2016—2017年度

区块链行业前瞻（二）以太坊

——洞悉区块链 2.0 技术未来发展趋势

链行 LHANG

共享财经 SHARED FINANCE

上海交通大學 Shanghai Jiao Tong University

上海云基地 SHANGHAI CLOUD VALLEY

2016-2017 以太坊发展简报

——洞悉区块链 2.0 技术未来发展趋势

关键词：数字资产，区块链，智能合约，以太坊

导读：

2016 年，是区块链技术和数字资产行业飞速发展的一年，区块链 1.0 概念主要围绕支持虚拟货币的实现，虽然它有一定的灵活性，但是用来支撑虚拟货币以外的应用场景还显得非常局限。以太坊为代表的区块链 2.0 的概念也随之产生。通过增加链上的扩展性功能，把区块链的技术范围扩展到支撑一个去中心化的市场，基本内容可以包括房产契约、权益及债务凭证、知识产权、甚至汽车、艺术品等。

链行位于上海自贸区，毗邻陆家嘴金融中心、张江高科技园区，是一家定位前沿数字资产交易与专业化管理的金融服务平台，由币林网络科技（上海）有限公司独立运营。新年之交，链行联合共享财经、上海交通大学计算机科学与工程系、上海云基地通过对行业的观察、总结撰写 2016-2017 年度区块链行业分析报告，以供区块链与数字资产行业投资者、从业者、爱好者参考，旨在帮助关注区块链技术、数字资产、以太坊的人士全面了解 2016 年行业的动态及 2017 年的趋势方向。

目录

1. 以太坊（Ethereum）基础介绍

以太坊因为其创新性的应用，继比特币区块链 1.0 之后，被称为区块链 2.0。比特币的区块链架构主要围绕支持虚拟货币的实现，虽然它有一定的灵活性，但是用来支撑虚拟货币以外的应用场景还显得非常局限。近年来，区块链逐渐引起 IT 业界的关注，并逐渐成为独立于比特币的一个平台架构，其重要性越来越受到重视。区块链 2.0 的概念也随之产生。其核心理念是把区块链作为一个可编程的分布式信用基础设施，支撑智能合约应用，以与过去比特币区块链作为一个虚拟货币支撑平台区别开来。具体说来就是，不仅仅把区块链作为一个去中心化的虚拟货币和支付平台，而是通过增加链上的扩展性功能，把区块链的技术范围扩展到支撑一个去中心化的市场，基本内容可以包括房产契约、权益及债务凭证、知识产权、甚至汽车、艺术品等。

1.1 以太坊的结构

图 1 以太坊结构示意图

以太坊区块链中同样包含基础的分布式数据库结构、智能合约、加密算法模块、共识机制、前端应用模块等，其中基于以太坊虚拟机（EVM）运行的智能合约（Smart Contract）可以说是以太坊在比特币基础上最具意义和发展潜力的设计和创新点。

1.2 以太坊编程语言

以太坊的编程语言有四种：Serpent（来源于 Python）、Solidity（来源于 JavaScript）、Mutan（来源于 Go）和 LLL（来源于 Lisp）。都是为面向合约编程而从底层开始设计的语言。

其中，Solidity 作为以太坊的首选语言，内置了 Serpent 的所有特性，但是语法类似于 JavaScript。Solidity 充分利用大量现有数以百万程序员已经掌握 JavaScript 这一现状，降低了学习门槛，易于被掌握和使用。目前 Solidity 也是以太坊开发者中最流行的的语言。

1.3 以太坊的特点

智能合约

以太坊创新性的引入智能合约概念。相较比特币，其智能合约采用内置方式，因此效率和安全性都更高。其编码难度低，逻辑设计合理。利用其智能合约的特性，可以达成借贷、众筹、自动交易、智能交易等用途。

图 2　智能合约交易方式

图灵完备

以太坊区块链的一个关键特征就是它的“图灵完备性”，这保证了以太坊可以解决所有的计算问题。此外，因为以太坊的语言视为区块链专门设计的，具有账户的概念，为交易的可视化和查询账户状态提供了实时性。账户是一个受人欢迎的功能，但对比特币而言，实现起来具有一定的挑战。在比特币上，由于只有 UTXO（Unspent Transaction Output，“未花费的输出”）而没有账户的概念，我们需要导入区块链数据库，解析所有的交易，并为了抽取出在区块链上的某个用户的交易情况而查询交易。而用以太坊，我们则可以在实时的区块链上，根据一个地址情况实时查看当前账户情况和交易状态。

2. 以太坊应用

DApp（Decentralized Application）

目前，以太坊的大多数应用都是通过 DAapp 方式实现。Dapp 是由智能合约和客户端代码构成的。智能合约就像加密的包含价值的箱子。只有当特定条件被满足时它才会被打开，它封装了一些逻辑、规则、处理步骤或者双方间的协议。

