浅析私有区块链技术

蔡维德[1]罗佳[2]

区块链技术，滥觞于中本聪的“比特币”开源密码协议。比特币技术的本旨在于开发不受任何金融机构控制的“数字货币”。由于其本身具有特殊的非中心化主义倾向，因此作为匿名者的中本聪其后不久也销声匿迹。但从那时起，对数字货币底层的区块链技术的讨论却从未停止。目前区块链技术主要指通过特殊的算法、加密手段保证网络中数据库的一致性、安全性及可维护性，互联网中的所有节点都可以公平自由的跟其它任意节点通信，但是这个技术只解决了通信问题，没有解决信用问题，区块链技术的应用恰好解决了信用问题。

区块链可以分为公有区块链和私有区块链，公有区块链虽依托比特币贵为区块链技术之发端，当前大部分讨论文章也主要集中于公有区块链，但囿于自身对于网络技术的依赖以及特殊属性，其适用领域仍有局限性[3]。

目前研究或开发应当将目光聚焦于私有区块链，即将私有区块链技术应用于银行清结算、证券交易、互联网金融、版权保护、互联网彩票、电子合同等领域。

[1] 北京航空航天大学千人计划教授；北京航空航天大学工信部工业和信息化法治战略与管理重点实验室高级研究员；计算法律学专家；亚利桑那州立大学名誉教授；前清华大学长江讲座教授；前明尼苏达大学教授；麻省理工学院学士，加州大学伯克利分校博士，OW2（中国-欧盟开源软件联盟）副理事长。

[2] 国家信息中心中经网基金管理有限公司总经理。

[3]参见：R3 发布最新研究报告，证明公共区块链不可作为金融机构解决方案。Link：http://www.wanbizu.com/news/201511225765.html

1. 公有区块链技术简介

公有区块链意味着所有的节点都可以加入，任何有计算机且有网络接入地方都可以加入。公有区块链多采用P2P网络[4]，用节点之间的相互信息交换而连接形成网络。由于所有的节点都可以加入，导致节点传递信息速度比较慢。但其优点也是显而易见的，由于网络的参加者数量庞大，使公有链非常不易被封锁。同时公有链具有极强的容错性，一旦开启要关闭公有链几无可能。公有链使用众多节点构成的非中心化的分布式网络来记录交易信息，所有节点中都存有类似的交易记录，保证了信息的公开性、安全性、可信赖性。

作为原初模型的公有区块链，初衷为任何互联网上的个体都可以加入，但现实问题随之而来，最为严重的问题是公有链速度慢。其中一种解决路径是修改公有链，即不必须经过所有的节点同意，选择适当的投票节点即可。此种方法可以大幅提高交易速度，但是也引发了争议。有学者认为此种模式非常安全，但是也有学者质疑到，参与投票的节点减少，意味着节点的安全性难以保障。有限的参与节点使得区块链容易受到攻击并被篡改，当然目前对于此问题尚在讨论中，尚无定论。

[4] P2P 是一个运行在 TCP 协议之上的应用层协议，在 P2P 网络中，接入网络的每个设备都彼此对等，网络中不存在中心节点，每个节点都随机连接很多其它节点，为这些节点提供服务，同时也从这些节点获取服务，P2P 网络也因此具有去中心化性、可靠性及开放性等特点。近些年最成功的 P2P 网络应用发生在文件分享领域，如国外的 BitTorrent、国内的迅雷等，都是通过 P2P 网络进行文件下载的。参见：《区块链：比特币的灵魂，下一个风口》首次访问时间 2015 年 1 月 2 日 15：30 分 link： http://gd.qq.com/a/20151231/018615_all.htm

2. 作为发展方向的私有链

私有链节点不对外公开，只有被特殊允许的节点可以加入，所有节点均被保密且信任。私有链可以分为全封闭和半公开私有链。 全封闭私有链意味着只有加入节点的才可以查询相关信息，主要应用于金融公司、银行等领域。

半公开私有链提供可供无涉的第三方查询的节点，比较典型的是政府信息公开查询或彩票的节点。私有区块链通过一定的加密技术，将节点中的部分可公开信息对外披露，其他加密信息则供彼此掌握秘钥的人使用。

由于私有链可控的节点数量少，节点可以使用大型服务器、高速网络，这样在一定程度上保证了私有链的交易速度，当前欧美诸多大型公司都在紧锣密鼓的秘密开发私有链，例如：SETL公司公开宣布其目前已经开发了相对稳定和安全的私有链，且交易速度已经达到每日10亿次。R3 和 Bankchain 以及其他公司正在加紧开发私有区块链 。

