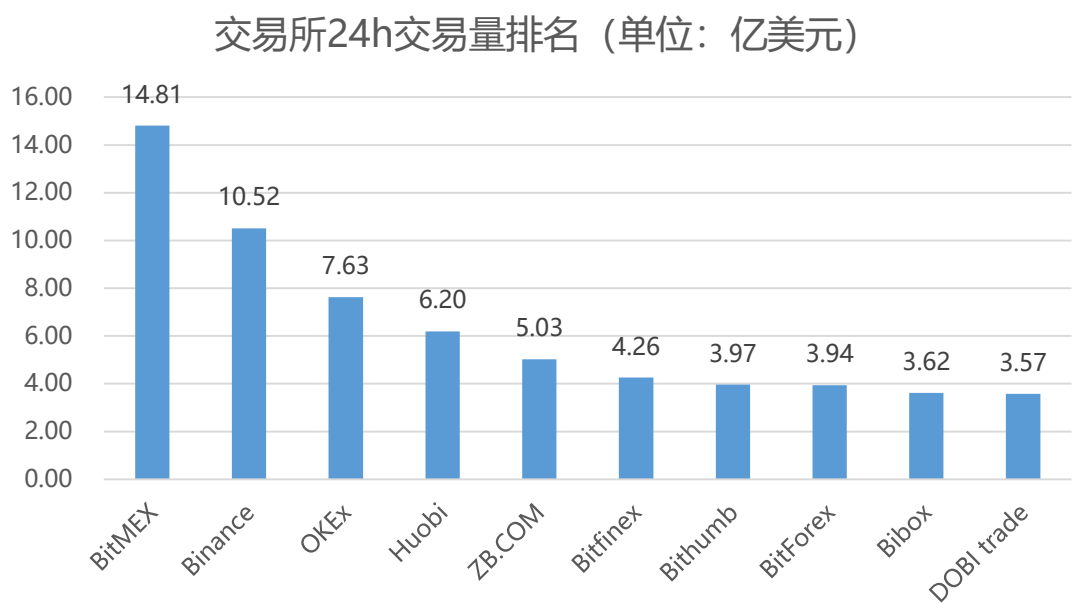
（“虚拟货币”币种市值 数据来源：coinmarketcap.com @2018.09.30）

在市场长久低迷过后，比特币和泰达币小有反弹，分别回升了 4.49%和 3.32%，瑞波币和恒星币回升较多，为 26.60%和 31.78%。但其他前几名代币没有那么幸运，均下跌了 20%以上，以太坊跌了近一半。除这些以外的其他“虚拟货币”下跌了 32.93%。排名前十位的“虚拟货币”，占总市值的 85.71%，其中比特币、以太坊分别占总市值的 51.35%和 10.69%。

这说明大部分参与者为了规避风险，都将资金投入看上去更稳定可靠的币种中抱团。而在如今资金持续流出“虚拟货币”市场的情况下，小众代币反弹的机会很小，整体市场呈现弱势，在此次动荡中可能会有大部分的代币和“虚拟货币”从此消失。

1.3 全球“虚拟货币”交易所排名

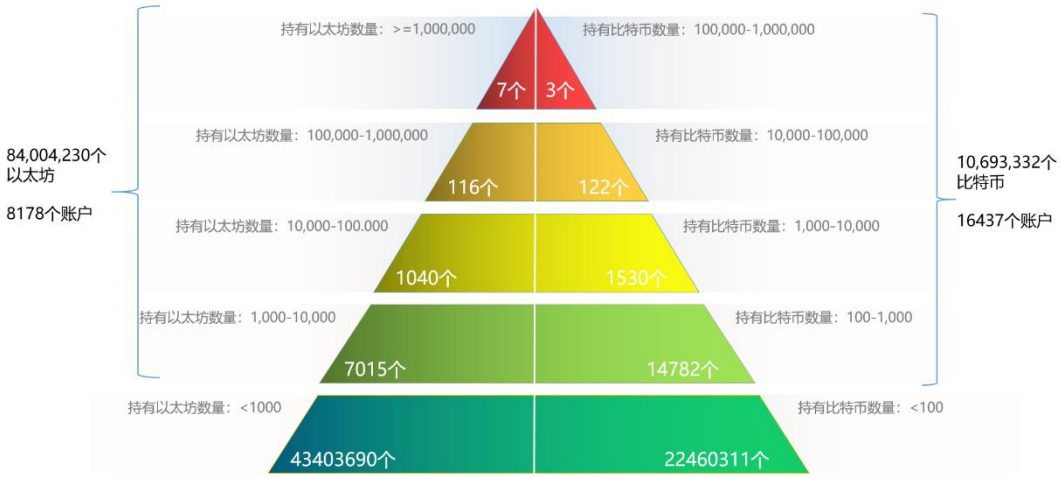
据统计，目前在全球范围内尚能产生交易额的“虚拟货币”交易所共有 188 家。根据 9 月 30 日 24H 交易所交易量排名，在交易量前十的交易所中，单日交易额高于 10 亿美元的有 2 家，分别为 BitMEX、Binance；5-10 亿美元之间的有 OKEx、火币、ZB.COM 三家；位于 3 亿美元至 5 亿美元的合计 5 家，分别为 Bitfinex、Bithumb、BitForex、Bibox 和 DOBI trade。



（全球“虚拟货币”交易所排名 数据来源：coinmarketcap.com @2018.09.30）

BitMEX、Binance 和 OKEx 这前三家的交易量就占了前十名交易量的 51.86%。由此可见，“虚拟货币”的交易主要集中在头部的几家大交易所。若这几家大交易所发生安全事件，势必会引起全球“虚拟货币”价格的动荡。

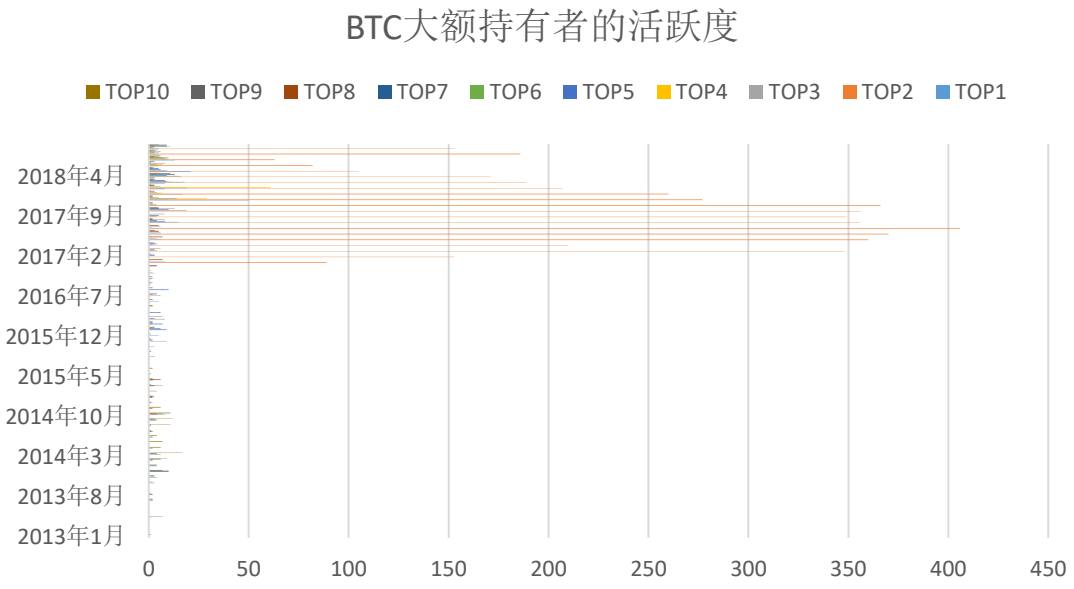
1.4 “虚拟货币”大额持有者的分布以及数据变动



（“虚拟货币”大额持有者的分布 数据来源：bitinfocharts.com, etherscan.io @2018.09.30）

比特币前1655个账户中最低账户持有资产超过656万美元，以太坊前1163个账户中最低账户持有资产超过 231 万美元，这些账户如果损失 1/1000 资产都将达到数千美元，这部分高净值账户的持有者更应该注意对自身持有虚拟资产的保护。

下图为比特币（BTC）大额持有者历年来的活跃度变化。



（BTC 大额持有者的活跃度 数据来源：bitinfocharts.com @2018.09.30）

BTC 大额持有者在 2013 年底到 2014 年第一季度的活跃度较高，第二季度

活跃度下降，随后第三季度活跃度提升。之后的活跃度很低，直到 2017 年第三季度，BTC 大涨，大额持有者的活跃度猛增。到 2018 年，BTC 的价格开始下跌，大额持有者的交易量逐渐降低。BTC 持有量排名前 10 的账户，有 7 个账户在 2017-2018 年大量交易，有 3 个账户在前期大量买入 BTC 后很少有交易，到 2018 年的第三季度，交易量才有所回升。

1.5 安全风险是造成区块链现在熊市的重要原因之一

“为什么区块链上的数字值钱？因为有共识。资产是由数学、由程序来控制的，当发现黑客可以绕过所有程序，随便偷钱的时候，就没有共识，没有信任了。这个时候，资产的价值就是 0 了，就是垃圾。” ——知道创宇 CEO 赵伟

