

以下为本入门手册目录：

一、以太坊是什么？

二、以太坊代币

三、节点、网络、账户与钱包

四、以太坊挖矿

五、智能合约与DApp开发

六、以太坊的发展历史

七、以太坊社区治理：基金会、社群、贡献者介绍

八、其他

一、以太坊是什么？

什么是以太坊？根据以太坊白皮书定义，以太坊是一个全新开放的区块链平台，它允许任何人在平台中建立和使用通过区块链技术运行的去中心化应用；它是一个开放源代码的项目，由全球范围内的很多人共同创建，允许用户按照自己的意愿创建复杂的操作；以太坊核心是以太坊虚拟机（“EVM”）/智能合约，可以执行任意代码，用计算机科学术语说，以太坊的虚拟机是“图灵完备的”。

以太坊究竟是什么？推荐阅读以太坊创始人 Vitalik Buterin 的文章《以太坊是什么》。

此外，我们建议大家阅读一下以太坊白皮书，尽管不一定能全部看懂，但是可以从一个更高的维度去把握以太坊。除了白皮书，以太坊还有黄皮书、紫皮书。

以太坊白皮书：2014 年初，由以太坊创始人 Vitalik Buterin（V 神）发表，从技术方面来看，白皮书只是描述了一种新技术的理论（英文版/中文版）；

以太坊黄皮书：2014 年 4 月，由 Gavin Wood 博士（以太坊联合创始人兼 CTO）发布，号称以太坊的技术圣经，将以太坊虚拟机（EVM）等重要技术规格化（中文版/英文版）；

以太坊紫皮书：2016 年，V 神发布了一份紫皮书，为解决区块链的效率和能耗问题，提供了一种将 POS 和基于分片证明进行合并的解决方案，包括提高可扩展性、确保经济终结性和提高计算机抗审查等（英文版/中文版）。

关于以太坊，国内和国外都有一些以太坊文库可以参考，Odaily 星球日报推荐：《以太坊官方中文文档》、以太坊爱好者知识库、ethdocs 英文版；如果不愿意看文字版的，视频也是个不错的选择，推荐《以太坊入门》。

## 二、以太坊代币

2014 年 1 月，Vitalik

在美国佛罗里达州迈阿密举行的北美比特币会议上正式宣布了以太坊。

同年 6 月，以太坊基金（Stiftung Ethereum）在瑞士楚格成立，并在随后的 42 天内对第一批公开预售的以太币进行分配，净赚 31591 比特币，当时价值 1840 万美元，售出大约 6010 万个以太币。销售所得首先用于偿还日益增加的法律债务，回报开发者们数月以来的努力，以及资助以太坊的持续开发。

代币是什么？

什么是以太坊代币？简单来讲，以太坊代币是内置在以太坊区块链上的数字资产。如果将以太坊区块链看作一个程序，代币在某种程度上就是程序中的流通货币/积分，不同的是，传统的积分只能由程序的设置者发行，而以太坊上的代币任何人都可以发行。

以太坊上的代币分为两种：一种是以太坊区块链原生代币以太币（ETH）；另一种是按照以太坊提供的工具和标准开发所发行的代币（比如BNB）。两者的区别最直观在于流通场景，ETH是以太坊网络的通货，链上的每次操作/交易都需要付燃料费（有点像手续费）；BNB等代币无法支付燃料，只有ETH可以。在币安、火币和OKex等链下交易所、链上去中心化交易所或线下P2P，BNB等代币也可以按一定比率换成ETH。

代币可以固定总发行量以及流通量，也可以不固定，比如ETH至今仍未停止增发，尽管去年4月Vitalik曾提议将ETH供应量上限定为1.2亿。

代币可以用来做什么呢？每个代币的属性和功能都要遵守其预期用途的约束，比如支付访问网络、驱动智能合约、激励用户对某个协议的使用或者充当生态运行燃料（即Gas，下面会解释）。当然也有一些代币没有任何实际用途，在其生态中也并非完全必须的，发行代币也只是项目圈钱的手段。

