


2018年10月11日区块链技术晚报 第28期

一.Tech News

 比特币侧链 Liquid Network 正式上线 寻求减轻交易流动性问题

旧金山新创业者 Blockstream 公司策略长 Samson Mow 在 10 日 宣布 推出比特币侧链「Liquid Network」。这是个承诺让数位货币结算更快且更安全的交易平台。这个平台连结世界各地的加密货币交易所、经纪公司与金融机构， 迄今为止，已有包括 20 多家公司签约合作， 包括 Bitfinex、Bitmex、OKCoin 等交易所。

Samson Mow 表示，

这个侧链的目标是改善流动性， 因为流动性一直是市场上的问题，交易所之间的流动性肯定还不存在，随着 Liquid 的出现， 加上更快的结算时间， 我们应该能够透过让移转更快且更容易的方式来改善流动性。

Blockstream 公司将 Liquid 描述为一种「在比特币网络上的创新侧链， 可促进企业与个人之间加速比特币交易，同时能具有拓展的功能。」这项技术的主要目的是加快结算速度， 提高交易机密度并让各种资产代币化。

侧链的角色是扮演比特币区块链的第二个资料层， 它将最新的帐本储存为複製备份， 但是侧链上发生的交易不需要被纳入主区块链的区块。这代表不会产生任何网络手续费， 而且区块链的区块不会充满侧链的纪录。至于「挂勾」(pegged)一词则代表侧链上的区块链会与比特币的区块链相符合。Liquid 的「双向挂勾」代表链上的原生资产能够无缝地在链上来回交换比特币。

联盟侧链 (Federated Sidechains) 和中心化的疑虑 Liquid Network 运用名为「Liquid Bitcoin」(L-BTC) 的原生资产， 扮演与比特币双向挂勾的角色， 也可以随时透过网络赎回。根据 Samson Mow 的说法， 这种原生结算的资产可提高隐私度与速度。

根据 Blockstream 公司表示， Liquid Network 将仰赖加密货币产业公司所运作的硬体与软体：

参与的交易所与比特币企业已部署可形成 Liquid 网络的软体与 硬体， 因此他们能够为他们的交易者挂勾上比特币区块链并提供 Liquid 的功能。Liquid 为交易方的比特币在网络上的移转提供更安全且有效率 的系统。

然而，随着交易所获得比特币价值更易于移转的好处， 但这个好处却让矿工付出代价，因为他们无法获得挖矿的奖励。只有当「L-BTC」换成真正的比特币，矿工才会受惠。

此外，Liquid 是一个依赖「可信赖的负责人员」的网络， 这些负责人员是由「参与者的共识」组成， 因此 Blockstream 公司坦承它「永远不会像比特币一样去中心化」。虽然 Samson Mow 的声明指出，没有任何一方或 Blockstream 将控制 Liquid Network， 也没有任何参与者能控制超过一部以上的 Liquid 作业伺服器， 但这种做法如何实践将有待观察， 就像 EOS 与其他更中心化的网络以往所显示的例子一样。

Blockstream 是在 2015 年首次宣布 Liquid 将成 为比特币的第一条侧链。该公司在 2016 年获得 5,500 万美元第一轮资金，用于为比特币加密货币网络增添侧链。最新宣布的进度稍落后于进度，因为进度定在今年第 1 季就要推出侧链。

1 手把手教你学习zkSNARK proof!

Part3

特性：

从创世配置中 Sign up beacon chain node 节点 通过RPC将验证器客户端连接到 beacon chain 节点 验证器客户端在每个周期转换时被混合到给定时隙的特定shardID 验证器在其指定的时隙期间提出/证明规范Beacon块 Casper FFG奖励/惩罚包含在本新闻稿中, 尽管它们是一个不断发展的研究领域 通过libp2p和mDNS发现协议进行基本的, 本地联网的p2p Beacon链通过p2p传入块同步 一个有用的Beacon块模拟器 (这允许我们模拟其他Beacon节点本地向我们的节点中继信息) 将块/证明/状态存储到levelDB, 持久键值后端 gRPC公共API客户端/服务器, 用于查询规范块, 状态和最新验证器分配的Beacon节点 一个强大的, 可扩展的构建系统, 称为Bazel, 用于Google, Pinterest, Dropbox和其他行业巨头的生产 Web3订阅服务, 用于侦听最新的主链块和验证器注册

[illegible]