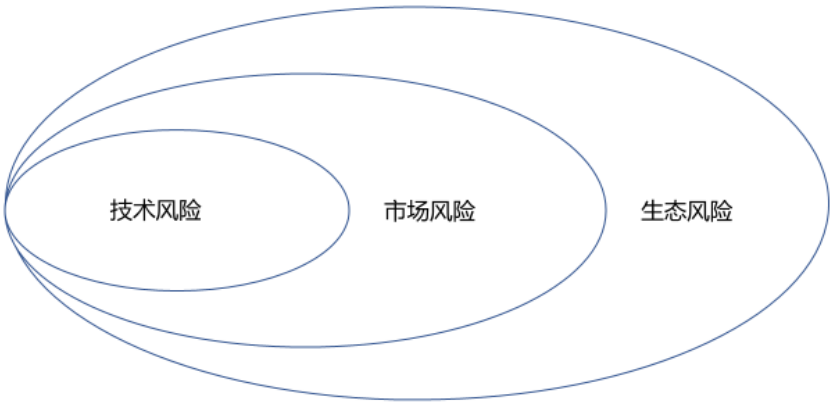
（“虚拟货币”安全事件及损失 数据来源：公开事件收集数据整理 截至 2018 年 9 月）

随着区块链的经济价值不断升高，“虚拟货币”安全事件爆发率逐年增加，案值增大。不法分子以用户财产为目标，利用各种攻击手段获取更多敏感数据，试图盗窃、勒索。“虚拟货币”安全事件的爆发点由区块链生态安全向区块链自身机制方面转移，尤其是智能合约存在较多安全方面的挑战。以太坊网络出现漏洞造成安全威胁已经不算新鲜事，使“虚拟货币”的安全形势变得更加复杂。虽然说区块链技术在某些角度上说更加安全，但在系统自身方面同样存在薄弱环节，容易被攻击，造成损失。

2 “虚拟货币”风险分析

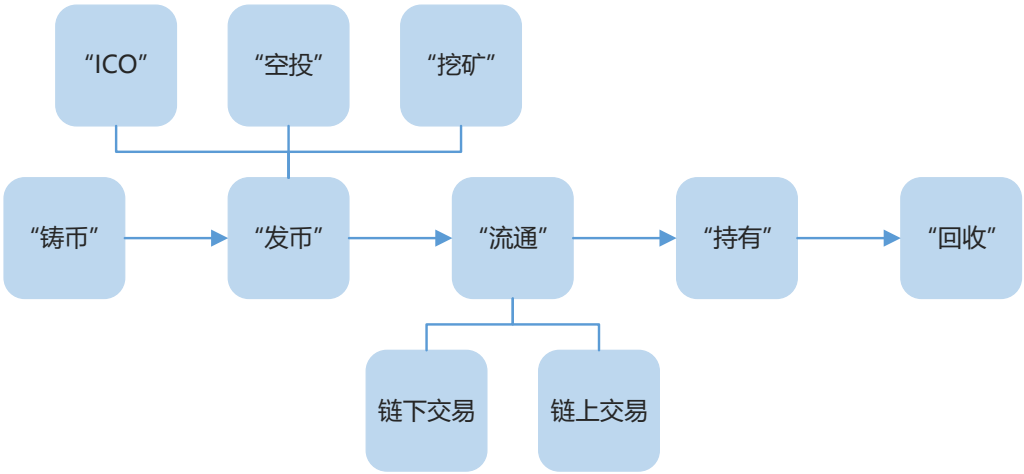
近几年代币和“虚拟货币”所吸纳的资金量呈现井喷式爆发，在这些“虚拟货币”手握重金的同时，以金钱损失为核心，涉及的“虚拟货币”的安全风险也不断涌来。

根据我们对“虚拟货币”市场安全事件的梳理，我们发现可以从“虚拟货币”的技术风险、市场风险和生态环境风险来分析风险问题。



2.1 技术风险

“虚拟货币”完整的生命周期如下：



在这个周期的各个阶段，“虚拟货币”面临着不同的技术风险。

（1） “铸币”

“铸币”时，比较显著的是漏洞带来的风险。项目所选择的智能合约族可能存在合约漏洞，而由于智能合约无法修改，可能造成损失。项目使用的虚拟机和公链的漏洞也有被攻击者渗透的风险。

（2） “发币”

“发币”有 ICO（首次代币发行）、空投、挖矿三种方式。

ICO 可能有漏洞问题，并且可能受到垃圾交易攻击。

空投是发行方赠送出“虚拟货币”的过程。可能会有漏洞植入、羊毛欺诈、货币劫持等风险。

挖矿的矿机可能被远程控制，并且面临着 DDoS 攻击的风险。此外在今年，51%算力攻击也成为了可能。

（3） 流通

“虚拟货币”的流通包括链下交易和链上交易。

链下交易指用户间自发的交易，不利用区块链技术。链下交易可能面临

DDoS、漏洞渗透、应用过载风险。

链上交易是基于区块链和网络的交易，可能被交易延展性攻击、双花攻击、扣块攻击；账户冻结的技术难度也使不法分子利用“虚拟货币”进行洗钱等违法活动变得难以阻止，给监管带来了困难。

（4） 持有

在用户持有“虚拟货币”时，需要面临保存“虚拟货币”的介质或机构产生的技术风险，如钱包安全性不足、私钥盗取、钓鱼网站、交易平台有漏洞或突发技术故障等。

密钥生成的风险：目前市面上在售的硬件钱包，密钥的生成机制存在伪随机滥用、密钥存放安全机制欠缺等安全问题。

设计及元件的风险：在硬件结构设计方面也存在着易被黑客利用的漏洞，同时在元器件使用方面并未进行安全审查。

设备固件的风险：目前的硬件钱包普遍存在设备固件未校验、核心数据未加密、固件和关键信息已被提取的风险。

通信机制的风险：硬件钱包冷端和热端 APP 的通信（USB、NFC、蓝牙、二维码等），均未进行严格的通信加密。

升级机制的风险：市面上大多数硬件钱包设备在升级过程中缺失安全保护机制，极易被不法分子篡改利用。

（5） 回收

“虚拟货币”在由发行方回收后，必须要永久销毁，不可还原，否则容易使“虚拟货币”的价值失去稳定性，导致“超发”风险。

2.2 市场风险

2.2.1 稳定性

市场上的主流“虚拟货币”都是非稳定的，它们的价格随着市场波动不断发生巨大的变化，这种波动让它们不适合进行日常支付和交易。

目前市场上有三种稳定币：

第一种是通过中心化的资产抵押实现，比如 Tether（USDT），其保证 1：1 的兑换比例来保证价值。但 USDT 长期以来因为暗箱操作，缺乏透明度、审计程序不够充分，涉嫌超发和操纵市场，使得 Tether 一直饱受争议。

第二种方式是以加密资产抵押，因为去中心代币本身没有信任风险，所以这种稳定“虚拟货币”能直接解决信任风险，比如 MakerDao 推出的 DAI。但会有浮动性风险，如果抵押物的价值大幅波动，抵押物价值（collateral value）严重低于了相应的代币票面价值，那么就会出现爆仓。

第三种方式是算法稳定币。算法稳定币是用智能合约模拟中央银行的方式保持代币的稳定性，基本思路是：代币的供应量是有弹性的，在供大于求的时候就少发，在供不应求时就多发，从而实现稳定价格的目的。但算法稳定币是建立在对稳定“虚拟货币”未来需求会一直增长的假设下的，如果算法稳定币跌破发行价，需要吸引其他人来购买“虚拟货币”，一旦没有足够的“接盘侠”，最后只能崩盘。

相比以上三种稳定币，新发行的 GUSD 和 Pax 在透明性和风险控制上具有更大的优势。GUSD 部署在以太坊的公链上，公开透明而且监管部门会查账，不可能像 USDT 一样存在暗箱操作和操控的问题；以 1:1 的比例和美元挂钩，得到

保险公司保障并定期披露审计报告，购买力稳定；也不会有崩盘的风险。

下面是几种“虚拟货币”的原生价值衡量标准：

币种	原生价值
BTC	全球电力损耗
LTC	全球电力损耗
ETH	31,529 个 BTC+一部分电力消耗
EOS	366,000,000 ETH
ERC20 token	部分 ETH
REP	18,630.8749 BTC+1,149,880 ETH
NEO	6119.3 BTC

从表中我们可以看出，相比于其他“虚拟货币”，比较稳定的是 BTC 和 LTC，大部分“虚拟货币”都是依托于 BTC 和 ETH，如果 BTC 和 ETH 发生大额市场变动，比如比特币遭到垃圾交易、双花攻击、交易延展性攻击等，对某些“虚拟货币”造成的影响是巨大的。

2.2.2 通胀率

下面是目前市场上比较流行的币种以及发行量：

币种	发行量
BTC	21,000,000
ETH	72,000,000+18,720,000 /年
EOS	900,000,000
XLM	100,000,000,000

币种	发行量
LTC	84,000,000
BNB	20,000,000
XRP	100,000,000,000
REP	11,000,000
NEO	50000000

