云享家 | 区块链干货拿走不谢！

原创：戴剑 BespinGlobal 8月14日

本期阅读在下方留言

互动交流好书领回家

互联网的本质是连接、是分布式，是由TCP/IP协议构建的。**区块链的技术本质是可信，是通过多方共享的分布式的不可篡改的账本来实现的。**这个账本，或称为数据库相对于传统数据库的基本功能：增、删、改、查的角度看，有两个功能被阉割了，只留下了增、查这两个维度。但，这却是一个伟大的创新，一个精巧的设计。下面我从几个维度针对这点进行阐述。

区块链 技术原理

区块链技术概括起来是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术。其实，区块链技术并不是一种单一的、全新的技术，而是多种现有技术（如加密算法、P2P文件传输等）整合的结果，这些技术与数据库巧妙地组合在一起，形成了一种新的数据记录、传递、存储与呈现的方式。简单的说，区块链技术就是一种大家共同参与记录信息、存储信息的技术。过去，人们将数据记录、存储的工作交给中心化的机构来完成，**而区块链技术则让系统中的每一个人都可以参与数据的记录、存储。**区块链技术在没有中央控制点的分布式对等网络下，使用分布式集体运作的方法，构建了一个P2P的自组织网络。**通过复杂的校验机制，区块链数据库能够保持完整性、连续性和一致性，即使部分参与人作假也无法改变区块链的完整性，更无法篡改区块链中的数据。**

区块链技术重新定义了网络中信用的生成方式：在系统中，参与者无需了解其他人的背景资料，也不需要借助第三方机构的担保或保证，区块链技术保障了系统对价值转移的活动进行记录、传输、存储，其最后的结果一定是可信的。

区块链 构建的理论基础

▼ 区块链背后依赖的是密码学、共识算法和博弈论 ▼

密码学

区块链网络更倾向于安全性更高的椭圆曲线方案，也包含一些常规的摘要、加密、密钥交换算法。密码学中也涉及一些抽象代数学科的内容。

共识算法

共识算法的核心抽象是拜占庭将军问题。拜占庭将军目前解决方案较为成熟的是 Paxos 和 Raft 算法。拜占庭将军问题延伸到互联网中来，其内涵可概括为：在互联网大背景下，当需要与不熟悉的对手方进行价值交换活动时，人们如何才能防止不会被其中的恶意破坏者欺骗、迷惑从而做出错误

的决策。进一步将拜占庭将军问题延伸到技术领域中来，其内涵可概括为：在缺少可信任的中央节点和可信任的通道的情况下，分布在网络中的各个节点应如何达成共识。**区块链技术解决了闻名已久的拜占庭将军问题——它提供了一种无需信任单个节点、还能创建共识网络的方法。**

博弈论

博弈论在区块链的设计中起着非常隐性的核心作用，其最终目标是如何让网络达到一个平衡，坏人没有动力使坏，好人会努力维护网络。

关于区块链 未来的一些思考

从Smart Contract变成Smart Contractor

当前谈论的智能合约其实并不智能，它只是基于一些静态的，预定义的一些规则，远远算不上“智能”。未来如何从自动化的合约变成智能合约？那就必须要有面向未知场景的推演，面向未知的场景，如果出现A场景我应该怎么办？出现B场景我应该怎么办？所以这是一种What if的场景推演，基于这种能力才有真正的智能。**而且这个智能合约它不应该只是人和人之间签订的一个协议，它应该是合约和合约之间签协议。未来的趋势，从现在的smart contract变成smart contractor。**所以在这个基础之上就会有涌现出的社会智能或者叫可编程社会，从简单到复杂，从无序到有序，从有限理性到完全理性，自上而下的涌现出来的分布式的、去中心化的社会智能。

智能合约范式

未来在区块链中最重要的应该是智能合约范式。今天传统企业在数字化转型过程中最大的问题就：落地难。这个问题的核心是传统行业不知道怎么用。面对这样的场景问题，就需要开发一些所谓的智能合约范式，这是合约范式系统。需要跟各种传统行业去合作开发它所在行业的合约范式，而这些不能直接面对业主，而应该面对系统服务集成商。**智能合约范式在设计的当中有买卖合约、评价合约和竞标合约，这是比较通用的做法，还有一些更精细的做法。**

完

写在后面的话

区块链是一个以技术为导向的全新产业，被称为开发者的春天的一个产业。虽然区块链技术目前还有很多需要完善的地方，但，如同互联网在90年代，用56K猫拨号的时代；我们设计网页，我们网上冲浪一样有相应的技术、产品和服务。同样有顶级的公司伴随技术的迭代而持续跟进。

往期精彩回顾

云享家 | 传统企业区块链化、云化，BespinGlobal有何妙招？

你不知道的区块链的前世今生

阅读原文