第5讲 | 如何理解数字货币？它与区块链又是什么样的关系？

2018-04-04 陈浩

深入浅出区块链 进入课程 >

讲述：黄洲君
时长 10:38　大小 4.87M

从历史进程来看，货币的形态主要经历了几次变化。从早期社会如兽皮、牲畜、陶器的物物交换，到各种贝壳类的货币，再到后面的铜币，乃至后来人们选择了黄金和白银作为流通货币。

随着消费需求不断增加，人们发现可以通过发行纸币来替代贵金属，于是，我们就一起进入了信用货币的阶段。后来，技术的发展促进了电子货币的产生。现如今区块链技术的大热，它的第一个应用就是数字货币。

数字货币的概念

数字货币通常是国内的叫法，在国外，它一般称作“加密货币”。数字货币听起来比加密货币更抽象一点，“数字”旨在表现它不同于传统货币的行为，即它可以通过“数字”表现更

多自定义的行为。

那么，如何用一句话来解释什么是“数字货币”（加密货币）呢？我们可以这样形容：数字货币通常是基于区块链技术、在全球范围内公开发行的、并且没有任何国家政府背书的虚拟货币，这种虚拟货币具有“去信任”、“点对点”、“公开记账”、“不可篡改”等特征。

既然聊到了虚拟货币，我们正好可以把电子货币、虚拟货币、数字货币（加密货币）的概念捋一捋。

1. 电子货币

近年来，现金使用的频度降低，很多人首选使用电子支付。电子货币和数字货币一样都是无形的，但是电子货币其实就是将法币电子化，例如第三方支付平台，银行卡电子现金，银行大小额支付系统等等。它只是以电子的方式记录了原来法币的账目，从本质上来说，它们仍然需要在多个中心化系统中进行稽核、对账，“电子”本身并没有成为金融的一部分。

2. 虚拟货币

在 2017 年区块链投机狂热的时候，“虚拟货币”这个词基本是用来指区块链项目的基础代币，这样的叫法大多源自于圈外投机者。其实不然，虚拟货币所指代的概念远比电子货币以及数字货币都要更加广泛。

虚拟货币通常是由非金融机构发行的非实体货币，大致分为三类。

第一类比如游戏代币，通常不与实体经济发生联系。例如在《王者荣耀》这款游戏中，如果你想要得到新的道具，就必须有足够的游戏代币（钻石和点券），这种虚拟货币还有个特征就是封闭性，即只能在这款游戏中使用。

第二类是积分类，它可以与实体经济发生联系，比如常旅客积分，超市礼品卡，这种虚拟货币也有个特征叫做单向性，即只能流入，而不能流出。

第三类自然就是我们主要讲的数字货币（加密货币）了，比特币便是其中典型。

综合来看，与法币的“有形”对应，虚拟货币更多地体现在它的“虚拟无形”上，随着互联网的发展，虚拟货币本身也在逐渐发展，从而诞生了更多新的模式与机遇。

3. 数字货币

数字货币一般是指公有区块链平台底下的基础代币，该代币被记录在由密码学保证的一套公开账本上，与传统货币不同的是，由于去中心化以及可编程等特性，此种货币具有可自定义行为的属性。

在比特币中，我们可以定义多重签名交易来实现真正意义上的“由多人共同掌管的机构型账户”。

比如，在元界上，用户可以自定义交易的行为，例如在转账时可以指定代币的一个锁定期，并且指定解锁条件；而在比特股中，这种行为更被强化为具有衍生品特性的货币，这在传统货币领域是不可想象的。

与数字货币对应的，还有数字资产这个概念，不过这是另外一个话题了，□后续我会有详细的讲解。

传统货币与数字货币

正因为数字货币的诸多新特性，所以金融机构和互联网公司纷纷加入研究行列，越来越多的人想要研究数字货币，这里，我想带你对比数字货币和传统货币的不同特性，以便你可以更直观地了解数字货币和传统货币的不同。

匿名性 vs 实名制

传统货币在支付过程中，除了现金，其他任何方式基本都或多或少地保留了交易者的信息，无论你是个人还是机构，运营商都可以使用这些交易数据来跟踪你的活动。

而在数字货币领域，这件事就无足轻重了，目前大部分数字货币具有假匿名性，即化名性，所以并不会被查到你自己的私人资料。

同时，由于区块链上未提供 KYC（Know Your Customer）功能，也就是充分了解你的客户，对账户持有人的强化审查，所以让监管者很难追踪到交易者的信息，也让数字货币成为了黑市交易的温床。

