第29讲｜互联网身份与区块链数字身份

2018-05-30 陈浩

前面的一系列的文章，我们一起从区块链技术聊到了数字货币，接下来又讲到了数字资产的话题。相信你应该对区块链应该有了一些了解。接下来，我们将要进入一个全新的专题， 来聊聊区块链可以与互联网发生什么反应。

今天我要讲的是数字身份，为什么要聊身份这个概念呢？

这也是从比特币身上获得的启发，比特币上不存在无主的资产，也就说任意的资产必然归属到一个地址上。所以我们就在思考，是否可以更进一步，这种联系是否可以不仅限于地址，而是可以扩大到人的身上。

什么是身份

数字身份是一个依托互联网产生的概念。那么在谈论数字身份之前，我觉得有必要先和你达成一下“身份”这个概念的共识。

如果说比特币记账记录的是资产的转移，那么对应到身份上，也可以 抽象出类似的概念。

想象一下，“你的出生”这一事件是被谁所记录，“你昨天发的朋友圈”都在被谁所记录？

这么一来，身份的概念几乎也呼之欲出，身份是指有关你发生的一切客观历史的事件集合。

例如，你的身份证上简要记录了有关你的客观事实：你的出生日期、民族、户籍所在地，为了证明这些信息属实，所以国家给了这么一个证件，为此还额上了一个唯一编号，也就是你的身份证号。

但我们要弄清楚的是，身份证并不是你的身份，只是你的凭证，你真正的身份托管在政府机构、银行、医院、社交平台的数据库中，换句话说，有关你的重要客观历史事件记录被这些机构所记录下来，这些记录组成了独一无二的 你，使得你变得具有一定的辨识度。

你的身份记录也分为了两种，一种是资产和消费记录，另外一种是社交记录。支付宝做了前者，微信做了后者，这两者都是中心化的设施。

“身份”的前世今生

关于身份的难题古往今来一直有之，上至皇帝大臣，下至教书先生普通老百姓，如何证明自己的身份一直是一个难题。

从历史上来看，主要经历了三个阶段。

1. 印章实物身份

这个很好理解，就是自己给自己颁发一个刻章，这个章由于带有私人标记，一般独此一份，很难被人模仿，例如玉玺、虎符等，这些就是为了表达 身份的概念。

但是这个概念特别弱，因为古代生产力低下，无法大量记录客观事件，才把所有事件集合归并退化成一个小小的章。这也是不得已而为之，所以在古代谈不上准确的可定义身份概念，但是，现代的身份却也都是基于这种逻辑下产生的，例如我接下来要讲的卡片型身份。

2. 卡片型身份

随着技术发展，卡片的流行发展了身份的概念，这里的典型就是名片、护照、身份证、驾照等等。

但这些卡片背后记录的依然是割裂的身份片段，例如医院就诊记录归医院所有，出入境记录归出入境管理局所有，商场消费记录归商场所有，这些记录都是割裂的。

如果出入境管理要你出具商场的消费记录，显然就变成了你的跑腿工作，这就是你的身份片段割裂所引起的。

不过这种情况在国内稍有改善，这得益于身份实名制的强制实施，身份证编号是被所有系统统一的唯一索引，通过打通身份后台系统，可以共享一些基本信息。

卡片型身份也在自我迭代，目前多数都被做成了芯片卡的样式，里面集成了一些基本的终端验证信息，所以可以提供电子化身份。

3. 互联网身份

这个阶段就有了一些真正意义上的身份概念了。

你的出生地、户籍、微信朋友圈的记录、授权过的 App、消费记录、挂号就医记录，通过微信或支付宝可以将以往的身份片段串联起来，形成一个可定义你的唯一身份。

举个典型例子，微信和支付宝可以满足大多数场合的身份证明的要求，例如医院就诊使用微信预约，医院需要知道你登记的信息是否准确，所以可以通过微信授权。支付宝也是如此，芝麻信用甚至可以提供身份声誉的概念了。