[原文点这里](<https://medium.com/prismatic-labs/ethereum-2-0-prysm-demo-release-v0-0-78d33e9cdbdf>)

3 快进/回滚的 snark 侧链可达约 17000 tps

目前，每个签名需要约500k个constraints。通过优化，我们认为我们可以将其减少到2k constraints。

目前我们的哈希函数（sha256）每秒花费50万笔交易。我们可以用符合1k constraints的XXXX承诺来取代它。

如果我们将merkle树制成29层，我们可以容纳536,870,912片叶子。

我们必须为每笔交易

确认签名= 2k constraints 确认旧叶子在树中= $1k * 29 = 29k$ constraints 添加新叶并重新计算
 $root = 1k * 29 = 29k$ constraints 这相当于每笔交易的60k constraints。

每个snark确认 $10000000000 / 60,000 = 16666$ 个交易

验证一个snark需要500kgas，我们每块有800万个gas。这意味着每个块可以包含16个这样的更新。

每块 $16666 * 16 = 266656$ 笔交易

$266656 / 15 =$ 每秒17777笔交易。

通过构建比它们更大的集群，我们可能达到比这更高的tps率。

注意：运行硬件以达到此速率可能相当昂贵，但同时远低于当前的块奖励

[原文谈论](#)

4 为什么用户还没使用Dapp?

目前，以太坊区块链上的dapps总数约为945(? 错误).乍一看，这个数字似乎令人印象深刻，但是，如果你仔细研究数据，事实可能是令人担忧的。总共有945个dapps，以太坊区块链上的dapps的每日总用户数仅为13,106，仅占交换区域链的61,525笔交易或12%。

以Bancor为例，去年筹集了超过1亿美元的项目，仅有300名每日用户，鉴于其估值为9200万，这是不可接受的。我们知道区块链是一项将使行业发生革命性变化的新技术，但在早期阶段，在获取和留住用户方面，障碍和障碍是不可避免的。下面列出了dapps处于毁灭性地位的原因：

可扩展性

将可扩展性视为用户适应区块链应用程序的主要阈值之一应该不足为奇。与互联网的早期阶段类似，区块链上的单笔交易或传统网页上的页面请求可能需要几分钟，遗憾的是社会上的人已经习惯了高速网络，整个社会都认为“速度”，以及此时分散的应用程序没有必要的基础设施或能力来与其集中的竞争对手/同行竞争。

产品市场适合

虽然许多Startups或Enterprise都强调产品，这意味着他们正在尝试构建一种能够满足市场需求的产品，但通常被忽视的是“市场”本身，在dapps领域常见的是人们正在构建一种能够满足市场未来需求的产品，而不是当前的需求。也许这就是为什么少数活跃的dapps主要是交易所，因为它为加密投资者和交易者提供了一个解决方案，强调“投资者”和“交易者”这个词不是用户。

dapps的市场仍远未成熟，基础设施尚未完成（再次强调可扩展性），公众对该市场的了解和兴趣接近0.了解何时推出您的产品至关重要，特别是在这个熊市中区块链和加密货币的兴趣暂时已经减弱。

效用还是投资？

最初设计为众筹工具，令人现在经历了一个痛苦的过渡时期，成为一个公用事业令牌，不仅从技术角度而且从心理学的角度来看。

无论发行人如何看待，通常在市场上，大多数代币持有者都在猜测产品的未来或投资产品。它们不一定是您产品的用户。即使令牌持有者是用户，使用令牌的机会成本也非常高。

如果您知道令牌在不久的将来会增加价值，为什么要将代币换成服务？虽然这可能不适用于大多数dapps，但它是值得关注的事情。

用户不友好


众所周知，dapps在响应时间方面要慢得多，并要求用户通过更复杂的安全和密码管理要求以及了解燃气费以进行交易所需的知识。























如上所述，人们更习惯于集中式系统，只需输入密码即可登录，并且不怕忘记密码。在dapp中，通常您会在创建新用户帐户时从几个不熟悉的额外步骤开始。公钥，私钥，gas限制等新术语通常会吓跑用户。当然，还有一个事实是，只有当您的钱包中有以太币（用作燃气费）时才会发生令牌转移，在这种意义上，这对于最终用户来说是不合逻辑的。

