

区块链技术目前很难大规模普及。一是消费设备存储、算力仍然无法满足需求;二是区块链App体验很糟糕，吓退许多用户;三是区块之间各自为政，无法有效联通。本文来自编译。

技术创新的确美妙，可是事情又并没有那么简单。

第一台洗衣机虽然带来了便利，但它不够人性化，对用户并不友好。

当第一台煤气灶出现时，做饭的效率虽然提高了，但它也带来了火患。从诞生第一天到小规模普及，煤气灶用了近三十年时间。

再看福特T型汽车。它没有安全带、底盘差劲、刹车不可靠.....作为第一款大规模量产的汽车，它的确是技术奇迹。虽然福特汽车让民众受益，但许多人还是忍不住问：汽车滋生的问题是否比解决的问题还要多？

人们常说，我们的一生有两样东西是肯定的，一是死亡，二是税收。但我想告诉技术创新者，还有一样也是肯定的：任何新兴技术进入市场时都不是完全成熟的。

正因如此，面对区块链、加密货币、DeFi、dApps等新的网络垂直新技术，我想谈谈自己的看法，指出当中存在的一些固有缺陷，供各位参考：

现有消费硬件无法支持区块链技术大规模普及

当人们鼓吹区块链技术时总是喜欢谈到“去中心化”，将它说成是区块链技术最大的优势之一。

什么是去中心化?简言之，就是通过各种软件和计算机代码，我们可以在传统网络世界完成一些原本没有外部权威就无法完成的活动。

汇款就是一个好例子。将钱汇到海外，现在我们可以选择银行与电汇，完成交易时需要中间人，汇款要等3-5个工作日才能到账，而且还要交手续费。

数字货币是一种很好的替代手段，它不需要手续费，即时到账。

那么这种“去信任/纯代码”解决方案有没有什么缺点呢？

区块链的交易纪录是无法修改的，比如比特币，它的底层架构就是区块链，支付或者收取的每一个比特币都有交易记录，而记录是永久的。但是无限持续的交易副本

必须依赖于设备，也就是存在于比特币网络中每一个人的设备。

比特币交易存储在block中，每一个block的大小约为1MB，目前比特币网络内约有70万个block。

如果只是几百万个block，每一个block占用的空间比数字照片小一点，要解决存储问题当然不难。不过未来如果我们完全过渡到基于区块链的计算架构又会怎样呢？

每台智能手机可能安装了几十个App，如果这些App的底层都是区块链会怎样？

基于区块链的WhatsApp会不会强迫我们将所有对话记录存储到我的物理设备？

区块链版YouTube会不会强迫我将所有上传的、观看的、分享的4K大容量视频存储到我的物理设备？

如果区块链技术的计算模型不做根本调整，随着区块链的持续创新，现有消费硬件存储不够、处理能力不够的难题迟早会出现。

对于一般用户来说区块链应用的互动体验仍然糟糕

当你打开电脑或者智能手机，下定决心开设一个账户，你会发现开户体验很不好。

你可能要寻找并上传特定文档和个人数据，这些东西经常并不在手边。随后你点击邮件，结果银行告诉你重新开始。无奈之下你只能投降：“新密码是什么来着？”

不管你信不信，这种“安全”“无摩擦”体验是经年累月在用户不断的测试中建立起来的，它的最终目标是让普通用户以最容易、最高效的方式在App内做自己想做的事。

许多人熟悉银行开户流程，但感到困惑的人仍然有很多很多，正因如此，仍然会有很多人前往银行网点开户。

某天你可能会苦口婆心告诉奶奶，让她明白加密货币钱包需要设置随机12个单词的恢复短语，然后再能继续，不只如此，如果想使用钱包内不同的账户，还需要短语的算法加密版本，两个密码以离线方式安全存储在某个地方，不会丢失，不会被盗。

如果奶奶想汇出或者接收加密货币，或者想进入区块链线上App，必须拥有256位公开密钥，密码要么是原始形式，要么是二维码，奶奶的设备还要支持可以与dAp

p互操作的加密钱包。

老天爷，真是复杂!

如果遇到麻烦怎么办?老实说答案并不多。

如果你忘了线上银行账户密码，可以再生成一个。如果黑客窃取你的密码，从你的线上账户偷钱，你仍然受到保护，因为美国银行一般会为你的资金自动投保至一定额度。

如果是加密货币账户出现上述问题，用户无可奈何，只能面对并承受损失。

正因如此，我认为在部分关键问题解决机制达成一致并确立之前，Web3和区块链技术不太可能大规模普及。

一个健全的金融生态系统不只要保护用户免受作恶者的侵害，也应该保护用户免受自身错误行为的损害。

到目前为止这一问题还没有找到解决方案。

区块链App相当于互联网的巴别塔

简单说说巴别塔的故事!

古巴比伦人想建造一座极高的塔，它可以通往天堂，所以巴别塔又叫通天塔。上帝不喜欢人类的宏大计划，为了捣乱，上帝让人类说不同的语言，让他们无法在建塔大事上达成合作。

最后塔垮了，于是世界便有了各种各样的语言。

巴别塔故事和区块链有什么关系呢?

现在运行的区块有很多很多，正如建造巴别塔的工人一样，区块之间无法进行有意义的沟通。

许多加密货币、区块链应用是根据只在自身虚拟环境中运行的方法和代码架构搭建的。

从纯粹的实用角度看，这样的做法无疑是在破坏传统互联网创造的价值。