以太坊综述

Ethereum

2018.10

为什么要学习以太坊

- 庞大的开发者社区，目前最大的区块链开发平台
- 相对较成熟，有代表性，资料众多
- 以应用入手，学习曲线不那么陡峭
- 与JavaScript结合紧密，方便开发人员上手

课程简介

课程名	子课程	主要内容	预计课时
以太坊基础	以太坊综述	以太坊整体介绍	3
	初识以太坊	钱包、测试网、简单交易	4
	以太坊客户端	客户端；Geth的安装和使用；搭建私链	5
深入理解以太坊	以太坊账户和合约	账户详解，合约特性	3
	以太坊交易、gas和EVM	交易详解，EVM简介	3
以太坊编程及应用	Solidity基础	Solidity语法，简单合约	6
	简单投票DApp	ganache，简单投票DApp	6
	web3.js及简单应用	web3.js API，转币脚本，监听脚本	6

课程名	子课程	主要内容	预计课时
深入理解 合约工作流	合约工作流	深入理解合约工作流	1
	自动化编译和部署	编写编译脚本和部署脚本	5
	自动化测试	Ganache	4
深入理解 以太坊原理	以太坊的理念与实现	白皮书，黄皮书	3
	源码结构及分析	代码结构，MPT，GHOST	3
DApp项目实战	基于token的投票	Truffle，加入token的合约	12
	基于ipfs的去中心化eBay	IPFS，多合约交互	24
	ICO DApp	next.js + react + material-UI + mocha	36

学习目标

- 掌握以太坊的基本概念和工作原理
- 理解以太坊与比特币的联系和区别
- 掌握以太坊客户端的使用
- 深入理解智能合约
- 掌握 Solidity 语法，并能够写出复杂的合约
- 掌握 web3.js 的调用，并能够实现具体的 DApp
- 综合运用各种工具，完成较复杂的项目

主要参考资料

- 《精通以太坊》(Mastering Ethereum)

  https://github.com/ethereumbook/ethereumbook

- 《以太坊白皮书》(A Next-Generation Smart Contract and Decentralized Application Platform)

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

- 《以太坊黄皮书》（《以太坊：一种安全去中心化的通用交易账本 拜占庭版本》）

- 以太坊官方文档 (Ethereum Homestead Documentation)

  http://www.ethdocs.org/en/latest/index.html

- Solidity官方文档

  https://solidity.readthedocs.io/en/latest/

涉及工具

- MetaMask - 浏览器插件钱包
- Remix - 基于浏览器的 Solidity 在线编辑器
- Geth -以太坊客户端（go语言）
- web3.js – 以太坊 javascipt API库
- Ganache – 以太坊客户端（测试环境私链）
- Truffle – 以太坊开发框架

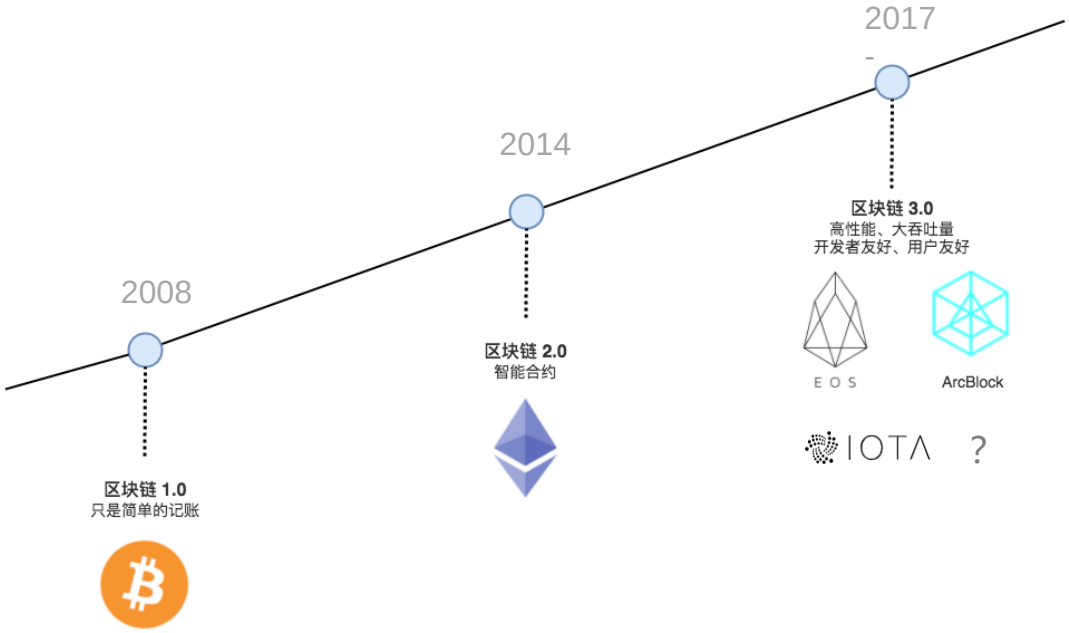
环境准备

- Chrome浏览器（最新版本 70.0.3538.67）
- Linux 系统或虚拟机（ubuntu 16.04.3）

  需要安装：go(1.9)，git(2.7.4)，node(9.0.0), npm(5.7.1)

