

2017年火币区块链资产评估报告

火币区块链资产研究中心 编写

学术支持：清华大学五道口金融学院互联网金融实验室

北京 2017/6/22

出品： 火币
huobi.com

学术支持： 清华大学五道口金融学院 / 互联网金融实验室
TSINGHUA UNIVERSITY PBC SCHOOL OF FINANCE / FINANCE @ INTERNET LAB

官方媒体： 未央网
www.weiyang.com

目录

页码

1、摘要	3
2、研究目的及方法	4
3、区块链资产梳理	5
4、区块链资产基本介绍	7
4.1、一般数字资产项目简介	7
4.2、匿名数字资产项目简介	12
4.3、智能合约类项目简介	16
4.4、结算兑换类项目简介	17
4.5、区块链平台应用类项目简介	19
5、SMARTChain区块链应用综合量化模型分析	26
5.1、Smart Analysis模型分析	26
5.2、Smart Quantity模型分析	27
5.3、SMARTChain量化模型结论	33

1、摘要

- 区块链近几年获得了大量的关注，中国人民银行行长公开表示人民银行要研究区块链技术；2015年区块链成为美国创投中获得融资最高的板块；26岁少年Vitalik创建的开源区块链平台以太坊，2015年7月上线时市值飙升至10亿美元，成为新晋独角兽。
- 火币此区块链项目评估报告梳理了目前市值排名靠前的区块链资产，了解区块链应用项目的发展状况，通过构建评估模型判断和预测区块链应用项目的发展趋势及投资价值，全报告共分为三个部分：

第一部分：区块链资产梳理

- 主要梳理了交易所上市市值排名靠前的区块链应用项目

第二部分：区块链资产简介

- 研究整理了区块链资产的基本信息，对目前市值排名前二十的项目展开详细介绍

第三部分：SMARTChain区块链应用综合模型分析

- 通过火币SMARTChain区块链应用综合模型，定性和定量分析区块链资产

2、研究目的及方法

本次区块链项目评估报告旨在分析区块链项目的投资价值，尝试量化项目价值，提供投资决策依据；主要采用的研究方法包括：调查研究法、归纳演绎法及模型分析法。

研究目的

区块链的飞速发展和广泛运用必然会对人们的经济生活产生重大影响，对区块链应用项目的发展和价值研究，对行业投资具有重要的指导作用。

判断区块链资产的投资价值

- 目前区块链资产鱼龙混杂，项目价值参差不齐，评估区块链项目的投资价值值得去探索

判断最具价值的区块链应用项目

- 众多公司积极布局区块链在金融、共享经济、云存储等方面的应用
- 区块链在哪些领域存在较高的应用价值，判断探索区块链项目发展潜力值得去探讨

研究方法

此区块链行业研究报告主要采用的研究方法包括以下三类：

调查研究法

- 利用第三方的调查数据、访谈获得最新资料和信息，并对此进行研究开展区块链应用场景发展分析

归纳与演绎法

- 通过区块链现有应用场景项目，归纳总结区块链场景的应用领域
- 基于逻辑或者理论预期模型，观察检验目前区块链应用价值判断是否正确

模型分析法

- 构建区块链综合模型，定性和定量两个层面共同判断研究最具价值的区块链应用项目。

3.1、区块链资产梳理—项目市值

按照全球区块链应用市值统计⁽¹⁾，比特币市值远领先于其他其他区块链项目；国内区块链起步晚、发展缓慢，区块链项目上市较少，且市值小排名较靠后。



(1) 排名数据截止2017年3月
资料来源:火币区块链资产研究中心, 2017; Coinmarketcap.com, 2017年3月

3.2、区块链资产梳理—市值排名

按照全球区块链应用市值排名⁽¹⁾，区块链应用项目市值排名前二十的项目主要为四类应用场景：数字资产、智能合约、全球支付及平台类的应用服务。

排名	项目	市值	排名	项目	市值
1	Bitcoin (比特币)	\$16,924,343,645	11	MaidSafeCoin	\$68,775,450
2	Ethereum	\$4,623,923,391	12	Zcash	\$69,518,210
3	Ripple	\$709,436,837	13	Decred	\$60,742,385
4	Dash (达世币)	\$547,182,661	14	Tether	\$54,953,054
5	Litecoin (莱特币)	\$327,599,714	15	Iconomi	\$53,209,200
6	Monero (门罗币)	\$292,029,561	16	PIVX	\$46,126,710
7	Ethereum Classic	\$260,584,922	17	Steem	\$41,517,800
8	NEM (新经币)	\$131,635,800	18	DigixDAO	\$39,844,000
9	Augur	\$114,136,000	19	Waves	\$38,507,400
10	Golem	\$76,152,416	20	Dogecoin	\$38,506,994

数字资产

- 一般数字资产：比特币、莱特币、NEM、Decred、Dogecoin
- 匿名数字资产：Dash、Monero 及 Zcash、PIVX

智能合约



全球支付



平台类的应用服务

基于区块链打造的市场预测平台、去中心化的云存储平台、计算资源交易平台、社交内容平台等等

(1) 排名数据截止2017年3月31日
资料来源：火币区块链资产研究中心，2017；Coinmarketcap.com, 2017

4.1.1、项目介绍——一般数字资产：比特币

比特币诞生于2009年，是一种建立在全球分布式网络上、没有央行和第三方机构参与发行、总量固定的加密数字资产。

比特币去中心化、不可篡改等特征克服了以往中心化交易成本高、效率低、信息掌握在少数人手工等弊端

比特币技术参数

- 研发者：Satoshi Nakamoto
- 核心算法：SHA-256
- 发布时间：2009年1月9日
- 共识机制：POW
- 发行总量：2100万
- 区块时间：10分钟
- 区块奖励：当前12.5BTC/区块
- 减半时间：4年
- 已发行量：1629万枚



比特币特色、不足与风险

- 主要特色
 - 数字资产的创始者：公众认可度高、信任度高
 - 流通广：世界各国对比特币的接受度较高，受众广
- 不足之处
 - 随着用户的增长，区块容量不足
 - 确认时间长
- 风险
 - 扩容之争，存在潜在的分叉风险

4.1.2、项目介绍——一般数字资产：比特币

比特币 (Bitcoin) 诞生于2011年11月9日，是一种分布式加密数字资产，人气高、国内几大交易网站均支持比特币交易。

比特币受到了比特币的启发，并且在技术上具有相同的实现原理，旨在改进比特币，与比特币相比具有诸多优点，在数字资产中享有很高的地位，因此又有“比特币，莱特银”的说法。

莱特币技术参数

- 研发者：Charls Lee
- 核心算法：Script
- 发布时间：2011年11月9日
- 发行总量：8400万
- 减半时间：4年
- 共识证明：POW
- 区块时间：2.5分钟
- 区块奖励：最初50LTC，当前25LTC
- 已发行量：5081万



莱特币特色、不足与风险

- 主要特色
 - 发行量大：相比比特币发行量，莱特币是其4倍，为8400万
 - 交易快速：确认时间只要2.5分钟，交易过程比比特币更加迅速
 - 隔离验证激活
- 不足之处
 - 莱特币的推广工作止步不前
 - 相关应用还较少
- 风险
 - 隔离验证后，网络的漏洞风险

