说信任区块链时究竟在信任什么?

原创 张开翔 FISCO BCOS开源社区 2019-02-28

点击上方**蓝字**，成为社区一份子

张开翔

FISCO BCOS 首席架构师

然鹅，下一篇我却要告诉你“几乎什么都不能信”！

AUTHOR — 作者

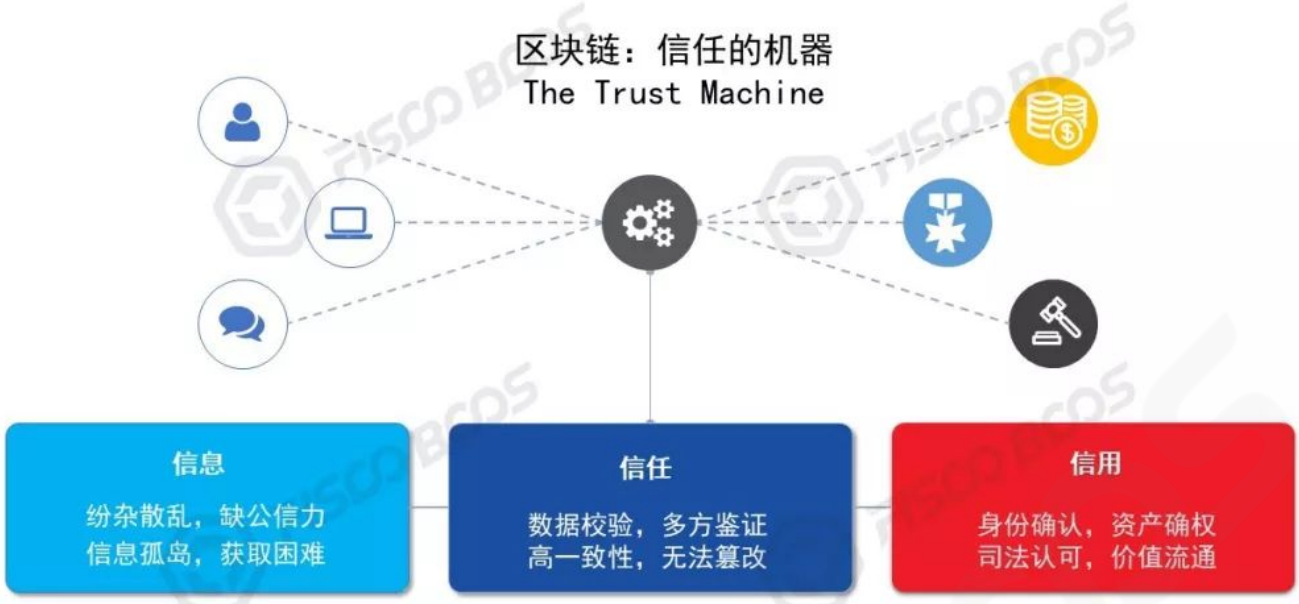
大家好，我是张开翔。

如你所见，【FISCO BCOS开源社区】开通了，很高兴和你在此以文相会。这个号将由你，由我，由FISCO BCOS背后117家成员单位的工程师们，乃至社区沉淀下来的数千开发者通力打造。我们开放了多元化的社区协作通道，希望和你，和广大区块链爱好者，一起聊聊从事区块链技术研发的切身感悟，一起分享踩过的每一个坑、越过的每一道槛，一起将咱中国自己的联盟链技术推向世界的顶端。