代币通常通过“原始货币众筹”（Initial Coin Offering, ICO）的销售方式或者挖矿（后文会解释）的方式进入公众视野。代币创建者会通过提供内置代币，来交换以太币、比特币或其他数字资产。2017年的ICO热潮就是这样被炒起来的，鱼龙混杂，各种跑路事件层出不穷。

推荐阅读《代币为什么存在，如何使用》、《以太坊代币入门指南》以及以太坊创始人V神的文章《关于代币发售模型》。

## 代币标准

目前，以太坊上代币超过1000种，不同的代币发行标准也各不相同。最常见的就是ERC-20代币，它也是各个代币的标准接口。不同的标准有不同特点，比如ERC-20代币可以继续分解，更类似货币；但是ERC-721即非同质代币（NFTs）却是不可以。目前ERC-20是最多项目用于发币的标准。

然而，ERC-20代币标准很可能造成终端用户的资金丢失，主要的问题在于无法处理ERC-20代币转账函数执行的ERC-20收入交易，ERC-233应运而生。ERC-233定义了一

个标准函数，能够防止意外发送代币到（不支持该标准的）合约中，同时也让代币的转账就像以太坊转账一样。

除此之外，还有 ERC-777（基于操作者的代币标准）、ERC-809（非同质代币的租赁标准）等 23 种不同的代币发行标准。想要了解更多，可以阅读。

### 查询工具推荐

关于ERC-20 代币，有一个专门的网站可以查询，这便是 ethplorer——它可以查询以太坊上代币及代币排名比较。你知道以太坊生态中除了ETH，那个代币的市值最高吗？这个网站可以给你答案。除此之外，它还有其他功能，包括钱包、ICO查询（收费）。

对于二级市场的参与者，尤其是参与过多次私募的投资者而言，最害怕的就是项目方套现跑路。dapppcapitulation浏览器不仅可以看到以太坊创世“巨鲸”的账户余额，还能看到以太坊上各个项目方的账户余额，防止项目方套现跑路。

最后推荐一个可以查看以太坊链上的大额转账的浏览器——Tokenview，除了以太坊还有其他几十种代币都可以，数据可以追踪到几个月前。

## 三、节点、网络、账户与钱包

### 节点

节点可以简单理解为运行着以太坊客户端的计算机/服务器，所有以太坊节点通过网络连接组成主网。根据运行的客户端类型不同，可以分为全节点和轻节点，轻节点需要通过连接主节点获取最新数据和发起交易。

关于全节点、轻节点以及归档节点的区别，推荐阅读Odaily星球日报编译的《以太坊节点运行成本》；想要查看各个节点，推荐使用节点浏览器ethernodes。

### 帐户与钱包

以太坊帐户可以用来存储所有的以太坊代币（不仅仅是ETH），创建时不需要花费gas（EOS的账户创建要花费少量gas）。一个帐户就是一个私钥和公钥地址对。公钥可以理解为账户地址，私钥可以理解成账户的密码、钥匙。

区块链地址是根据非对称加密算法，生成私钥和公钥，从公钥根据一系列的计算推

导出地址。任何人都可以生成大量的私钥、公钥、地址，可是用人力自己计算非常不现实。区块链钱包正是帮助我们生成私钥、公钥、生成符合某个公链规范的工具。具体计算方式请参照《什么是区块链钱包》。

区块链钱包可以分为热钱包、冷钱包、托管钱包等不同种类，不同的钱包性质、安全性与易用性不同，其中热钱包易用性较高，但因为联网而容易被盗私钥；冷钱包本质是私钥存储工具、安全性较高；托管钱包则私钥由运营方托管。具体差异，推荐阅读《区块链数字货币钱包分类》。

以太坊钱包客户端也有很多种，推荐阅读《6种以太坊(ETH)钱包的基本介绍》：

**Ethereum 官方钱包：浏览器 Mist。**Mist是一个全节点钱包（全节点钱包通俗来说就是同步了全部的以太坊区块信息的钱包）。也就是说打开钱包后，电脑会自动同步全部的以太坊区块信息。优势是安全度高，不需要经过第三方发起交易，节点未同步完成之前无法查看地址余额；劣势是无法调整Gas价格，对网络要求高，需要连接全节点，才能发起交易。