- 文本编辑器（VisualCode）
- 科学上网工具

区块链（公链）发展简史



比特币（1.0）-- 以太坊（2.0）-- ？ （3.0）

以太坊的出现

- 2014 年1月， Vitalik Buterin在自己任编辑的比特币杂志(Bitcoin Magazine)上发表了《以太坊：一个下一代智能合约和去中心化应用平台》（Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform）

Vitalik Buterin

- 2014年的迈阿密比特币会议中，布特林宣布了以太坊项目，并且提出了多项创新性区块链技术，该年7月，启动以太坊众筹募资，募得3.1万枚比特币（当时约合1840万美元）
- 2015年7月30日，当时作为以太坊项目CCO的成员Stephan Tual在官方博客上正式宣布了以太坊系统的诞生，以太坊主网上线

发展阶段

- **“前沿”(Frontier)** – Block #0

  以太坊的初始阶段，持续时间为2015年7月30日至2016年3月

- **“家园”(Homestead)** - Block #1,150,000

  以太坊的第二阶段，于2016年3月推出

- **“大都会”(Metropolis) Block #4,370,000**

  以太坊的第三个阶段，于2017年10月推出的“拜占庭”(Byzantium)是 Metropolis 的两个硬分叉中的第一个，也是我们现在所处的阶段。

  “君士坦丁堡”(Constantinople)

  Metropolis 阶段的第二部分，计划于2018年推出。预计将包括切换到混合POW/POS 共识算法，以及其他变更。

- **“宁静”(Serenity)**

  以太坊的第四个也是最后一个阶段。Serenity尚未有计划的发布日期。

重大分叉

- **Block #200,000**

  "Ice Age" - 引入指数难度增加的硬分叉，促使向 Proof-of-Stake 过渡。

- **Block #1,192,000**

  “The DAO" - 扭转了被攻击的DAO合约并导致以太坊和以太坊经典分裂成两个竞争系统的硬分叉。

- **Block #2,463,000**

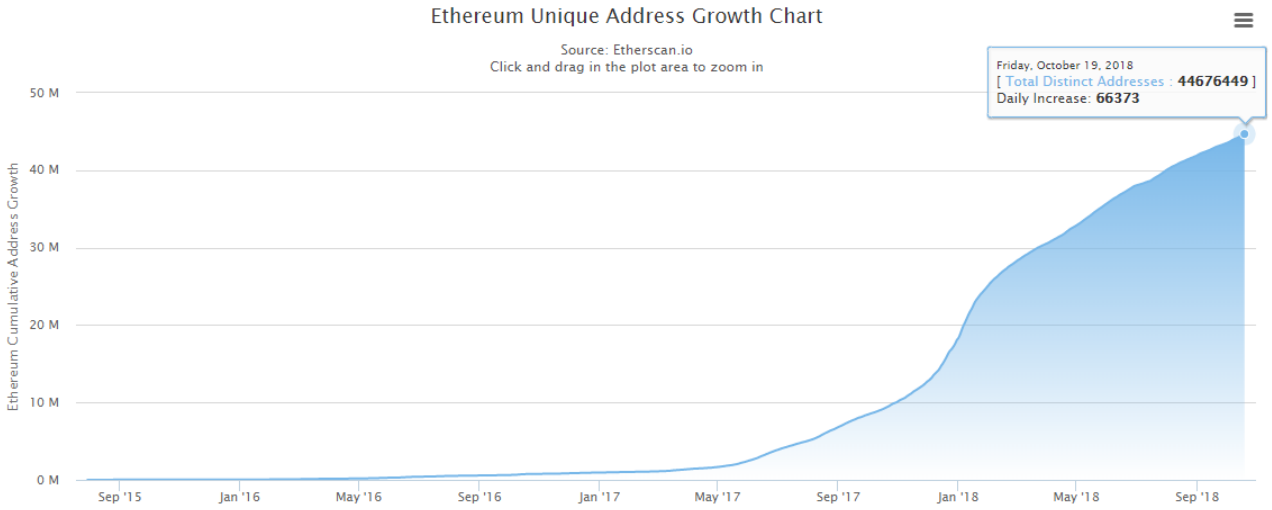
  “Tangerine Whistle” - 改变某些IO运算的 gas 计算，并从拒绝服务攻击中清除累积状态，该攻击利用了这些操作的低 gas 成本。