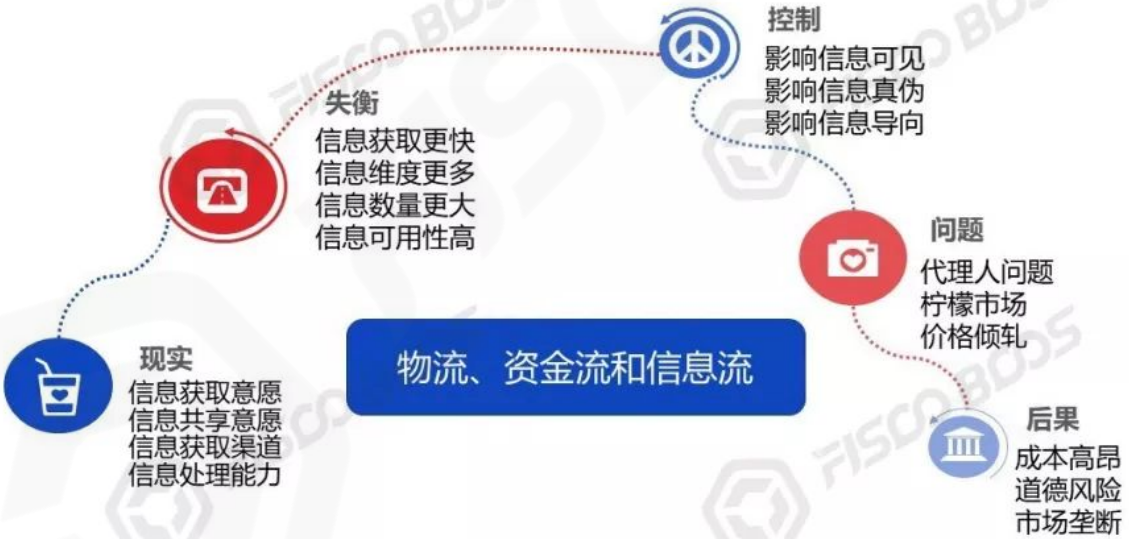
这是本号第一篇文章，就从The trust machine、Code is Law、信链得永生这些近乎痴迷的口号说起吧。我会在今明的两篇文章里抛砖引玉，谈谈在区块链的世界里，我们的信与不信。

FISCO BCOS

当前，“区块链，信任的机器（Blockchain：The trust machine）”已经成为了一句口号，紧接着就是“去中心化、群体共识、不可篡改、高一致性、安全和保护隐私”等一系列听起来很厉害的术语。究竟区块链具有多大的魔力能让人如此信任，或者说，我们在说“**信**”的时候究竟信的是什么。



信息，指身份、资产、价格、地理位置等自然属性和行为信息，它并不是先天可信任的，因为信息散乱、不完整，可能虚假，甚至可能会有人利用信息的不对称性牟利。



把信息整理成结构化数据，通过数据校验的方式，保证其在传播中可保持完整性、全网一致性、可追溯性，不会被恶意篡改；通过冗余存储的方式，保证其公开、共享、可访问，保证数据一直有效。那么，这信息本身就可以被“信任”，从而成为大家的“公共知识”，成为全网参与者都认可的“**最大公约数**”。

如果信息体现着价值，且这些价值被大家认知、认可，能被量化，具有可交易的等价物属性，或可能随着时间增值，甚至得到司法背书承认，这些信息才具有商业意义上的“信用”。

好比我们认识一个人，但不代表我们信任他。然而这个人一贯表现不错，在社群里言行一致，渐渐地获得了大家的信任。这时的信任依旧不等于信用，除非这个人拥有可观的资产，或者其个人历史上有盈利和偿还的能力，未来也大概率能持续持有资产和承兑债务，那么这个人才具备了“**信用**”。

区块链体系基于算法而不是人治，有望通过其独特的分布式架构、加密算法、数据结构、共识机制等，把信息固化成大家的**信任**锚点；有望通过技术手段把各种现实世界的资源转换成可兑付的数字资产，并展开一系列多方商业协作的活动，这就是所谓的 “信息到信任到信用”，甚至于因为区块链这个黑科技的、行之有效且难以理解的玄妙，这个“信”字仿佛升华成了“**信仰**”。

那么我们说信区块链时，信的是什么呢?

