

第21讲 | 引人瞩目的区块链项目：EOS、IOTA、Cardano

2018-05-11 陈浩

深入浅出区块链

[进入课程 >](#)



讲述：黄洲君

时长 09:30 大小 3.29M



在第 8 讲中，我们已经讲过了一些成熟的区块链项目，这些项目多数都属于数字货币项目。

今天我们来聊几个比较创新型的区块链项目，它们□非常吸引人们的视线，容易引起话题，一方面它们的市场营销非常成功，另一方面它们也提出了革新的区块链技术概念。

下面我们来聊聊三个项目。

柚子 EOS

1. 什么是 EOS

EOS 全称 EOS.IO 软件，EOS 也是 EOS.IO 上的平台代币缩写，它暂时没有准确的中文翻译，中文社区把 EOS 叫柚子，这一点其实得益于 EOS 的发音与水果“柚子”相近。

EOS 是一个以太坊的竞争型区块链，它提供了全新的区块链架构，使得去中心化平台水平扩容和垂直扩容都成为了可能。

如果智能合约是程序，那么可以把 EOS 看成是一个超大的操作系统了，它为所有的程序，也就是智能合约提供了基本设施。例如账户、授权、数据库、异步通信等接口。

它甚至可以跨平台驱动大量的 CPU 或者集群，所以 EOS 的 TPS 肯定是远超以太坊的，这也使得构建基于区块链的应用几乎没有成本而且快速高效。

2.EOS 的瞩目之处

在说 EOS 之前，我们来回顾一下 DPoS。

DPoS 其实是 BM 参照现实世界中的议会制度而设计的共识算法。DPoS 的核心理念其实是投票，□它的设计理念是延迟性惩罚，它假设参与者绝大部分都是没有恶意的。

“人性本善”的假设虽然让系统的作弊成本降低，但是随之而来的惩罚也非常严厉，就是丧失见证人的资格，但是带来的好处则是效率的提升。

我们来看看 EOS 吸引人的地方，这里一共有两点，第一是 EOS 号称可以提供百万级 TPS 交易性能，第二是 EOS 的链上治理机制：区块链宪法以及 21 个超级节点（见证人节点）。

在 EOS 中，记账节点又被称作超级节点，EOS 一共有 21 个主节点，另外还有 100 个备选超级节点，这些超级节点完全是等价的。

超级节点的基本职责包括了忠实打包交易、执行并验证智能合约、向全网广播有效区块以外，还多了一项职责：保障并促进 EOS 项目的发展。

□如何促进呢？BM 在 EOS 中强化了 DPoS 算法的投票机制，并首次提出了区块链宪法的概念，我们可以直接引用 EOS 技术白皮书中的内容来一探究竟。

EOS.IO 应用使得区块链创建了一个点对点的服务条款协议或者绑定用户到一个合约，这都需要用户对其签名，简称“宪法”。

宪法的内容定义了仅仅依靠代码无法在用户间履行义务，同时通过建立管辖权和可选的法律来解决相互间的争端。

每个在网络广播的交易都必须将宪法的哈希值作为签名的一部分，从而显性地将签名者绑定在合约中。

宪法还定义了人类可读意图的源代码协议。这个意图是用来识别错误和功能之间的差异，当错误发生时，引导社区对什么是适当或不当修复。

可以看出区块链宪法是一种非代码强制执行的规则，有点像我们安装软件时的“同意”协议，所以它更像是一种人为承诺，为了弥补 DPoS 较弱的抵抗恶意规则的缺陷。

那么什么人可以发起并修改宪法呢？就是超级节点，也就是记账节点，它规定了 17/21 以上的节点同意才能发起修改提案。

我们可以看出超级节点的权力十分巨大，这也引来了人们对此产生了争议。

3.EOS 的争议

Vitalik 针对 EOS 超级节点竞选发表过意见。他认为 21 个节点的 DPoS 虽然引入了治理结构，但也很容易受到选民和持币大户的操纵，最终导致“财阀统治型”的治理结构。

在超级节点竞选过程中，某些节点为了获得更多的选票，承诺当选后可以给投票者分红，这在西方文化中是无法接受的，这一点似乎违背了 BM 设计 DPoS 的初衷，所以 BM 以及 EOS 团队都表示坚决反对。