一些代币发行制度设计为通货膨胀的形式，这里有潜在的代币贬值风险。参与者投的都是对项目的预期。以 EOS 为例，主链上线后，如果未能达到大家的心理预期，价格必然会出现下调。此外由于 EOS 本身有通胀机制,每年最高可以有 5%的新币增发来奖励“数据包”验证者（可以理解为比特币的矿工），需要有持续的新资金流入，才能消化这部分通胀出来的新币。

2.2.3 流通性

币种	流通渠道
BTC	国外交易所，暗网
ETH	ERC20 生态，ICO，交易所
USDT	法币与“虚拟货币”之间兑换
ERC20 token	特定的交易所

“虚拟货币”在小范围内流通使用，对实体经济的影响有限。然而比特币发展至今已有八年，基本形成一个较为稳定的运行市场。正如一把双刃剑，比特币的缺点也会带来负外部效应。“虚拟货币”流通的主要问题是发行的去中心化导致信用缺失，为非法交易提供可能性，价格的上下波动使风险积聚等。

2.3 生态风险

“虚拟货币”生态的健壮性以规则为基础。就目前看来，“虚拟货币”的生态是为支撑区块链运行及与现实世界相对接的一系列支撑系统或应用。“虚拟货币”的生态中包括资产存储、增值、支付、交易、第三方服务连接等。

这些生态都因为既是区块链中的一个支持环节，又存在于现实世界中采用已有架构模式构建，导致它们依然会存在区块链之外的一些传统系统或应用所面临的安全问题。

2.3.1 违约风险

违约风险，是指在信用活动中由于存在不确定性而使本金和收益遭受损失的可能性。换句话说，就是指因交易对手不能履约或故意不履约所造成的损失。

在“虚拟货币”资产中，代币发行者可以是跨国的初创公司、项目、网络社区或一群临时组合的自然人，参与者对发行者信用情况和相关项目知之甚少，这为蓄意诈骗的犯罪分子提供了可乘之机，有些所谓的“XX 币”可能仅仅是一种普通的借据甚至骗局，与区块链技术应用或创新项目毫无关系。这类虚假宣传、做庄、价格操纵、内幕交易等不法行为，存在较大的信用风险。

2.3.2 流动性风险

传统上，流动性风险是指由于流动性的不确定变化而使金融机构遭受损失的可能性。流动性包含两层含义：一是指金融资产以合理的价格在市场上流通、交易及变现的能力；二是指金融机构能够随时支付应付款项以及能以合理的利率方便地筹措资金的能力。当发生储户挤兑而银行头寸不足时，就会发生流动性风险，若控制不力会波及整个金融体系的安全。

区块链透明度研究所（BTI）认为，全球前 10 大“虚拟货币”交易所中，至少有 7 家存在交易额注水的情况，其公布的交易额相当于真实交易额的 12-100 倍不等；该机构指出，大家耳熟能详的“虚拟货币”交易所中，OKEx 的每日交易金额很有可能被注水放大了 19.2 倍，而火币的每日交易金额很有可能被注水放大了 12.5 倍，80-90%的交易额系伪造。这种交易所对交易量的注水就是对流动性造假，我们并不能知道交易所实际上的资产量能否支持得住用户兑现，放进去的“虚拟货币”可能提不出。

2.3.3 政策管制风险

比特币等“虚拟货币”以及形形色色的代币，存在较多法律盲区，在监管合规方面也存在较大不确定性；同时，“虚拟货币”可以用于匿名进行贩毒、洗钱等非法交易，如果涉足其中，风险不言而喻；此外，不同国家的监管严厉程度不同且缺乏明确的市场交易规则。

由于“虚拟货币”的性质特殊，各国家和地区政府对“虚拟货币”的政策均有不同。日本、白俄罗斯、澳大利亚有正式法规；美国、韩国、新加坡、瑞士等有监管政策，其中新加坡、瑞士呈鼓励态度；俄罗斯正在建立法规；英国未有明确规定；而在印度、中国、越南等国代币和“虚拟货币”交易被明令禁止。

各国政策还在不断调整变动，整体趋向于加强监管，例如 2018 年 7 月，美国金融业监管局（FINRA）要求其成员公司在“虚拟货币”领域的活动提供更多细节、对监管部门更透明。“虚拟货币”随时面临加重管制和监控的风险，现有的币种、交易所等等可能在未来的某一天被下令整改甚至关停，如 2018 年 3 月，日本金融厅对 2 家交易所实施关停一个月、5 家交易所整改的行政处罚。而就在

8 月 28 日，中国互联网金融举报信息平台已在“互联网金融举报范围”（https://jubao.nifa.org.cn/ipnifa/range.html）内列入“代币融资发行”内容。

因此，“虚拟货币”在政策方面具有不确定性，这种风险可能给参与者和平台方带来损失，也可能对整个市场带来冲击。

2.3.4 保管监管风险

传统资产有较为完善的保管和监管体系，比如银行保险箱、信托、银监会等。而“虚拟货币”缺乏相关的保险保管机制，保管方式也与传统资产有较大区别，基本只有个人钱包、交易所几种；监管制度难以确定也难以施行，当前的“虚拟货币”游走在监管边缘。

如果个人未能妥善保管钱包密钥，或委托保管的服务方失信或出现事故，或相应监管不力，都会带来损失财产的风险。

“虚拟货币”整体生态的安全水平会因某一方面的安全水平较低而被拉低，所以要注意生态中各环节中可能存在的风险，补足短板，提高安全性。

3 “虚拟货币”风险与传统资产风险对比

3.1 从传统资产继承的风险

“虚拟货币”市场继承了传统金融市场的种种风险，如市场风险、财务风险、经营风险、操作风险等。

在此仅介绍比较典型的两种风险。

（1） 市场风险

市场风险是指由于金融市场变量的变化或波动而引起的资产组合未来收益的不确定性，主要由价格、利率、汇率等市场风险因子的变化引起。常常是其他金融风险的驱动因素。

代币或“虚拟货币”价格波动大，参与者面临较大的市场风险；代币首次发行后一般都要到“虚拟货币”交易平台挂牌交易。

（2） 操作风险

操作风险是指由于不完善或有问题的内部操作过程、人员、系统或外部事件而导致的直接或间接损失的风险。再细分操作风险的类型，可分为内部欺诈、外部欺诈、制度/业务事故、流程管理事件等。

目前除少数国家（如日本）实行持牌经营外，代币和“虚拟货币”交易平台大多处于自由发展状态，存在虚假宣传、蓄意操纵价格等情况；交易平台或“虚拟货币”钱包在安全性方面一般达不到金融机构的安全级别，因此有受到黑客攻击导致交易系统瘫痪、客户资金被盗等风险。

3.2 “虚拟货币”与传统资产有差异的风险

在一些其他的方面，传统资产和“虚拟货币”都具有这种特征，但程度不同。以下将从交易时间、波动幅度等维度进行分析，并在需要时从传统资产中取股票、期货、外汇举例，和“虚拟货币”对比。

3.2.1 交易时间

（1）股票

在中国，股市交易时间为每周一到周五上午时段 9:30-11:30，下午时段 13:00-15:00。周六、周日及上海证券交易所、深圳证券交易所公告的休市日不

交易。中国香港、美国、欧洲股市也类似，一般在周一至周五的固定时段开市。股票一般每天交易 4-6 小时，每周 5 天。

（2）期货

期货交易时间依具体交易所而定，一般有上午、下午、夜盘三个时段，有的交易所还在法定节假日休市。以上海期货交易所为例，交易时间为上午 09:00-10:15，10:30-11:30，下午 13:30-15:00，夜间 21:00-02:30。期货一般每天交易 6-9 小时，每周 7 天。

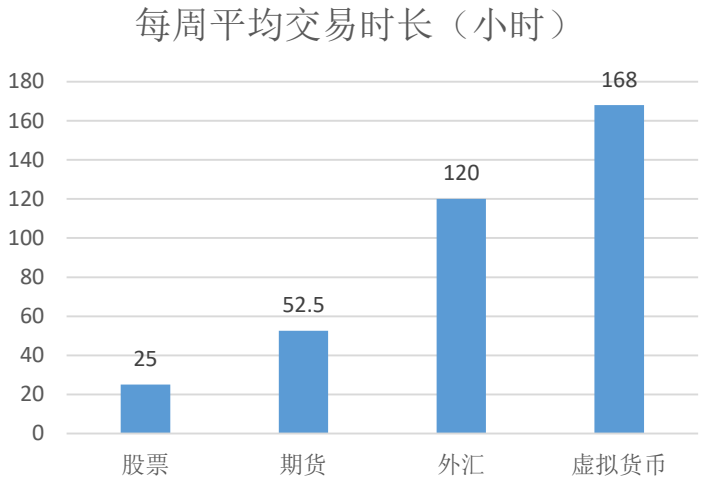
（3）外汇

国际各主要外汇市场开盘收盘时间对北京时间来说都不同，所以外汇市场其实是一个 24 小时不停止的市场。一般周末全球都是休市的，周一凌晨 5 点左右开市。以中国外汇交易中心为例，人民币外汇即期的交易时间为北京时间 9:30-23:30，周六、周日及法定节假日不开市。所以外汇一般每天交易 24 小时，每周 5 天。

