【2020.1.6】巴比特专栏 |区块链行业要落地，这几方面仍需大幅改进

一、现状

虽然我们每个人都希望区块链能尽早的落地，而且从每天的新闻当中，好像也看到有一些区块链的产品陆续落地了，比如说腾讯的区块链发票，比如说央行的基于区块链的数字票据系统，比如说阿里巴巴的基于区块链的跨境汇款系统等等。

这样的新闻给我们的感觉是区块链好像已经有很多方面落地了，而且距离大规模的落地已经不远了。但是去深究这些项目，这些项目内部的区块链元素其实并不是太多，它们的落地更多的是利用传统互联网公司巨头公司的原有能量，做了一些技术上的改进。

也就是说，他们的成功普通中小区块链项目可能难以借鉴，但是也只有中小区块链项目能大规模的落地铺开，真正有人开始使用，那才能叫做区块链行业的落地，而我们距离这一天可能还很遥远。

这个遥远主要体现在区块链的基础设施还非常不完善，非常不人性化。区块链大规模落地的时候，一定是很多人参与的时候，一定是区块链能惠及到每一个普通人的时候，而那个时候对基础设施的要求非常高。就好像互联网一样，如果今天的互联网还是使用的DOS系统，还是使用命令行模式，还没有邮箱、微信这些东西，你想在互联网上获取巨大的商业成功，让互联网链接每一个人是一件不可能的事，而目前区块链却正好处于这种状况当中。

我个人认为区块链行业要真正落地的话，至少需要在以下这几方面有大幅改进：

二、帐户、密码

帐户、密码是每一个项目都会碰到的问题，也是一个非常令人头疼的问题，不太客气的说，就目前区块链的帐户和密码系统就能够成功“劝退”一半想要参与进来的人。

目前很多区块链项目都是基于公钥私钥的帐户系统，同时加上助记词的辅助，拥有私钥就拥有资产，丢失私钥就等于丢失资产。

但是私钥和助记词这个东西实在是有点反人性，比如私钥，那么长一串无规律的数字、字母，靠人脑记住是不可能的，所以你必须用其它的记忆手段。比如物理方式，把私钥记在纸上，然后问题就变成了如何保存这张纸：夹在笔记本里怕丢了，存在保险柜里怕偷了，即使没这些意外，纸放个一二十年也自然就发黄了，万一某笔巨款的私钥长时间没动，一二十年后还能不能找回来还真不一定。

如果保存在网上，一旦上网，又会面临各种被黑客盗取的风险，这种方式的安全性感觉还不如放在交易所，大交易所至少风控能力比普通个人要强一些。

即使不考虑被盗的问题，私钥的输入也是一个大的麻烦，那么多的字母得一个一个输入，一个一个核对，错一个要查半天，这种帐号密码系统太反人性了，虽然它本身是一个非常精妙、安全的设计。

区块链要想大规模普及，一定要首先解决这个问题，既保留现在公私钥密码对的安全性，又要方便人脑记忆，同时如果丢失，还要有办法能够找得回来。一定有某种方法可以做到这点，比如将私钥与个人的生物特征指纹、眼膜之类的东西做一个映射之类，或者能够通过大数据、社交关系等办法找回来，具体实现方法可能不一样，但是目标是一样的，就是大幅降低普通用户的使用难度。

三、付费模式

在互联网时代，流行一句经典的话，叫做“羊毛出在猪身上，狗来买单”，互联网主要的模式是免费，靠免费吸引流量，靠流量来做其它的业务来盈利。

互联网时代的用户基本上习惯了免费的模式，而现在所有区块链的交易都是用户付手续费，很麻烦，技术上很复杂。比如以太坊的GAS系统，你想要使用以太坊的业务，你必须先有以太坊，如果没有，就得先购买以太坊，也就是必须去交易所转一圈再回来。有些新手朋友可能只是想简单使用以太坊的某项功能，他可能并不太熟悉交易所的功能，但是没办法，想要使用这项功能，你就得先去买。

以太坊相对还算是简单的，EOS的CPU、NET的设置更是复杂，别说新人朋友，即使混过一两年的“老鸟”，也很容易“迷路”。

必须有相应的技术，把区块链的交易习惯大幅优化，比如从现在的用户付费模式转变成商家付费，但其实最后也是用户付钱，因为最终都会转嫁给消费者，但这样的话用户体验就会好很多，会省略很多不必要的程序，也更加符合消费心理学。