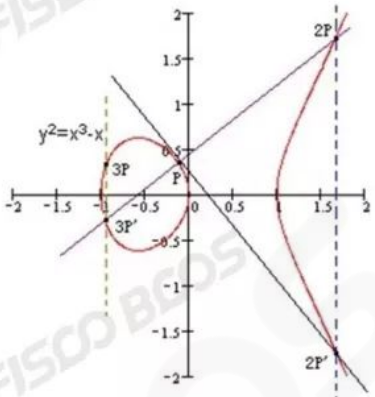
1
信密码学算法

区块链是用算法达成信任的，其中最重要的算法之一，就是密码学。区块链中最基本的密码学应用是HASH摘要、对称加密和非对称加密算法，以及相关的签名验签算法。

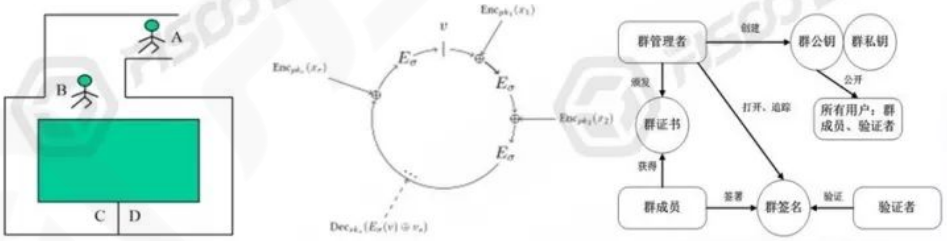
HASH算法的旧版本已经被证明可破解而被抛弃了，目前在用的SHA256等算法依旧坚不可破。HASH算法的特性是把一堆数据单向生成一段定长的数据，基本不会发生碰撞，可起到原始数据的“指纹”作用，其单向性不可逆，推不出原始数据，具有一定的抗量子性，是能隐藏原始数据又能在必要时提供校验凭据的最佳方式。

数字签名一般基于公私钥体系，用私钥签名，公钥验签或者反之。数字签名源自密码学的牢靠性，使得不可能有人能伪造别人的私钥签名，所以一个拥有私钥的人可以通过数字签名，对他的资产签名确权，或者在双方交易时，采用对手方的公钥发起交易，将资产转移给对方，对方用自己的私钥才能验签解开，以获得所有权。

- **公私钥体系：**在身份认证和通信过程中采用公私钥
- **哈希函数：**SHA2、SHA3和RIMPID160等各种哈希函数
- **椭圆曲线原理：**椭圆曲线方程，公私钥的产生算法
- **ECDSA签名：**签名算法、验证算法，ECC与DSA的结合
- **对称和非对称加密：**在双方通信过程中加密解密
- **国密商用算法：**SM2，SM3，SM4，SM9



AES、RSA、ECC椭圆曲线等几种对称和非对称算法广泛地用于数据加解密、安全通信等场景，其安全级别取决于算法本身和密钥长度，当AES使用128~512位密钥，RSA/ECC采用1024甚至2048位密钥时，其保护的数据理论上需要普通计算机上亿年的计算时间才能暴力破解。这些算法在商业、科学、军事领域都经受了考验。



- 零知识证明
- 同态加密
- 属性加密，格密码学
- 群签名，环签名，盲签名、代理签名、门限签名…
- 量子密码

加密学领域里还有同态加密、零知识证明、环签名群签名、格密码等新的方向，目前都处于从理论发展到工程的阶段，都在功能、安全强度、效率方面快速优化中，已经可以看到落地使用的可能性了。同时我们也意识到，密码学通常需要经过长期的发展、验证，稳定后才能获得广泛认