4.1.3、项目介绍——一般数字资产：新经币

新经币 (New Economy Movement) 诞生于2015年4月1日，是第一个采用测试驱动的开发模式开发出的数字资产。

新经币平台从头到尾使用Java开发，融入了智能合约功能，能够处理和开展主流用途的手机应用，在设计之初就意图打造成一个对用户友好的平台。

新经币技术参数

- 研发者：NEM团队
- 共识机制：重要性证明（根据交易量、活跃度等维度而不是工作量决定区块奖励的归属。）
- 发布时间：2015年4月1日
- 发行总量：90亿
- 区块时间：60秒
- 区块奖励：交易手续费
- 已发行量：90亿



新经币特色、不足与风险

- 主要特色
 - 融合智能合约功能：提供基于规则的解决方案，通过智能合约自动触发一连串规定动作
- 不足之处
 - 市场推广不够，关注较少
- 风险
 - 目前POI算法机构采用少，算法的可用性存在一定风险

4.1.4、项目介绍——一般数字资产：Decred

Decred诞生于2016年2月8日，与比特币类似，但重点强调社区投入、公开治理和可持续挖矿的数字资产。

Decred旨在成为开放性和进步性的数字资产，任何人只要愿意均可以参与项目治理，并引入POW+POS机制，目的是在POW矿工和POS选民中取得平衡。

Decred技术参数

- 研发者：btcsuite开发人员
- 核心算法：Blake-256
- 发布时间：2016年2月8日
- 发行总量：2100万
- 共识证明：POW+POS
- 区块时间：5分钟
- 区块奖励：25.82DCR（每21天调整一次）
- 已发行量：518万



Decred特色、不足与风险

主要特色

- **POW+POS共识机制**：POW打包记账+POS投票治理，两者结合制衡矿工和选民的权利

不足之处

- 确认流程繁琐，时间较长

风险

- POW与POS结合的共识机制，存在矛盾冲突、网络不稳定的风险

4.1.5、项目介绍——一般数字资产：狗狗币

狗狗币 (DogeCoin) 诞生于2013年12月8日, 是结合Doge文化产生的一种分布式加密数字资产, 在欧美地区比较受欢迎。

狗狗币与其他数字资产不同, 有自己的核心文化, 好多人参与狗币交易, 并不是为了投机才参与其中, 而是把它作为了一种表达分享和感恩的方式。

狗狗币技术参数

- 研发者: Jackson Palmer & Shibetoshi Nakamoto
- 核心算法: Scrypt
- 发布时间: 2013年12月12日
- 发行总量: 1000亿, 挖完后增加50亿/年, 减半时间约为2个月
- 共识证明: 辅助工作量验证机制 (AuxPoW), 与莱特币合并挖矿
- 区块时间: 60秒
- 区块奖励: 100000Doge



狗狗币特色、不足与风险

主要特色

- 小费文化: 狗币是靠小费发展起来的, 比特币价格偏高, 所以更便宜的DogeCoin更适合网络打赏
- 交易便捷: 确认时间短, 转账快

不足之处

- 由于狗狗币交易量大且区块时间短, 从而导致区块占硬盘大

风险

- 发行总量没有限额, 存在通货膨胀风险

4.2.1、项目介绍—匿名数字资产：达世币

达世币 (Dash) 诞生于2014年1月18日，是一款支持即时交易、以保护用户隐私为目的的数字资产。

达世币与其他数字资产不同，其匿名程度较比特币更高，交易无法被追踪查询，对于不想暴露交易记录和财政隐私的用户是理想选择。

达世币技术参数

- 研发者：eduffield
- 核心算法：X11算法
- 发布时间：2014年1月18日
- 发行总量：2200万
- 共识证明：POW+POS混合挖矿
- 区块时间：2.5分钟
- 区块奖励：3.6Dash
- 已发行量：725万
- 难度调整算法：DGW



达世币特色、不足与风险

- 主要特色
 - 匿名属性：达世币通过使用相同面值和被动现金的混币技术实现强匿名
 - 区块奖励：奖励由公式自动确定
 - 挖矿创新：采用11种加密算法
- 不足之处
 - 目前技术门槛较高
- 风险
 - POW+POS混合机制易产生冲突，机制不稳定风险

4.2.2、项目介绍—匿名数字资产：门罗币

门罗币 (Monero) 诞生于2014年4月18日，是一种使用CryptoNote协议的虚拟币币种，具有隐私性、去中心化、拓展性三大特点。

门罗币与其他数字资产不同，通过数字环签名提供更好的匿名性，目前国内对该币种匿名技术宣传较少，国外知名度较高。

门罗币技术参数

- 研发者：门罗币团队
- 核心算法：CryptoNote
- 发布时间：2014年4月18日
- 发行总量：1844万
- 区块时间：60秒
- 区块奖励：7.8XMR
- 已发行量：1436万
- 共识机制：POW



门罗币特色、不足与风险

- 主要特色：一次性环签名
 - 首先将签名者的公钥和另外一个公钥集合进行混合
 - 然后在对消息进行签名，使得外界无法区分集合中哪个公钥对应真正的签名者
- 不足之处
 - 在国内尚未进行推广
- 风险
 - 用户基础小，易出现流通低情况，流通风险大

4.2.3、项目介绍—匿名数字资产：Zcash

Zcash诞生于2011年11月9日，是首个使用零知识证明机制的区块链系统，它可提供完全的支付保密性。

Zcash灵感来源于比特币，代币的供应形式也与比特币极其相似，例如2100万总量和4年减半机制，并进一步完善了匿名功能方面的不足。

Zcash技术参数

- 研发者：Zooko Wilcox
- 核心算法：Equihash
- 发布时间：2016年10月
- 发行总量：2100万
- 共识证明：POW（但前4年20%所得自动分配给Zcash团队和投资者）
- 区块时间：2.5分钟
- 区块奖励：12.5ZEC
- 减半时间：4年
- 已发行量：117万



Zcash特色、不足与风险

- 主要特色：零知识证明机制
 - 不用向对方展示可证明身份的密钥，即可向对方证明身份
 - 极大程度保证了资金安全和身份保密性。（如：在不给失主看钱包的情况下证明钱包是失主的）
- 不足之处
 - 屡屡出现问题（2016年11月短期内出现7个漏洞）
- 风险
 - 系统不稳定，技术风险大

4.2.4、项目介绍—匿名数字资产：PIVX

PIVX诞生于2016年2月1日，是一种分布式加密数字资产，在匿名和交易安全性方面表现突出。

PIVX的运行基于Bitcoin core 0.10.x代码库，旨在实现近乎即时的私人支付交易，为所有使用者带来便利。

PIVX技术参数

- 研发者：PIVX团队
- 核心算法：Quark
- 发布时间：2016年2月1日
- 发行总量：无限制
- 发行速度：每年大约增长260万
- 共识证明：POW转为POS2.0
- 区块时间：60秒
- 区块奖励：4.32PIVX
- 已发行量：5314万