这两者的最终一步只需要打通和政府机构的身份数据管理，那么互联网身份有了这份加持以后就可以变成身份的完全体了。

在中国的任意区域的绝大部分场景，出示微信或支付宝来证明身份似乎不再遥远。

现阶段的身份问题

总结来说，我们正处于卡片型和信息化身份混用的阶段，我们在日常交流中需要的身份证件，例如护照、驾照、社会保险卡、商品序列号等，基本都是由国家或第三方机构颁发的，虽然这可能是模拟现实世界运作的首要方法，但这种方式也逐渐凸显了许多问题。

1. 如果国家撤销其证书，个人可能会失去他们的身份，身份应当是与生俱来的概念，国家可以选择承认与否，但不应该存在黑户这样的人群。
2. 某个中心机构签发的身份证明，往往不能被其他 机构所接受。
3. 集中控制的身份管理，只能在一个锚区或一个在线服务内有效。

随着区块链的出现，身份证明的瓶颈逐渐缓解，就像使用比特币并不需要申请账户一样，它也创造了重新定义身份的崭新机遇。

从互联网身份到区块链数字身份

互联网本身其实是围绕着机器建立的，而不是人类，换句话说，互联网虽然提供了信息高速公路，但是并没有提供中立、开放、统一的身份层。

于是，我们在 互联网里，无法知道谁究竟是谁，它帮助谁连接了谁。当然，这在互联网早期是一件好事，它们并不能从我们身上窃取太多数据。

但是现在随着互联网应用程序变得越来越丰富多样，场景也十分复杂，典型的就是电子商务和社交媒体的普及。

W3C 以及一些标准化组织，提供了一些互联网身份的标准，这些标准的初衷是为了更好地服务互联网应用，但是这些标准被实施的过程中，仍然凸显了很多问题，例如前段时间 Facebook 8000 多万账户数据滥用事件。

面对这些问题，我们这里总结了互联网身份问题以下的几个点。

1. 身份数据的安全性问题，面临泄露和被篡改的风险。
2. 不同机构之间的身份数据的兼容成本很高，带来身份数据碎片化且不一致的问题。
3. 用户无法控制属于自己的数据，例如你今天发布的照片，并不知道会被哪个推荐系统采用。
4. 重复创建和管理不同应用下的身份，典型案例就是重复注册各种账户。
5. 虚假身份欺诈，这个比较好理解，就是被我的身份被盗用，尤其在账户泄露的时候。

概括起来主要是三个方面：非用户自主的身份、身份数据安全与隐私问题、身份数据所有权问题。

以上这些问题， 例如 W3C、Sorvin 基金会和 OpenID 基金会正在寻求一些去中心化的数字身份方案，微软也在关注如何利用区块链构建去中心化的区块链身份，这也是区块链数字身份研究的前沿。

如果想做区块链数字身份，我认为，这里必须涵盖身份的两大核心功能：验证和授权。

有关授权的内容，区块链天生就可以做授权，基于密码学的账户体系可以很好地控制数据自主，也会强制性地让运营商把身份控制权还给用户，并且，一切的关键数据都可以被登记下来。

这似乎迎合了我们一开始对身份的定义，记录客观事件的集合，并且，数据的集合可以被登记到区块链上。

另外，区块链数字身份还有个天然的优势，可以无缝与区块链数字资产进行连接，把以往割裂的信息化身份和金融身份打通，这也是支付宝一直没有做到的。

换句话说，区块链的数字身份系统，它自带了去中心化用户自主的身份、并且可以与用户的资产进行连接，这些都是以往没有做到的内容。

当然，机遇越大，挑战也越大，这里，我也总结了一下区块链数字身份面临的三个挑战。

1. 如何控制个人身份在区块链上的隐私边界？
2. 现实中会产生庞大的身份数据，区块链无法承载这么多数据该如何解决？
3. 如何兼容上述三种类型的身份，例如已经存在的互联网身份？

在光明与挑战兼具的路途之下，区块链的数字身份究竟会如何发展，关于未来，让我们拭目以待。

总结

好了，今天我带领你一起探讨了区块链数字身份的话题，我们先从身份的原始概念开始讲解，接着介绍了身份的简要发展和现在面临的问题，最后介绍了区块链数字身份和它面临的挑战。

那么今天的问题是，你觉得区块链数字身份 会是接下来的热门概念吗？你可以给我留言，我们一起讨论。感谢你的收听，我们下期再见。

精选留言