量子计算来了，区块链必须改造

价值互联网是支撑数字经济健康运行的基础设施。价值互联网的核心是在网络中实现数字化的价值创造，价值表达，价值流通。人们要实现价值互联网，必须首先理解互联网信任形成的机制。正如汪洋大海当中每条鱼的运动都离不开水一样，人类的每次互动都在信任的介质中进行。随着人类文明，社会和市场的发展，对信任的作用和意义愈发重要。

信任是价值创造的本源，经济运行的基础，社会秩序的保障。想想如果缺乏信任，人们会用手机支付给互联网上素未谋面的厂商吗？厂商会将其货款通过银行转账给供应商吗？银行会贷款给还没有工资收入的学生吗？信任机制是价值互联网的基石。在商品经济时代，国家法定货币是经济中的信任介质，银行是经济中的信任托管者。在价值经济时代，数字货币和金融证券成为信任介质，互联网平台和区块链形成了数字化的信任机制。

区块链技术出现是互联网生命进化的必然。区块链技术第一个被大规模采纳的基于机器信任的互联网协议。区块链创造的价值和产生的问题都揭示了未来伟大的互联网企业一定建立在信任之上。我们需要注意，现有区块链技术只是实现了部分的机器信任，距离价值互联网的整体的系统信任存在巨大差距。要真正实现价值互联网，一个必须要解决的问题是理解区块链技术的局限，并将区块链改造成信任价值互联网。

我在研究人类历史上信任基础技术时，发现实际上去中心化这样的想法，中国人最早就想到了。一张名画为了辨别真伪，需要几十位画师和皇帝一起辨别真伪，每个鉴别者都要加盖自己的印章，这可以算是“区块链”

的原型。当时没有计算机和互联网，鉴别的时间成本非常高。

区块链的出身是一种数字加密货币的骨干技术。区块链是一个去中心化的分布式数据库，其中记录了已在参与方之间执行和共享的所有数字资产交易或数字文件的记录。每个交易都由系统的大多数参与者验证并进行数字验证。区块链的公共账本中包含每笔交易的每条记录，以层层链接的数据块加密格式存贮。由于每个参与的计算机结点都保存完整的公共账本，极大地提高了破解数据和交易造假的计算成本，降低了交易各方的信任成本。区块链的这种去中心化记账机制使得数字资产的流通没有中央服务器，也不需要类似银行的第三方中介和信用管理机构，于是提高了数字资产交易的效率。

区块链运行需要一个节点网络。节点是连接到区块链网络的计算机，使用应用软件连接到区块链，将区块链数据公共账本下载到系统中，并且该节点与区块链上的最新数据块同步。在区块链节点构成的算力网中，为了激励参与节点将自己的计算机算力用于区块链验证和记账，区块链给参与节点发放数字通证（Token)并将其记入公共账本。通证可以作为数字资产在互联网上流通或者兑换其他数字货币或法定货币载体。以换取通证奖励的节点被称为“矿工”。从治理结构上，区块链是用“全民中介”取代了“寡头中介”，避免了中心服务器数据丢失或者被篡改的风险。

区块链特别适合于互联网自发的数字资产管理，包括跟踪资产所有权和资产状态数据。在保险、供应链和资本市场中都可以找到例子，在这些

市场中，分布式分类账可以解决痛点，包括效率低下，过程不透明和数据篡改。现有的区块链主要依靠五种技术和方法来实现数字资产的管理：

去中心化：分布式账本与连接到区块链的节点之间的每笔交易共享和更新。由于没有中央服务器来控制数据，所有这些都是实时完成的。

安全保证：通过区块链密码技术不可能对区块链进行篡改和擦除。

开放透明：由于区块链中的每个节点或参与者都有区块链数据的副本，每个节点可以访问所有交易数据并可以自己进行验证。

共识机制：所有相关的网络参与者必须认同交易有效。这是通过使用共识算法来实现的。

智能合约：可以将根据特定条件执行的智能合约写入公共账本，随着业务流程自动执行合约。

然而，现有区块链并不能够解决价值互联网的信任问题，甚至还制造出了社会信任问题。我们实际应用当中发现这五种技术和方法存在一系列的问题和风险，

虽然区块链标榜“去中心化”能够让价值体系更加公平民主，其实是区块链是记账工作去中心化，但是整个平台的数字资产更加集中了。例如，在比特币一共设定了 2100 万枚上限，2020 年 4 月大约 1831 万枚已经被挖出，在 10 万多节点当中，大部分是挖矿计算机占有和分配到的比特币非常少。最大的持有者是匿名的早期创建的团队估计，估计超过 100 万枚，