BM 对此也给了回应，BM 表示自己的目标是降低创建社区的准入门槛，并允许市场竞争来奖励最高效的社区以及惩罚最腐败的社区。

他也认为善良是主观的，而且每个社区都能定义持有什么样的价值观是好人，并积极驱逐他们所认为的坏人。

Vitalik 和 BM 都相互发文怒“怼”对方，但是总的来说，Vitalik 和 BM 这种公开讨论推进了区块链行业的发展，给人们带来了更多哲学和设计原则上的思考。我在附录中给出了社区翻译版文章，你可以进行查询。

埃欧塔 IOTA

IOTA 是一个为了物联网 (IoT) 而生的区块链项目。严格来说, IOTA 不是“区块链”, 因为它没有区块, 也不是链式结构。

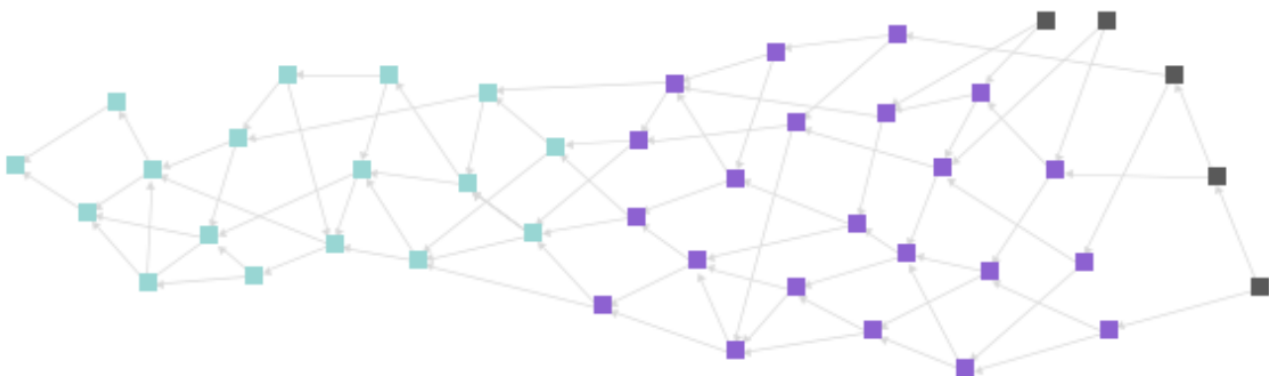
IOTA 提出了一种基于有向无环图 (DAG) 的分布式账本结构, 这种结构 IOTA 将其命名为 The Tangle, 探戈。

Blockchain



上图是常见区块链账本结构, 而下图展示了 Tangle 的账本结构。

Tangle (DAG/ Directed Acyclic Graph)



我们来看看这两张图的区别，首先区块链账本结构的打包单位是区块，而 Tangle 直接就是交易，或者“交易引用”。

□任意交易 Tx-black 会引用过去的两条交易记录，这样被引用的交易 Tx-purple 相当于有了一次确认，间接地证明了合法性，随着一次又一次的被引用，Tx-purple 会转变成 Tx-green。

1. Tx-black 相当于图种的黑色图块，代表未确认的交易；
2. Tx-purple 相当于紫色图块，代表已确认但还未成熟的交易；
3. Tx-green 相当于是绿色图块，代表已确认已成熟的交易，是可信的。

也就是说，我们发送交易的目标是成本绿色部分的交易，成为绿色部分的交易，可信度是可以计算的，面对不同的交易场景，可信度可以设置为 51%，90% 或者百分之百。

那么说，如何计算这种可信度呢？

IOTA 上的共识算法叫做 MCMC 算法，它可以任意选择黑色部分的两笔交易，进行引用。

□我们回到 DAG 的结构中，我们□发现每一个□绿色的交易都会有一条从□黑色起始位置通往它的路径，那么你这笔交易的□可信程度就可以很容易计算。

例如我们执行 MCMC 算法 N 次，这笔交易被全网接受的概率就是 M/N ，其中 M 就是从底部通往这笔交易的数量。

Tangle 结构和 MCMC 共识是非常具有吸引力的，它□也带来了以下特性。

1. 0 交易费：由于没有记账节点，目前没有考虑设置交易费。
2. 水平扩容：由于 Tangle 的结构不涉及记账节点，交易吞吐可以随着规模大容量也跟着提升。
3. 分区再合并：由于不是单链结构，私下记账以后也可以合并到 Tangle 账本中，不存在分叉这一说。