PIVX特色、不足与风险

- 主要特色：匿名属性
 - 通过使用相同面值和被动现金的混币技术实现强匿名
 - 将金额等分拆为几个固定金额，再拆分为几笔交易转入目标账户
- 不足之处
 - 代码创新不够
- 风险
 - 总量不限额，存在通货膨胀风险
 - POW转POS，存在后期技术不兼容风险

4.3、项目介绍—智能合约项目：ETH & ETC

区块链2.0重要的是智能合约、智能资产，以太坊在智能合约领域一直处于领先地位，后经过硬分叉形成了Ethereum (ETH) 和Ethereum Classic (ETC)。

以太坊是一个平台和一种编程语言，支持众多的高级功能，包括用户发行代币、智能合约、去中心化的交易或去中心化自治公司应用。

	技术参数（技术两者基本无差异，ETH发行总量无限额，ETC发行总量限额）	运营参数	风险
ETH	<ul style="list-style-type: none">• 研发者：以太坊团队• 核心算法：Ethereum• 发布时间：2015年3月20日• 发行总量：6000万+1872万/年• 共识机制：POW• 区块时间：12s• 区块奖励：5• 流通个数：9155万	<ul style="list-style-type: none">• 开发者人数：原以太坊团队• 哈希率：23924GH/s• 网络哈希占比：92.47%• 投资工具：ETH交易基金ETF	<ul style="list-style-type: none">• 共识机制将从POW转为POS，存在系统不兼容风险• The DAO事件更改了技术代码，存在恶意更改代码的风险
ETC	<ul style="list-style-type: none">• 研发者：以太经典团队• 核心算法：Ethereum• 发布时间：2015年11月1日• 发行总量：2.1亿，每500万个区块减速20%• 共识机制：POW• 区块时间：12s• 区块奖励：5	<ul style="list-style-type: none">• 开发者人数：4位• 哈希率：1948GH/s• 网络哈希占比：7.53%• 投资工具：以太坊信托基金	<ul style="list-style-type: none">• 网络哈希占比逐渐减少，存在网络不稳定的风险

4.4.1、项目介绍—结算兑换类项目：Ripple

区块链在金融领域备受关注，全球结算的Ripple是目前区块链金融应用较成功的应用之一。

Ripple是基于一个开放、中性协议构建的，支持全球不同分类账和网络之间即时、确定、低成本的国际支付

Ripple参数

技术参数

- 研发者：Ripple Labs
- 核心算法：OpenCoin算法
- 共识机制：协议共识 (RPCA)
- 发布时间：2011年04月18日
- 发行总量：一十亿
- 区块时间：秒到
- 已发行量：37,955,579,225 XRP

运营参数

- Top50银行中与Ripple合作的银行数：15
- 外汇交盘的覆盖范围为87%
- 2016年6月13日，Ripple从纽约金融服务部获得了虚拟货币许可证

XRP分配机制及风险

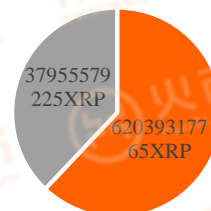
分配机制

- Ripple 的架构不要求挖矿，其代币XRP可在Bitstamp、Gatehub及Kraken上购买获得
- 目前Ripple主要通过业务开发交易来分发 XRP，奖励那些更小差价的流动性提供商，并向有兴趣投资 XRP 的机构销售 XRP

风险

- Ripple团队持有超过50%的代币，存在团队恶意操控币价的风险

瑞波币持有
占比

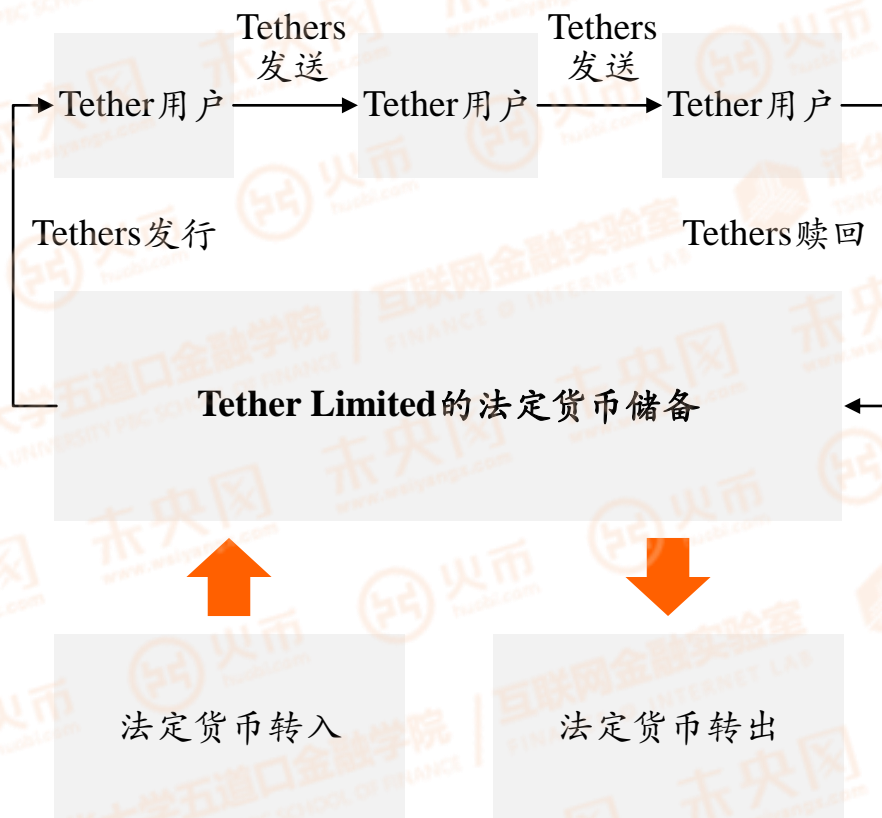


■ Ripple
■ Others

4.4.2、项目介绍—结算兑换类项目：Tether

为确保代币交易价格的稳定性，Tether基于法定货币产生的等值数字资产，可实现法定货币与数字资产的等值兑换。

Tether的代币与美元价值绑定，与美元维持一对一兑换比率，1美元=1 USDT



分配机制

- 发布时间：2014年6月10日
- 代币总量：64951600
- 现流通量：62399949
- 共识机制：POR储备证明
- 用户通过Tether Limited 发行Tether，发行的Tether数量等于用户存放的法定货币金额
- 用户可在Tether Limited赎回法定货币，将储存的Tethers兑换成法定货币
- 用户在二级市场上可相互流通、交易Tether