这样的缺点主要是因为不少公链代币设计中没有加入身份的概念，不过这在我这样的技术人的角度来看，只是算是一个需求，而不是数字货币本身存在的缺陷。

点对点 vs 中心化

数字货币的发行主体通常是项目发起方，并且会在白皮书中定义好数字货币的发行过程；在主网上线以后，所有的代币会根据一开始设计好的发行过程缓慢释放到市场，这个过程其实就是大家喜闻乐见的“挖矿”过程。

所以在主网上线以后，即使作为项目发起方，也几乎很难有权利再次修改发行机制，所有人只能以提案的形式递交到社区进行讨论，讨论的最终结果决定了能否被再次修改。

这个过程其实与民主选举的过程很相似，而在□信用货币领域，发行主体通常是央行，央行可以通过货币的政策进行宏观调控，从某种意义上来说，央行模式是中心化的极致体现，□而数字货币则属于点对点机制的体现。

自理型安全性 vs 托管型安全性

由于数字货币的交易过程需要网络中每个节点的认可，且每一笔交易都被记录在区块链上，所以历史交易记录永远不用担心丢失或者被篡改。

只要数字货币基础的加密算法不被攻破，并且保护好私钥，你的资产便是真正意义上、只属于你自己的资产。

传统货币的交易过程最终是落到银行的，所以银行系统的安全性决定了传统货币在使用过程中的安全阈值，这也表示你的资产是托管在银行的。

广区域流通 vs 国家内部流通

传统货币是有主权的，通常只在主权国家范围内流通；数字货币目前却没有这样的限制，只要你能连上互联网，你就可以随时随地发送交易到任意地域。

总结来看，数字货币目前也有很大风险，如今还没有比较完整规范的法律法规来约束数字货币的使用者，所以使用数字货币会有较高的法律与投资的风险□。

而且普通人已经接受了信用货币这种设定，目前对数字货币的接受度在各国并不一样，例如在中国大陆接受度低，在日本接受度高。

数字货币的发行过程

数字货币在 2016 年开始加速，2017 年借助 ICO 呈井喷式发展，数字货币市场形成了一个大泡沫，这与 2000 年初的互联网泡沫十分相似，但是泡沫并不可怕，它只是一个热门新生