**Parity 钱包：**原以太坊基金会部分成员开发的钱包。功能强大，也是一个全节点钱包。优势是安全度高，不需要经过第三方发起交易；劣势是对网络要求高，需要连接节点才能发起交易。

**imToken：**移动端钱包，操作简便，在imToken上生成的钱包私钥保存在手机本地，平台方并无备份。

请注意：这里我们需要辨析一点，节点、钱包、浏览器三者并未完全冲突的，成为节点可以说是做区块浏览器基础。就拿Mist来说，它是一个浏览器，因为它要查询数据，因此是构建在一个全节点上的；但与此同时，它也有管理功能，可以管理私钥和公钥，因此也是一个钱包。当然，并非所有的钱包都要求是全节点。

## 主网与测试网

以太坊一直以来有两种网络——主网以及测试网。主网，通常是所有客户端的默认网络；所谓的测试网是用来模拟主网的行为，功效与主网相同，因此开发者可以在测试网上开发和测试自己的智能合约、发币等等，作为上链前的环境评估。反之，当主网对以太坊协议进行任何重大改变时，其测试主要在这些测试网络上完成。

最常用的3种测试网分别是 Ropsten、Kovan、Rinkeby。

**Ropsten：**只支持 geth 客户端，一个 POW

的区块链，非常类似于以太坊主网，但由于低计算量，容易遭到 DDOS 攻击。过去受到垃圾攻击，问题较多。

Kovan：只支持 Parity 客户端；一个 POA 的区块链，不能挖矿。

Rinkeby：支持 geth和Parity 客户端；一个POA的区块链，不能挖矿。尽管计算量低，但是对恶意行为者更有弹性。

对于开发中的测试环境，建议使用 Rinkeby 或 KoVan 测试链。这是因为他们使用的工作量证明POA共识机制，确保交易和块能够一致并及时的创建。

关于主网与测试网的更多内容，推荐阅读《以太坊测试网络testNet汇总》。

如果想要搭建自己的测试网络，推荐使用 kubernetes或者docker-compose，具体搭建过程可以参考《接入以太坊（Ethereum）测试网络》。

## 四、以太坊挖矿

### 挖矿

上文已经提到，代币获得一个重要途径就是挖矿。“挖矿”实际上是一个增加货币供应量的过程。关于什么是挖矿，可以阅读Odaily星球日报的专栏《数字货币中的挖矿是什么？》

挖矿本质是在争夺记账权，获得某轮记账权矿工会获得：区块奖励，包含3个以太币（君士坦丁堡硬分叉后将降为两个）；区块链中交易发起人所支付的 gas 费；作为被引用叔块的区块，可以获得挖矿报酬的1/32。

由于以太坊采用 PoW（工作量证明）共识机制，计算（其实就是乱猜）出特定随机数的矿工可获得本轮记账权，理论上算力越大获得记账权的可能性越高，因为每秒可以计算（猜）的次数更多。难度动态调整的方式是每 15 秒整个网络会产生一个区块。