风险

- Tether能冻结和没收资金，存在资金没收风险
- 套利风险，由于Tether赎回有一定的时延，Tether在二级市场的流通价格可能会低于1美元

4.5.1、项目介绍—平台应用类：Augur市场预测平台

Augur基于以太坊区块链打造去中心化预测平台，用户基于强大的预测数据对未来事件展开预测，对正确预测未来事件的用户支付奖励。

Augur用户可在预测市场基于事件的结果对赌以获得奖励，资金存储于智能合约中，可以有效地消除对手方的风险和中心化的服务器

账户充值

创建预测市场

- 提交对新预测市场的描述和问题，应该是一个是或者不是的问题
- 输入打算提供的初始流动量，并设置交易费
- 选择一个到期日，应该是事件发生后的某时

参与预测市场

- 选择事件，购买事件结果的股票
- 如果你认为事件将发生，就购买“yes”股，否则购买“no”
- 股票的当前市场价格是对事件概率的预估

事件结果报告

■ REP分配

- 发行总量：11000000 REP，80%出售给公众
- 用户可在Poloniex、Kraken、Bittrex、Gatecoin和ShapeShift购买REP，大量购买可与Augur团队联系
- 用户通过现金、Augur代币REP及以太坊进行账户充值

■ 风险

- 预测市场在美国存在很大的监管阻力，存在由于美国政府施加压力而关闭的风险

4.5.2、项目介绍—平台应用类：MaidSafe去中心的云存储平台

MaidSafe借助区块链打造去中心化的云存储平台，网络完全开放，任何人都可以参与其中；通过在全网统一地发放奖励，从而激励节点自我保护管理网络数据。

MaidSafe将用户数据加密分布在网络中，用完全去中心化架构来取代互联网昂贵的数据中心

- 发布时间：2006年2月3日
- 代币总量：40亿
- 共识机制：POR资源量证明，验证节点及确定节点对网络的贡献
- 自加密：用户文件上传至safe网络，文件将自动分解成块，块自动加密

工作原理



风险

- 技术风险：POR共识算法的稳定性存在风险
- 市场风险：safecoin目前的受众及认可度还不高，用户基数少，其代币价格市场波动风险较大

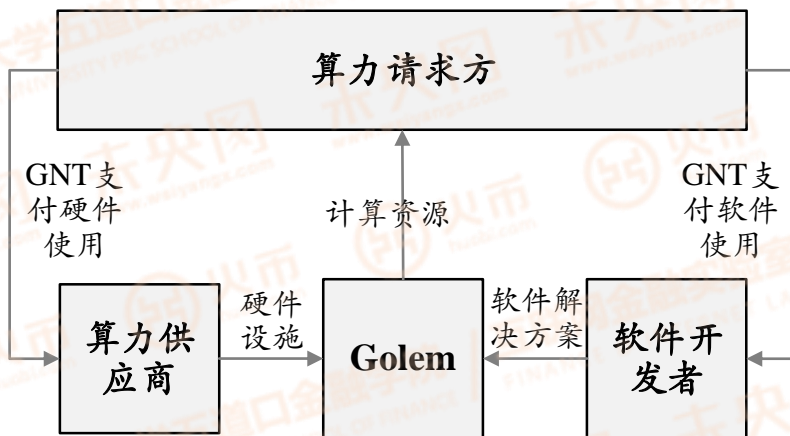
4.5.3、项目介绍—平台应用类：Golem计算资源交易平台

Golem聚合算力供应商，打造基于区块链打造计算资源交易平台，允许用户通过网络交易计算资源，实现计算能力的全球共享。

Golem基于智能合约实现参与者的直接支付，参与者分为算力资源卖家、把需要计算任务上传到网络的任务创建者以及软件开发者，通过其网络代币GNT支付酬劳。

- Golem的网络代币GNT在众筹阶段创建，是算力请求方使用设备资源并对算力供应商及软件开发者支付酬劳的唯一币种。
- GNT代币基于广泛应用的以太坊平台，使用以太坊钱包即可管理
- 代币总量为10000000000，1ETH=1000GNT

工作原理



风险

- **技术风险：**计算资源共享需要强大的算力技术支持，算力能否达到需求存在一定的风险
- **市场风险：**Golem发展与平台参与者的数量存在强相关，商业模式替代性强，未来其发展市场风险较大

4.5.4、项目介绍—平台应用类：Iconomi数字资产管理平台

Iconomi是基于以太坊区块链打造开放式的数字资产管理平台，是一种能够访问各种数字资产和数字资产阵列（DAA）的应用程序。

在**Iconomi**上，用户从各种数字资产创建自己的数字资产阵列（DAA），管理并比较自己与他人的表现，从而吸引支持者，从中获得一部分收益。

Iconomi资产管理金融工具

■ ICNX (ICONOMI.INDEX)

- 是很多流行数字资产组成的指数型投资基金
- 衡量符合ICONOMI资格标准的数字资产的表现
- 可帮助最大限度地降低风险

■ ICONOMI.PERFORMANC

- 主动型管理基金，以高收益预期为目标，由获得证书的专家级交易员进行管理

Iconomi资产管理平台特点及风险

■ 特点

- **信誉评分**：通过DAA的管理记录在社区中建立声誉，来吸引支持者，增加收益
- **购买便捷**：可在几秒内同时购买多种数字资产
- **有效管理DAA**：可通过与竞争对手对比以优化自己的DAA，且可和其他用户分享

■ 风险

- 市场波动较大，市场流动性风险大
- 技术相关较少，稳定性风险大

4.5.5、项目介绍—平台应用类：Steem社交内容平台

STEEM是一个基于区块链的社交内容平台，将社交媒体的概念与数字资产社区建设相结合，以虚拟资产回报的方式激励人们参与社交内容和在线社区。

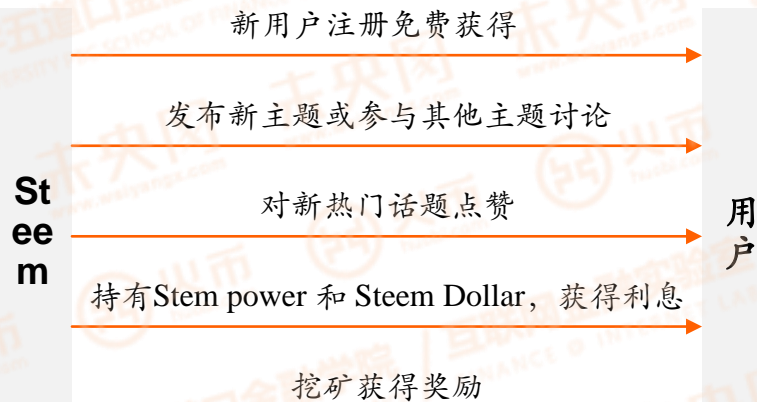
Steem奖励报酬分为Steem、Steem Power及Steem Dollars三种形式，之间可相互转换

Steem可直接流通购买，或通过论坛上发表或参与讨论主题获得奖励；Steem Power不可直接使用，需转换为steem，另外Steem Power越多，用户发表的话题更易置顶；持有STEEM美元可获得相应的利息

奖励机制

- Steem构建经济激励机制，推出对个人贡献内容进行打分的算法，对贡献内容进行评估和提供奖励，推动社区发展

Steem奖励



技术参数及风险

技术参数

- 研发者：Steem团队
- 发行总量：252332270 STEEM
- 区块时间：3s
- 算法：elliptic curve signature verification椭圆曲线签名核验算法
- 共识机制：工作量证明和投票证明；挖矿主要采用工作量证明，其平台内容评估主要采用投票证明
- 块交易吞吐量：每秒10000或更多笔

