第一讲 数字货币

引言

区块链，一门现代而潮流的技术；密码学，一门古老而神秘的学问；区块链的技术原理是怎样的？密码学就是加密的学问吗？它是怎样在区块链中大放异彩的？

我们在接下来的课程中，以区块链在数字货币中的应用为主线，为你讲述密码学的技术原理及其在区块链中的运用。

尽管现如今区块链也在数字货币之外的其它很多场景中得到使用，但区块链确实脱胎于数字货币——比特币，生来就是为数字货币服务的；另一方面，区块链的分布式记账机制又依赖于类数字货币的激励。所以，可以说区块链和数字货币是一对孪生兄弟，在某中程度上互相依存。所以要搞清楚区块链，我们需要从数字货币开始讲起。

比特币的重要历史事件

只要你不是原始人，你一定听说过比特币。作为全球第一大数字货币，它是怎么来的呢？

- 2008年11月1日，小光棍节，中本聪发布了比特币白皮书，这个白皮书只是当时好多好多种数字货币方案中的一种，并没有引起足够重视；
- 2个月后，中本聪发布了自己开发的比特币客户端，通过挖矿生成了比特币区块链的第一个块，并由此获得50个比特币奖励；
- 一年后，中本聪向另一个人的账户转账了10个比特币，实现了历史上第一次不依赖于信任中心的转账；
- 又是一年多后，这一天被称为比特币披萨日，这个人Laszlo Hanyecz花了1万比特币买了披萨，标志这有人开始把比特币作为货币流通；
- 既然比特币基本具备了货币流通的基本功能，那么它就会和其它法定货币之间产生汇率，于是很快出现了比特币交易所；
- 到2011年2月份时，1比特已经与1美元等价；
- 2个月后，中本聪宣布离开，从此杳无音信；
- 到2017年年底时，1比特币报价首次突破2万美元；
- 到我们课程制作时，1比特币报价又跌破4000美元

听完关于比特币重要历史时刻的介绍，你可能已经冒出了好多问题。

比如，

- 中本聪是什么人啊？一个大活人怎么说消失就消失了呢？
- 为什么要数字货币？
- 数字货币和区块链又是什么关系？

中本聪何许人也，这要从密码朋克说起，cypherpunk，是由一群密码学家自发成立的一个组织，他们致力于用密码学、匿名邮件转发系统、数字签名、电子货币保障隐私。

中本聪正是使用匿名邮件转发系统在2018年发布了这个著名的帖子。在这个帖子中，他提及：我正在开发一种新的电子货币系统，采用完全点对点的形式，而且无需授信第三方的介入。这个电子货币系统，就是比特币。

不仅如此，他还在行文中不停变换语言习惯，避免被别人发现他的真实身份；完全可以用神龙见首不见尾形式，尽管外界对他的真实身份有很多猜测，也不乏自称中本聪的人，但中本聪究竟何许人也依然是个谜。

为什么有人要研究货币数字化

为什么那么多人要研究货币数字化?

便捷

第一个原因：为了支付便捷。从远古的贝壳，到古代的黄金、白银，近代的银票、钞票，再到现代的支付宝、微信钱包等，货币的形态的演变都是为了支付越来越便捷。

去除对中心节点的依赖

如果仅仅是为了便捷的话，现如今的支付宝、微信钱包等支付平台已经将货币数字化做的足够好了。很多人研究货币数字化的另一个重要原因是为了去除对中心节点的依赖。例如法定货币依赖于银行，支付宝依赖于阿里巴巴、微信钱包依赖于腾讯。有很多人试图建立一种无中心节点的货币，密码朋克的成员就不乏这类人，而中本聪则是他们中的佼佼者。

怎样对货币数字化

朴素方案——钞票数字化

那怎样把货币数字化呢？最朴素的想法，当然是把钞票变成数字，谁拥有这个数字就代表谁拥有这张钞票。只要稍微考虑一下支付的场景，你就知道这个想法行不通。比如我找你买一杯咖啡，我把代表钞票的一串数字发送给你，你把咖啡给我了；但是我把这串数字发给你了，并不代表我就不知道这个数字了，我还是拥有这个数字的副本的，之后我还可以把这串数字发给另一个人去买个一个面包。**这就是双花问题，double spending，把一份钱花两遍。**