结论

无论我们作为开拓者所面临的挑战如何，区块链的未来都是光明的。最终，我们预计区块链技术的采用将与现在的互联网一样无缝，但为了实现这一目标，我们作为开拓者应该专注于建立基础设施和环境，以实现这一目标。

[原文点这里](#)

 今日Dapp表现 基于DAU和DTV

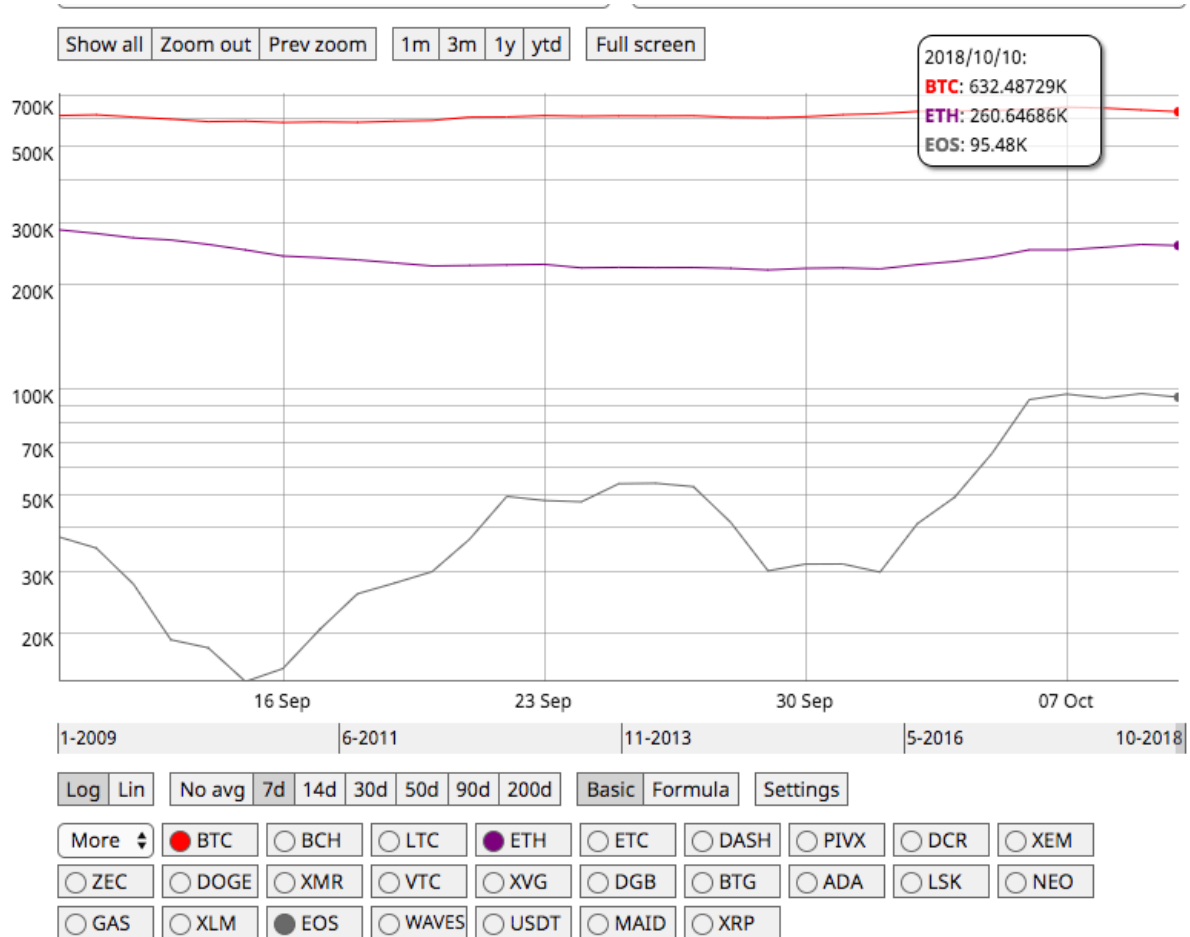
Dapp	Dapp.com Ranking	Dapp Balance	DAU	DTV
1  IDEX	 91 -0.10% ↓	47917.18 ETH 0.04% ↑	1263 -10.23% ↓	2888 ETH -12.85% ↓
2  dice2.win	 90 0.69% ↑	429.55 ETH -1.81% ↓	83 13.70% ↑	917 ETH -4.31% ↓
3  ForkDelta	 89 2.11% ↑	29871.57 ETH 8.33% ↑	900 -14.37% ↓	2609 ETH 46.75% ↑
4  Bancor	 89 1.98% ↑	0.00 ETH 0.00% ↑	343 4.89% ↑	2243 ETH 45.22% ↑
5  CryptoMiningToken	 87 1.64% ↑	4025.37 ETH -15.10% ↓	1006 15.77% ↑	1986 ETH 44.83% ↑
6  Local Ethereum	 78 0.48% ↑	145.25 ETH -12.03% ↓	181 -9.05% ↓	350 ETH -5.16% ↓
7  Kyber Network	 74 8.07% ↑	69.25 ETH -20.08% ↓	135 36.36% ↑	334 ETH 221.91% ↑
8  AirSwap	 70 25.02% ↑	0.00 ETH 0.00% ↑	92 55.93% ↑	292 ETH 726.89% ↑
9  Augur	 69 -0.32% ↓	5922.67 ETH -0.50% ↓	39 30.00% ↑	135 ETH 1.65% ↑
10  Token Store	 66 -3.15% ↓	937.01 ETH -0.67% ↓	551 5.76% ↑	69 ETH -31.51% ↓
11  CryptoKitties	 66 4.20% ↑	215.25 ETH 10.27% ↑	394 0.51% ↑	71 ETH 40.49% ↑