风险

- Steem链上的流通性较低，网络可用性存在一定风险

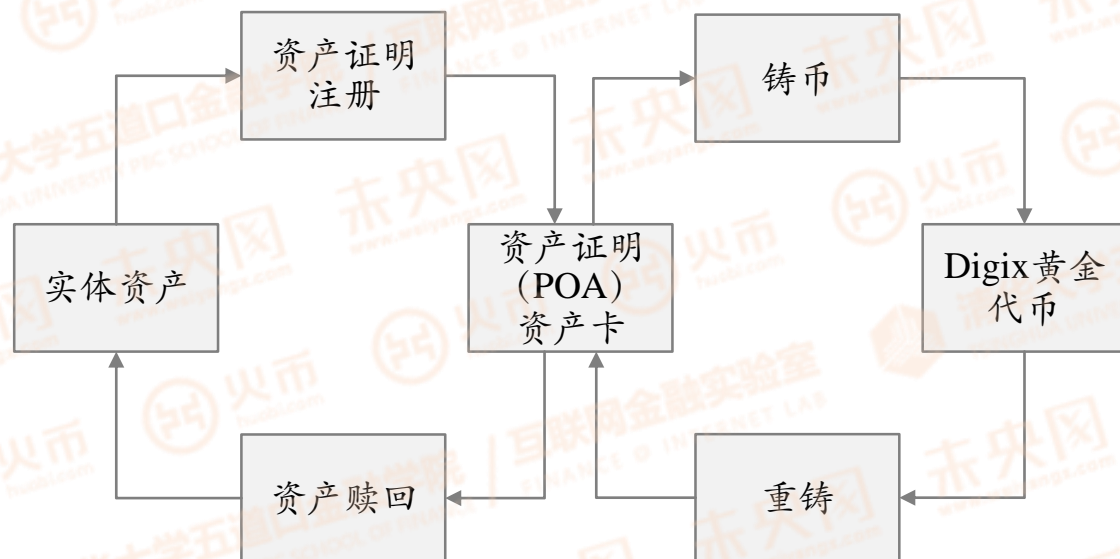
4.5.6、项目介绍—平台应用类：DigixDAO数字代币化平台

Digix是一个基于以太坊区块链构建的资产代币化平台，开发了一个证明资产存在和所有权的制度，证明记录将会通过IPFS 和Ethereum永久性地发布。

DigixDAO通过它的资产证明（PoA）协议为实体资产代币化和文档化提供了使用实例

- Digix的PoA协议利用以太坊和星际文件系统（IPFS）通过监管链（chain of custody）追踪资产
- Digix无需一个中心化数据库，实现了开放和公开的资产存在性认证
- Digix提供一个应用程序接口（API），允许其它应用建立在其资产代币化服务之上

运行机制



风险

- 链上交易流通不足，网络的可用性存在一定的风险
- 流通风险：代币流通性较低，流通性风险较大
- 市场风险：目前其市场关注及用户基础较少，市场风险较大

4.5.7、项目介绍—平台应用类：Waves可定制代币平台

Waves是基于区块链的可定制代币平台，允许用户直接在区块链上发行、转账和交易可定制的代币，其主要的价值定位于更容易地进行融资、众筹和区块链金融工具。

Waves发布1亿社区代币，用于通过周期性的激励来奖励WAVES的持有者以及参与社区；另外平台的参与者需持有WAVES代币才可在平台上进行其他功能操作。

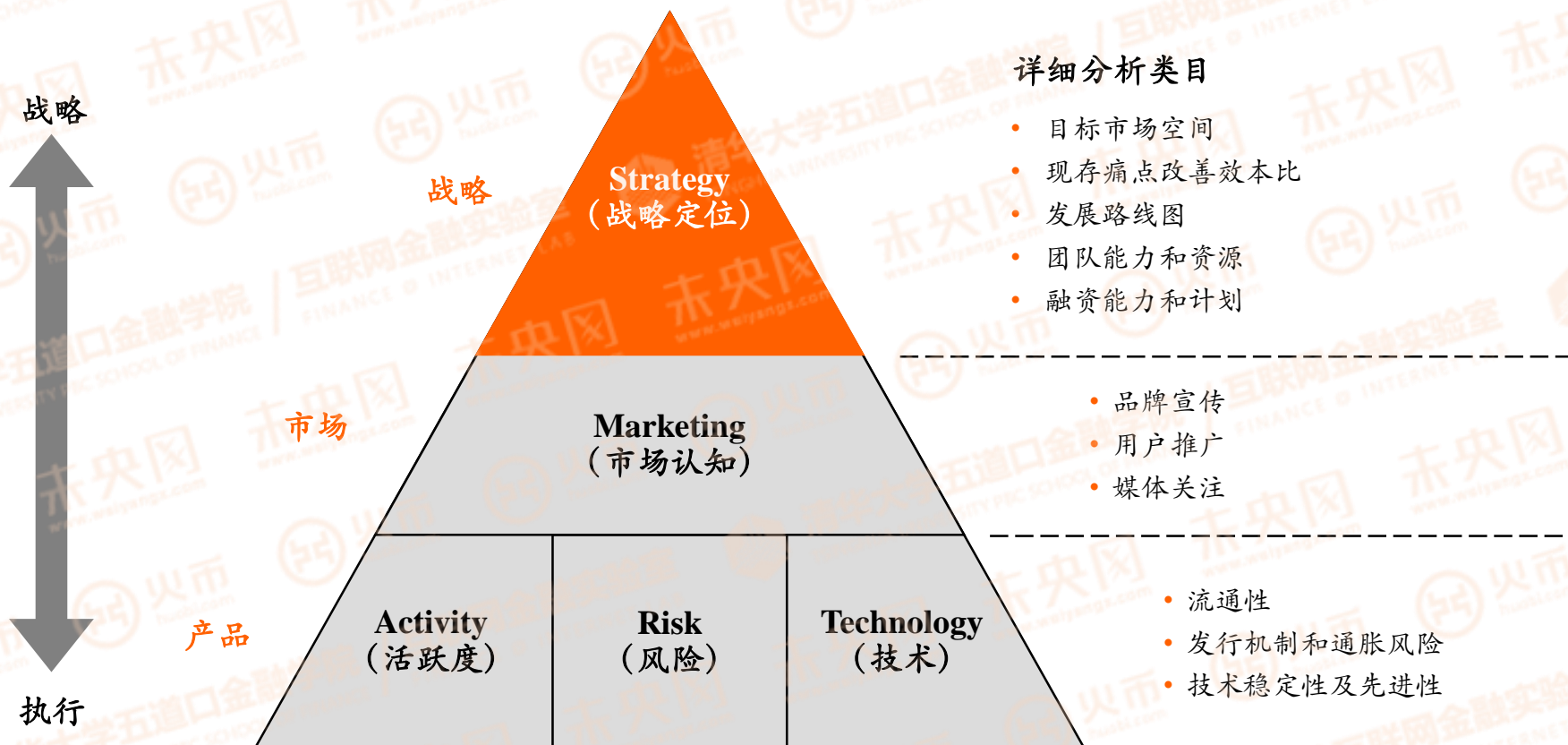
- 共识机制：对POS机制进一步增强，采用租用POS机制，减少交易时间且增加交易吞吐量
- 轻量级的客户端：采用搭建在Scorex平台之上的双层结构，无需大量的存储空间和加速应用的开发