是全球比特币交易所每天交易量的 10 倍，这足以操控对比特币汇率市场价格。以太坊的创始人和团队持有超过 16%的以太币，实际控制着整个数字资产价格。和股票投机市场一样，大多数投资人关注高回报率不在乎公司真实业务和技术，于是数字货币打着区块链去中心化的旗号，实现了超过很多上市公司的数字资产集中度。

为什么比特币没有价格稳定机制？一种解释是代号中本聪的创始团队原本是为赌场开发电子赌博系统的，比特币是比照赌场的筹码设计的，天生就是一种网络赌博平台。另一种解释是当初创始人设计比特币也许是一种货币民主思想，但是这些工程师没有宏观经济治理的意识，虽然做了加密货币的技术，但是没有稳定货币的机制，比特币里面定了 2100 万枚挖矿的算法出来。如果一种货币不能根据通货膨胀指标增加和减少货币供应量，这是很差的货币。不论哪种解释，市场上货币需求增加，但发行者限制货币供应数量，这不会出现通货膨胀，而会出现通胀紧缩。比特币就出现了严重通货紧缩，价格越高涨，知名度越高，兑换的投资者越来越多，但是量供不上或者是被寡头操控市场，导致价格越来越高，更多投机者开始囤货，黑客开始攻击网络窃取数字资产，市场混乱导致大量用户的损失。

从安全保证看，区块链所采用的基于 RSA 的加密算法主要依靠现有计算机的算力成本实现。这只是是一种电子计算暂时安全，未来几年量子计算确定能够攻破传统 RSA 加密算法。只要区块链一半以上的公共账本被瞬间解密和篡改的可能性存在，区块链就不能声称自己的绝对安全。另外一

个方面，区块链通证数字货币被设计成匿名的，网络交易所被黑客攻击和数字钱包被盗窃的案件频发，追查破案成本比线下案件更高。

在数字货币和区块链网络中的安全漏洞，往往会有更严重、更直接的影响。由于区块链网络去中心化的计算特点，一个区块链节点实现上的安全漏洞，可能引发成千上万的节点遭到攻击。甚至，在传统软件漏洞领域被认为相对危害较小的拒绝服务漏洞，在区块链网络中则可能引发整个网络瘫痪的风暴攻击，对整个数字货币系统造成巨大冲击。

近年区块链的安全事件多发，暴露出区块链技术的漏洞。例如，EOS 是被称为“区块链 3.0”的新型区块链平台,其代币市值曾高达 690 亿元，在全球市值排名第五。EOS 区块链部分漏洞可以在节点上远程执行任意代码，即可以通过远程攻击，直接控制和接管其上运行的所有节点。攻击者会构造并发布包含恶意代码的智能合约，EOS 区块链超级节点将会执行这个恶意合约，并触发其中的安全漏洞。攻击者再利用超级节点将恶意合约打包进新的区块，进而导致网络中所有全节点（备选超级节点、交易所充值提现节点、数字货币钱包服务器节点等）被远程控制。由于已经完全控制了节点的系统，攻击者可以“为所欲为”，如窃取 EOS 区块链超级节点的密钥，控制数字货币交易；获取 EOS 区块链节点系统中的其他金融和隐私数据，例如交易所中的数字货币、保存在钱包中的用户密钥、关键的用户资料和隐私数据等等。更有甚者，攻击者可以将 EOS 区块链网络中的节点变为僵尸网络中的一员，发动网络攻击或变成免费“矿工”，挖取其他

数字货币。

区块链的共识机制貌似公平，实为计算资源浪费。比特币的区块链技术采用机器工作量证明（Proof of Work，即 PoW）共识算法，10 万台挖矿计算机为了获得比特币奖励要不停地进行加密运算，同样市场价格的比特币的平均成本已经是黄金开采成本的三倍。大量能源资源和计算资源被浪费。尽管以太坊等改良区块链号称采用了股权证明（Proof of Stake，即 PoS）等改良共识机制以降低计算消耗，但是通过研究其核心代码我们发现仍然是过去算法。因为已经发布大量数字通证，进行平台层面的基础算法改变需要重新计算和修改账本，这是得不偿失的方式。

区块链所支撑的数字货币的价值波动巨大，与法定货币和其他数字货币的汇率波动要比股票指数高很多。大量的交易所设立虚假交易账户虚构交易数量以吸引投机者。因为数字通证的价值非常不稳定，价格波动不断，区块链智能合约的真实价值和惩罚被迫改变含义，违约率大幅上升，智能合约也就失去了契约保障价值。尽管区块链在公共账本数据层面透明，但是在人与人的社会信任层面确实典型的“暗网”。由于交易主体是数字通