以太坊在很多方面与比特币类似，但也有些不同——以太坊区块不仅包含交易列表也包含最近状态，除此之外，区块数和难度也储存在区块中。

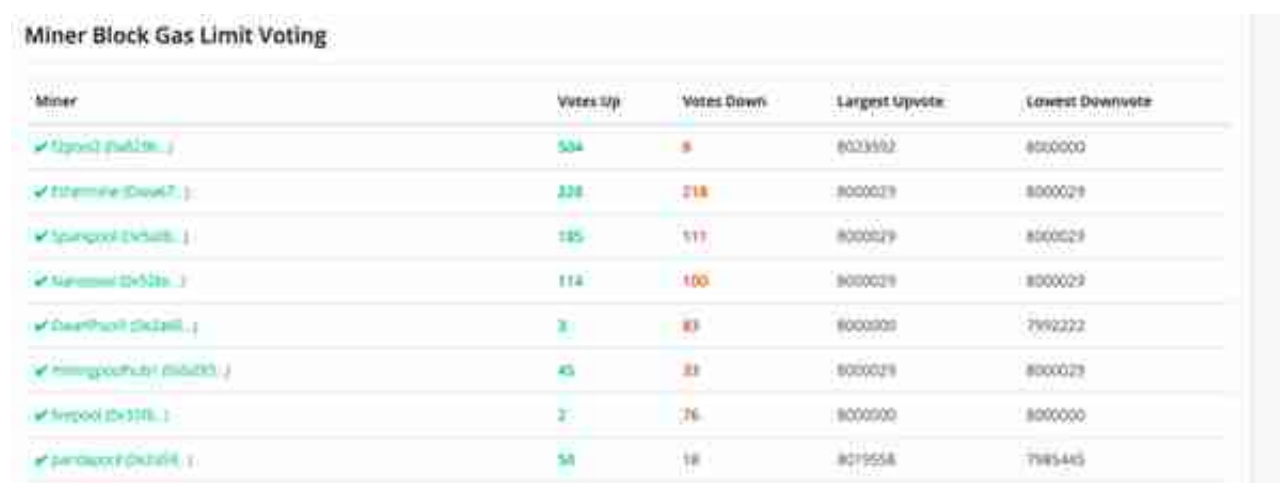
以太坊使用的 PoW 算法叫Ethash（Dagger-Hashimoto算法的改良版本），Ethash的工作量证明是内存难解的，这使它能抵抗ASIC。

## Gas

在以太坊上执行的每个计算步骤都需要花钱，这里的钱就是 gas。Gas 的设计目的—是为了避免繁琐的操作占用较多的有限资源，堵塞网络；二是为了避免整个网络遭受恶意攻击；三是为了让记账矿工获得一定的收益。

Gas 的价格由市场决定，类似于比特币的交易费机制。如果你的 gas 价格高，节点则将优先打包你的交易。

在这里，gas 费用其实是由两部分相乘得来： $\text{Gas price} * \text{Gas}$ 。这里的 Gas price 可选范围为 1 到 60 GWei，数额越大，交易处理速度越快；Gas 的可选范围是 800 万以上，如果数额较小，就会造成 gas 费用太小，因而不会被矿工打包。



Miner	Votes Up	Votes Down	Largest Upvote	Lowest Downvote
✓ Gpool (2x420k)	534	8	8000000	8000000
✓ Ethernine (2x407k)	328	218	8000029	8000029
✓ SparcPool (2x348k)	185	111	8000029	8000029
✓ Nanopool (2x328k)	114	100	8000029	8000029
✓ DeerPool (2x288k)	3	83	8000000	799222
✓ MiningpoolHub (2x285k)	45	83	8000029	8000029
✓ f2pool (2x278k)	2	76	8000000	8000000
✓ Antpool (2x268k)	54	18	8019554	7985445

总体而言，以太坊上“计算和存储”比在传统环境中做的更为昂贵；在以太坊网络上“读取状态”是免费的，只有“写入状态”是收费的。关于 Gas，要想了解更多，推荐阅读《计算以太坊合约成本》。

## 叔块

在比特币协议中，如果一个块不是最长链的一部分，那么它被称为是“孤块”。它也是合法的，但是发现得稍晚，或者是网络传输稍慢，而没有能成为最长的链的一部分。在比特币中，孤块没有意义，随后将被抛弃，发现这个孤块的矿工也拿不到采矿相关的奖励。

但 Ethereum 的 GHOST 协议，不认为孤块没有价值，而是会给与发现孤块的矿工以回报。在以太坊中，孤块被称为“叔块” (uncle block)，它们可以为安全链的安全作出贡献。