- **Block #2,675,000**

  “Spurious Dragon” - 一个解决更多拒绝服务攻击媒介的硬分叉，以及另一种状态清除。此外，还有重放攻击保护机制。

发展现状

- 根据 State of DApps 的统计，目前运行在以太坊上的合约多达 47228 个；而以太坊的地址数也达到了 4000W 以上，如下图：



以太坊特点

- 以太坊是“世界计算机”，这代表它是一个开源的、全球分布的计算基础设施
- 执行称为智能合约（smart contract）的程序
- 使用区块链来同步和存储系统状态以及名为以太币（ether）的加密货币，以计量和约束执行资源成本
- 本质是一个基于交易的状态机(transaction-based state machine)
- 以太坊平台使开发人员能够构建具有内置经济功能的强大去中心化应用程序（DApp）；在持续自我正常运行的同时，它还减少或消除了审查，第三方界面和交易对手风险

以太坊的组成部分

- **P2P网络**

  以太坊在以太坊主网络上运行，该网络可在TCP端口30303上寻址，并运行一个名为ÐΞVp2p的协议。

- **交易（Transaction）**

  以太坊交易是网络消息，其中包括发送者（sender），接收者（receiver），值（value）和数据的有效载荷（payload）。

- **以太坊虚拟机（EVM）**

  以太坊状态转换由以太坊虚拟机（EVM）处理，这是一个执行字节码（机器语言指令）的基于堆栈的虚拟机。

- **数据库（Blockchain）**

  以太坊的区块链作为数据库（通常是 Google 的 LevelDB）本地存储在每个节点上，包含序列化后的交易和系统状态。

- **客户端**

  以太坊有几种可互操作的客户端软件实现，其中最突出的是 Go-Ethereum（Geth）和

以太坊中的重要概念

- **账户（Account）**

  包含地址，余额和随机数，以及可选的存储和代码的对象。

  - 普通账户（EOA），存储和代码均为空
  - 合约账户（Contract），包含存储和代码

- **地址（Address）**

  一般来说，这代表一个EOA或合约，它可以在区块链上接收或发送交易。

  更具体地说，它是ECDSA 公钥的 keccak 散列的最右边的160位。

- **交易（Transaction）**

  - 可以发送以太币和信息
  - 向合约发送的交易可以调用合约代码，并以信息数据为函数参数
  - 向空用户发送信息，可以自动生成以信息为代码块的合约账户

- **gas**

  以太坊用于执行智能合约的虚拟燃料。以太坊虚拟机使用核算机制来衡量gas的消耗量并限制计算资源的消耗。

以太坊的货币

以太坊的货币单位称为以太（ether），也可以表示为ETH或符号Ξ。

以太币的发行规则：

- 挖矿前（Pre-mine，Genesis）

  2014年7月/8月间，为众筹大约发行了7200万以太币。这些币有的时候被称之为“矿前”。众筹阶段之后，以太币每年的产量基本稳定，被限制不超过7200万的25%

- 挖矿产出（Mining）

  ——区块奖励（block reward）
  ——叔块奖励（uncle reward）
  ——叔块引用奖励（uncle referencing reward）

- 以太币产量未来的变化

  以太坊出块机制从工作量证明（PoW）转换为股权证明（PoS）后，以太币的发行会有什么变化尚未有定论。股权证明机制将使用一个称为Casper的协议。在Casper协议下，以太币的发行率将大大低于目前幽灵（GHOST）协议下的发行率。

