3-2 以太坊

现代社会的我们在日常生活中使用电子邮件、社交软件、电子支付、电子商务等各种各样的应用程序与服务。但是，这些机制都是服务商承担了中央集权型管理，因此如果对服务商没有一定程度信任是享受不了这么多样化的服务的。服务总是存在停止的可能性的，实际上因为服务停止而遭受损失的案例时有发生。

比如，云存储服务、电子商务网站或社交软件停止的话，该服务就会无法使用。还有，全部的信息都集中在服务提供商的一个地方，即使服务没有停止，也有数据损坏丢失或外泄的风险。最近通过源码寄存管理服务“GitLab”[1]的数据丢失的事故也不再是新闻了。

另外，发送给服务商的信息应该存放于从外部无法访问的地方，可还是每天都有企业信息外泄的新闻传出。实际上，虽然使用条款与约定中记录了服务商将如何使用信息，但是现状是很难令人相信的。还有国家对聊天内容会做的审查，这就很难让人对管理者报以全部的信赖。

但是，区块链的结构是不需要管理员的。在区块链结构上构建的应用程序，可以实现不需要管理员的服务，根据这种设想而来的就是以太坊（Ethereum）了。

3-2-1 什么是以太坊?

以太坊是由以太坊基金开发的分散式应用程序平台，是2013年由当时19岁的Vitalik Buterin开始开发的，基于比特币的创意在区块链网络上安装应用程序、支持Script语言的平台。

通过使用一种被称为ETH的虚拟货币可以实现应用程序的开发和利用。在以太坊上运行的应用程序，需要事先确定程序运行的前提条件，运行中会按照规定操作，一般这就是前面所说的智能合约了。

1 https://gitlab.com/

3-2-2 以太坊的起源

Vitalik Buterin在17岁时与比特币结缘（从父亲处听说）。对比特币很有兴趣的Vitalik开始通过网络论坛等收集信息，并开始撰写一些比特币相关的栏目（当时写一篇文章可以得到5 BTC）。

在大学学习时，Vitalik每周30小时以上的精力都投入到与比特币相关的项目，后来退学，为了见识到更多项目而开始了世界旅行。在5个月的旅途中明白了可以将区块链用于加密货币之外的事情，但那时的区块链项目对应用程序的开发和运用来说并不怎么好用。

因此Vitalik有了一个设想，开发一个通用区块链，代替转为特定应用程序而开发的区块链，只要写好应用程序的源码就可以在区块链上运行。

这种实验性开发出来的应用程序运行平台就是以太坊。以太坊之前的区块链程序，都是为了达成各种特殊目的而开发的，而以太坊则订立了具有通用性的协议。

3-2-3 以太坊=世界计算机

Vitalik曾将以太坊解释为“世界计算机”。世界计算机意味着将整个世界都当作一台计算机来使用。

以太坊区块链是由世界中存在的无数的电脑构成的，即使有的计算机出故障或者断电关机，只要有1台运行的话，在分散式网络上的区块链就不会停止。所以，区块链上运行的应用程序不会有故障，将会一直运行。

以太坊区块链不受国家限制，不受管束，其运行日志与状态会保存在区块链上，并且保持公开不断运转。

3-2-4 以太坊的历史与轨迹

以太坊在发布最初的定位是实验性平台。经过4个阶段的反复升级，将最终进化成理想的完整形态。该升级过程是以硬分叉形式被实施的。

以太坊的发展轨迹如下表所示（表3.2.4.1）。

截止本书起笔时，仍处于下表第三行中的Metropolis阶段（2018年1月）。因为原计划Metropolis是分为两部分实施的，目前进度是第一阶段的Byzantium。经过提供平台功能、稳定化与高速化，以及加密化与匿名化的优化安装，最终的目标是共识算法Proof of Stake。

表3.2.4.1：以太坊的历史和轨迹

Flontier	2015年7月30日实施，安装命令行界面、分散式应用程序的开发基础、测试、挖矿
Homestead	2016年3月14日开始实施，交易的高速化和稳定化
Metropolis	第一阶段的Byzantium于2017年10月17日起实施，零知识证明zk-SNARK、区块生成时间稳定化，返还Gas，准备Pos迁移 第二阶段的Constantinople预定于2018年实行
Serenity	施行日期未定、预定安装Proof of Stake

接下来预定在第四阶段中安装的Proof of Stake是指根据保有的加密货币数量获取区块生成的报酬。由于在比特币的工作量证明中是根据计算量来获取报酬的，所以会形成计算量的竞争，产生的现实问题就是为了得到区块链生成的报酬而消费大量电力。

Proof of Stake的目标是降低工作量证明的资源消耗成本。而且，比特币中恐怕会有非法用户用大量的计算力来篡改区块的危险。在Proof of Stake中攻击网络的话，自己所持货币的信用价值将会下降，这算是一种遏制攻击动机的机制。Proof of Stake相关内容将会在“10-2 Proof of Work协议的扩展”中详细说明。