通过鼓励引用叔块，使引用主链获得更多的安全保证(因为孤块本身也是合法的)；给与叔块报酬，可以一定程度上缓解采矿中心化(矿池集中化)的问题。

关于叔块的更多内容，可以阅读《以太坊中的叔块(uncle block)》以及《以太坊叔块相关技术解析》。

## 矿机与矿池

在以太坊早期，可以用电脑的中央处理器（CPU）挖以太币，但自从显卡（GPU）矿工的效率高出两个数量级，CPU就不再盈利了。

后来出现了专门只用于数字货币挖矿的计算机，被称为“矿机”。

以太坊目前挖矿使用显卡挖矿，可选显卡是 AMD 显卡（简称“A卡”）或者 NVIDIA 显卡（简称“N卡”）——N卡常见选项是 GTX 1060、GTX 960、GTX 950、GTX 750 Ti等型号。

想要自己尝试挖矿的读者，推荐阅读《以太坊新手挖矿指南》。

显卡挖矿采用的 Ethash 算法曾被广泛认为是“抗ASIC”的，然而去年 4 月 4 日，比特大陆在 Twitter 上宣布正式发布适用于以太坊挖矿的 ASIC 矿机 Antminer E3，旨在打破以太坊本身设计中“抗 ASIC”的挖矿算法（EtHash 算法）。

不过，以太坊社区开发者们也并没有善罢甘休，他们不断提出新的方案，想以此抵抗来自比特大陆的侵染。据 Cointelegraph 1 月 5 日报道，以太坊核心开发人员已经就实现一种新的工作量证明（Prog-PoW）算法达成初步共识，该算法不仅可以增加 ASIC 矿机的挖矿“难度”，而且还可以稳定哈希速率，提高基于 GPU（而不是基于 ASIC）的网络挖矿效率。

不过目前，社区关于是否采用 Prog-PoW 以及何时采用尚未达成一致意见，在今年 2 月 1 日的公开电话会议上，以太坊开发人员决定推迟提交 ProgPow 升级代码，转而继续进行审计。

如果你想关注最新消息，可以加入以太坊群组 ProgPoW 参与讨论。

挖矿的另一个维度则是矿池垄断算力。根据 etherchain.org 数据，以太坊矿池算力占比目前排名是：Ethermine（30.37%）、SparkPool（16.24%）、NanoPool（15.51%）、F2Pool（12.37%），并且在过去 30



天乃至往前追溯半年，这个排名一直如此。

此对于散户而言，由于算力并不占优，出块的幸运值不高，很难挖到区块，因此不得不加入矿池，手续费大概在 1% 到 5%。

## 查询工具

查询挖矿收益可以参考网上的鱼池热门矿机页面或挖币网数据；

查询关于以太坊的算力、挖矿难度、出块数等各种数据，可使用各家以太坊区块链浏览器，除了基础数据，关于历史数据会用图表展现，适合各类统计，比如 etherscan和etherchain；

此外，BTC.com旗下的浏览器也可以查询以太坊相关情况。

## 五、智能合约与DApp开发

### 智能合约

以太坊上的程序称之为智能合约，它是代码和数据的集合。智能合约可以理解为在区块链上可以自动执行的、以代码形式编写的合同。很多博彩类区块链游戏就宣称自己使用了智能合约，可以自动赔付，不会有庄家操盘。推荐阅读Odaily星球日报专栏《智能合约是如何工作的？》以及《什么情况下智能合约应用案例难以实现？》

#### （1）编程

智能合约官方推荐的编程语言是 Solidity，文件扩展名以 .sol 结尾。Solidity 语言和 JavaScript 很相似，可以用它来开发合约并编译成以太坊虚拟机字节代码。