6 EOS 10月1-至今回顾

Date	Accounts	Days between	Daily accounts in period	A
02.06.2018	169930	0	-	
10.07.2018	196134	38		690
18.08.2018	288559	39		2370
05.10.2018	354090	48		1365

date	txVolume(USD)	txCount	marketcap(USD)	price(USD)	exchangeVolume(USD)	medianTxValue(USD)	activeAddresses	paymentCount	blockCount
2018/10/1	63690010.8	1416553	5197660279	5.74	695608000	1.435	36951	372509	172788
2018/10/2	47042344.59	1883906	5202480272	5.74	564671000	0.7175	75943	507607	172793
2018/10/3	57454858.25	1377687	5083643720	5.61	595740000	0.70125	99742	406992	172800
2018/10/4	52165132.03	1472277	5098014680	5.63	613679000	1.4075	72562	384275	172772
2018/10/5	55295052.38	1461405	5247946540	5.79	554553000	0.579	135802	461164	172728
2018/10/6	38995259.92	1668258	5269277407	5.81	486075000	0.581	210680	643966	172798
2018/10/7	33683383	2118245	5193475087	5.73	525930000	0.573	50548	558341	172684
2018/10/8	176306101.3	1876704	5226386210	5.77	627571000	1.4425	19103	506036	172689
2018/10/9	67797114.51	2210207	5368459762	5.92	538883000	0.9472	96145	509187	172784
2018/10/10	120929142.8	2020724	5341903994	5.89	533169000	1.4725	83520	538653	172290