平台功能		风险
代币定制	平台允许用户可直接在区块链上发行自己的定制代币	<ul style="list-style-type: none">• 分布式自治易遭到黑客攻击，网络稳定性存在一定的风险• 链上交易流通性不足，网络可用性存在一定的风险• 代币流通性低，市场波动较大
去中心化交易所	代币之间可以直接在Waves平台上进行交易，而不需要将两种代币分别单独与基准货币进行交易	
去中心化众筹	WAVES内置了自己的众筹平台Crowstarter，允许企业家发行众筹代币，以去中心化的方式来发起自己的项目	
法币网关	平台将国家货币通过兼容网关运营商进行整合，允许用户以很低的成本以及很快的速度在区块链上转账法币	

5.1、SMARTChain^{beta} 综合模型：Smart Analysis

火币构建了SmartChain模型，旨在使投资研究更加清晰智能，有助于投资者获得更有价值的区块链信息。整套火币SMART模型包括Smart Analysis和Smart Quantity。

Smart Analysis基于战略、市场及产品三个层面打造专业的区块链项目研究工具



5.2.1、Smart Quantity—量化因子

火币Smart Quantity模型对Smart Analysis定性分析进行量化，通过最佳的建模技术开发而出。适用于全球区块链应用和市场环境，帮助投资者在多元化的区块链应用中获取更高回报。

Smart Quantity选取符合基本经济学原理的影响因子，多角度量化产生更深入的见解

火币SMARTChain量化模型每月更新一次项目量化因子的评分数据；每季度基于coinmarket.cap上项目市值排名，重新更新评级项目

Strategy

战略定位

- 可比现实市场规模
- 现存痛点与区块链应用相关性

Marketing

市场认知

- 新闻资讯报道评分⁽¹⁾

Activity

活跃度

- 重点交易市场接受度
- 全球交易活跃度

Risk

风险

- 发行机制风险
- 代币通胀风险

Technology

技术先进性

- 技术稳定性和先进性
- 联盟实力

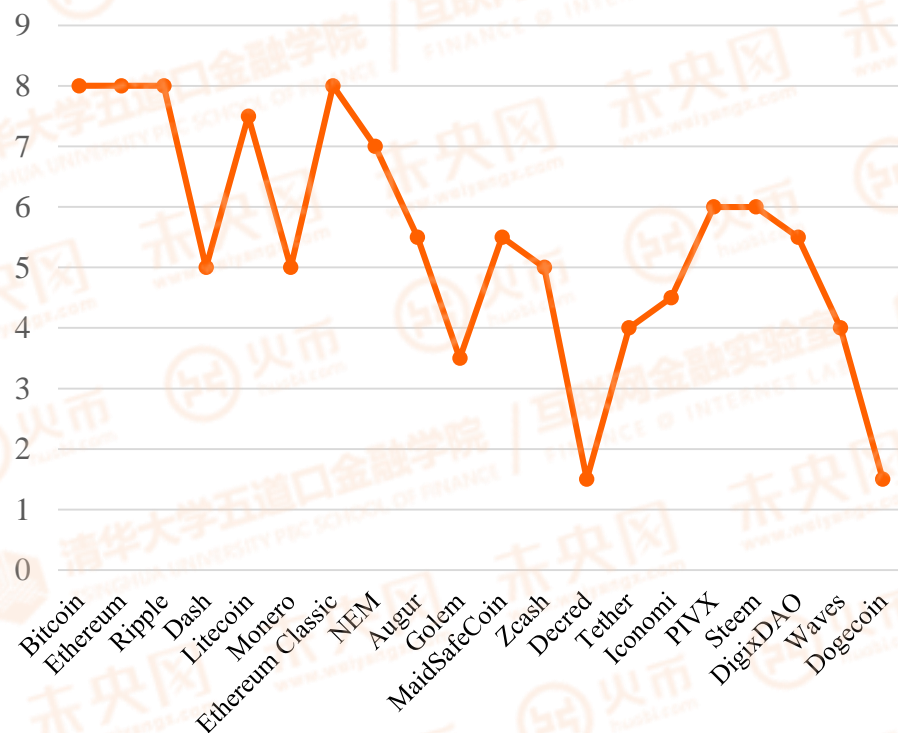
(1) 以动态市场关注以及搜索为依据
资料来源:火币区块链资产研究中心, 2017

5.2.2、Smart Quantity—战略量化分数 (1)

战略定位主要从项目的现实市场规模及与区块链的相关性评估，战略评分越高表示区块链项目的可发展空间大，否则反之。基于评分可看出比特币和以太坊的发展前景较大。

项目	现实市场规模	相关性	Strategy评分
Bitcoin	9	7	8
Ethereum	7	9	8
Ripple	9	7	8
Dash	5	5	5
Litecoin	8	7	7.5
Monero	5	5	5
Ethereum Classic	7	9	8
NEM	7	7	7
Augur	5	6	5.5
Golem	4	3	3.5
MaidSafeCoin	4	7	5.5
Zcash	5	5	5
Decred	3	0	1.5
Tether	5	3	4
Iconomi	7	2	4.5
PIVX	6	6	6
Steem	6	6	6
DigixDAO	5	6	5.5
Waves	4	4	4
Dogecoin	3	0	1.5

火币Smart Quantity模型战略量化图



(1) 9分为最高分，0分为最低分

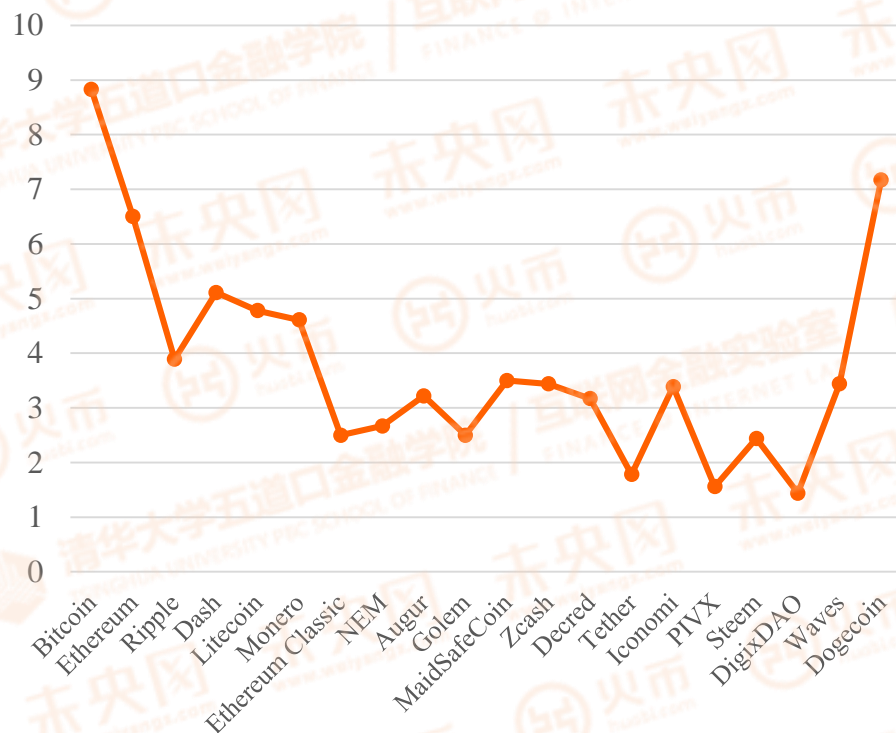
资料来源:火币区块链资产研究中心，2017；Google及区块链应用项目团队访谈，2017

