基于新时期区块链技术发展的安全性分析

文/李赞

摘要

区块链技术以一种非常火热的姿态席卷而来。作为早在2008年末就在《比特币：一种点对点的电子现金系统》论文中被提及的区块链概念，近两年因比特币的疯狂行情而逐渐被人们关注。区块链作为一种分布式账本，可在业务网络中被参与者高度共享，因其可附加的、有序的、不可篡改的链式数据结构以及方便高效、高安全性的交易业务实现逻辑而受到技术研究人员以及机构的青睐。目前，对于基于区块链技术的去中心化商业系统或金融系统实现的研究已经开展，旨在利用区块链为新型贸易提供更安全高效的方式。同时其高发的安全性问题以及新时期下新技术对区块链安全的威胁也日益显现。

【关键词】区块链技术 安全威胁 去中心化

1 区块链技术缺乏标准化以及跨链通信的问题

虽然目前国际标准化组织ISO、万维网联盟W3C等标准化机构纷纷启动区块链标准化工作，国内工信部也拟筹建区块链和分布式记账标准委员会，但是仍未有一套严格的技术标准和规范提供参考。在推出区块链技术的标准化规范之后，如何实现国内外对标准化达成共识也是需要考虑的。

另外，去中心化的区块链系统由多个相互独立的参与者或节点组成，一条链只能实现一个区块链系统内部的交易和通信。对于未来区块链的发展趋势来说，仅仅只是在系统内部通信远不能满足对信息交互的需求，为了解决这一问题，出现了跨链通信技术，以实现链与链之间的交互。这一最新的跨链技术在具体实现以及安全性方面仍旧存在问题，在跨链技术真正投入使用来解决实际应用问题时，不得不考虑链与链之间基础协议的协调情况，同时还需要对智能合约部分进行改进和优化，使其能高效地运作。

2 区块链的共识机制引发的安全问题

目前主流的共识机制有，工作量证明机制（POW）、权益证明机制（POS）、实用拜占庭容错算法（PBFT）、授权拜占庭容错算法（DPBF）、Pool验证池。能适用于各种区块链网络的完美共识体制是不存在的，共识机制的选择要基于不同业务网络的需求，在可监管性、容错性能、共识效率以及安全性各方面都要能满足业务运行的基本标准。

行情火爆的比特币采用的是工作量证明机制，所谓工作量证明依赖于网络中节点依靠计算能力进行数学运算，从而获得区块的记录权，这一机制消耗大量的计算资源和电力资源，同时受监督的力度小，为了保证交易记录的真实可靠，需要不断调整计算难度，使之与算力的快速发展相匹配。这种机制下工作的区块链系统，容易产生分叉，需要等待多个区块来进行确认。目前使用POW机制还存在一个问题，由于较大程度的算力已经投入比特币市场，如果还有规模较大的区块链网络使用这一共识机制，可能无法得到等量规模的算力进行安全保障。

POS机制中节点所持有代币与节点被选为验证者的概率成正比。在哈希运算方面，资源消耗少于POW，可监管性与容错性等同于POW，在验证方面，从节点中随机选择验证者，节点持有代币越多，所占权重就越大，选中概率越大。但这一切只是在概率上的表达，具有非确定性，在理论上有被攻击的可能。DPOS和POS存在一个共同问题，这两种机制都是依赖于代币的，实际上并不是所有区块链系统都需要代币。

PBFT是一种少数服从多数的机制，具有可监督、能耗低、性能高的特点，不过也存在缺陷，它只是最适用于联盟链，并非公有链。容错率较低，仅有33%，即允许1/3的节点出错。DPBF是国内首先提出的一种共识方案。虽然基本不会产生分叉，而且容错率很高，但是当记账人中有1/3不记账时，系统会停止服务，所以恶意的记账人可能会利用这一漏洞使区块链分叉。Pool验证池是基于分布式一致性算法工作的，比如Paxos算法，区块链系统中不使用代币也能使用这种机制，共识验证速度快，可以实现秒级验证。但是只适用于去中心化程度低的系统，比如多中心化的商业系统。

因此在开发区块链时，要根据需求选择合理的共识机制，要考虑到机制投入使用后可能产生的各种问题，同时设计好突发情况的解决方案以及安全防护机制，防止攻击者利用机制固有漏洞进行恶意攻击。