EOS 7d active address



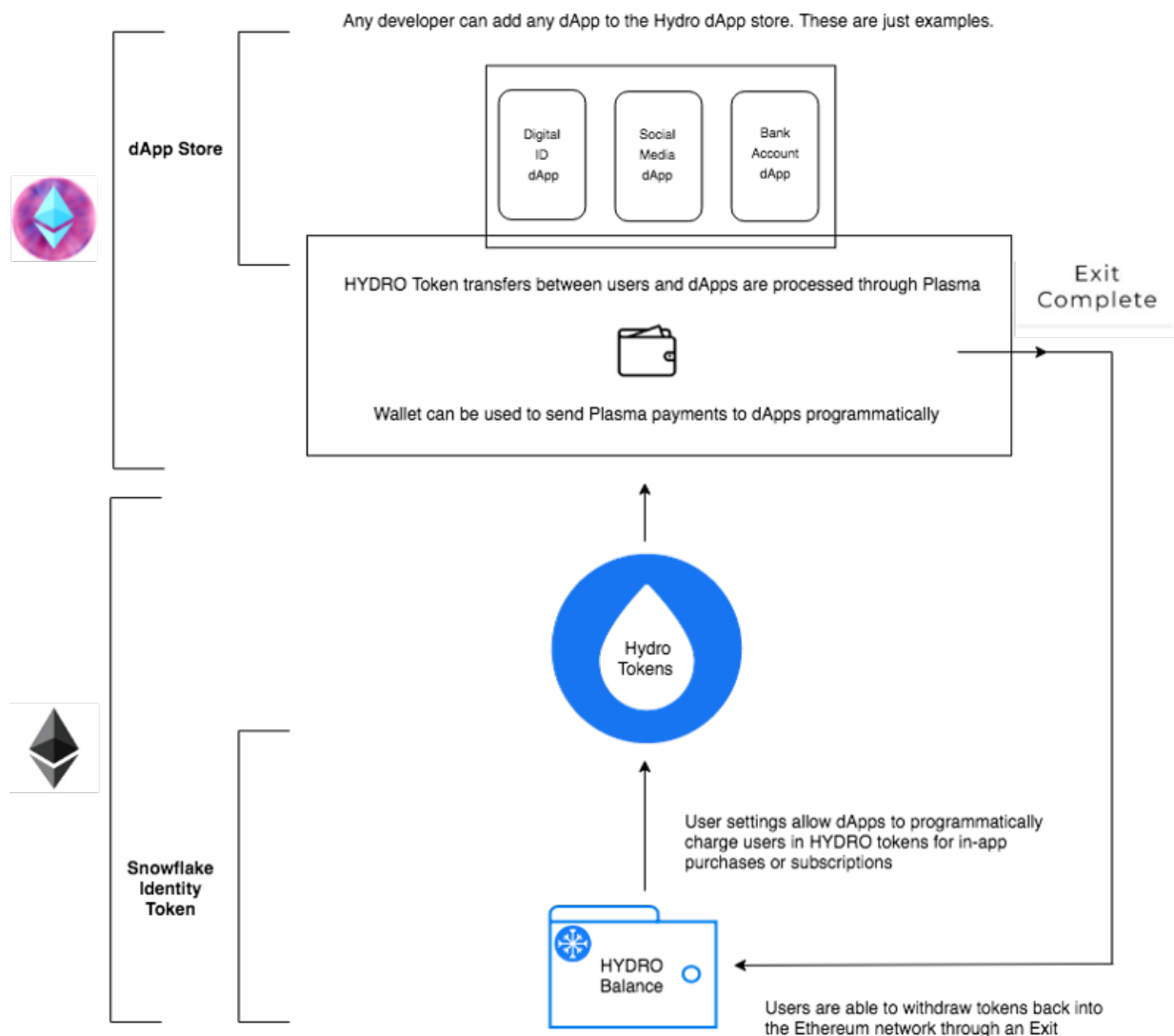
7 ST-20 Security Tokens 2.0

[Part 1](#)

[Part2](#)