四、稳定币

区块链上的数字资产波动性都很高，需要有一种东西能够保持价值稳定，给出一个价值的锚定。

虽然我们现在已经有了USDT，USDT也能够比较好的完成任务，但是USDT毕竟锚定的是美元，美元与人民币当中还需要加上一层价格换算的程序，这中间存在一些麻烦。而且在币币交易中还没有那么明显，如果数字资产有一天真的能够接入现实商业的话，大家就会发现USDT的不方便之处，因为国内的现实商业中很少有用USD计价的商品。

央行的DCEP可以解决这个问题，但是目前来看央行的DCEP与USDT还是有很大的区别，而且在额度、是否支持数字货币交易上面都还有很多的疑问，所以我们也只能先观望，等待它的落地。

当然了，其实不用等DCEP，只要支付宝开放数字货币支付接口，这个问题也能基本解决，所以这个问题重点不是技术问题，而是政策问题。

五、去中心化交易所

目前我们的中心化交易所已经比较成熟了，去中心化交易所也在如火如荼的发展当中，但是我认为目前的去中心化交易所普遍都还缺少一个维度。

虽然效率和深度都远不如中心化交易所，但是有一些去中心化交易所已经基本能用了，这些交易所基本上主打的都是安全。安全是指自己掌管自己的私钥，除非自己的私钥泄露，要不然你的资产就永远是你的，即使交易所被盗，你的资产也不会被盗，这样就能彻底解决交易所被盗的事。

但是伴随着安全一起的，还有匿名这个特点，目前很多去中心化交易所都不用实名制就可以进行交易，不用暴露自己的身份就可以进行大规模的资产转移，这样就很容易成为洗钱等各种犯罪份子温床，如果这种行为不受约束，那对整个经济系统的冲击也是非常大的。

对于去中心化交易所而言，我们真正需要的是它背后的技术，比如UTXO帐户系统，比如让自己管理资产的公钥私钥系统，比如它的高效确认特性等等，这些技术是去中心化交易所真正的优势所在，安全才是去中心化的核心特点，匿名不是。

这里说到的并不是不要匿名，而是不能绝对匿名。举个例子，我们可以通过技术手段保证在所有交易转帐过程中，完全不暴露我们的真实身份，即使是各大交易所、去中心化交易所、对手方也不知道我们的真实身份，但是在最底层，也就是在警方那里，在政府机关那里，一定要有实名身份，因为要确保真正出事的时候，如果要追查身份是可以追查到的。

匿名和去中心化这两者如何协调，如何在保证去中心化特性的同时能够实现对犯罪行为的打击（因为也许有一天，我们会成那个受害者），这是一个非常有挑战的话题。

六、融资

融资是整个行业发展的咽喉所在，毕竟资金就像是粮草，“兵马未动，粮草先行”，一旦融资这个穴位打通了，那整个行业都会有迅猛的发展。

但是目前国家对融资这一块查的很严，因为毕竟是行业发展早期，行业存在着很多的乱象，政府规则的制定、法律的出台也需要一个过程，未来整区块链行业的融资市场要重新开放需要一些条件。

首先，区块链融资这件事得以正规化，一定是发生在我国资本市场全面转向注册制这个大背景下。2019年12月28日证券法修订草案在十三届全国人大常委会第十五次会议闭幕会上表决通过，修订后的证券法明确将在资本市场全面推行注册制，这是非常重要的前提。我国的新三板、科创板目前已经基本算是注册制了，区块链项目作为更早期的项目，风险更难以把控，依赖人为审核来进行风险控制是一件非常困难的事，所以区块链项目未来一定是实行注册制。

在这种前提下，再配合各种制度的规范化，比如说类似于强制第三方审计等措施，比如说制定各种财务标准、强制信息披露标准，比如说定期公布月报、季报、年报，比如说做好合格投资者资格认定、开户风险警示这些东西，相当于可以实现宽进严出，国家把重心放到制度建设和查处诈骗项目上来，这样既最大程度保护好投资者，又最大程度保护创新和活力。

目前这种依靠平民的没有任何风险管控的融资模式，很明显是不可持续的，是很有必要先暂停的，等上述这些措施都完善起来之后，区块链行业的融资体系才会真正成熟。

以上我提到的几点都是整个行业最基础的设施，帐户、密码、交易所、法币、融资这些都是每个项目发展都必然会遇到的东西，在这些最基础的东西没有解决之前，我个人认为整个行业要想爆炸式的发展是很难的。