可，要么实践中经历了大量考验，要么经过权威机构的审核和认证，才能在生产领域大放异彩。密码学里的理论到工程，常常有很长的时间周期。

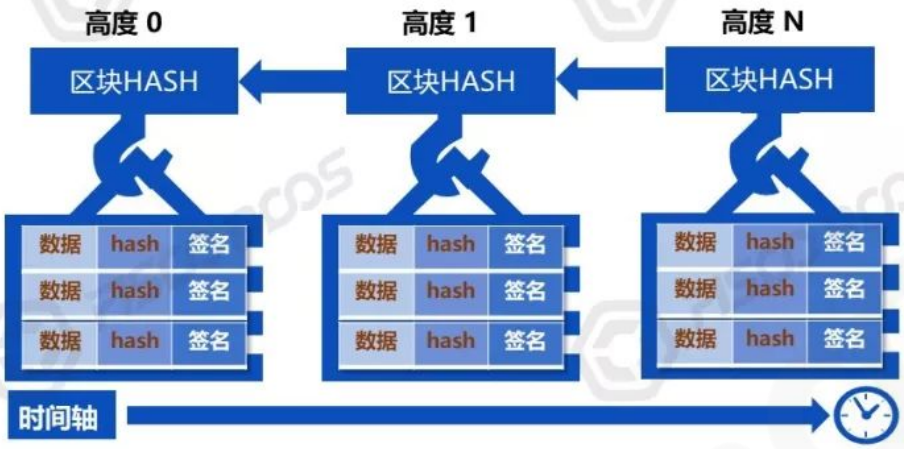
加密算法的一个基本哲学是**计算成本**，当一个算法保护的资产价值，远低于攻破该算法所需的成本时，就是安全的。但如果用一个算法保护一个无价之宝，自然就会有人不计成本地去攻击获利，所以，密码学的安全，也是辩证的、需要量化的。

随着量子计算机等学说的兴起，经典密码学可能会经受一些挑战，但量子计算机的理论完善和工程实现还有待时日，目前来看，基本上我们可以近乎“无条件”相信区块链里已经采用的密码学算法，同时，区块链领域的实践者也在陆续引入各种抗量子的密码学算法，这是一场持续的博弈。

2
信数据

区块链的数据结构，无非是区块+链。新区块将自己的区块高度、交易列表，和上一个区块的HASH，共同再生成一个HASH做为新区块的标识，如此循环，形成了一个环环相扣的数据链。这个链条里的任何一个字节甚至一个Bit被修改，都会因为HASH算法的特性被校验发现。

- 每个区块包含一段时间（如10秒）内产生的交易数据
- 把相关的数据汇总计算摘要，进行汇总的完整性正确性证明
- 每个区块计算摘要时，把前一个区块的摘要做为一个数据计算在内，构成了数据链
- 最新区块包含了所有数据链的完整性证明，整个链条上的任何数据改动都会破坏数据链的相关性



同时，区块数据被广播给全网所有参与者，参与者越多，规模效应越强。少数人即使强行修改、删剪自己的区块数据，也很容易被其他人校验出异常并不予采纳，只有多数人认可的数据得以留存和流传。也就是说，数据是大家人盯人的形态盯着的，且存在多份副本，一旦落地，只要链还在，数据就可以永远留存。

- 多方参与保存数据
- 具有高度一致性
- 单方修改/删除无效
- 可互相备份和监督

基于容易验证的链式数据结构、群体冗余保存、共同鉴证，区块链数据是“难以篡改”的，所有人拿到的数据也都是一致的，信息公开透明，公共知识得以彰显和固化。

从另一个角度看，数据达到信任，但能否达到“信用”还要看数据的价值，也就是数据本身携带的信息，是否能代表有价的资产、有用的信息，诸如身份、交易关系、交易行为、大数据等等，都能代表一定的商业价值。这些数据如果分享出来，足以构建完整的商业基础。

但如果是在过于强调隐私的场景里，大家愿意分享的信息本来就很少，那样就很难达到信用的“最大公约数”。然而，在当前的商业环境里，信息隔离和隐私保护是硬诉求，信息共享和隐私保护成了严峻的矛和盾的关系，除非整个商业关系和商业逻辑出现了革新。