（4）“虚拟货币”

“虚拟货币”市场则是真正的 7×24 小时全年无休，无时无刻不在交易。

将各金融产品的交易时长进行对比，可以得出下图。“虚拟货币”的每周交易时长长达 168 小时，分别是股票的 6.72 倍、期货的 3.2 倍、外汇的 1.4 倍。

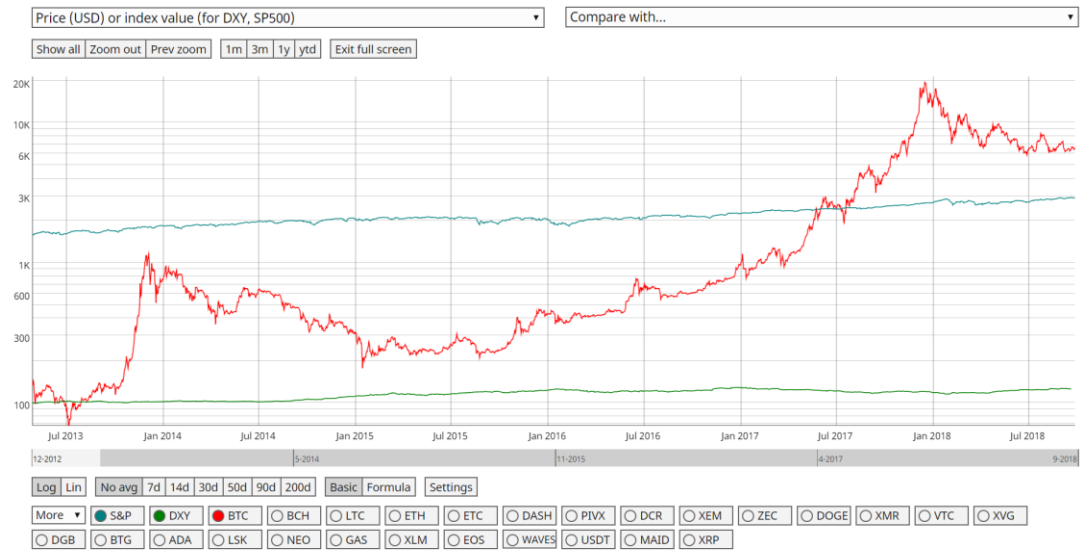


各金融产品每周平均交易时长

交易的时间差异也能在一定程度上反映出交易频度的差异。显然“虚拟货币”的交易频度与传统金融市场相比更大。

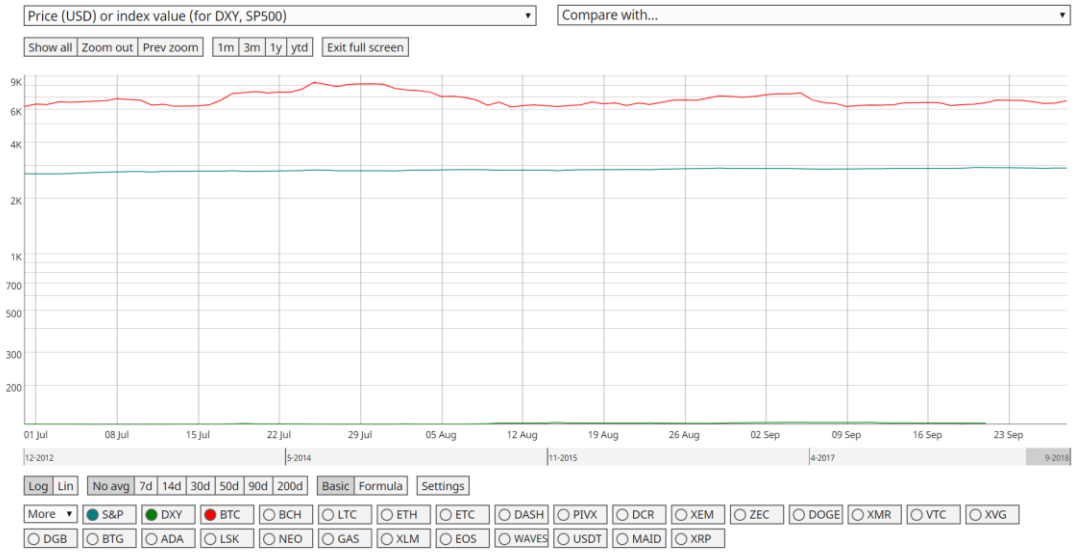
3.2.2 交易的波动幅度

以标准普尔指数 (S&P)、美元指数 (DXY)、比特币 (BTC) 为代表，从 2013 年 4 月末至 2018 年 9 月的三者的价格或指数值如下图。



S&P、DXY、BTC 长期价格对比（图片来自 https://coinmetrics.io/）

而从 2018 年 6 月 30 日开始至 2018 年 9 月 28 日，三个月的数据如下图。



S&P、DXY、BTC 短期价格对比（图片来自 https://coinmetrics.io/）

可以看出，无论是长期还是短期，美元指数最为平稳，标普所代表的股市变化较为曲折，而比特币在图表上有明显的锯齿，波动剧烈。并且从 13 年到现在，比特币有非常明显的价格差异，从 100 多美元增长到了 6000 多美元，峰值时有近 2 万美元。

其余像以太坊（ETH）、EOS 等代币大多也同比特币一样，波动剧烈。这样动荡的市场，使不可预测性更强，投资风险更大。

3.2.3 限额

（1）股票

股票最低单笔交易 100 股，没有上限，但大额交易要经过大宗交易系统。各个交易所在它的交易制度中或者在它的大宗交易制度中都对大宗交易有明确的界定，而且各不相同。

（2）期货

期货交易以“手”为单位计量，最低单笔交易一手。期货有持仓限额。

影响期货限仓数额的因素较多，期货的限仓数额会根据不同交易所、不同商品、不同时期、甚至不同角色变化。

不同商品期货交易所的规定持仓限额不同，一般在不同的时期，同一交易所的规定限额也会不同。下表是以上海期货交易所为例的铜期货合约在不同时期限仓的具体比例和数额（单位：手）。

	合约挂牌至交割月前第二月的最后一个交易日				交割月前第一月			交割月份		
	某一期货合约持仓量	限仓比例（%）								
		经纪会员	非经纪会员	投资者	经纪会员	非经纪会员	投资者	经纪会员	非经纪会员	投资者
铜	≥12 万手	15	10	5	8000	1200	800	3000	500	300

注：表中某一期货合约持仓量为双向计算，经纪会员、非经纪会员、客户的持仓限额为单向计算；经纪会员的限仓数额为基数。

（3）外汇

外汇最低限额根据外汇平台的不同，有迷你版本的 0.01 手可以操作。而最大持仓限额就是参与者本金的最大倍数以下的限额。以中国外汇交易中心为例，人民币外汇即期撮合最小交易金额为 100 万美元。

（4）“虚拟货币”

“虚拟货币”交易所都有自己的提币限额，但没有单笔交易限额或持仓限额。也就是说，交易所想要使自己持有的资产最大化，防止资产被兑走，规避交易所自己的流动性风险，但没有对整体市场风险的有效控制。交易所更多考虑的是自己，并没有切实考虑参与者的利益。

3.2.4 冻结

股票、期货均有未完成的交易可以冻结的机制，当交易失败后还可以回滚。在期货中，下单未成交会出现资金冻结，在非交易时间转账资金也会出现冻结。

当账户涉及违法交易时，银行、交易所也有权冻结账户。

但在“虚拟货币”交易中，冻结一笔交易有技术上的难度。在交易所内的交易有冻结机制，但真正的链上交易是没有冻结机制的，因此会导致不诚信问题，使双花攻击成为可能。

此外，账户资产冻结的技术难度也给监管带来了问题。日本经济新闻发表文章表示，6 月 13 日“虚拟货币”交易所以“技术上困难”为由，未对法院命令冻结“虚拟货币”账户的资金一事做出相应措施，从这一事件来看，“虚拟货币”是无法被强制冻结的。丽泽大学的中岛真志教授指出：“没有管理者的“虚拟货币”不应该被公共权力机构查封，技术上也不能保证其被强制执行。”他表示，这可能会成为洗钱和资产隐藏等的温床，“目前的情况下，它不适用于健全的金融交易，必须通过制定法律和规则来允许交易所能够冻结存款等问题，这是必不可少的。”

3.2.5 杠杆额度

（1）股票

法定的融资融券杠杆比例为 1:1，实际上可以达到 4-5 倍；股票配资目前被大家广泛接受的最大比例为 1:5，甚至有部分客户要求 1:10 的高杠杆。

（2）期货

期货的杠杆比例一般根据商品种类固定，在 5-10 倍左右。期货配资目前被大家广泛接受的最大比例为 1:10，但配资客户通常在 1:5 范围内做。

（3）外汇

外汇杠杆比例视交易平台而定，一般有 10-20 倍。

（4）“虚拟货币”