IOTA 的 Tangle 账本结构，为区块链技术带来了新的视角，这也是它吸引人的关键。

卡尔达诺 Cardano

卡尔达诺 (Cardano) 也是一个正在开发中的新一代区块链智能合约平台。

卡尔达诺项目最大的特色是由理论研究主导，严格采用□数学形式化验证的来证明严谨、安全性的区块链。

卡尔达诺认为现阶段基础公链在无论在可规模化性 (Scalability)、可互操作性 (Interoperability) 和可持续发展性 (Sustainability) □均存在不足，卡尔达诺希望进行概念□和技术上的创新，最终解决上述三个方面问题。

□卡尔达诺的团队认为目前区块链面临着两个□比较突出的问题：

1. 区块链协议的□升级将会导致区块链分叉； 2. 区块链的水平扩容和垂直扩容能力不足。

所以 Cardano 提出了分层架构理念，这似乎与传统 IT 架构模式：分层式架构模式有点像，□卡尔达诺由两个层次组成。

1. Settlement Layer 清算层：□卡尔达诺的代币 ADA 在该层流动，是整个系统的支付和清算的基础。
2. Computation Layer 计算层：□卡尔达诺将在计算层提供智能合约、身份认证、消息通信等功能。

相比于概念创新，卡尔达诺的团队研究了一种被命名为 Ouroboros 的算法，它其实也是 PoS 共识算法的变种，不同的是卡尔达诺团队为此提供了数学形式化证明，证明了它是高效、安全的共识算法。

卡尔达诺是一种理论研究驱动实践的尝试，无论是两层设计，还是 Ouroboros 算法，都为区块链技术的发展提供了值得参考的视角。

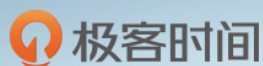
总结

今天，我们介绍了 EOS、IOTA、ADA 三个受人瞩目的区块链项目，EOS 和 ADA 都是致力于区块链去中心化的应用平台，IOTA 致力于为物联网提供分布式账本。这些项目引领了区块链的发展方向，无论是技术层面还是市场层面，他们都是非常出色的。

所以，你还可以想到那些技术或者市场做得出色的区块链项目呢？快来分享一下吧。感谢你的收听，我们下次再见。

参考链接:

1. [EOS.IO 技术白皮书](#)
2. <https://github.com/EOSIO/eos/wiki>
3. [BM 回怼 V 神：加密经济治理有局限，所以我选 DPOS](#)
4. [V 神回应 BM：你说的没错，但我必须要提醒你](#)
5. <https://steemit.com/cn/@niking/iota>
6. <https://docs.iota.org/introduction>
7. <https://whycardano.com/cn/>
8. <https://iohk.io/blog/ouroboros-at-crypto-2017/>



深入浅出区块链

你的区块链入门第一课

陈浩 元界 CTO



新版升级：点击「👤 请朋友读」，10位好友免费读，邀请订阅更有**现金**奖励。

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 第20讲 | 区块链项目详解：比特股BTS

下一篇 第22讲 | 国内区块链项目技术一览

精选留言 (7)

写留言

小白

1

2018-05-13

技术白皮书宪法这一部分的翻译是用的 EOSLaomao 的版本吧，我参与了这个翻译，据我所知这段翻译还没有被 merge 到 EOS 的主分支上。

作者回复: 你好，参考的是github上eosio下的白皮书哦，好像改为15/21了。



荔荔要去看...

2018-05-13

👍 1

只是介绍了基本情况。如果能更深度分析就更好了。自己再看的话，应该要结合白皮书

作者回复: 篇幅所限，尽可能抛砖引玉给大家。谢谢支持



徐威

2018-05-12

👍 1

cosmos

展开 ▾

作者回复: 谢谢补充呢



Ricky

2018-08-20

👍

除了EOS外，IOTA和ADA都持有。不知道为啥，总是觉得EOS有点虚

展开 ▾

作者回复: 哈哈，厉害的，现在熊市，大家都差不多。



有风的林子

2018-05-13

👍

宪法~~一个有意思的设计。

展开 ▾



徐軒会 ...

2018-05-13



因为是小白一枚，一直默默听陈总讲课，今天真是太兴奋了，有一种拨开云雾的感觉，谢谢！ 🍷

作者回复: 感谢支持呢，嘻嘻



吹牛老爹

2018-05-13



很棒的一篇文章，学习了、

展开 ▾

作者回复: 感谢支持。