关于Solidity 语言开发，以太坊官方准备了下面的工具：

Solidity Documentation

· Solidity在线实时编译器

· 标准合约API

· Useful Dapp Patterns

## （2）运行

### EVM (Ethereum Virtual

Machine) ——以太坊虚拟机是以太坊上智能合约的运行环境。EVM 运行在以太坊节点上，把合约部署到以太坊网络上，合约就可以在以太坊网络中运行了。

虚拟机、智能合约和智能合约语言之间的关系，感兴趣的读者可以阅读《一文看懂区块链虚拟机》。

以太坊虚拟机上运行的是合约的字节码形式，我们需要在部署之前先对合约进行编译，可以选择 Browser-Solidity Web IDE或solc 编译器。

在以太坊上开发应用时，常常要使用到以太坊客户端（钱包）——使用钱包是用来管理代币的，这里有一个完整的 以太坊客户端列表。

Geth 是开发以太坊时最常使用的客户端，基于 Go 语言开发；另一个最常使用的是Parity，基于 Rust 开发。

## （3）部署

智能合约的部署是指把合约字节码发布到区块链上，并使用一个特定的地址来标示这个合约，这个地址称为合约账户。

合约部署之后，当需要调用这个智能合约时，只需要向这个合约账户发送消息（即交易）即可；通过消息触发后，智能合约的代码就会在EVM 中执行。

具体操作细节，推荐阅读《以太坊是什么 - 以太坊开发入门指南》，另外推荐以太坊开发者网站ethdev以及remix，他们提供基本的编译、测试网络、执行合约。

如果你想参考以太坊上已经开发的项目，可以登陆 Ethereum·Github。

## DApp

### 去中心化应用程序 (DApp) 与传统 APP

一样，都是提供一种服务，实现用户和提供商之间的直接交互。但区块链 DApp 拥有一些智能合约组合，这些合约组合可以实现 DApp 特定的功能。

去年下半年，区块链 DApp 被抬上风口，不少人认为它可以改变传统的中心化 App 所固有的问题（不透明、缺乏隐私等），然而目前 DApp

应用最广泛还是博彩类，游戏类次之。根据 Dapprader数据，以太坊 DApp 应用最高日活不超过 1500人。推荐阅读《什么是dapp？》

### （1）查询

您可以使用下列这些 DApp 查询工具：

- dappradar与dapp.review：除了查看以太坊，还可以查看EOS及Tron链上dapp；
- Mist：以太坊官方的 DApp 浏览器。
- Status：手机上可以使用的 DApp 浏览器。
- MetaMask：Google浏览器扩展，把 Chrome 变成了一个 DApp 浏览器。可以管理你的钱包，以及连接到不同的以太坊网络，包括本地的开发网络。
- Parity：以太坊客户端，也是一个 DApp 浏览器。

### （2）开发

如果想要开发一个Dapp，怎么操作？首先，Dapp 开发需要了解 Web3 Javascript API、Solidity 等编程语言，如下所示：

- Web3 JavaScript API- 当您想要与以太坊节点交互时，这是主要的 JavaScript SDK；
- Solidity Docs- Solidity是以太坊开发使用的智能合约语言，它为EVM（以太坊虚拟机）提供编译操作码；
- Solium- 严格遵守官方Solidity Style Guide制定规则的开发工具；
- 测试网络- 测试网络可帮助开发人员开发和测试以太坊代码以及进行网络交互；
- Dapp开发资源- 有助于开发、调试和部署以太坊应用程序，具体包括：智能合约ELI5、101 noob编写智能合约的介绍、标准化合约API列表。

关于dapp开发，也有一些教程，可供参考：

- 关于ethereum.org Dapp教程
- Dapps初学者教程系列
- Solidity教程系列
- 高级Solidity教程
- A contract packager for Ethereum and Javascript (formerly ether-pudding)

## 六、以太坊的发展现状

### 以太坊路线图

根据以太坊创始人 Vitalik 及 Gavin Wood 的规划，以太坊的发展被分为 4 个阶段：Frontier (前沿)、Homestead (家园)、Metropolis (大都会)和 Serenity (宁静)。

以太坊路线图如下：

Frontier (2015.7-2016.3)：以太坊发布测试版（非正式版），供开发者学习、试验并开始建立以太坊去中心化的应用和工具；

#### Homestead

(2016.3-2017.10)：以太坊发布正式版本，普通用户也可挖矿，中间经历了 4 次硬分叉，分叉出ETC；

Metropolis (2017.10-现在)：由 PoW 向 PoS

过渡，中间经历两次硬分叉——拜占庭与君士坦丁堡硬分叉；

Serenity (待定)：成为真正主流区块链，升级为 ETH 2.0。

目前，以太坊尚处于 Metropolis

(大都会)阶段，并且君士坦丁堡硬分叉还被推迟到 2019 年 2 月 27 日。关于 Serenity 阶段更多细节，推荐阅读 Vitalik 的《以太坊 Serenity 设计依据综述》。