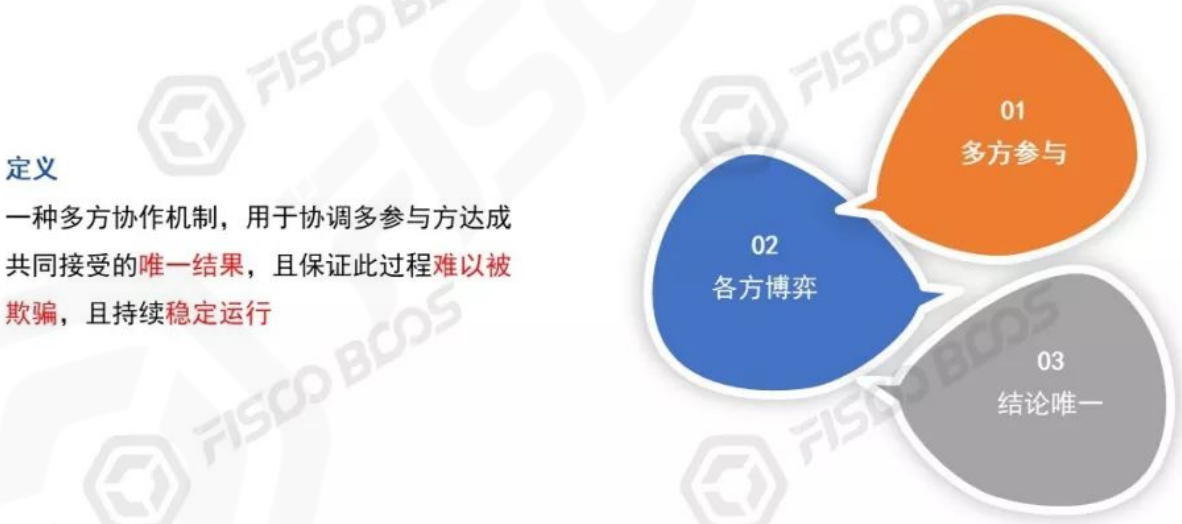
所以，隐私保护相关的研究被大量关注，诸如“多方安全计算”、“零知识证明”的理论大行其道。理