“虚拟货币”的杠杆比例在全球范围内没有固定标准，小到 1:2，大到几千都有出现。而“虚拟货币”的波动很大，使用好高杠杆可以获得难以想象的巨大利润，因此不乏高杠杆投机者；但同时，使用杠杆的风险也成倍增长。

我们可以以今年四月欧洲证券市场管理局（European Securities Markets Authority, ESMA）出台的新措施为例。ESMA 为不同的金融产品设置了不同的杠杆：主要外汇 30:1，指数、非主要外汇、黄金 20:1，其他商品、非主要指数 10:1。个股参考值 5:1，而“虚拟货币”只有 2:1。

可以看出，越是稳定的金融产品，其杠杆比例越大。因此 ESMA 将“虚拟货币”的杠杆压到了 2 倍，对高风险进行控制。

3.2.6 抵押

传统资产中，有抵押、质押、留置等抵押方法，以及资产抵押债券（ABS）、股票质押融资等对应的金融工具，并有相应的监管证明机构进行公证。

而“虚拟货币”交易基于互联网，难以进行实物抵押，其他抵押也难以保证公正性和可信度；其本身价格变动大，使用“虚拟货币”作为质押，也要面临价格变动引起的风险。与“虚拟货币”相关的抵押面临着金融层、监管层、业务合法性的三重风险。

3.2.7 保险

传统的财产保险已有成熟的体系，众多保险公司相互竞争，提供的保险规则、保额也不尽相同，还有中国保险监督管理委员会（简称保监会）进行监督管理，维护保险市场秩序。

“虚拟货币”保险在国内已被禁止，国外可以说是刚刚起步。业内有伦敦劳埃德保险公司提供代币和“虚拟货币”保险。

3.2.8 管理

传统资产有较为完善的保管体系，比如银行、证券、保险、信托和基金管理公司，在我国，还有证监会、银监会、保监会等监管部门进行监督、管理。

代币和“虚拟货币”的资产管理在国内已被禁止，国外各方也在尝试和探索阶段。虽然也有 Coinbase 等平台提供相关衍生期货、信托、借贷甚至 ETF（交易型开放式指数基金）等产品，但良莠不齐，参与者进行“虚拟货币”管理面临着产品不成熟、交易所不诚信等风险。

4 “虚拟货币”风险案例

“虚拟货币”资产的风险既包括传统金融领域的风险，也包括区块链自身的一些风险，在这里通过列举交易市场操纵风险、交易平台风险、诈骗风险、钱包风险以及继承风险等方面的案例，来介绍“虚拟货币”资产所面临的风险。

4.1 交易市场操纵风险

4.1.1 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。

4.1.2 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。

4.2 交易平台的技术故障

4.2.1 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。

4.2.2 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。

4.3 交易平台“内鬼”风险

4.3.1 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。

4.3.2 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）。

4.3.3 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。”

4.4 诈骗风险

4.4.1 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。

4.4.2 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。

4.4.3 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%。

4.4.4 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。

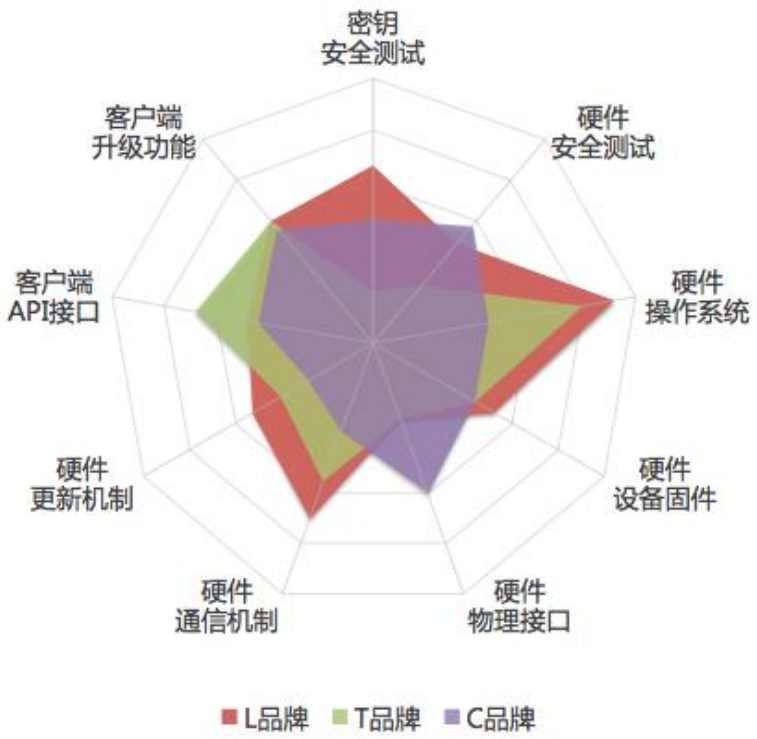
但是仍有一部分参与者对 CoinDash 表示支持，并继续将以太坊发送至这个地址，这就使得被盗取的资金从 700 万美元上升至 1000 万美元。

4.5 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。[1]



4.6 “虚拟货币”的继承风险

[1] L/T/C 品牌均为化名，不指代任何品牌

4.6.1 失去一半密钥

把“虚拟货币”钱包密钥弄丢或不记得的事情层出不穷，迄今估计有 300 万枚比特币被遗失，价值接近 250 亿美金。

据《纽约时报》报道，Michael Yang 在加州旧金山湾区经营“虚拟货币”交易所，他和一位朋友决定各自记下一半密钥。不料某天朋友意外去世，也把一半密钥带走了。两人共同持有的比特币至少有 500 枚，但没有密钥无法从账户中领取出比特币，导致损失了约 400 万美元。

4.6.2 家人得不到遗产

被福布斯评为“虚拟货币”十大富豪之一的美国纽约梅隆银行（Bank of New York Mellon）接班人马修·梅隆（Matthew Mellon）传出在戒毒所逝世，但他家人始终找不到钱包密码，留下市价约 10 亿美元的比特币。

梅隆是纽约梅隆银行和德雷克塞尔家族的后裔，起初他以 200 万美元投资“虚拟货币”使资产增值至 10 亿美元，他生前曾担任过纽约共和党财务委员会主席、Ripple Labs 的顾问。

5 “虚拟货币”未来展望

当前区块链加持的“虚拟货币”依然风险重重，安全问题面临严峻挑战，对于参与者来说，如何有效的保护“虚拟货币”资产成为了首先要解决的问题。宏观上，可以采用国家制定相关政策宏观约束市场发展的手段。微观上，也需要“虚拟货币”机构内部对交易流程的监管，以及国家对灰色交易的监管。在这样的前提下，才可能让“虚拟货币”走向正轨，应用在更广阔的地方。

有了监管框架后，可以从技术安全和管理手段两方面进一步保护资产安全。技术上可以参考现在较为先进的安全数字钱包，而管理手段可以参照传统行业做法。同时，引入适合的风险评估机制，进一步控制风险。

在监管和安全发展成熟的情况下，可以在银行、保险业务、ETF 指数基金和虚拟资产托管、信托服务等角度上进行探索，以及结合其他行业诞生出良性的应用，使“虚拟货币”为实体产业服务。

5.1 监管、管控展望

5.1.1 “虚拟货币”资产的监管

随着“虚拟货币”资产的热度升级，各国监管对其重视程度越来越高。多个国家政府都逐步开始制定相关的监管框架，对行业进行规范。

中　　国：中国当前禁止开设“虚拟货币”交易所，对“虚拟货币”的监管也较为严格。中国香港地区秉承与大陆统一的思想主线，对“虚拟货币”也是持严格监管的态度。但香港证监会推出了一个金融科技监管沙盒，允许企业在一定程度上超出现有法律条文的范围探索金融科技的新应用，目前，已设立三大监管沙盒及基础建设，共有 33 项新科技产品进行试行，其中 25 项试行已完成并推出了产品。只是是否会将沙盒应用到区块链领域还未可知。

俄 罗 斯：拟定法案，实际推动 ICO 监管及区块链技术落地。俄罗斯政府对比特币的态度呈现出由禁止到逐步放开的趋势，2018 年 1 月俄罗斯出台“虚拟货币”和 ICO 法律草案，法币交易将获许可。

美　　国：美国对“虚拟货币”的管理主要还是在现有的法律框架内，而不是出台新的法律。由于美国国内监管机构仍然没有提出一个明确的方案来监管比

特币、其他“虚拟货币”与 ICO，所以美国仍不确定“虚拟货币”的地位如何。目前有许多美国国内监管机构谈及了“虚拟货币”，而所有这些机构对比特币等“虚拟货币”的看法都不一：有的将其视为证券，有的将其视为货币，也有的将其视为资产或视为商品。此外，各州之间的监管法规也有所区别。

欧　　盟：重点针对 KYC（Know your customer 政策，对账户持有人强化审查）和 AML （Anti-Money Laundering，反洗钱）监管。欧盟理事会通过了一项影响欧洲“虚拟货币”的指令。该指令批准了一项欧盟的新反洗钱法案，以解决“与‘虚拟货币’相关的风险”。新规则旨在减少用户和交易的匿名性，要求“虚拟货币”交易平台必须实现的 KYC 的要求。