以太坊的挖矿产出

- **区块奖励（Block rewards）**

  每产生一个新区块就会有一笔固定的奖励给矿工，初始是5个以太币，现在是3个。

- **叔块奖励（Uncle rewards）**

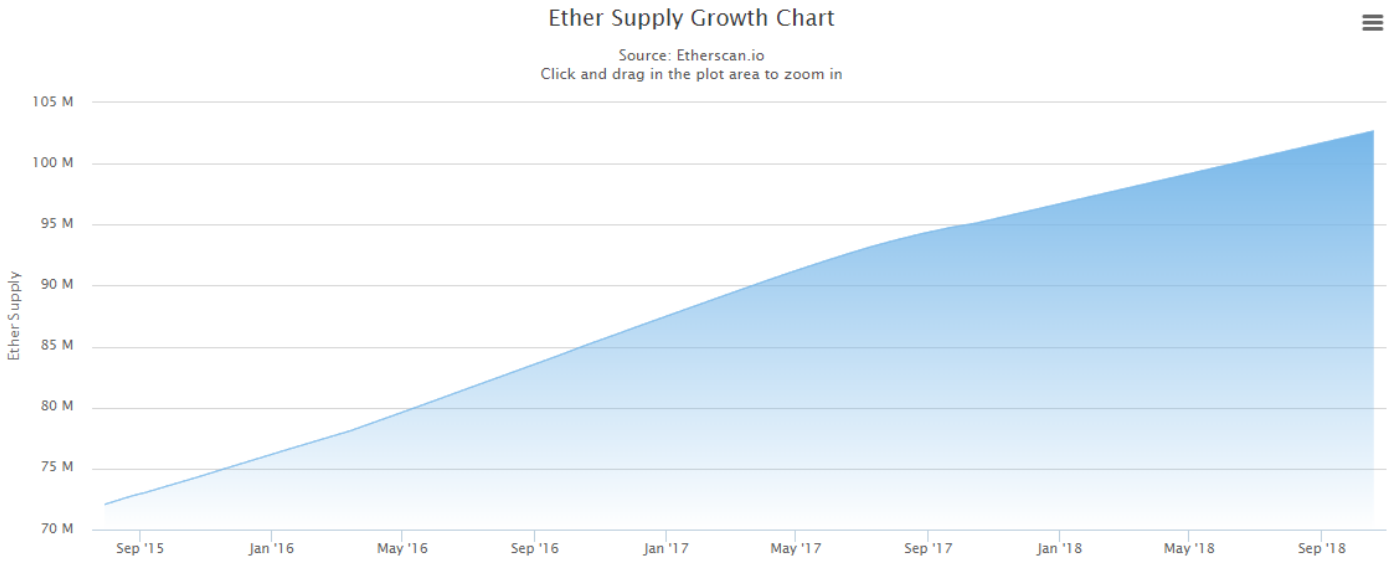
  有些区块被挖得稍晚一些，因此不能作为主区块链的组成部分。比特币称这类区块为“孤块”，并且完全舍弃它们。但是，以太币称它们为“叔块”（uncles），并且在之后的区块中，可以引用它们。如果叔块在之后的区块链中作为叔块被引用，每个叔块会为挖矿者产出区块奖励的7/8。这被称之为叔块奖励。

- **叔块引用奖励（Uncle referencing rewards）**

  矿工每引用一个叔块，可以得到区块奖励的1/32作为奖励（最多引用两个叔块）

- 这样的一套基于POW的奖励机制，被称为以太坊的“幽灵协议”