论上讲，确实可以做到公布很少的信息就能做到可验证，但其复杂性和计算开销，又是工程层面要去解决的事情了。

FISCO BCOS

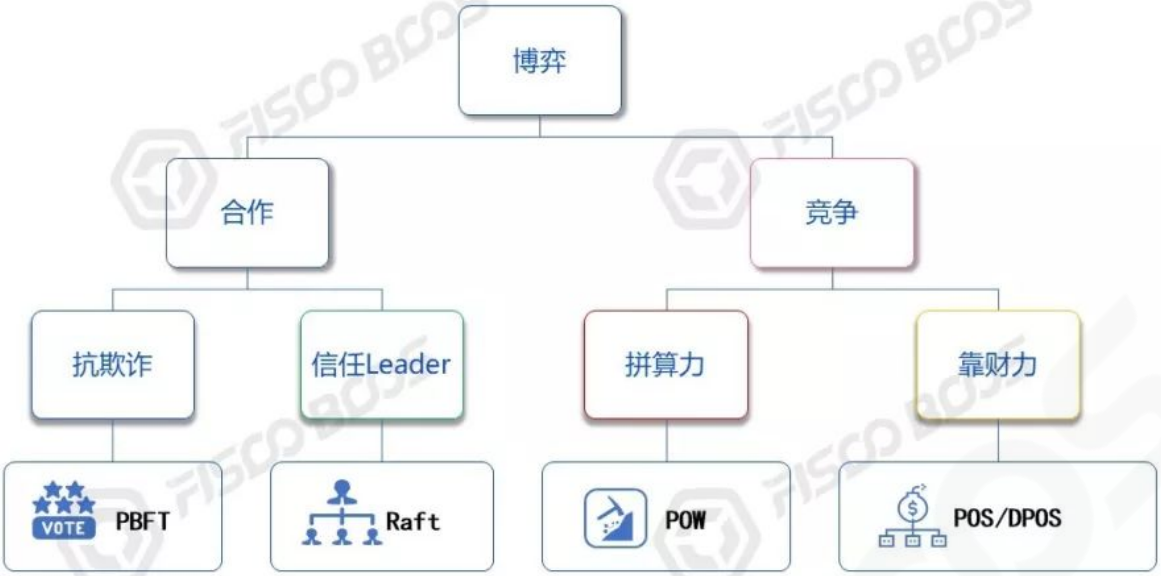
3
信博弈论

区块链中最玄妙的部分是“共识算法”。共识算法的定义是在一个群体中，用一种机制协调大家共同或轮流记账，得出无争议的、唯一性的结果，且保证这个机制可以持续下去。



换句话说，大家一起维护一个账本，选择谁做为记账者？凭什么相信记账者的动作是正确的？怎么防止记账者作恶？如果记账者正确记账如何得到激励？共识机制完整地回答了这些问题。

共识的逻辑是发生在线上的，但实际上，背后是现实世界的竞争博弈。



POW（工作量证明）采用算力去竞争记账者的席位和获得记账者的奖励。现实生活中，为了构建具有竞争力的算力工厂，矿工通常需要研发或购买大量的新型号矿机，运输到有稳定和便宜电力供应地区，消耗大量的电费、网费以及其他运营费用，在被监管时又得举家搬迁，浪迹全球，实际上投入了大量（现实世界的）资金、精力以及背着巨大的风险。如果要在POW竞争中获得稳定可观的收益，投入的资金动辄以亿计，并不亚于办一家企业。

POS和DPOS用权益证明代替了算力消耗，看起来是环保多了。而代表权益的token，除了创始团队自己发行的之外，“矿工们”一般需要通过币币兑换，或者直接法币购买数字币的方式获得，即使是币币兑换，掏出来的币也常常是采用法币购买的，或者至少这些权益都能以法币进行标价，这其实也是现实世界里的财富注入和背书。

然而，和现实的商业关系对比，POW和POS等共识并没有法律和监管机制兜底，也容易受不断变化的博弈形势所影响，比如社群的规模、矿工的更迭、核心技术运营团队的变化。慢慢地，本来有钱和有能力的人，或许会更加有钱和有权力，去中心化的网络可能逐渐变成了卡特尔组织，矿工和技术社区的瓜葛也会不停地掀起波澜，造成分叉、回滚、价格倾轧、对韭当割等现象。

总的来说，人们还是信任区块链上的“自治”，在这种分布式自治里，单个事件（如一笔交易）具有“概率性”,同时全网又追求“最终一致性”（公共账本的一致）。这种短期的概率性和长期的确定性，一定程度上可以达成动态的“**纳什均衡**”，支撑起链的生态，给人演化出一种玄妙的“信仰”感。

- 拥有记账权的人更倾向在维护整个体系过程中获利（纳什均衡+帕累托最优）
- 使用网络的人需要付出一定的成本（手续费、计算费）以免滥用 （避免公地悲剧）
- 少数人作恶的成功几率很低，参考赌徒破产问题（Gambler ‘s Ruin problem）
- 只有极端势力才有可能不顾一切的颠覆这个体系
- 整个局势不存在“确定性”，一直在动态的多方博弈

另一方面，联盟链的记账者一般是机构级的角色。联盟链要求记账者身份可知，参与者们经过许可才能接入网络，他们之间是一种**合作博弈**。联盟链引入了现实世界里的身份信息作为**信用背书**，如工商注册信息、商业声誉、承兑信用、周转资金，或者行业地位、执业牌照、法律身份等，参与者在链上的一切行为均可审计、追查，也让相关的监管部门在必要时可以有的放矢，精准惩戒，强制执行，具有很高的威慑力。

