**比特币、区块链、分布式总账的递进**

*区块链是一种技术，是一种共识算法。*

*比特币是一种使用了区块链技术的电子货币。*

*分布式总账是一种使用区块链技术的数据库。*

**一．半年前的认识**

比特币是一种业务。从经济学的角度讲，他重新定义了货币，使得“一般等价物”这个名词，重新回到了最原始的状态。不再依靠权力机关，而仅仅依靠人们的共识。他使用了很多技术，区块链只是其中的一种。

但是，比特币使用的各种技术：区块链、工作量证明、挖矿、匿名交易等等，环环相扣。以至于看起来像一个整体。以至于所有这些技术，都被冠之以“区块链技术”。

我熟悉比特币使用的所有这些“区块链技术”的细节，并为之惊叹。以我的能力，只能应用这些，而不能对其提出改进。而这种技术带来的结果：完全的去中心化、完全的内容公开，成为我根深蒂固的观念。以至于认为，用到了“区块链技术”，就只能完全的去中心化、完全的内容公开。

而这样的一整套“区块链技术”，并不适合金融业务。

**二．掘墓人还是救世主**

两年前，比特币被金融业视为洪水猛兽，是金融业的掘墓人；而从2015年起，区块链却火热的成为了救世主。

这两者没有矛盾。区块链技术是金融业的救世主，因为区块链解决了一个以前没法解决的问题“对账”，从而成为金融业数据交换、传递的救世主。而比特币等电子货币，因为其去中心化的特质，会对货币这一概念进行冲击，还是掘墓人。（至少是各家央行的掘墓人）

认识到区块链技术与“区块链技术”的差别，即可以有不同类型，不同种类的区块链，才让我真正认识到区块链的应用场景，想清楚了他的未来。

**三．数据的分分合合**

银行各个大数据中心的建立，说明了数据必须合，统一的数据有利于效率。

但有两个原因，造成了没法再合并了。其一是数据太大，合不下；其二是数据分属各家，合不了。

**四．共识算法**

当有多份数据必须保持一致时。保持一致的算法被称为共识算法。可分为主从式共识、竞争式共识两类。

传统的分布式数据库，主从复制，读写分离等技术，均可归于主从式共识。主从式共识的难点在于判定主节点的失效，以及竞争生成主节点。

竞争式共识没有中心节点，其难点在于发生共识分歧后的判定。

简单说，目前区块链技术使用的工作量证明方式，通过对HASH结果比大小，来判定分歧。并通过自带的P2P网络，将结果广播。在没有恶意攻击的情况下，同样会出现分歧；将拜占庭解提升到N/2，不过是其附带的结果。

对应上节两个问题，主从式共识更多用来解决，数据太大的问题；竞争式共识更多用来解决，多家数据的问题。

目前区块链技术尚未遇到数据量过大的问题，比特币运行7年，全部数据不过几十G。终有一天，这两种共识将合并。

**五．区块链技术解决了什么**

区块链技术，从原生就解决了多家数据对账的问题，并附带了唯一性、不可抵赖性、不可更改性。使得基于这一技术的业务系统，不用再考虑冗余、容灾、备份、对账（特别是对账）等问题。

有人说，区块链技术，不过是共享式数据库的别称。从纯技术的角度讲，可以这么理解。但其根本差别是：共享存储是一种纯粹的技术，是为数据库技术、文件访问技术等解决可扩展性的基础技术。本质上不解决业务问题。他解决了多人可以看到同样的数据，但别人看到的这份数据，并不是你自己的数据，你需要其他措施来保证两套数据的一致。

而分布式总账，是为了解决业务问题（就是对账）而创立的技术。多套数据的一致性是其原生的属性，他解决了别人看到的数据，就是你自己的数据。说的绕口一点，前者是：别人知道，你应该知道这些；但别人无法确认，你的确知道这些。而后者是：别人知道，你知道这些。