事物的必然过程。

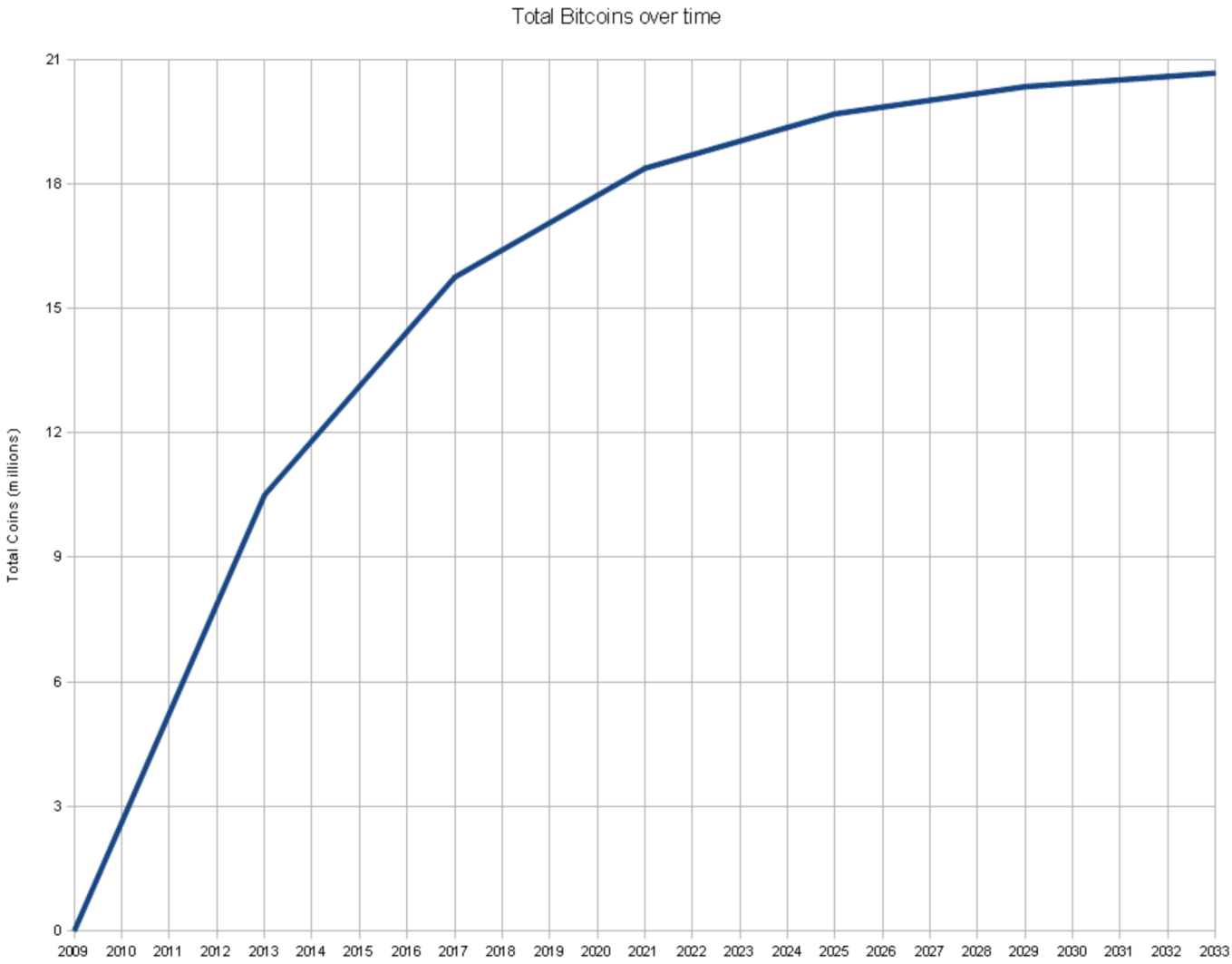
我们需要在这个泡沫中找到规律，那么首先就要了解数字货币的发行过程。我们可以以比特币为例子来聊聊它的发行过程。

比特币的发行过程是通过挖矿维持的，是依靠矿工挖矿产生比特币。相当于矿工自己就是一个小型的印钞机。

矿工每挖出一个区块，也就是在第二篇文章中提到的“打包一个信封”，会产生一个 Coinbase 交易，这个 Coinbase 交易相当于凭空产生了币，矿工□可以从 Coinbase 获得比特币，作为维护系统的奖励。

Coinbase 的产出是每 4 年衰减一半的，□第一个 4 年是挖出每个块 50 个比特币，第二个 4 年的周期就是挖出每块产出 25 个，目前比特币处于第三个 4 年，Coinbase 产出 12.5 个比特币的阶段。