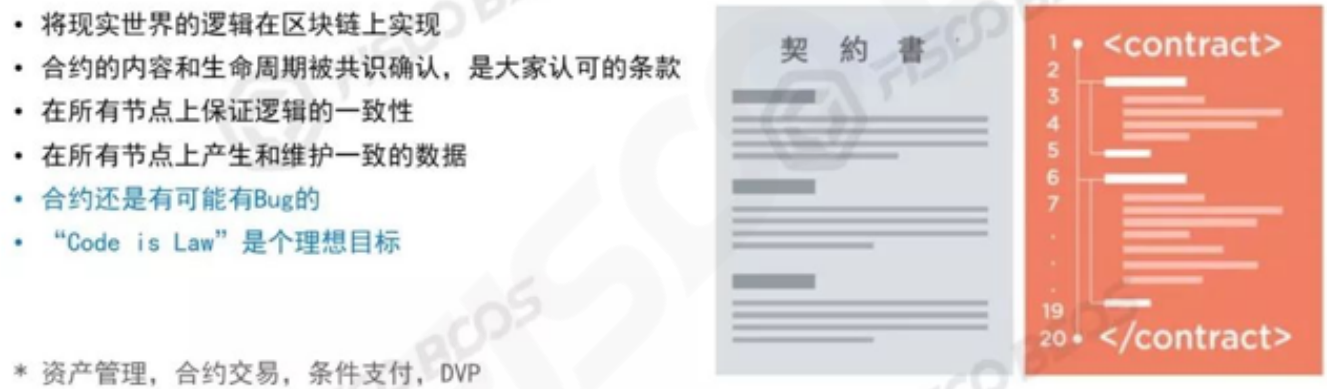
在这种环境里，联盟链的参与者一起协作维护网络，共享必要的信息，在平等透明、安全可信的网络里开展交易，只需要防止少量记账者的恶意操作风险，避免系统上的可用性风险。因引入了现实世界里必要的信任背书，即使联盟链业务逻辑非常复杂，而信任模型却更直观。

所以，所谓的共识机制，背后依旧是现实世界里财力物力的竞争和信用背书，以及相应行之有效的激励和惩戒机制。

天下并没有免费的午餐，也没有平白无故的爱恨。“信”一个记账者，是信他在现实世界里所投入的成本、付出的代价，以及考虑到整个机制有震慑他的惩罚，相信记账者为了持续的收益和增值，不会无故破坏这个网络。

4
信智能合约

智能合约是由多产的跨领域法律学者尼克·萨博（Nick Szabo）提出来的。他在发表于自己的网站的几篇文章中提到了智能合约的理念，定义如下：
“一个智能合约是一套以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议"。



简单地说，可以理解为纸质合约的电子版，用代码实现，无差别地运行在区块链网络的每一个节点上，在共识的作用下执行既定的合约规则。

智能合约一般基于一个特制的虚拟机，使用沙盒模式运行，屏蔽掉可能导致不一致性的一些功能。比如获取系统时间这个操作，在不同的机器上，时钟都可能不同，这就可能导致依赖时间的业务逻辑出现问题。再比如随机数，以及外部文件系统、外部网站输入等，这些都可能导致虚拟机执行结果不同，都会被虚拟机沙盒环境隔离。

如果要采用java语言写合约，要么裁减掉jdk里的相关函数（系统时间、随机数、网络、文件

等），要么放到一个有严密权限管控和隔离设定的docker里运行。或者干脆设计一门新的语言，如以太坊的Solidity，只实现特定的指令。又或者放弃掉一些“智能”特性，用简单的堆栈指令序列完成关键的验证判断逻辑。

所以，在区块链上执行智能合约，基于沙盒机制控制，凭借区块链的共识算法，达到全网一致、难以篡改、不可否认等特性，运行结果输出就是全网认可的一份合同，江湖人称“Code is Law”。

然而，只要是代码，就一定有出现bug或漏洞的概率，可能来自底层虚拟机和网络漏洞，更多的可能来自逻辑实现。随便搜一下“智能合约 安全 漏洞”，就有一堆搜索结果，包括溢出、重入、权限错误等，甚至就是低级错误。近年来，这些漏洞已经造成各种资产损失，最著名的是DAO项目代码漏洞、Parity的多签钱包漏洞、某互联网公司的代币交易过程溢出归零……