日　　本：重点针对 KYC 和 AML 监管。日本财务省近期的公告显示，根据“外汇及外国贸易”法，在日本和外国之间或居住者和非居住者之间，如果进行债权债务或财产转移是通过“虚拟货币”交易和支付、且超过 3000 万日元，则需要向财政部长报备。

澳大利亚：重点针对 KYC 和 AML 监管。澳大利亚被称为对比特币最为宽松的国家。澳大利亚税务局（ATO）将比特币归类于金融资产，否认比特币作为货币的属性。在对其征税方面，澳大利亚税务局将比特币的各个环节分别纳入其原有的税务体系中，在没有突破原有体系的前提下，解决了比特币税务的问题。澳大利亚议会通过了《2017 反洗钱和反对恐怖主义融资修正案》，旨在填补有关可转换“虚拟货币”的监管空白，强化澳大利亚的 AML/CTF 机制。

新 加 坡：支持区块链技术发展，推出“沙盒”监管机制。2017 年，新加坡金融管理局特别推出了针对 FinTech 企业（金融科技企业）的“沙盒”机制，只要 Fintech 公司在沙盒中注册，便允许其在事先报备的情况下，从事和目前法

律法规有所冲突的业务，并且即使该业务之后被政府终止叫停，企业也不会被追究相关法律责任。同时新加坡政府确定对“虚拟货币”征税，新加坡企业无资产税，需缴纳所得税和商品增值税，海外收入无需纳税；新加坡个人报酬或收入所得“虚拟货币”需缴纳最高 22%的个人所得税。

马 耳 他：开放性倡导。马耳他的“虚拟货币”立法更多地是为了吸引投资、促进当地经济发展。2018 年 4 月 24 日，马耳他内阁正式批准了与“虚拟货币”和区块链技术相关的三项法案，这三项法案分别是 MDIA 法案，建立马耳他数字创新局（MDIA）；TAS 法案，为基于分布式账本技术的平台运营商进行政府认证；VC 法案，监管首次币发行和其他“虚拟货币”的相关服务。马耳他通过立法来规范尚未受到监管的领域，表明了其对打造全球最完善的“虚拟货币”市场监管机制的决心。尤其值得一提的是，即将建立的“数字创新局”（MDIA），在认证区块链公司的同时，还会为 ICO 提供法律框架。

从“虚拟货币”资产全球政府和机构监管政策来看，各国监管政策分歧较大，部分国家政策仍不明确，联合监管较为困难。有监管的国家主要都是在 KYC、AML、ICO 和税收方面提出的监管策略。监管存在升级的发展态势，这将促使行业更加规范，交易更加透明化、可追踪。整体来看，监管将有助于行业朝着良性方向发展，未来的数年注定是“虚拟货币”资产行业迈向合规的阶段。

5.1.2 “虚拟货币”资产的管控

（1）个体管控

“虚拟货币”技术本身可以被用来提高效率、降低成本，但也可以被不法分子用来做灰色交易，所以“虚拟货币”资产的监管和溯源就显得尤为重要。买家

在交易发起之后，要注意资产的流向，是否到达了对方的账户，资金储存在哪个钱包之下，对方是否把币转到自己的地址上。在收到币的时候要注意检查“虚拟货币”资产的来源，保护好自己的私钥。

当在交易所发生交易时候，平台要对用户账户进行监管，一旦发现大额度或者非法交易时候，要及时采取措施，防止不法分子进行财产转移，给用户带来资产的损失。

当前，企业往往不清楚有关“虚拟货币”本身的规定，条例中也缺少关于“虚拟货币”存储的安全规定。行业未来的发展，需要第三方监管机构介入，为企业间竞争和良好的市场环境制定规则。

在“虚拟货币”监管领域中，最有可能的结果是，将“虚拟货币”交易的技术创新与传统金融服务的管理流程、风控经验结合起来，从而助推“虚拟货币”市场成熟，行业迅速成长。

（2）机构流程管控

随着“虚拟货币”资产市场规模的迅速增长，越来越多的投资机构、企业、创业团队进入到这个领域，他们持有的各类“虚拟货币”资产规模也在快速增长。但是目前针对企业的“虚拟货币”资产管理工具极度缺乏，大量的资产被保存在个人钱包、交易平台或冷钱包中，这种情况与企业传统的资产管理流程存在巨大的差别。不断被媒体爆出的个人钱包被盗、私钥丢失、交易平台钱包被盗等新闻，使得企业对“虚拟货币”资产安全、便捷等问题产生严重担忧，加强“虚拟货币”资产的机构流程监管显得尤为重要。

市场上的某“虚拟货币”管理系统在执行转账前需要先构建企业转账审批流，该审批流为多级审核模型，最底层为员工管理组，其上可以有多级审核，每级审

核可以有多个审核人。当企业确认了审批流，则可以通过管理 APP 录入系统，构建成系统可识别的 A 协议。A 协议建立完成之后授权，转交给接入层，接入层检查格式后通知签名机。由私钥 APP 授权签名机将审批流哈希写入公链。企业可以通过该 A 协议进行转账。

5.2 保护展望

5.2.1 “虚拟货币”资产安全展望

伴随着代币和“虚拟货币”一路突飞猛进，整个人类社会对各种“虚拟货币”资产业务空前期待的同时，涉及到”虚拟货币”资产的安全事件也伴随新兴应用频繁发生。

就目前来看，一方面“虚拟货币”资产自身存在挑战，智能合约代码存在漏洞，共识机制存在安全问题，等等。因此未来的“虚拟货币”资产需要有更高级别的安全来保障。另一方面基于区块链的贷款结算、跨境支付等业务，对传统的业务模式提出了挑战。传统银行和信贷机构由于对“虚拟货币”资产了解不深，大部分对“虚拟货币”资产持观望态度。这时候需要政府加大对“虚拟货币”资产的监管，让传统行业深入了解认识到新兴技术和业务手段，推动对传统行业的改革。

面对“虚拟货币”资产的各种安全性挑战，应考虑综合运用密码学，拟态防御等网络安全技术，从算法、协议系统等方面提高“虚拟货币”资产的安全性，应对现存的安全性挑战。比如，尽早设计合适的抗量子攻击算法，使用安全的冷热钱包以及使用可有效防御黑客网络攻击的拟态防御技术，来应对“虚拟货币”资产所面临的系统安全性挑战。

5.2.2 数字钱包

数字钱包就是生成私钥和保存私钥的容器，它用来管理密钥和地址，跟踪地址的余额，创建和签名交易。根据载体进行分类，目前市场上加密钱包主要分为热钱包和冷钱包。

热钱包就是私钥存储在与互联网连接的终端上的钱包，如 starteos 钱包等。热钱包的私钥是通过加密存储在手机中的，加密的密钥就是钱包的交易密码通过哈希加盐法生成的口令文件。

冷钱包就是与互联网进行过物理隔绝的私钥存储容器，如 MemoryBox，USB 硬件钱包等。Trezor 钱包就是早期的硬件钱包，私钥的生成和存储完全离线完成，发送交易时，私钥也不会在联网的计算机上缓存，所以冷钱包是较为安全的私钥存储方式。

由于业务场景的快速迭代以及推广需求，无论热钱包还是冷钱包都会有一些安全隐患会被忽视。安全性和使用便捷性之间的冲突短时间无法解决。市面上的“虚拟货币”钱包良莠不齐，部分开发团队在以业务优先的原则下，暂时对自身钱包产品的安全性并未做到足够的防护，导致黑客有机可乘。

我们认为作为资产保管的硬件钱包必须和钱包 APP 结合在一起才能使用硬件钱包的完整功能。独立使用只能分别作为硬件钱包的观察钱包（钱包 APP）和密钥管理器（硬件钱包）使用。如果采用软硬钱包结合，硬件冷钱包主要负责构造交易并对交易进行数字签名，联网客户端负责联网查询余额及广播发送交易。设计上采用 EAL4+认证芯片进行纯硬件的算法加密算法的方式进行密钥的防护及存储，采用硬件 ECC 加密算法进行地址转换及交易签名的方式，可以极大程度商规避风险，让个人的“虚拟货币”资产管理变的更加有序，保障资产安全。