以后银行之间的数据交换，不再需要什么中介机构了，这也就是SWIFT最最心急火燎的原因。

**六．分布式总账**

分布式总账强调了两点，一是“分布”，二是“总”。（分布就是“云”，总就是“互联”。好吧，再加上这是一种的“技术”，三家子公司全了）

其“分布”是在物理上的，是通过使用竞争性共识算法的区块链实现的。其“总”是逻辑上的，是应该包含尽可能多的数据，特别是多个业务主体之间交互的数据，以避免信息孤岛。

举个类比的例子：区块链相当于实现了数据库的引擎，实现了按字段、按行、按表的存取；而分布式总账需要实现视图、触发器、DDL、DML等SQL语句的解析。在此基础上，才便于应用系统的开发。

**七．小结**

**比特币——区块链——分布式总账，这不是名词的变更，是业务触发技术、技术推动业务的循环。**

**八．做什么**

分布式总账尚未成型，只能在区块链技术的基础上先行摸索。

区块链能做什么？什么都能做！

虽然对区块链有很多高大上的说辞，但从纯技术的角度来讲，区块链就是一种带了很多定语的数据库引擎技术，而且还是非结构化数据的数据库。所以什么都能存。

因为区块链从原生解决了对账的问题，所以区块链更适应解决，含有多家数据交换的应用。

如：中证报价与参与人之间的行情发布。区块链所内置的冗余容错机制，是深证通根本无法比拟的。

即便在区块链基础上，重建报价系统，也是可行的。当然，这一过程如果有分布式总账的支持，则会更好。

**九．以太坊的大致结构**

比特币使用的可以称为第一代区块链技术，在区块链上仅能记录比特币的产生、交易过程。（当然，可以对其进行扩展）。

以太坊使用的可以称为第二代区块链技术，除了上述以外，原生的支持在区块链上存放程序（合约），被称为图灵完备。是目前看来，所有区块链技术研究者中，最为有前景的。

在区块链上存放的程序是一种伪汇编，所有的以太坊节点，都能够解释并执行这种汇编（这被称为以太坊虚拟机EVM，与JAVA虚拟机类似）。

有多种编写合约的语言，最常用的是Solidity，通过以太坊开发环境编译为伪汇编，并发布到区块链上。

以我们目前的技术能力，对区块链的开发，只能是编写合约语言（Solidity），并发布到私有链上。尚不具备改进、调整以太坊源程序的能力。

**十．Solidity的特点**

Solidity的大体结构与JAVA相近（不像Lisp那样反人类）。与其说是学习一门新的语言，更像是学习一种新的JAVA开发框架。

与传统程序不同：传统程序仅在开发者指定的计算机上运行。而EVM程序（编译后的伪汇编）需要在所有节点计算机上运行，所以需要一种机制，保证EVM程序不会无限制的占用节点计算机资源。

所以发布EVM程序到区块链时，必须支付一定的Gas，每执行一条伪汇编，消耗一定Gas。如果Gas先于程序耗尽，则终止程序。

**所以合约语言，使得编程重新变得需要斤斤计较，以尽可能的减少Gas消耗。**以后程序员的收入增长点，可能就是改进合约语言，并抽取佣金了。

所以需要合约语言的编写者，有相当的数据结构经验，甚至是汇编经验。并有相当的编程洁癖。

**十一．前台程序**

以太坊节点程序，按http协议，json结构定义了RPC调用接口。可以使用传统的前台开发方式，支持以太坊程序。

**十二．开发团队的组织**

需要三个层次的技术力量。

第一个层次，需要理解其基础原理，能够部署区块链；第二个层次，仅需要了解合约编程，以及部分区块链技术；第三个层次，普通的前台WEB开发。

**十三．目前的完成情况**

目前，已经完成私有链的部署，从创始块开始，完成了一个完整的私有链。可在私有链上实现挖矿、以太币的交易、合约的部署。

对合约语言的研究仅涉及已有的示例。

**十四．推荐阅读**

<http://ethfans.org/posts/r3-corda-announcement>

<http://ethfans.org/posts/You-Can%E2%80%99t-Do-It-Without-a-Blockchain-Here%E2%80%99s-Why>

<http://www.8btc.com/private-blockchain>

目前先写这些，请领导指正。