技术文章可以参考：
https://paper.seebug.org/601/

- **DAO漏洞**：黑客利用代码的BUG转走大量的金额导致项目失败
- **多签钱包漏洞** ：1）越权的函数调用，黑客转走大量资金 2） 删除底层库的权限未限定，被锁死大量资金
- **数字溢出漏洞**：大数溢出后，数值归零，导致余额判断失败，黑客可转走大量资产
- **在线节点解锁帐号漏洞**：在线上节点发送交易需要解锁帐号，被扫描到的帐号不设防
- **不可404的BBS**：无法修改，无法删除，无法堵截

- CodeisLaw还是个理想
- 需要严谨的合约模板和更安全的虚拟机
- 缺乏控制，治理，补救，追责
- 需要更严格的审核和形式化证明

目前，行业里对智能合约的安全也是各出奇招，包括安全公司和白帽子审查、形式化证明、众测等，对安全问题会有一定地改善。如果再出问题，要么是黑客太厉害，或者只能抓程序员祭天了：）

所以，信智能合约，是有条件的，是要信经过严格测试、长时间稳定运行、万一出错还有办法补救（而不是绝望的只能等分叉大招）的合约。联盟链里的智能合约一般是经过严格测试的，上线时会执行灰度验证流程，运营中监控运行过程，且根据治理规则设计事后追责、补救（冲正，调账，冻结...）等措施，还是比较可信的。

FISCO BCOS

5
信中间人（？）

注意本小节标题打了问号，区块链推崇“去中心或多中心，去中介或弱中介”的运作模式，但是由于

目前发展尚未完善，很多场景实际上还是引入了中介，如币币兑换通常需要经过交易所，尤其是中心化的交易所。其交易原理是要求用户把资产存入交易所的帐户里，交易时其实是在交易所的数据库里进行记账，只有在存币或提币时，才会和区块链网络发生交互。

交易所的信任模型和区块链某种程度上是脱钩了，这时，交易所本身的资质，运营方的技术能力、安全防护能力、资产信用和承兑能力，才是用户最需要关心的。一旦交易所出了问题，比如跑路、破产、暗盘操作、监守自盗，基本上散户就只能做韭菜了。

多的不说，参见著名的“门头沟事件”：
https://baike.baidu.com/item/Mt.Gox/3611884

所以，相信一个托管者，是一个见仁见智的事情，只是现行的模式里，类似交易所这样的角色还在某些区域运作着。2018年，全球虚拟数字资产交易所有1万多家，其中多少能做到高规格的安全，运营规范，干净……那就看情况了。

最后提一点：联盟链默认是没有公链那种虚拟数字资产交易所的。

区块链领域的细节还有很多，以上先罗列主要的几个点，信任技术，信任共识机制，信任规模化的社群博弈，超过了信任“人”。“人”是一种不确定因素，你可以信任一个你很熟悉很老铁的人，也可以信任一大群有共同理念且有完善机制协作的人，但你不能信任某一小撮居心叵测的人，要不分分钟变成韭菜：）

总结一下，在区块链世界中，人们可以建立以下基本的信心：

- 我持有的资产和信息，只有我能动用或披露
- 我可以按公允的规则参与交易，分享信息，转入转出资产
- 别人给我转过来的资产一定是有效的，不会被重复花费而失效
- 一旦交易完成，就是板上钉钉的事情
- 一切已经发生的事情都可验证，可追溯
- 违反规则的人会损失更大
- 维护网络的人付出了劳动会有恰当的回报，整个模式可持续

基于这些信心和信任，在合法合规的前提下，人们给网络注入各种资产，开展互补互利、规则透明、公开公平公正的商业行为，将会是一种理想的状态。

FISCO BCOS

FISCO BCOS的代码完全开源且免费

下载地址↓↓↓（可戳 阅读原文 直接打开）

https://github.com/fisco-bcos

长按“二维码”关注

明天同一时间，张开翔继续和你探讨

《区块链世界里不能信什么》

注：部分图片来源于百度、Pixabay等网络渠道，特此鸣谢相关平台及创作者。

阅读原文