5.2.3 “虚拟货币”资产的风险评估

风险评估主要从下面几个方面进行：

1) 识别面临的各种风险

包括数据存储器是否隔离，私钥存放是否安全，智能合约是否存在漏洞，“虚拟货币”资产价格变动，国家政策影响。

2) 评估风险产生概率

把风险列举出来，根据数据分析计算出发生的概率，把发生概率按照“非常低”，“低”，“中等”，“高”，“非常高”分级。

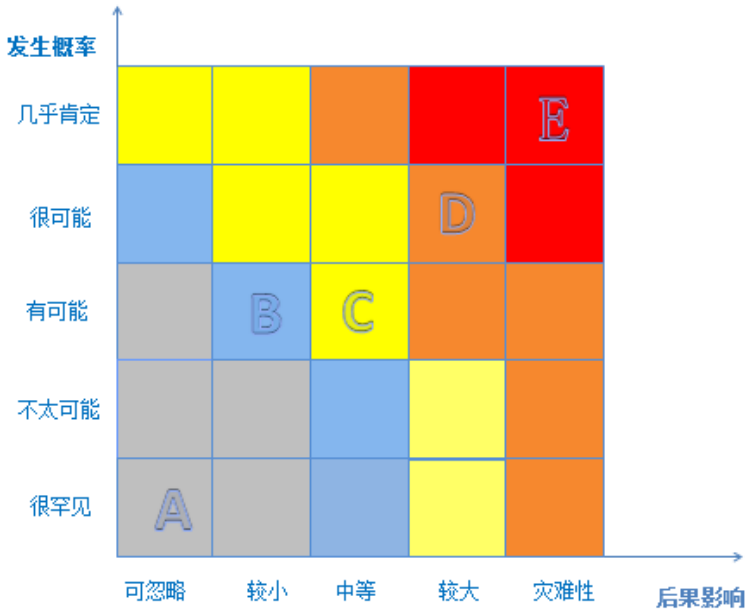
3) 可能带来的负面影响

对信用级别的影响，对投资的影响等等，把后果影响分为五级：“非常低”，“低”，“中等”，“高”，“非常高”。

4) 判断丢失的“虚拟货币”资产是否在承受能力范围内

5) 确定风险消减和控制的优先等级

在进行风险决策的时候可以运用风险管理矩阵。从风险的发生概率和影响后果两个维度来分析，针对不同类型的风险制定不同的管理策略。风险管理矩阵如下图所示：



发生概率较低，影响相对较小风险应对：

发生概率比较低的风险相对比较容易管理，例如数字钱包出现使用上的问题，参与者可向有关人员咨询并修复。

发生概率较低，影响严重风险应对：

如果是发生概率较低但影响后果严重的风险，需要重新进行风险分析。但这样的情况一般由不可抗力引起，往往也不是参与者能影响的。例如交易所遭到黑客攻击，或发生盗币事件。此时参与者应该与平台负责人商议，运用法律手段保护自己的“虚拟货币”资产权益。

发生概率高，影响相对较小风险应对：

针对那些发生概率高，影响后果相对较小的风险，参与者应有自己的应急储备计划。参与者不能以讹传讹，轻信“权威专家”的分析。

发生概率高，影响严重风险应对：

针对那些发生概率高、后果严重的风险，需要制定切实可行的风险管理计划，采用风险回避策略。

5.3 发展展望

由于“虚拟货币”资产会对金融系统造成一定程度的冲击，国家很可能在短期内不会采取放开并进行监管的方式开放这一领域。总的说来，“虚拟货币”可能还需要较长期的发展积累，才能逐步成熟应用。目前来看，国外已经在银行、保险信托和指数基金等业务开始了探索。

5.3.1 “虚拟货币”银行

“虚拟货币”银行可以利用“虚拟货币”在区块链上的公证功能，使“虚拟货币”资产更便于“银行”之间的往来。“银行”通过相互连接，可以为世界各地的用户提供一个完整的金融平台，从而创造出更高质量、更可靠的金融服务。

关于业务模式，“虚拟货币”银行可以向用户收取一定数量的“虚拟货币”管理费以及再收费、提款和转帐费用。此外，“虚拟货币”银行还可以为客户保留“虚拟货币”资产，并收取保管费。在发生事故和客户死亡的情况下，根据客户的个人认证信息，“虚拟货币”银行将客户的“虚拟货币”资产转移给其合法继承人。

5.3.2 “虚拟货币”保险业务

传统保险业务伴随着时代的发展越来越成熟，而“虚拟货币”发展的时间并不是很长，自身发展并不是很完善。相比于传统保险业务，“虚拟货币”资产保险这一新兴业务暂时没有详细的参考模型，由于“虚拟货币”自身的不稳定性，相关人员暂时没有办法去判断风险是不是可以控制，所以没有相对应的风险模型和风险防治措施。国内现阶段由于没有整体的保障政策和有效的监管，对“虚拟货币”资产保险业务是令行禁止的。

在英国，伦敦劳埃德保险公司推出比特币存储保险。客户可以选择他们需要比特币的保险水平，并以英镑定价，用户支付的年费率为 2%，在每月月底支付比特币，按月分期。

5.3.3 “虚拟货币” ETF 指数基金

“虚拟货币” ETF 是一个“虚拟货币”投资加密组合基金，参与者购买“虚拟货币” ETF 就相当于购买了一揽子“虚拟货币”，可以分散风险，并且实时透明，流动性更好。因为现在申请的“虚拟货币” ETF 大部分配置比特币，所以现在大家多称“虚拟货币” ETF 为比特币 ETF。

5.3.4 “虚拟货币”资产托管服务

比特币亿万富翁 Mike Novogratz 曾指出：“托管业务带来的机构资金，或将能让比特币重现昔日的辉煌。”

简单来说，“虚拟货币”托管是指依赖第三方为“虚拟货币”提供存储和安全服务。作为一个新兴行业，它需要综合考虑上层监管、客户需求和安全等复杂因素，从而有效地防止网络犯罪。由于监管政策的影响，国内禁止开展相关业务，目前主要的托管机构均分布在海外。

现有的托管解决方案大多使用在线存储和离线存储相结合的方式。比如离线存储：用户需要验证私钥才能接触到这些资产，用户私钥需要多重签名才能生成；私钥的备份存放于世界各地的保险库中。此外，“虚拟货币”离线托管还附加了一些额外的安全审计元素，例如链上隔离、多层安全防御、冷储存审计报告等，进一步确保资产安全。但因为“虚拟货币”托管的风险性，相比传统托管，其费用要高很多。传统托管可能只需 1 到 2 个基点，而“虚拟货币”托管可以收取

50 至 100 个基点的费用。

未来，“虚拟货币”资产托管可以发展为托管机构、客户和第三方监督机构三合一的托管模式，来确实保障“虚拟货币”资产的安全问题。

5.3.5 “虚拟货币”资产信托

未来，“虚拟货币”资产将作为第三类资产，区别于传统的有形物理资产和无形权益资产，而信托则可以成为“虚拟货币”资产有效的管理工具，为其价值赋能。“虚拟货币”资产将会是新时代资产管理的重要内容，而虚拟资产信托有望成为管理“虚拟货币”资产的重要方式。

虚拟资产信托是委托人将其所有的“虚拟货币”资产作为信托财产设立信托，受托人按照委托人意愿，委托虚拟资产服务运营商对信托财产进行专业管理，由此产生的增值收益按照信托目的进行信托利益分配。合格参与者可以通过投资信托受益权的方式参与信托利益分配，委托人则通过信托受益权转让的方式获取现金对价，实现“虚拟货币”资产的价值变现。

虚拟资产信托具有独立性、安全性，此外还可以与大数据契合，改变传统信托行业。但在虚拟资产权属确定性、风险定价与交易、商业模式设计、行业发展趋势等方面，还应该进行更深入的探讨和实践。虚拟资产信托的最大价值在于利用信托制度优势实现虚拟资产价值优化、整合虚拟资产资源使用、促进虚拟资产利益互惠。

5.3.6 “虚拟货币”&区块链技术跨行业发展展望

金融业迅速发展的当前，依旧存在空白的“虚拟货币”资产市场。从 2009 年比特币诞生之后，资本市场仿佛又打开了一个全新的大门，而当前的“虚拟货

币”市场已经呈现了井喷的态势，行业内虽然存在多重风险，但也有不少机会。“虚拟货币”资产的应用在金融领域成熟之后，会带动很多其它跟金融相关的领域，如供应链金融、票据金融、跨境支付。“虚拟货币”资产业务能加速交易，能够降低交易的信任成本，跟随金融领域的应用一起成熟。

除此之外，区块链技术可以在互联网，制造业，人力资源行业，医疗健康行业和法律行业，零售业，还有公共部门等等方面发展。预计在几年的时间里，“虚拟货币”与区块链会在现代商业中创新出很多全新的商业模式和行业标准。越来越多的大公司、大企业会争先恐后地针对区块链技术及“虚拟货币”运行机制进行深入研究，争取在行业中占得先机。

结语

现在，“虚拟货币”整体行情走跌，参与者向比特币抱团，交易量下降，各方都处在观望状态。这是因为“虚拟货币”的一系列问题——逐渐暴露的自身风险、近期频发的安全事件、各国变化的监管政策和尚不稳定的保护体系——如同滚雪球一般越来越严重，最终导致了如今的状况。

中国信通院在《金融区块链研究报告》中写道：“现阶段，由于缺乏先例、长期实践不多，区块链技术可能对金融体系带来的风险和挑战，仍具有较大的不确定性，难以预判。因此，一方面，应结合相关产业实践，深入研究新兴技术对现有金融市场结构、风险管理模式、监管及法律框架产生的影响。另一方面，适时为区块链技术的应用提供必要的法律基础，明确现有法律和监管规则的适用性问题。”

“虚拟货币”及区块链技术本身并不存在善恶之分。它们所拥有的信息透明、不可篡改等特性在诸多领域均有良好的应用前景。话虽如此，现阶段对区块链和“虚拟货币”的炒作行为有极高的风险性，大部分参与者还抱有不理性的、投机的心理，而且很难监管。