8 Hydro Blocktoberfest: Plasma Integration For dApp Store & Tide!

Plasma is a Layer-2 framework proposed

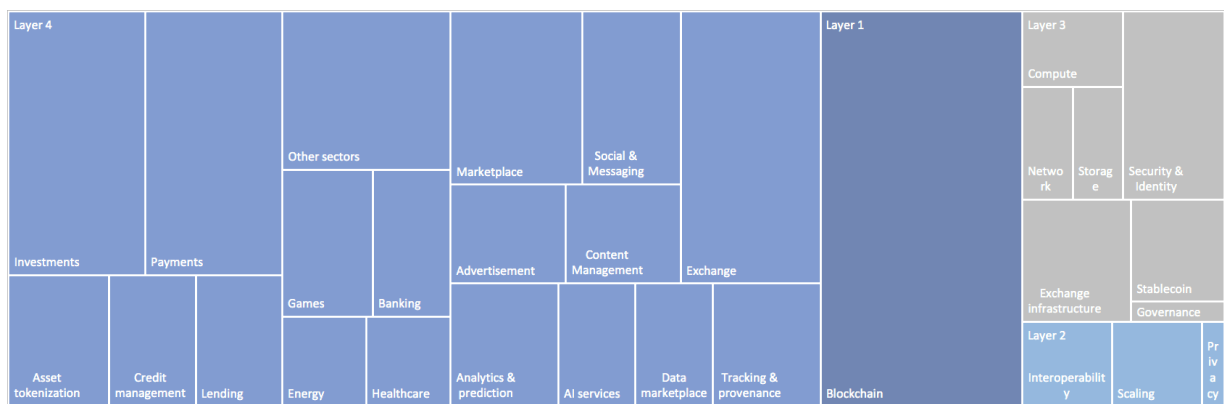
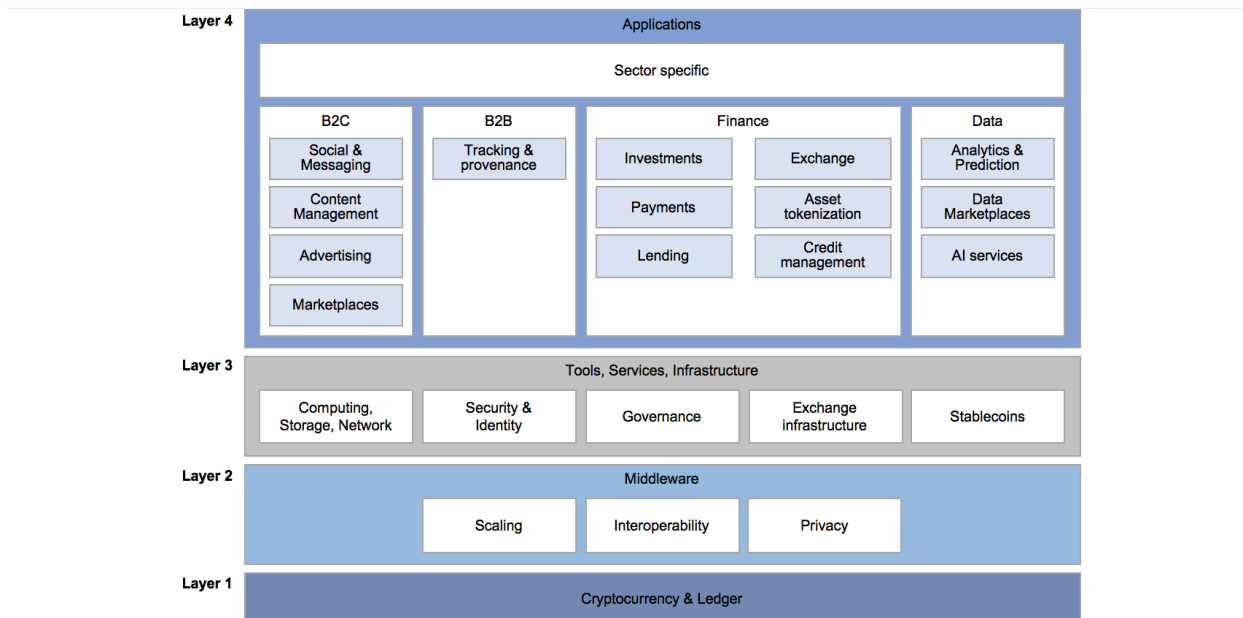


[原文点这里](#)

9 按市值分析前250个ERC-20代币

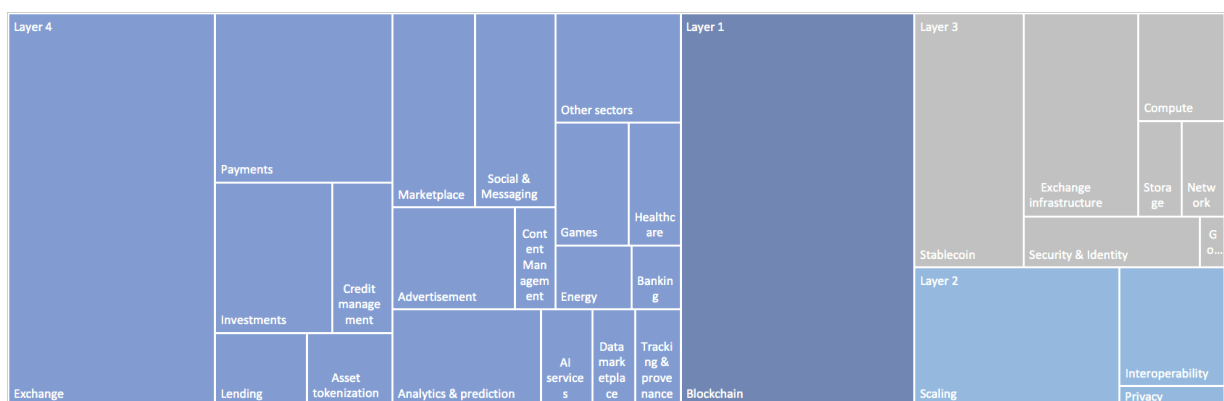
在2016年夏天，USV的Joel Monegro发表了所谓的Fat Protocols论文，关于在区块链/加密货币生态系统中创造价值的地方。他认为，由于应用层的成功推动了协议层的进一步猜测，因此投资使得市场上限较低的水平总是比构建在顶层的应用程序的总价值增长更快。正因为如此，区块链技术堆栈的性质促进了协议和其他较低层的创新。我很好奇是否在区块链协议的生态系统的不同层次中也是如此。