从架构角度而言，DApp 非常类似于传统的 Web 应用。主要区别是：在传统 Web 应用中，客户端有 JavaScript 代码，由用户在自己的浏览器中执行；服务器端的代码有主机运行。但是在一个 DApp 中，它的智能逻辑运行在区块链上，客户端代码运行在特殊浏览器 Mist 里面。

应用举例

Augur（www.augur.net），一个正在开发去中心化预测系统。Augur 在英文中的意思是“预言家”，用户可以在这个应用上对各种时间打赌并下注，例如希拉里会不会赢得 2016 年的美国大选；2017 年中国的 GDP 增长会不会超过

6%；上证指数 2020 年之前会不会超 10000 点，等等。对于参与者而言，如果预测准确，则将获得经济上的回报；而对于社会整体而言，Augur 便成了一个群体智慧的收集器，在它上面的下注信息反映了人民对于未来某时间发生的可能性的最佳评估。当你打开搜索引擎，输入“XXX 会不会赢得 2020 年美国大选”的时候，很可能搜到这样的结果：“Augur：该事件发生的可能性为 46.6%”。

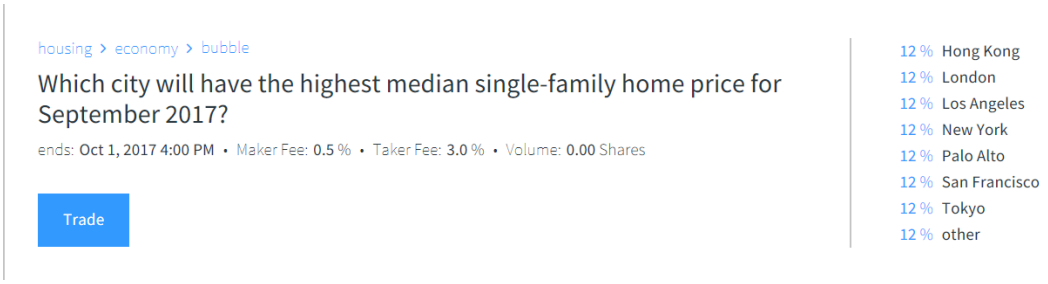

图 3　Augur 预测 2017 年 9 月独户住宅中位数价格最高的城市

3.　以太坊发展史（2014 年-2016 年）

诞生

2014 年 1 月初，一篇名为《以太坊发布加密货币 2.0 网络》的文章在 Coindesk 发表，即以太坊的白皮书。同年 4 月，Gavin Wood 博士发表了以太坊黄皮书，作为以太坊虚拟机的技术说明。按照黄皮书的具体说明，以太坊客户端已经用 7 中编程语言实现（C++、Go、Python、Java、JavaScript、Haskell、Rust），使软件总体上更加优化。与比特币不同的是，以太坊的总量不是固定的。以太坊前期通过预售售出超过 6000 万以太，之后每年发行 1872 万，没有上限。

盗币

2016 年 6 月，未知入侵者从 The DAO 中盗取了价值数千万美元的以太币，The DAO 是一个基于以太坊的智能合约，其在生态系统项目中的角色是融资工具。事件发生后，开发者试图通过分叉挽回 The DAO 被盗损失,保护剩余资金。

2016 年 7 月，以太坊开发团队在第 1920000 区块对以太坊进行硬分叉，从而从根本上抹去 The DAO 遭受的攻击。然而并不是所有以太坊社区成员都赞同此次分叉，为了表示对以太坊硬分叉的抗议，分叉在第 1920001 区块诞生了。以太坊原链（Ethereum Classic， ETC）使用的仍是旧的区块链，其宗旨是“延续一个去审查制度的以太坊”和“为反对硬分叉的人提供选择空间”。ETC 开发者坚持区块链系统的三大要素：公开、中立以及不可更改。开发者们坚信这三个要素是建立以太坊平台价值的关键，一旦脱离了这三个特点，区块链只不过是一个数据库而已。而分叉产生的另一条区块链则被称为以太坊新链或以太坊（ETH）。

ETC 出现之初，大多数人认为他们的存在不会长久，并未给予其太多的关注。真正的转折来自于全球最大的山寨币交易平台 Poloniex（P 网）上线 ETC 数字货币，使得 ETC 有了交易价值，也使得那些支持短链的矿工从“为了信仰”变得真正有利可图。

发展

迄今为止，以太坊共进行了四次分叉，但只有第一次分叉使社区真正分裂了。后续分叉都旨在修复重要漏洞，解决网络中不断的攻击问题，完成网络升级。相较于第一次硬分叉的巨大争议，纯粹的技术更新性质的分叉相对来说能够安然无恙地度过。

4. 以太坊行情

据 CoinMarketCap 截止 2017 年 02 月 05 日的数据显示，ETH 的市值超 10 亿美元，成为了仅次于比特币的第二大加密数字资产。而 ETC 在诞生之初市值出现过井喷，达到 2.25 亿美元，之后逐渐回落。目前 ETC 的市值 1.30 亿美元，