以太币供应量



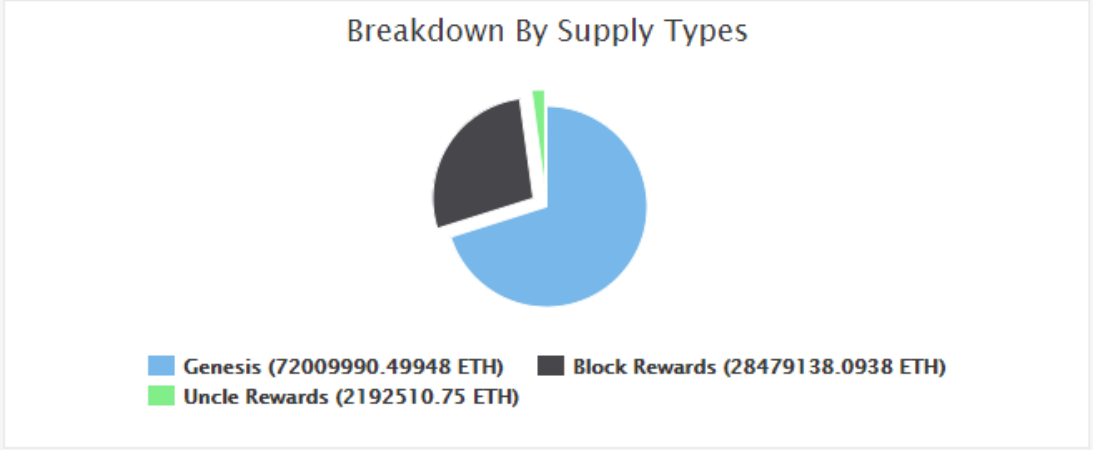
以太币供应量

102,681,639.34

Total Ether Supply

$20,923,437,648

Market Capitalization



以太坊区块收入

- **普通区块收入**

  — 固定奖励（挖矿奖励），每个普通区块都有

  — 区块内包含的所有程序的 gas 花费的总和

  — 如果普通区块引用了叔块，每引用一个叔块可以得到固定奖励的 1/32

- **叔块收入**

  叔块收入只有一项，就是叔块奖励，计算公式为：

  叔块奖励 = (叔块高度 + 8 – 引用叔块的区块高度) * 普通区块奖励 / 8

“幽灵”（GHOST）协议

- 以太坊出块时间：设计为12秒，实际14~15秒左右
- 快速确认会带来区块的高作废率，由此链的安全性也会降低
- “幽灵”协议：Greedy Heaviest Observed SubTree，”GHOST”

  ——计算工作量证明时，不仅包括当前区块的祖区块，父区块，还要包括祖先块的作废的后代区块（“叔块”），将他们进行综合考虑。

  ——目前的协议要求下探到第七层（最早的简版设计是五层），也就是说，废区块只能以叔区块的身份被其父母的第二代至第七代后辈区块引用，而不能是更远关系的后辈区块。

  ——以太坊付给以“叔区块”身份为新块确认作出贡献的废区块7/8的奖励，把它们纳入计算的“侄子区块”将获得区块奖励的1/32，不过，交易费用不会奖励给叔区块。

以太坊和图灵完备

- 1936年，英国数学家艾伦·图灵（Alan Turing）创建了一个计算机的数学模型，它由一个控制器、一个读写头和一根无限长的工作带组成。纸带起着存储的作用，被分成一个个的小方格（可以看成磁带）；读写头能够读取纸带上的信息，以及将运算结果写进纸带；控制器则负责根据程序对搜集到的信息进行处理。在每个时刻，机器头都要从当前纸带上读入一个方格信息，然后结合自己的内部状态查找程序表，根据程序输出信息到纸带方格上，并转换自己的内部状态，然后进行移动纸带。
- 如果一个系统可以模拟任何图灵机，它就被定义为“图灵完备”（Turing Complete）的。这种系统称为通用图灵机（UTM）。
- 以太坊能够在称为以太坊虚拟机的状态机中执行存储程序，同时向内存读取和写入数据，使其成为图灵完备系统，因此成为通用图灵机。考虑到有限存储器的限制，以太坊可以计算任何可由任何图灵机计算的算法。
- 简单来说，以太坊中支持循环语句，理论上可以运行“无限循环”的程序。

去中心化应用

- 基于以太坊可以创建**智能合约**（Smart Contract）来构建

  去中心化应用（Decentralized Application，简称为 DApp）

- 以太坊的构想是成为 DApps 编程开发的平台

- DApp至少由以下组成：

  —— 区块链上的智能合约

  —— Web前端用户界面

以太坊应用

- 基于以太坊创建新的加密货币（CryptoCurrency，这种能力是 2017 年各种 ICO 泛滥的技术动因）
- 基于以太坊创建域名注册系统、博彩系统
- 基于以太坊开发去中心化的游戏，比如 2017 年底红极一时的以太猫（CryptoKitties，最高单只猫售价高达 80W 美元）

代币（Token）

- 代币（token）也称作通证，本意为“令牌”，代表有所有权的资产、货币、权限等在区块链上的抽象
- 可替代性通证（fungible token）：指的是基于区块链技术发行的，互相可以替代的，可以接近无限拆分的token
- 非同质通证（non-fungible token）： 指的是基于区块链技术发行的，唯一的，不可替代的，大多数情况下不可拆分的token，如加密猫（CryptoKitties）

名词解释

- **EIP：** Ethereum Improvement Proposals，以太坊改进建议
- **ERC：**Ethereum Request for Comments的缩写，以太坊征求意见。一些EIP被标记为ERC，表示试图定义以太坊使用的特定标准的提议
- **EOA：**External Owned Account，外部账户。由以太坊网络的人类用户创建的账户
- **Ethash：**以太坊1.0 的工作量证明算法。
- **HD钱包：**使用分层确定性（HD protocol）密钥创建和转账协议（BIP32）的钱包。
- **Keccak256：**以太坊中使用的密码哈希函数。Keccak256 被标准化为SHA-3
- **Nonce：**在密码学中，术语nonce用于指代只能使用一次的值。以太坊使用两种类型的随机数，账户随机数和POW随机数

Q&A


尚硅谷