3 区块链分布式账本的可共享性受到来自新时期新技术的威胁

在比特币的加密体系中，随着量子计算的快速发展以及量子计算机的迅猛发展，在已知公钥的前提下，用量子计算机可以在很短的时间内推出私钥，紧接着用私钥进行签名即可冒充真正的私钥持有者的身份进行欺骗交易。那么如何来获取公钥呢？比特币账户进行交易时，会公开自己的签名以及公钥，用于交易的另一方验证发起者的身份，来确认不是伪造的或者是欺骗性的交易。虽然量子计算机还有待发展，但是仍然不能保证在传统的计算体系下，这种公钥体系是否安全，或者从国家的战略意义上来说，即使有研究人员或者科研机构找到了传统计算体系下的解密方式，也不会大张旗鼓地宣传。

虽然说存在上述这种可能性，但是从实际意义上来说，有能力破解密钥体系和哈希加密算法的个人或者机构也不会在意比特币的微小价值，所以就目前的形势而言，对于共享的区块链体系，私钥的泄露才是最大的威胁。对于普通区块链参与者来说，使用复杂且晦涩难懂的无规律私钥确实是比较尖锐的矛盾，区块链钱包在很大程度上解决了这个问题，同时为了保障安全性，在每次交易过后，节点可以更改自己的地址，这一点对于现有的技术手段来说还是十分行之有效的。另外，不少人使用可信的第三方密钥托管机构来保存区块链私钥，一般地，这些机构也有自己的一套密文的加密体系以及一系列的管理措施。但是从信息安全的角度出发，永远不能忽视潜在的安全威胁，比如来自机构内部涉密员工的威胁，来自机构操作疏忽的威胁，以及来自快速发展的攻击技术的威胁。对于个人来说，来自社会工程学的攻击方法也是屡试不爽，区块链私钥使用时间越长，安全威胁就越大，或许在个人还不知情的情况下，私钥已经被窃取。而且，在现有的区块链体系下，私钥就是一切，私钥泄露等于丢失一切。

另外一方面，随着大数据以及数据挖掘技术的快速发展，势必会对开放且共享的区块链网络产生不可忽视的影响。因为区块链中的账本在各节点是共享的，虽然无法完成对区块中数据的篡改，但是获取到各个区块的交易信

息还是轻而易举的。获取到区块链系统的各种信息之后，运用大数据分析技术可以分析得到某一时间段的交易量、以及各个节点的算力信息，同时从更大的层次去把握区块链市场，黑客甚至可以利用这些信息对有价值的节点发起攻击，来达成个人组织获利或商业企图。

4 缺乏中心调节机制的分布式商业系统能否真正得到实现

目前，数字加密货币还远非主流，加上缺乏中心化的调节机制，应用区块链技术的商业系统投入实际运行后，对于某些节点或者参与者来说，如果他们拥有了既得利益，然后紧接着联合起来反对后期对于系统增加的公平性和完整性的改善，那么系统便会面临崩溃。

在金融方面，用数字加密货币提供服务是否可以合法进行资产登记，区块链中的匿名验证机制是否会得到改进或者是颠覆性的改变，那么到时候区块链系统是否还会行之有效，是否会产生新的安全问题或者危险漏洞尚不清楚。

在可信性方面，区块链的共识机制并不能很好地融入商业系统的需要，而且其不能充当政府机构的角色，只是在计算方面算得上是权威。虽然智能合约可以高效地解决交易中的信任问题，但还是存在它的局限性，一个区块链系统的智能合同仅对于链内的节点有效，对于外部不起作用。

在法律价值方面，智能合约并没有特别明确的法律价值，它只被用来完成系统内的交易，并不等同于具有法律效力的普通合同，因此当使用智能合约的交易出现了问题，没有相应的法律为交易双方提供保障以及仲裁。

5 多重签名、智能合约代码漏洞对区块链安全的影响

多重签名并非是完美解决繁琐的签名和验证过程的方法，多重签名机制自身存在的漏洞也是需要关注的。多重签名机制类似于拜占庭问题的变形，根据其规则，发起交易和广播交易需要多把密钥进行签名，多重签名之后，才能最终动用交易地址的资产完成交易。这一机制也让攻击者有了可乘之机，2017 年以太坊的 Parity 钱包软件出现漏洞，导致了上亿美元的资产被冻结，使用这款软件的多重签名功能的用户都受到了这场危机的影响。对于这场危机，只有采用硬分叉来修复，但是硬分叉又是一种备受争议的升级机制，受到许多用户的抵制。因此无论从技术角度还是其他因素考虑，这个关于多重签名机制漏洞的修复都是极为棘手的，修复方案也值得推敲。