约为 ETH 市值的 13%，在全部加密数字资产市值排名中占第六位。

图 4　ETH 市值（百万美元）与 ETH 价格（以 BTC 计价），2015.08.07-2017.02.05

图 5　ETC 市值（百万美元）与 ETC 价格（以 BTC 计价），2016.07.24-2017.02.05

ETH

16 年年初，ETH 的价格约为 16 元。经过半年的持续增长，ETH 曾于 6 月份达到过最高价 145 元。而后便发生了 The DAO 被盗事件导致以太坊暴跌。虽然以太坊通过硬分叉挽回 The DAO 被盗损失，以太坊价格也于 7 月份有所回升，但回顾16年下半年，以太坊价格是处于下跌趋势中的，最低价曾下探到41元，跌幅超过 50%。ETH 价格的持续走低可能源于以太坊面临的垃圾交易攻击问题，以太坊团队执行技术硬分叉时产生了分歧，导致以太坊意外分叉。

ETC

ETC 在诞生之初有过一段价格的爆发期，之后便迅速回落，持续走低。直至 11 月底，因 ETC 没有执行 ETH 链的技术硬分叉而没有受到 ETH 意外分叉的影响， ETC 价格逐渐回升。

近期比特币的大涨也带动了其他品种数字资产的价格上扬，包括 ETH 和 ETC，随后比特币暴跌，以太坊和以太坊原链也出现了约 20%的跌幅。尽管不同的数字资产服务着不同的用户，比特币的价格波动性往往对其他数字资产具有连带效应。

图 6　2016.8-2017.2 ETH 对人民币价格走势

图 7　2016.8-2017.2 ETC 对美元价格走势

5. 以太坊展望

自以 ETC 诞生以来，诸如 ETC 的存在会不会威胁到以太坊整体发展、ETH 和 ETC 能否长期共存的争论就一直存在着。两者的区块链结构和功能基本一致，但是意识形态是两者间最根本的区别。ETC 通过拒绝从 The DAO 攻击者手中取回资金打造了一个真正交易不可逆的区块链，而 ETH 则被部分人认为是一个中心化的、易受影响的系统。目前 ETH 和 ETC 在开发社区和二级市场中都依然共存，投资者也可以同时从两种货币中获利，并且，ETH 和 ETC 的市值综合超过了分叉前的以太坊，形成了 1+1 大于二的发展效应。但从市场存量角度看，分叉后的 ETH 相较于 ETC 确实占据了更多的市场，无论市值还是算力，仍然保持领先状态。

而在未来，以太坊分叉将面临着共识算法的重大更改，即将推出的新共识算法 Casper 可看作是模仿 POW 的一种变种 POS 算法，届时以太坊分叉将面临重大考验。ETC 也在寻求改变，在 ETC 货币政策的改进协议中说明 ETC 可能从目前的 POW 共识模式转到 POS 或 POW+POS 的混合模式。另外，ETC 货币政策还把目前一个区块的发行量控制在 14.0625 个 ETC。这些改变都将给 ETH 与 ETC 的发展带来不确定性。

ETC 的存在毕竟还不足一年，我们还无法判断这一分支的技术优劣性，但这一次的区块链大分裂值得我们继续观察，也会给其他公有区块链的分叉带来借鉴意义。ETC 在开源社区中的人气和优势，也或将为这一分支带来更大的市场份额和吸引更多开发力量。

6. 附录

相关资料链接：

以太坊官方网站：

ETH:

https://ethereum.org/

ETC:

http://www.ethereumclassic.com/

以太坊白皮书：

英文：

https://github.com/ethereum/wiki/wiki/White-Paper

中文：

http://ethfans.org/posts/ethereum-whitepaper

以太坊爱好者论坛：

ETH:

http://8btc.com/forum-72-1.html

http://ethfans.org/

http://reddit.com/r/Ethereum

http://forum.Ethereum.org

ETC:

https://forum.ethereum.org/discussion/8590/ethereum-classic-etc

http://www.ethereumclassictalk.org/

https://bitcointalk.org/index.php?topic=1575335.0

以太坊新闻媒体报道：

https://www.ethnews.com/

https://news.bitcoin.com

https://btc-e.com/news

https://cointelegraph.com/news

https://etc.today

以太坊行情变化查询：

ETH:

http://ethereumprice.org/

https://coinmarketcap.com/currencies/ethereum/#

https://www.worldcoinindex.com/coin/ethereum

https://www.coingecko.com/en/coins/ethereum

ETC:

http://www.etcprice.com/

https://www.worldcoinindex.com/coin/ethereumclassic

https://coinmarketcap.com/currencies/ethereum-classic/

https://www.coingecko.com/en/price_charts/ethereum-classic/usd

2016—2017 年度报告

相关版权声明

联系我们：

币林网络科技（上海）有限公司

E-mail: services@lhang.com