“虚拟货币”的存续，还是需要国家和个人理性看待、脚踏实地地发展，保证行业健康有序。在经过一定的研究和探索，将相关风险明确后，以适宜的监管策略和有针对性的安全性提升对症下药，才能将“虚拟货币”从冰与火的夹缝间“解救”出来，回归到理性的发展方向上。

关于我们

关于知道创宇

北京知道创宇信息技术有限公司是国内最早提出网站安全云监测及云防御的高新企业，始终致力于为客户提供基于云技术支撑的下一代安全解决方案。知道创宇总部设在北京，在国内多地设有分公司。凭借强大的云安全技术与产品的高可用性、易管理性、合规性和业务连续性、以及动态保障关键 Web 数据资产安全的能力，帮助用户应对变化多端的互联网安全威胁，赢得了企业、政府与公共机构的青睐。知道创宇安全实验室在 0Day 安全威胁与云安全技术方面的研究得到了业内的广泛认同并享有极高知名度。

关于知道创宇 404 区块链安全研究团队

知道创宇 404 区块链安全研究团队的成员来自白帽黑客、安全渗透、安全硬件、智能合约、区块链基础研究及市场研究多个领域，研究团队核心成员早期曾参与多个区块链生态项目的安全防护和咨询工作。

知道创宇 404 区块链安全研究团队对区块链基础技术、智能合约、dApp、数字钱包（含软件及硬件）等方向均有深入研究。愿与各方专业人员精诚合作，共同携手，聚焦区块链安全解决方案，为区块链及整体生态产业的健康发展保驾护航。

引用资料

[1] 行情总在绝望中诞生 熊市大家抱团取暖吧 https://www.jinse.com/bitcoin/230671.html

[2] 研究团队发现以太坊网络大量智能合约存在安全漏洞 http://www.myzaker.com/article/5a9e780bd1f1496a3b000179/

[3] 关于首个受监管的稳定币 GUSD，你应该知道这些真相 http://dy.163.com/v2/article/detail/DRGAOT7O0511TH18.html

[4] EOS 代币每年通胀 5%，预计 2019 年 6 月后 EOS 才能真正起飞
https://baijiahao.baidu.com/s?id=1600160117669357765&wfr=spider&for=pc

[5] 虚拟货币流通性问题探析 http://www.fx361.com/page/2017/1215/2572041.shtml

[6] 莫衷一是：美国各监管机构对加密货币的看法仍不一，但监管方向大同小异 https://www.8btc.com/article/21348489

[7] 盘点：各国政府对待数字货币及区块链技术的态度 http://www.sohu.com/a/236725500_100190780

[8] 【三言】欧盟通过加密货币新法案，监管更清晰，市场更利好！ http://www.sohu.com/a/232049834_100117963

[9] 各国政府分别出台了哪些加密货币的监管政策？ http://www.xue63.com/toutiaojy/20180522A1O6B000.html

[10] 马耳他：建立全球首个完整的加密货币监管机制 https://www.jinse.com/blockchain/193230.html

[11] 《金融市场基础知识》. 成都: 西南财经大学出版社, 2015, 236-242

[12] 揭秘加密数字货币三大风险：信用风险、市场与操作风险_搜狐财经 http://www.sohu.com/a/234453293_499199

[13] 《互联网信贷风险与大数据：如何开始互联网金融的实践》. 北京: 清华大学出版社, 2015

[14] 原来，OKEx 和火币 80% 的交易额注水，全球加密交易所约 2/3 交易额系伪造
https://mp.weixin.qq.com/s?__biz=MzI1Mzk4ODIwOA==&mid=2247486845&idx=1&sn=cd3b398b6db5633d311b66ebffa89792&chksm=e9cd5162debad8749d7b658242c5011b5378b668050f46c9528a457796d0d45754a40442a16a&mpshare=1&scene=1&srcid=0828M2VFAhxXeYBwNYqfNZu5#rd

[15] 一文梳理美国、韩国、新加坡区块链政策：“监” 是亲，“管” 是爱_搜狐科技 http://www.sohu.com/a/243013212_257855

[16] 共享财经•数字资产市场发展白皮书（2018）_共享财经 http://www.gongxiangcj.com/posts/7993

[17] 股市交易时间_百度百科 https://baike.baidu.com/item/股市交易时间/1579365

[18] 期货交易_百度百科 https://baike.baidu.com/item/%E6%9C%9F%E8%B4%A7%E4%BA%A4%E6%98%93

[19] 外汇交易时间_百度百科 https://baike.baidu.com/item/%E5%A4%96%E6%B1%87%E4%BA%A4%E6%98%93%E6%97%B6%E9%97%B4

[20] 中国货币网--中国外汇交易中心主办 http://www.chinamoney.com.cn/fe/Channel/10825

[21] 各个期货品种持仓限额_百度文库 https://wenku.baidu.com/view/1abcdfa4b0717fd5360cdc4d.html

[22] 日本经济新闻：数字货币无法强制冻结_区块链新闻_陀螺财经 https://www.tuoluocaijing.cn/kuaixun/detail-7431.html

[23] 股票配资杠杆比例 10 倍合适吗？风险会不会太高？ https://www.xinhehui.com/zt-gppz/view-39010.html

[24] Breaking: ESMA Rolls-Out Draconian CFD Leverage Restrictions, Kills Binary | Finance Magnates
https://www.financemagnates.com/forex/brokers/breaking-esma-rolls-draconian-cfd-leverage-restrictions-kills-binary/

[25] 加密交易团体通过价格操纵获利 8.25 亿美元 http://www.54daxiang.com/web/viewDetail.do?id=394

[26] 过去 6 个月至少 8.25 亿美元交易活动 加密货币价格 遭市场哄抬炒作 https://www.jinse.com/bitcoin/223598.html

[27] 比特币一度崩跌近 25% 因平台技术故障致流动性骤降 http://tech.sina.com.cn/i/2017-11-30/doc-ifypceiq8014268.shtml

[28] 加密货币 —— 近期案例、争议及风险趋势
http://www.kwm.com/zh/hk/knowledge/insights/cryptocurrencies-risks-faced-by-investors-20180607

[29] ShapeShift 因前雇员泄漏数据损失价值 23 万美金的比特币 http://www.freebuf.com/news/102271.html

[30] 迪拜一交易所员工盗取了价值 20 万美元的数字货币 https://www.chainnews.com/articles/559812252201.htm

[31] 又一家比特币交易所被“黑” 这次可能是监守自盗 http://www.sohu.com/a/228226779_119759

[32] 加密货币与银行诈骗，谁更惊悚？ http://www.lianmenhu.com/blockchain-5433-2

[33] 央视揭秘五行币：5000 元一枚，1 年后价值 400 万？ http://money.163.com/17/0409/08/CHINCLR4002580S6.html

[34] 史上最大的 5 大 ICO 骗局，来看看有没有你熟知的？ https://www.wanlianzhijia.com/News/show/id/2157.html

[35] 黑客、骗局和攻击 ：细数 2017 年加密货币市场的灾难事件 http://www.bitcoin86.com/news/19211.html

[36] “一人记一半密钥”，朋友突然离世，400 万美金比特币“石沉大海”！ http://www.sohu.com/a/235371623_481746

[37] 巨头入场数字货币托管，比特币会重回巅峰？ https://www.8btc.com/article/248630

[38] BOX 白皮书 https://www.box.la/

[39] 高盛入场数字货币托管，比特币重回牛市已不远？ https://zhuanlan.zhihu.com/p/41749692

[40] HiveBanks http://hivebanks.com/introduction.html

[41] 监管沙盒 http://wiki.mbalib.com/wiki/%E7%9B%91%E7%AE%A1%E6%B2%99%E7%9B%92?from=singlemessage&isappinstalled=0

[42] 风险评估 http://wiki.mbalib.com/wiki/%E9%A3%8E%E9%99%A9%E8%AF%84%E4%BC%B0

[43] 项目风险分析策略 https://zhuanlan.zhihu.com/p/32794221

[44] 安全风险评价风险矩阵法 https://wenku.baidu.com/view/23995d72e418964bcf84b9d528ea81c758f52eeb.html

[45] 区块链技术在 ABS 领域的应用探讨：如何通俗理解区块链 http://www.360doc.com/content/17/1119/13/46341144_705256841.shtml

[46] 云保链白皮书 https://cichain.io

[47] 链调查评级 A+：首个区块链保险 CIC 评测 https://blog.csdn.net/sinat_41706544/article/details/79312108

[48] 一文读懂数字货币 ETF http://www.sohu.com/a/243447256_100215496

[49] 借道入场步伐加速 7 月迎指数基金热借道 ETF 规模大涨 http://www.cs.com.cn/tzjj/jjdt/201807/t20180730_5849918.html

[50] 指数型基金如何理解？ https://zhidao.baidu.com/question/293991010.html

[51] 2016 指数 ETF 基金排名 https://www.csai.cn/jijin/1130972.html

[52] 区块链在信托中的应用研究（四） http://trust.jrj.com.cn/2018/01/23072723988875.shtml

[53] 火币区块链产业专题报告：钱包篇 http://www.lianmenhu.com/blockchain-5400-27

[54] 全球区块链产业全景与趋势报告 https://www.jianshu.com/p/551014045828