以上逻辑是比特币白皮书和比特币代码规定好的，所有比特币的参与者可以进行验证。并且根据以上逻辑，我们可以画出如下的发行曲线。



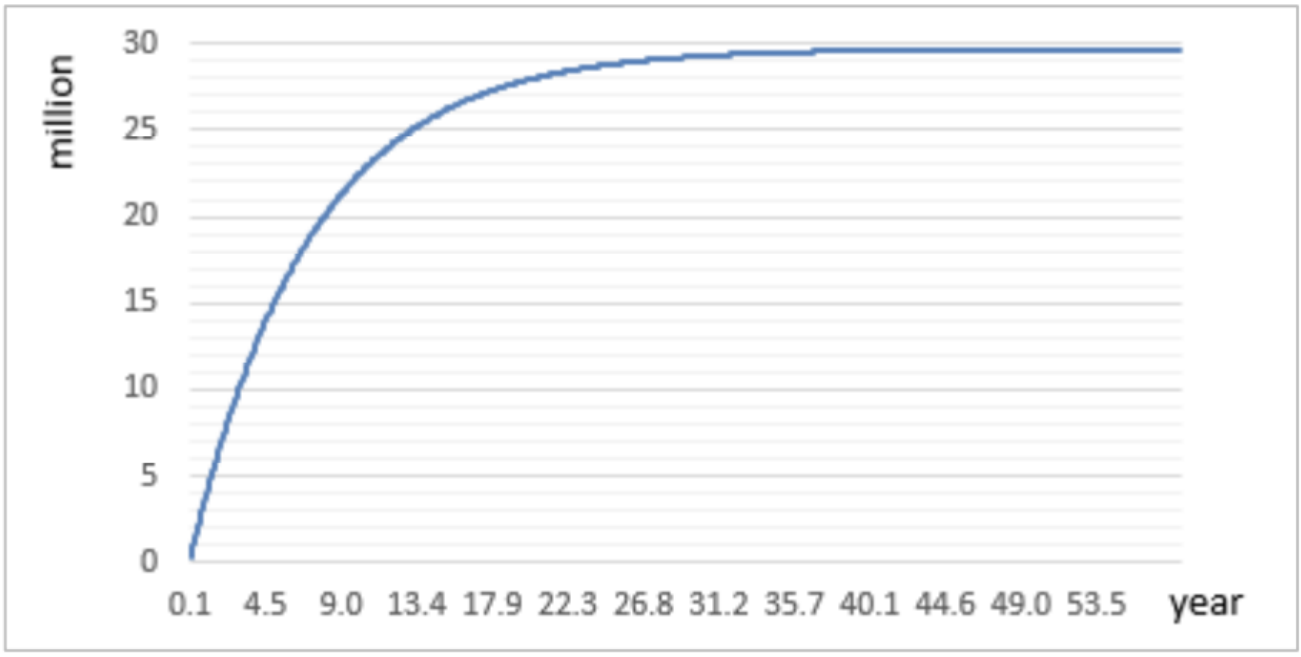
（图引用自网络）

我们可以看到，比特币的发行过程每隔四年发生一次改变，发行速率逐渐降低，随着时间推移趋于平缓。

同理，我们在其他数字货币项目就可以看到类似曲线，不过它们未必与比特币的发行曲线一样，有可能是离散式的，有可能是线性的，这取决于白皮书中规定的发行过程。

例如熵币 ETP 的发行过程也是一个衰减过程，不过 ETP 的衰减系数是 0.95，所以相对比特币可以说更光滑了，它随着时间收敛到挖矿总量 3000 万，那么这个曲线看起来是这样的。

POW 挖矿的 ETP 发行总量随时间变化示意图



每 50 万个块总奖励的衰减示意图

所以数字货币的发行过程可以认为是一个区块链项目的核心利益分配的过程，也是一个社区激励的过程，如何把有限的代币派发给愿意为项目付出的社区人，是考量一个区块链项目运营成熟度的重要指标。

总结

今天，我简单介绍了数字货币，相信你对于数字货币已经有了一个初步的了解，数字货币作为区块链的第一个应用，已经广泛地被人们所熟知，并且大有燎原之势。

除了社区型的非盈利性开源数字货币项目，央行也在推动基于区块链交易平台，同时，由央行发行的法定数字货币也已经在这种平台上开始试运行。

可见数字货币的发展已经是未来的趋势，顺应着这种趋势，作为技术人的我们可以从中看到更大、更复杂的挑战。

这里给你留一个思考题，你可以在数字货币中看见怎样的挑战呢，你可以在下面留言，我们一起交流，感谢你的收听，我们下次再见。

上一篇 第4讲 | 区块链的应用类型

下一篇 第6讲 | 理解区块链之前，先上手体验一把数字货币

精选留言 (29)

写留言

Jalins
2018-04-04

28

有个问题想请教，区块链是每个节点都保存了整个账本的信息，那是不是意味着当整个账本越大时节点所需要提供的存储容量就越大，举个几点的例子，假如某一天这个账本的容量是几千T，那么除了矿工节点外，普通节点是否会消失？毕竟个人电脑也就500G到1T。

阿痕
2018-04-21

17

我认为所谓的数字货币（比特币）离真正的货币还很远，原因有：
1）交易成本太高。比特币由于太耗电，平均支付成本是传统货币的几百倍，且交易确认太长，少则两个小时，长则两天。
2）币值不够稳定。比特币动不动一天浮动10%，谁敢拿它作结算货币呢！

3）无法对经济的冷热进行调控。当前各国央行最大的一个职责是通过控制货币的发行量...