关于以太坊发展历史的更多细节，推荐阅读《以太坊发展历史回顾》、《一篇文章带你了解以太坊的前世今生》以及《以太坊五年》。

## 扩容问题

以太坊至今仍处于成长初期，面临诸多问题——包括共识机制、吞吐量等问题，推荐阅读《以太坊的发展去向深度分析》。

对此，包括 Vitalik 在内的众多开发人员清楚认识到这一点，他们提出了一些基于“链下（off-chain）”和“第二层（layer 2）”的扩容解决方案——致力于构建基础架构和扩展以太坊性能——通常被称为扩展方案（scaling solutions），包括状态通道（state channels）、分片（sharding）、子链/侧链方案 Plasma 和 Truebit。Vitalik 更是宣称 Plasma 和 sharding 可能会产生一种协同效应，使得以太坊处理速度达到 100 万 TPS。

**状态通道（state channels）：**设计者希望通过“把很多处理流程转移到链下”，来提高区块链的使用效率，降低手续费，增加隐私的同时又能保留区块链可信赖的特性。状态通道是支付通道泛化出来的形式，但不仅限于支付，还可用于区块链上任意的“状态更新”，比如智能合约中的更改。

**分片（sharding）：**将以太坊网络的整个状态分割成一系列被称为分片的分区，其中包含自己独立的状态片及交易历史记录。在这种系统中，特定的节点只为特定的分片处理交易，从而允许在所有分片中处理的交易吞吐量比在单个分片中处理所有交易（像现在的主链一样）要高得多。

**Plasma：**和状态通道一样，Plasma 也是一种用于管理链下交易的技术，同时依靠底层的以太坊区块链来实现其安全性。但是 Plasma 采用了一种新思路，它是通过创建依附于“主”以太坊区块链的“子”区块链。这些子链又可以循序产生它们自己的子链，并能依次循环往复。

**Truebit：**Truebit 是一种帮助以太坊在链下进行繁重或者复杂运算的技术。它可以让基于以太坊的应用程序处理更复杂的事务并仍能被主链验证，对于提高以太坊区块链的总交易吞吐量更有效，这使得它与状态通道和 Plasma 不一样。

更多详细内容，推荐阅读《以太坊第2层扩容方案》、《什么是状态通道》、《V神：以太坊上的分片》、《如何扩展以太坊：分片原理解释》、《以太坊分片：overview and finality》、《以太坊 Plasma 解说》以及《Truebit × 管理未来》。

## ETH2.0

以上方案计划在 ETH 2.0 实现，目前以太坊研究团队提出了关于以太坊2.0的一些计划和设想。如果您希望详细了解，可以阅读

Odaliy星球日报编译的《以太坊2.0是什么？分成几个阶段？》以及Vitalik的《ETH 2.0》。根据文章，各阶段大致为：

阶段 0 引入信标链（ The Beacon Chain ）：这条链承担的其中一个职能是让验证者可以参与质押系统、替代矿工的角色而成为链的构建者。另一个职能是存储分片状态的索引。对信标链的详细介绍可阅读《以太坊2.0协议核心Beacon链详解》；

阶段0+ 入股：信标链以及每一条分片链将使用 Casper FFG 来完成出块。FFG 是一种权益证明算法（ Proof of Stake ），用于对链上不良行为实施罚没（即削减权益）；

阶段 1 分片：旨在就分片链的内容达成共识，并非对其意义达成共识。换言之，这是一次对分片结构的“试运行”，而不是尝试使用分片进行扩容（ Scale ）。信标链将分片链视为没有结构或意义简单的位（ Bit ）集合。分片链尚未拥有账户、资产或智能合约。

阶段 2 智能合约：熟悉的以太坊系统开始回归。此时，新的以太币 BETH 可实现转让，并且将重新引入智能合约。每个分片将基于 eWASM（我们称之为“EVM2”）管理一个虚拟机。