5.2.3、Smart Quantity—市场量化分数 (1)

市场认知主要考察项目的市场关注度及用户搜索热度，市场评分越高表明市场对项目反应高，用户认知高；否则反之。基于评分可看出比特币的用户认知高，狗狗币次之。

项目	市场关注增长	市场搜索指数	市场评分
Bitcoin	9.00	8.50	8.83
Ethereum	7.00	5.50	6.50
Ripple	4.33	3.00	3.89
Dash	4.67	6.00	5.11
Litecoin	5.67	3.00	4.78
Monero	4.67	4.50	4.61
EthereumClassic	3.00	1.50	2.50
NEM	3.00	2.00	2.67
Augur	4.33	1.00	3.22
Golem	3.00	1.50	2.50
MaidSafeCoin	3.00	4.50	3.50
Zcash	3.67	3.00	3.44
Decred	3.00	3.50	3.17
Tether	1.67	2.00	1.78
Iconomi	3.33	3.50	3.39
PIVX	2.33	0.00	1.56
Steem	2.67	2.00	2.44
DigixDAO	1.67	1.00	1.44
Waves	3.67	3.00	3.44
Dogecoin	8.00	5.50	7.17

火币Smart Quantity模型市场量化图



(1) 9分为最高分，0分为最低分

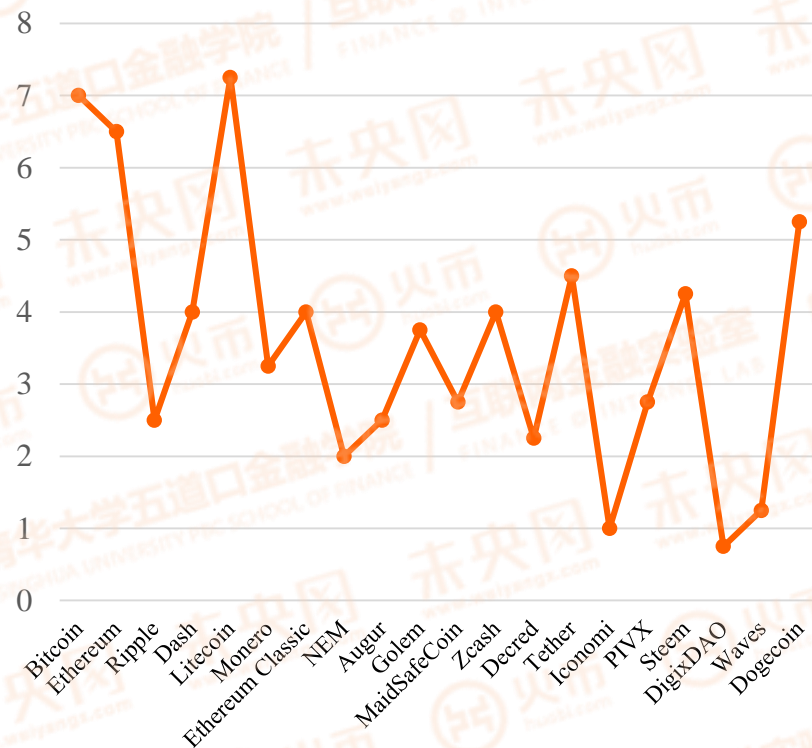
资料来源:火币区块链资产研究中心，2017；Google及区块链应用项目团队访谈，2017

5.2.4、Smart Quantity—活跃度量化分数 (1)

项目活跃度考虑项目代币交易活跃度及块交易活跃度两个层面，活跃度评分越高表明项目市场流通性好；否则反之。基于评分可看出莱特币市场流通较好，比特币次之。

项目	交易市场	重点交易市场上市	日成交量 换手率	日块交易 换手率	活跃度 评分
Bitcoin	8	9	3	8	7.00
Ethereum	6	8	3	9	6.50
Ripple	3	6	1	0	2.50
Dash	4	7	5	2	4.00
Litecoin	8	8	9	4	7.25
Monero	2	7	4	0	3.25
EthereumClassic	2	8	5	1	4.00
NEM	1	6	1	0	2.00
Augur	2	6	2	0	2.50
Golem	1	5	7	2	3.75
MaidSafeCoin	1	6	2	2	2.75
Zcash	3	7	6	3	4.00
Decred	1	5	3	0	2.25
Tether	3	6	9	0	4.50
Iconomi	1	1	1	1	1.00
PIVX	1	2	3	5	2.75
Steem	2	6	9	0	4.25
DigixDAO	1	2	0	0	0.75
Waves	2	2	1	0	1.25
Dogecoin	7	6	7	1	5.25

火币Smart Quantity模型活跃度量化图



(1) 9分为最高分，0分为最低分

资料来源:火币区块链资产研究中心，2017；区块浏览器及区块链应用项目团队访谈，2017

5.2.5、Smart Quantity—风险量化分数 (1)

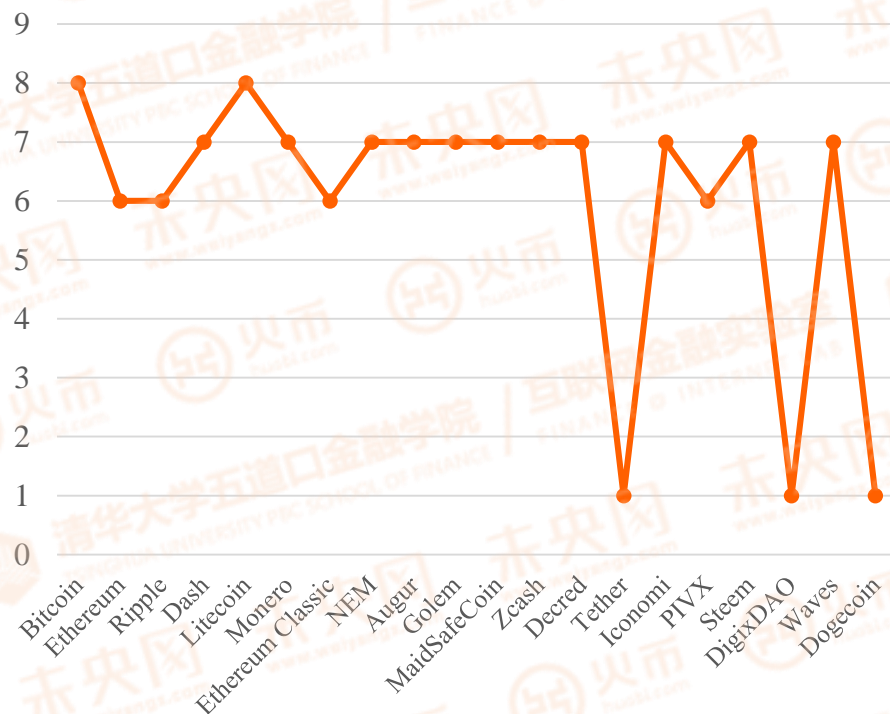
Risk衡量该项目代币的发行机制风险及通胀风险，风险评分越高表明推动项目的信用及通胀风险小；否则反之。基于评分可看出比特币、达世币、Zcash等通胀风险小。