怎么解决双花问题呢？我们再来听一个故事，这个故事能够进一步揭示货币的本质。

石币之岛的故事

这个故事就是著名的石币之岛的故事。

太平洋上有个岛叫雅浦岛，这个岛上有一群土著居民，距离这个岛400英里之外有另一个岛帕劳岛，帕劳岛岛上有一些石灰岩。这些土著居民就用这些石灰岩作为货币。为什么不用自己岛上的石头，而要用400英里之外的岛上的石头呢，因为实物货币一定要使用某种稀有物品代替，这和我们古时候用贝壳作为货币是一个道理。用石头做货币也没什么新奇，新奇的是，这些石头当然会有大有小，当石头太大时不便运输，他们就约定收款方不用把大石头从付款方家里搬回自己家，而是在这块大石头上把这笔交易记录下来并公示，得到大部分居民公认之后，这笔交易就生效了。这样一来就可能会出现一种奇特的现象，可能某个穷光蛋家里有好多石头，而一个土豪家里一块石头也没有。因为穷光蛋家里的石头记满了账，都是付款给别人的，而土豪有很多账记录在别人家里的石头上。

更神奇的还不止如此，岛上的首富并不是因为有很多账记录在别人家里，而是因为他们祖上曾经千辛万苦跑到400英里外的帕劳岛去开采石灰岩，当时他们挖到一块巨大无比的石头，但是很可惜在运回雅浦岛的途中掉海里了。虽然掉到海里了，但是当时很多人都见证了他们开采了这么一块巨大无比的石头，所以大家都公认他们家拥有这块大石头，于是他们家就成了岛上首富了。

你可能要问，他家里没有这块大石头，那他们家给别人付款时账记在哪里呢？很简单，记在大家的心里，只要这些账得到岛上居民大部分人的认可，就算是有效的。

通过这个故事，我们可以得到这样两点启示。

- **第一**， 货币数字化未必要对货币本身数字化，而应当是对交易数字化。你看岛上居民交易时未必真的要交换石头，只要交易记账生效即可；
- **第二**， 交易记账只要得到大部分人认可并由部分人记录下来即可生效，而不需要依赖某个信任中心统一记账。

由此可见，无中心货币数字化的切入点在于**交易数字化**和**记账去中心化。**那怎样对交易数字化呢？

交易数字化

如何将交易数字化呢？咱们先来看看交易应当包含哪些内容？

其实所谓交易，就像我们平常所说的转账单或者支票。

比如说，支票上最重要的信息有

1. 收款方账户
2. 付款方账户
3. 金额
4. 签名

所以归结起来，交易数字化需要解决的问题包括**账户数字化、金额数字化和签名数字化。**

其中，

- 账户在中心化数字货币中由中心节点（银行）按照某种规则为用户编码，其作用是唯一标识，保证唯一性即可；
- 金额的作用是区别资金数量，用整数或有理数表示即可；
- 签名在中心化数字货币中常用口令、指纹、签字等方式实现，其作用是身份认证；

可是如果没有中心节点，该怎么保证账户的唯一性？又该怎样实现签名机制来进行身份认证？

记账去中心化

在中心化数字货币中，可由中心节点（银行）检查交易是否合法，并承担记账的任务。那么在无中心节点的数字货币中该由谁来记账？如果秉承人人平等自愿的原则，就可能出现两方面问题。

- 无人记账。记账显然要耗费计算和存储资源，所以没有人会做损己利人的事；
- 账本不可信。既然人人可以记账，那么人人就都可以故意记错账或者篡改被人记的账，这样的分布式账本当然不可信。

所以在没有中心节点的情况下，该设计怎样的机制才能既有人记账，又让账本可信？

小结

在本堂课中，我们了解了为什么要研究货币数字化，即为了便捷和去除对中心节点的依赖；还了解了数字货币化所需解决的问题，也就是账户数字化、签名数字化和记账去中心化。

解决上述这些问题的钥匙，就是**区块链。**

再看这些问题，他们所要解决的本质问题实际上分别是唯一性问题、身份认证问题和分布式数据完整性问题。密码学则是解决这些本质问题的强有力工具。

货币数字化问题	**本质问题**
账户数字化	唯一性问题
签名数字化	身份认证问题
记账去中心化	分布式数据完整性问题

在接下来的课程中，我们就为大家介绍区块链中的密码学。