2015 年 12 月底，Linux 基金会 (Linux Foundation)结合二十几家投资公司、银行及科技公司包括埃森哲(Accenture)，思科(Cisco)，富士通(Fujitsu)，IBM，英特尔(Intel)，VMware 等大型科技公司，一起联合起来抛弃比特币技术，并研发区块链。[5]可以预见，最快的网络（思科），最快的虚拟机（VMware），最好的服务器（富士通、IBM、英特尔），最好最快的数据库（富士通、IBM）都将用于区块链的开发。

[5] 参见：IBM 联合银行业巨头，抛弃比特币欲打造新区块链 Link：https://www.baidu.com/link?url=9Ao5rFZF9ohRreSNnTPLA6vI--m2hLcHBa6gfohFcVGzMQI5khQAAuqHkkRV3nF3&wd=&eqid=b97a076a00016df100000003568cf75e

3. 私有链技术应用

当前的金融公司多采中心主义的记账模式，银行 A 用自己的信息系统为用户记录账户余额，银行 B 也用自己的信息系统为用户记录账户余额，第三方支付 C 也用一套系统记录银行A和B的账户余额及交易记录，这意味着每一次交易都必须由C统一管控并备份。问题也随之而来，一方面人们往往对第三方支付的信赖存疑，若是C与A串通，显然可以更改备份资料及交易数据。另一方面，A、B银行都必须花费大量的时间与金钱去开发和维护系统用来记录信息，也需要花时间和金钱在各银行之间互相检查对账。一旦银行A的顾客与银行B的顾客发生纠纷，C作为唯一掌控交易信息的源泉，虽有披露义务，但其可援引商业秘密加以抗辩，举证难度可想而知。以周雅芳诉中国银行股份有限公司上海市分行名誉权纠纷案[6]为例，中国人民银行以征信系统相对封闭，只有本人或者相关政府部门、金融机构因法定事由才能对该系统内的记录进行查询，进行抗辩。若采半公开的区块链技术，针对他人的私人征信数据向外公开，且每一次修改均有不可修改的痕迹，显然可以充分避免上述情形的发生。

由此可见，如果我们在A、B、C之间采用私有链，创建一个共享网络，使用分布式记账本，银行A、B、可信赖的第三方C都在共享网络中，不完全由可信赖的第三方维护账本，网络中所有的银行、可信赖第三方均掌握账本的最新内容，账本中的流水及其账目均由网络中的所有参与

6 参见“周雅芳诉中国银行股份有限公司上海市分行名誉权纠纷案”link：http://www.pkulaw.cn/case/pfnl_118320768.html?keywords=%E5%91%A8%E9%9B%85%E8%8A%B3%E8%AF%89%E4%B8%AD%E5%9B%BD%E9%93%B6%E8%A1%8C%E8%82%A1%E4%BB%BD%E6%9C%89%E9%99%90%E5%85%AC%E5%8F%B8%E4%B8%8A%E6%B5%B7%E5%B8%82%E5%88%86%E8%A1%8C%E5%90%8D%E8%AA%89%E6%9D%83%E7%BA%A0%E7%BA%B7%E6%A1%88%20&match=Exact

者共同维护，这样就可以充分账本信任度，防止账本被篡改。由于每个参与者都是账本的持有人，其自然有动力充分账本的安全与稳定。

金融公司采用私有链有其合理性，由于私有链有特殊的加入和配对机制，这就保证了金融公司对私有链的完全控制，金融公司现在可信赖的组织和机制， 再加上私有链安全的算法，可以充分保证金融公司数据的安全性和确定性。同样，私有链的节点可以置于被信赖第三方机构，例如公安、法院或者非政府组织（NGO）中，由于在区块链中的每笔交易不可修改，这在一定程度实现了所摄取的证据具有绝对关联性和不可更改性。同样区块链技术的不可更改性充分保证在纠纷时有据可循，这也符合证据法所要求的客观性[i]和合法性[ii]。

	公有区块链	私有区块链
参与投票	任何节点都可以参与投票	只有被特殊允许的节点可以参与投票
参加投票者	数量庞大	数量小
投票机制	工作证明	拜占庭协议
速度	慢	快
网络	P2P网络（Peer-to-Peer network）	高速网络（high-speed network）
节点存储	个人计算机	大型服务器
交易数据	公开	非公开
属性	不变的数据存储 加密, 时间戳技术	不变的数据存储 加密 时间戳技术