由于它是迄今为止最大的令牌生态系统，我决定研究以太坊生态系统来解决这个问题。根据Coinmarketcap的数据，以太坊（目前为止）已经实现了目前> 800以上的最多代币，其次是NEO，只有25。所以我看看以太坊上的顶级250令牌；在撰写本文时，从顶部降至约500万的市值。这些项目的总市值约为10b，因此与以太坊的~20b相比，Fat Protocol论文的最初前提似乎也适用。为了进一步调查，我对项目进行了分类，并将我发现的类别映射为4层结构（见下文）。



Distribution of number of projects by layer and category

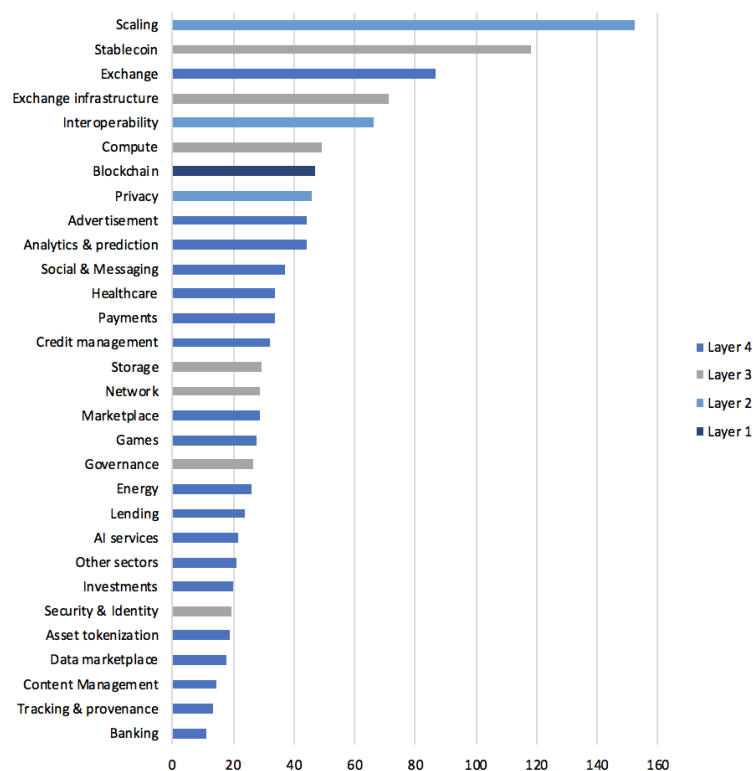
67%的项目正在应用层（第4层）上开发，交换，支付和投资项目是最大的子类别，每个项目占有所有项目的8%左右。第二大类别（16%）是新的基础层协议，尚未启动自己的区块链，实际上它们不属于以太坊生态系统的一部分。第2层和第3层项目仅占少数项目的4%和13%。



Distribution of market cap of projects by layer and category

第4层仍然是最大的，但第2层和第3层的17%项目的总市值为36%，即平均交易价值是其他项目的两倍。第2层和第3层的最大子类别是Scaling（6%），Stablecoins（6%）和Exchange基础架构（5%）在应用层内，交易所最突出的是17%。然而，11%来自Binance Coin。