智能合约在实际应用过程中也会产生许多问题。智能合约的出现是为了能自动地类智能化地完成条约规定的内容，避免第三方中间机构的介入，以最大限度减少意外或恶意情况的发生。智能合约的执行不左右于个人的意志，一旦程序执行，没有人可以阻止它的运行，双方会按照既定条件完成交易，不用担心某一方毁约。智能合约名义上是“智能”的，在实际的系统中其实是单调的、存在安全问题的傻瓜式的合约，它只是用算法的思想来简化实际处理的问题。暂且抛去智能合约的法律价值，以及当智能合约与现有法律产生冲突的处理办法。对于合约的安全性还需要考虑诸多方面：

（1）智能合约可以由多种程序设计语言进行编写，既然是人为开发的，便不能排除产生漏洞的风险，据可靠数据显示，目前已经出现的智能合约中并不是所有的都平等，有不在少数的合约中存在安全漏洞，面临着被盗的潜在威胁。另外智能合约签署之后被发现 bug 怎么进行修复，交易方已经产生的损失该怎么处理。首先智能合约一经发布到区块链上就不能进行修改，即使合约中有漏洞需要进行修复或者业务逻辑需要进行变更，并不能在原有的合约基础上直接修改再重新发布，在理论层面上，修改合约需要同一时间内所有的合约持有节点共同完成，只有所有节点同步进行，才能完成对合约的升级。因区块链网络的去中心化性以及没有相关的法律支持，对于合约漏洞直接或者间接造成交易双方的损失而言，没有比较好的解决方案。

（2）智能合约接收的信息源信息的质量也十分重要，如果合约代码中涉及到调用第三方数据或网络数据，当外部信息是错误的、或者被恶意篡改的，便会造成合约判定失误，从而导致交易失败。比如还有在现有的技术能力下，在智能合约缺乏协议和标准化准则的前提下，智能合约是否能满足交易双方的所有需求。

（3）在某些情况下合约的内容需要律师或仲裁机构介入审查，比如合约内容歧义、利益关系模糊或合约的执行流程太过繁琐。当存在智能合约的漏洞未被审查出而被黑客利用时，便会导致比较危险的后果。虽然智能合约作为一种新的交易模式会产生许多的安全问题，但是也有它的价值体现，随着合同审查机制的标准化、专业化，智能合约或许会对现有体制产生冲击。

6 如何合理应用区块链技术实现具体系统

一个区块链系统应包含三个主要部分：面向各节点的应用、智能合约以及分布式账本。系统的最顶层是面向节点的应用，用于满足参与者的需求。该应用让用户调用智能合约在网络中触发交易，智能合约封装系统的业务逻辑，每次调用智能合约都会在网络中创建一笔交易并且添加到账本中，账本保存了智能合约的当前状态，并且分发到各个节点。智能合约像软件开发一样，设计利用区块链技术的系统之前，要进行需求分析。首要的，要保证业务系统涉及多个节点，并且这些节点之间组成业务网络，比如企业与企业之间、企业内的各部门之间，也可存在于个人之间。满足这一条件之后，下面四个条件中至少满足其中一个，区块链技术就可以成为服务于该系统：

（1）系统需要引入共识机制进行交易验证。

（2）需要创建审计来检验线索和信息来源。

（3）业务网络中各节点的交易信息需要是不可改变而且防止被篡改的。

（4）在系统实现过程中，对争议的解决方法需要是最终解决方法。

在应用区块链技术的商业系统中有多种共识机制可供使用，在各节点信任度很高的情况下，进行简单的投票就可以解决共识，否则应该选择更复杂的策略。在加密方面，采用安全有保障的密钥体系，公钥的传递可以使用 PKI 机构进行证书的下载获取公钥，同时也要防止多重签名漏洞，设计好对恶意攻击以及意外状况的应对方案。

参考文献

[1] 唐文剑 . 区块链将如何重新定义世界 [M]. 北京：机械工业出版社 , 2016.

[2] 朱建明 . 区块链技术与应用 [M]. 北京：机械工业出版社 , 2018.

[3] 钟伟 . 数字货币：金融科技与货币重构 [M]. 北京：中信出版集团 , 2018.

[4] 陈俊 . 区块链技术基础：术语和用例区块链的关键术语和无限可能的潜在应用场 景 [DB/OL]. http://m.chinavalue.net/Finance/Blog/2018-1-24/1495253.aspx, 2018-01-24.

[5] 匡堂，陆惠文，文泽中 . 铁炮粗纱机升级改造的实践 [J]. 棉纺织技术 , 2012, 40(09): 33-35.

作者单位

天津理工大学计算机科学与工程学院　天津市 300384