展开

杨洪林

2018-04-05

5

数字世界的交易如何约束物理世界？例如我通过比特币网络支付购买一部手机，但对方收到比特币就是不发货，谁来制约它呢？

作者回复: 你好，目前已经有基于比特币的第三方支付，如bitpay。

另外可以通过信用上链，让作弊成为单次博弈，无法多次使用。

在西方文化中，契约精神是商业的根本，所以相对来说，对比特币更宽容一些。

KingLiang

2018-04-04

5

您好，本人是程序开发人员，如果想加入区域链开发这块，目前需要做那些准备？有哪些书籍可以参考。

地瓜

2018-04-05

3

区块链本质上是一种新兴信息技术，数字货币是基于区块链技术的成功应用，比特币应运而生。虽然技术可以去中心化，但是社会管理仍然需要必要的中心化。没有政府背书的数字货币前景是令人担忧的！

展开

ytl

2018-04-04

3

去中性化数字货币面临的挑战是效率。
去中心化带来效率低下，账本每页（区块）不能太大，否则广播给每个节点的速度降低，账本大小被限制导致交易记录的数据量被限制。例如比特币平均一秒钟3-4笔交易。

老于

2

2018-04-05

不明白...数字货币怎么和钱发生关系?

展开

teletime

2018-04-04

2

数字货币发行，很容易变成非法集资。如何有效界定这两种行为?

展开

作者回复: 1. 看团队背景
2. 看项目白皮书，长期规划
3. 定期信息披露的内容

如果纳入金融监管，将降低普通人的进入门槛。

良辰美景

2018-04-04

1

我认为最主要的还是信用吧，数字货币已经有这么多了但有交易的就那么几种。这也就可以解释为什么现在有很多大公司发的所谓数字币会有高的关注度。本质还是大公司信用背书。分布式系统必然带来系统的复杂性，比如交易量是个问题。数字货币安全性的基础是加密算法。而随着芯片的发展和量子计算机的成熟，这样的基础是否会对数字货币产生影响。

展开

加菲猫

2019-05-28

如何降低比特币的使用门槛?

展开

三木四水

2019-01-22

陈老师您好，我在网上看到说目前在我国数字货币是不合法的，央行也没有发行或者授权过任何机构发行数字货币?

maomaosty...
2019-01-01

如果单纯看数字货币的场景，这么多参与者图什么呢？就为了获得币？单纯为挖矿而卖力么？

---

niken
2018-09-12

在master bitcoin中有提到被挖空后，矿工就是拿手续费来维持运营

展开

> 作者回复: 这也是理想情况，实际上会把单笔交易的手续费推得非常高，可能会超过100元甚至更多

狩魔天使范...
2018-08-18

有意思

展开

meta
2018-08-02

越来越清楚！继续加油！

展开

> 作者回复: 感谢，希望你能通过本专栏快速入门哟

Xmen
2018-07-02

刚刚开始学习，1、请问是不是产生交易了，才会有挖矿；2、如果挖矿者迟迟没有算出，是不是交易就不能完成呢？麻烦解答一下，谢谢🙏！

> 作者回复: 1. 挖矿本身也会产生一种交易叫做coinbase交易，如果全网没有其他交易，这个叫做空块，是很正常的。
> 2. 是的，没有完成。

尼克

2018-06-29

老师，请解释一下token是什么，如何在数字货币的交易过程中发挥作用?

展开

作者回复: 抱歉，回复这么晚。token通俗讲就是一种凭证，可以是物权凭证，也可以是股权凭证。是一种泛化的登记和记账工具。

Xmen

2018-06-25

您好，才学习区块链，有一个问题不理解：每挖一个区块就会产生一笔交易，那要是没被挖出是不是交易就完成不了，这样是不是会影响效率。换一句话说，如如果没有交易是不是就没有区块可以挖?

展开

Xmen

2018-06-25

您好，才学习区块链，有个问题不理解：每挖出一个区块，就会产生一笔交易。那要是没被挖出，交易是不是就不能完成。换一句话说，没有交易，是不是就没有区块可以挖?

展开

乖乖

2018-05-31

现在数字货币的交易，更加依赖于契约精神，暂时不适用于祖国国情

展开

作者回复: 赞同