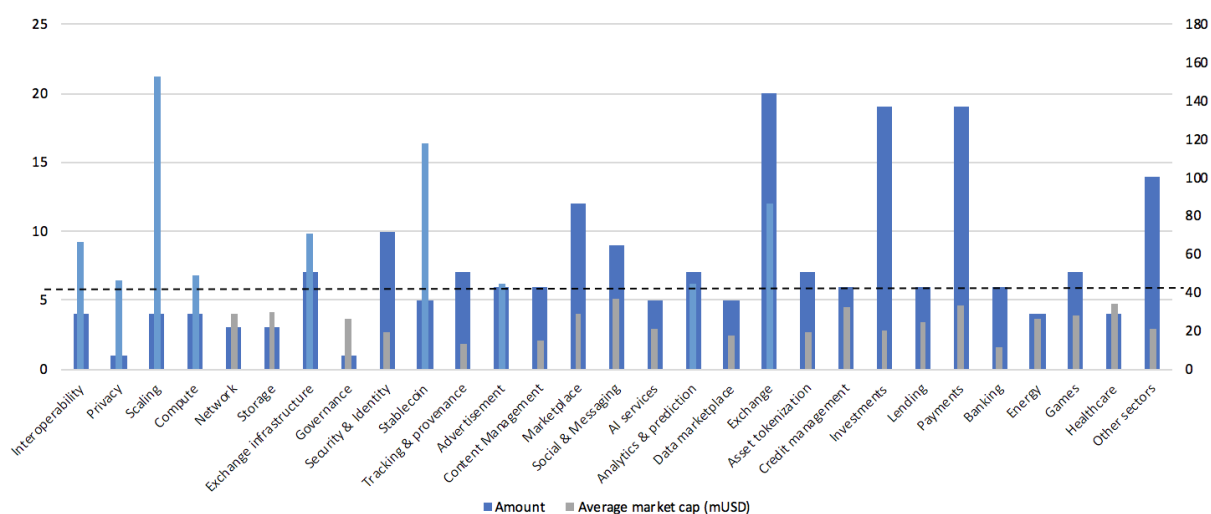
由于类别大小受到类别中项目数量的影响，我计算了下一个类别的平均市值：



Average market cap of projects per category

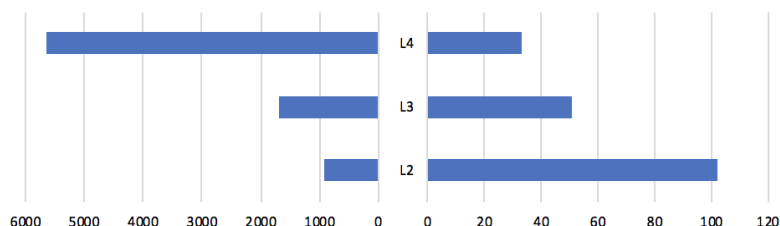
前10个类别显然由较低级别控制：所有2级类别和7个3级类别中的3个位于顶部。在4级类别中，只有交易所显然位居首位，再次受到Binance Coin市值的影响。还想将项目数量与平均市值进行比较。该图表显示了平均市值，在具有更宽条形的项目数量之上有一个窄条。对于左侧的项目数量，平均市值的比例在右侧。

此外，最后一个图表中的前10个类别以更亮的蓝色突出显示：



Comparison of number of projects and the average market cap per category

项目数量与平均市值的关系尤其突出了隐私类别;这似乎是市场上的一个缺口。扩展,稳定硬币和互操作性之间的关系也清楚地显示了高于平均水平的交易价值 虽然在将以太坊与建立在其上的所有项目的总市值进行比较时,Fat Protocol论文显然是正确的,但在上面的层面上并不是那么直截了当。较高层的项目在总体上占据更多市值,但较低层的项目具有较高的平均市值。



在某种程度上,较低的总市值可能是由于第2和第3层技术本身仍处于开发阶段,因此尚未被高层项目所使用。但并非所有第4层协议都需要所有第2层和第3层解决方案才能工作。从平均市值来看,Fat Protocol论文的前提似乎仍然存在。

另一方面,Binance Coin表明,重要的应计价值也可以在应用层进行,优于所有单独的第2和第3层硬币。即便在这种情况下,它也没有超越基层协议。

然后,加密货币空间仍然很年轻,价值更多地基于投机而不是基本面,因此我们可能不得不在一两年内重新审视这一点。

[原文点这里](#)

1. [\]\(https://medium.com/@eosfishforums/eos-wallet-comparison-which-wallet-is-right-for-you-e593eea5c269\)](https://medium.com/@eosfishforums/eos-wallet-comparison-which-wallet-is-right-for-you-e593eea5c269)

你要是忍不住打赏我点咖啡钱呐, 😊😊

我的BTC地址: 38weDdkcor1RNwxYAZoZfajS9ZaPc1si99



我的ETH地址: 0x8C1d4aCfF198AaE62e78944A5E49aed745162A89



微信打赏：



以上内容由平妈整理，感谢阅读！日报汇聚地址为：https://github.com/allinbc/BlockChain_Daily_Report（原先已经删除，待整理后，重新上传）

欢迎大家star&watch!