项目	风险评分
Bitcoin	8
Ethereum	6
Ripple	6
Dash	7
Litecoin	8
Monero	7
Ethereum Classic	6
NEM	7
Augur	7
Golem	7
MaidSafeCoin	7
Zcash	7
Decred	7
Tether	1
Iconomi	7
PIVX	6
Steem	7
DigixDAO	1
Waves	7
Dogecoin	1

(1) 9分为最高分，0分为最低分

资料来源:火币区块链资产研究中心，2017；区块链应用项目团队访谈，2017

火币Smart Quantity模型风险量化图

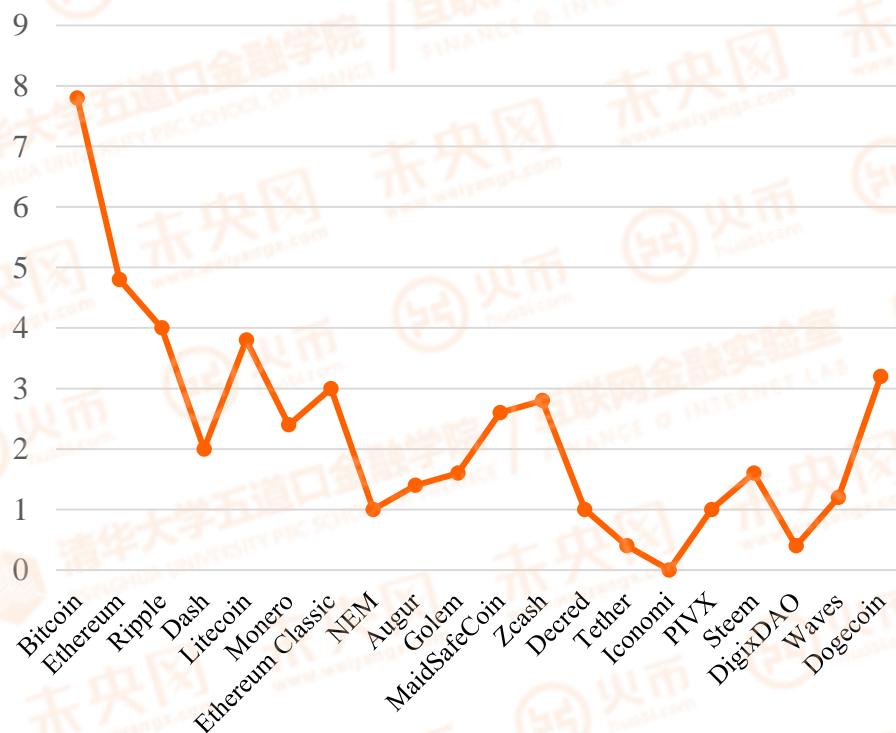


5.2.6、Smart Quantity—技术量化分数 (1)

项目技术主要考量项目使用的稳定性、代码的先进性及代码联盟实力，评分越高表明项目技术可用性较高，否则反之。基于评分可看出比特币技术可用性高，以太坊次之。

项目	稳定性	先进性	联盟实力	技术评分
Bitcoin	3	9	9	7.8
Ethereum	0	6	6	4.8
Ripple	2	4	5	4
Dash	2	3	1	2
Litecoin	5	4	3	3.8
Monero	2	3	2	2.4
Ethereum Classic	1	6	1	3
NEM	1	1	1	1
Augur	1	2	1	1.4
Golem	0	3	1	1.6
MaidSafeCoin	3	3	2	2.6
Zcash	0	5	2	2.8
Decred	1	1	1	1
Tether	2	0	0	0.4
Iconomi	0	0	0	0
PIVX	1	1	1	1
Steem	0	3	1	1.6
DigixDAO	0	1	0	0.4
Waves	0	2	1	1.2
Dogecoin	2	4	3	3.2

火币Smart Quantity模型技术量化图



(1) 9分为最高分，0分为最低分

资料来源:火币区块链资产研究中心，2017；区块链应用项目团队访谈，2017

5.3、火币全球区块链资产评估排名 —— Huobi Ranking beta

火币Smart Quantity模型量化分析结果基本可以判断相关区块链应用的发展潜力。比特币综合量化分数最高，符合比特币截至目前是区块链最成功应用的事实。

Item	Strategy	Marketing	Activity	Risk	Technology	Total (HR Score)
Bitcoin	8	8.83	7	8	7.8	88.07
Ethereum	8	6.50	6.5	6	4.8	70.67
Litecoin	7.5	4.78	7.25	8	3.8	69.62
Ripple	8	3.89	2.5	6	4	54.20
Ethereum Classic	8	2.50	4	6	3	52.22
Dash	5	5.11	4	7	2	51.36
Zcash	5	3.44	4	7	2.8	49.43
Monero	5	4.61	3.25	7	2.4	49.47
MaidSafeCoin	5.5	3.50	2.75	7	2.6	47.44
Steem	6	2.44	4.25	7	1.6	47.32
Dogecoin	1.5	7.17	5.25	4	3.2	46.93
NEM	7	2.67	2	7	1	43.70
Augur	5.5	3.22	2.5	7	1.4	43.60
Golem	3.5	2.50	3.75	7	1.6	40.78
PIVX	6	1.56	2.75	6	1	38.46
Waves	4	3.44	1.25	7	1.2	37.54
Iconomi	4.5	3.39	1	7	0	35.31
Decred	1.5	3.17	2.25	7	1	33.15
Tether	4	1.78	4.5	1	0.4	25.95
DigixDAO	5.5	1.44	0.75	1	0.4	20.21

(1) 9分为最高分，0分为最低分

数据截至2017年5月31日，火币区块链资产研究中心会定期更新火币SMARTChain模型和评估指标，并重新评估和更新结果。

感谢阅读

您的建议非常宝贵，欢迎随时与我们沟通！



Tel: 010-6298 7670

Email: blockchain@huobi.com

Add: 北京海淀区西二旗中路良
盛大厦2层 (100085)



清华大学五道口金融学院 / 互联网金融实验室
TSINGHUA UNIVERSITY PBC SCHOOL OF FINANCE / FINANCE @ INTERNET LAB

Tel: 010-7279 9551

Email: weiyangx@pbcfsf.tsinghua.edu.cn

Add: 北京市海淀区成府路43号五道口金
融学院 (100083)