4.私有区块链及数据库

区块链主要的应用方式为分布式记账本。私有区块链意指一种金融企业之间私密的分布式记账本，值得注意的是，分布式记账本与传统的数据库有很大的差异，传统的数据库的核心在于数据储存和数据查询，优秀的数据冗余性保证了其云端并行计算的稳定性及系统的容错性。在分布式账本中（区块链中），其主要属性为不可更改性、可追踪性及数据存储的可靠性。

区块链技术充分保证了证据法客观真实的需求，其自身具有不可更改性，数据来源可靠，及完整的数据信息三个特性，但区块链技术囿于自身的局限性，在交易管理,账目查询、并行操作等方面明显比传统数据库系统效率低。值得提醒的是，这并非区块链不可突破的技术壁垒，假以时日进行研究仍有突破之可能。

瑕不掩瑜，我们切不可否认区块链技术广阔应用前景。2015年，区块链持续得到世界各国金融领域的高度关注，据谷歌搜索算法统计，2015年10月以区块链技术为关键词的检索持续高居榜首。

可以预见，区块链技术可充分适应大数据技术的发展要求，并作为云计算及大型数据分析的基础，另一方面区块链基于其自身不可更性等属性充分被司法机构所采纳，区块链技术并非对传统数据库的替代，而是补充现有系统及技术不足，提升社会公信力。

结语

诚如前言，区块链技术的发展会对传统数据库技术带来极大的冲击，但作为是一个纯粹的技术应用，区块链技术的广泛应用并非对传统数据库的取代，而是对现有数据库“不可更改性”属性缺失的补充。笔者认为，私有区块链和公有区块链的发展也可以并存，只是从当下技术实现及推广应用角度，私有区块链值得高度关注。

---

[i] 《刑事诉讼法》第五十条 审判人员、检察人员、侦查人员必须依照法定程序，收集能够证实犯罪嫌疑人、被告人有罪或者无罪、犯罪情节轻重的各种证据。严禁刑讯逼供和以威胁、引诱、欺骗以及其他非法方法收集证据，不得强迫任何人证实自己有罪。必须保证一切与案件有关或者了解案情的公民，有客观地充分地提供证据的条件，除特殊情况外，可以吸收他们协助调查。

[ii] 第五十二条 人民法院、人民检察院和公安机关有权向有关单位和个人收集、调取证据。有关单位和个人应当如实提供证据。

行政机关在行政执法和查办案件过程中收集的物证、书证、视听资料、电子数据等证据材料，在刑事诉讼中可以作为证据使用。

对涉及国家秘密、商业秘密、个人隐私的证据，应当保密。

凡是伪造证据、隐匿证据或者毁灭证据的，无论属于何方，必须受法律追究。

第五十三条 对一切案件的判处都要重证据，重调查研究，不轻信口供。只有被告人供述，没有其他证据的，不能认定被告人有罪和处以刑罚；没有被告人供述，证据确实、充分的，可以认定被告人有罪和处以刑罚。

证据确实、充分，应当符合以下条件：

（一）定罪量刑的事实都有证据证明；

（二）据以定案的证据均经法定程序查证属实；

（三）综合全案证据，对所认定事实已排除合理怀疑。

第五十四条 采用刑讯逼供等非法方法收集的犯罪嫌疑人、被告人供述和采用暴力、威胁等非法方法收集的证人证言、被害人陈述，应当予以排除。收集物证、书证不符合法定程序，可能严重影响司法公正的，应当予以补正或者作出合理解释；不能补正或者作出合理解释的，对该证据应当予以排除。

在侦查、审查起诉、审判时发现有应当排除的证据的，应当依法予以排除，不得作为起诉意见、起诉决定和判决的依据。

第五十五条 人民检察院接到报案、控告、举报或者发现侦查人员以非法方法收集证据的，应当进行调查核实。对于确有以非法方法收集证据情形的，应当提出纠正意见；构成犯罪的，依法追究刑事责任。

第五十六条 法庭审理过程中，审判人员认为可能存在本法第五十四条规定的以非法方法收集证据情形的，应当对证据收集的合法性进行法庭调查。

当事人及其辩护人、诉讼代理人有权申请人民法院对以非法方法收集的证据依法予以排除。申请排除以非法方法收集的证据的，应当提供相关线索或者材料。

第五十七条 在对证据收集的合法性进行法庭调查的过程中，人民检察院应当对证据收集的合法性加以证明。

现有证据材料不能证明证据收集的合法性的，人民检察院可以提请人民法院通知有关侦查人员或者其他人员出庭说明情况；人民法院可以通知有关侦查人员或者其他人员出庭说明情况。有关侦查人员或者其他人员也可以要求出庭说明情况。经人民法院通知，有关人员应当出庭。