阶段 3 链下状态存储：尽可能减少链上状态，链上存储时并不用存储整个状态，用户将负责在链下存储完整的状态。EVM2 将支持我们熟悉的账户、合约、状态以及其他抽象内容。

阶段 4 分片智能合约：希望实现跨片通讯，但是存在很多尚待解决的困难，具体可看文章。

值得注意的是，2019 年 1 月 31 日，以太坊发布了向以太坊 2.0 网络演进的第0阶段第一个预发布版。

另外，核心开发者 Ben Edgington 每周会发布关于 Eth 2.0 信标链（ Beacon ）第 0 阶段规范的更新，值得关注一下。

以上关于以太坊研究研究进展的最新情况，均可以在下文的社群中获得最新消息，可以密切关注。

七、以太坊社区治理：基金会、社区、贡献者介绍

以太坊基金会

2014年6月，以太坊基金会瑞士注册成立，是一家非营利性机构，旨在管理以太坊销售中筹措的基金，以更好地为以太坊和去中心化技术生态系统服务。它主要但并非唯一的重心是促进以太坊协议和相关技术的开发，以及扶持使用以太坊技术及协议的应用。

以太坊基金会的官方沟通通常在以太坊博客上以发帖形式呈现——有些帖子是技术性的、有些是组织性的、有些是个人的，所有博客帖子都在Twitter和Reddit上公开。

另外，基金会还会在Youtube频道上主持一些开发者会议，比如1月18日晚上关于延迟君士坦丁堡分叉的核心开发者电话会议。

相关入口总结：官网网站（主要入口）；社区；博客；推特；Youtube；Facebook（不怎么更新）；电子邮件（很慢，但很有用，紧急情况可以发邮件）。

## 社区

以太坊 reddit论坛是最全面的以太坊论坛，很多讨论都是在这里完成的，其中的核心开发者也很活跃。但这里很难获得实际帮助和答案，建议大家选择Gitter Rooms和Stack Exchange。

Stack Exchange上采用问答形式，一人发帖，其他人踊跃留言，用户活跃度较高。

Gitter 是 Github 旗下的聊天软件，使用 Github 帐户登陆。它以太坊日常聊天的首选论坛，里面有很多的核心开发者，能够立刻获得想要的答案。开发者们通常在Gitter上聊天协作，然后在Github上提交代码。

另外 Gitter 不同的房间有不同的主题，最核心的是AllCoreDevs房间，这里聚集了几乎全部的以太坊开发者。

相关的 Gitter 房间总结：

go-ethereum——关于geth（与go实现相关的工具）

cpp-ethereum——关于eth（与C++实现相关的工具）

web3.js——关于web3.js（以太坊Java描述语言用户操作界面库）

Solidity——Solidity合约相关编程语言

serpent—— 用于合约开发的Serpent语言

mist —— GUI 资料获取和处理方式浏览器，官方钱包应用

light-client —— 关于light客户端和LES协议

research —— 以太坊研究

governance—— 关于开发者管理

whisper—— 匿名数据电报发表

swarm —— 去中心化的内容存储和分配网络

EIPs —— 以太坊改进协议(EIPs)讨论

ethereumjs-lib —— 以太坊核心功能的Java描述语言库

devp2p —— DEV' s点对点网络协议及框架

以太坊改进提案 ( EIPs )

以太坊改进协议计划 ( EIPS ) 旨在成为协调协议改进的框架和非正式商业流程。人们会首先向以太坊EIP资源库提出想法作为一个问题或pull请求。经过基本的过滤，提议会收到一个数字并以草稿的形式发布。必须经过社区一致同意，以太坊改进协议才能变成活跃状态。从提出改变到最终的同意，取决于以太坊用户的共识。对于以太坊改进协议的讨论，可进入 [gitter 关于以太坊改进协议的频道](#)。

EIP 指南和 EIP 示例

EIP 模板

EIP 存储库和 README

用于 EIP 讨论的 [gitter 频道](#)

Meetups

以太坊的 Meetups 分布在世界各地，他们通常会举办线下见面会，讨论技术以及



行业发展，抱团取暖。

Meetup 线下见面会资源表

以太坊论坛上的Meetup频道