跨境贸易领域中区块链智能合约安全机制分析

袁瑞瑞

大冶市裕丰矿业有限公司　湖北大冶

【摘要】当前所说的智能合约，就是能够自动执行已经预制好的规则、条约，且基于计算机而存在的交易程序，最近几年，伴随区块链技术的创新与发展，其不仅备受关注更在各个行业领域当中被广泛应用。因为智能合约属于是网络环境之下，独立地进行自我验证与自动执行，所以其中存在诸多安全问题。文中对区块链中智能合约存在的安全隐患进行分析，基于实际业务的开展场景，提出全面、有效的安全机制，希望能够为跨境贸易中区块链智能合约的安全应用提供一些帮助。

【关键词】跨境；贸易领域；区块链；智能合约；安全机制

Security Mechanism Analysis of Blockchain Smart Contract in Cross-border Trade Field

Ruirui Yuan

Daye Yufeng Mining Co., Ltd. Hubei Daye

【**Abstract**】The current smart contract is a transaction program that can automatically execute prefabricated rules and treaties. In recent years, with the innovation and development of blockchain technology, it has not only attracted much attention but also been widely used in various industries. Because smart contracts are independently self-validated and automatically executed in a network environment, there are many security problems. This article analyzes the potential security risks of smart contracts in blockchain, and proposes a comprehensive and effective security mechanism based on actual business development scenarios, hoping to provide some help for the secure application of smart contracts in blockchain in cross-border trade.

【**Keywords**】Cross-Border; Trade; Block Chain; Smart Contracts; Security Mechanism

在跨境贸易当中包含很多个参与方，比如国内外生产商、物流商、贸易商、金融机构以及政府监管部门等，同时也涉及到很多个贸易链条，比如资金链、物流链以及数据链等，而跨境管理属于是区块链智能合约当中的关键组成部分。跨境贸易中，自动执行智能合约能够让所有参与方的业务数据达成协同共享，能让参与方物权与资金实现跨境的转移与交付，所以智能合约安全管理极为关键。要求着手于智能合约的构建与应用，探析全面有效地安全管控，并且逐渐形成智能合约实际应用的安全规范，给跨境贸易往来区块链的有序发展提供有力保证。

1 区块链智能合约的应用优势

实际上智能合约是一种计算机程序，其不需要中介，能够进行自我验证与自动执行，在进行智能合约部署以前，同合约存在关联的每个条款对应的逻辑流程已然预制完成，智能合约会存在一个用户接口，让用户和已经预制完成合约实时交互，交互行为需要对已经预制完成的逻辑进行严格遵守[1]。对比传统形式的合约内容，区块链的智能合约存在很多应用优势：

智能合约无需中心化权威对其实际执行的合规性进行仲裁，合约监督与仲裁都是通过计算机完成的，其能够降低对外界的依赖。

部署完智能合约以后，合约内容无法进行修改，也就是说合约中的参与方无法对合约执行进行干预，更能够降低恶意、偶然情况出现导致的异常，也就是规避了人为干预产生的风险隐患。

执行智能合约无需第三方权威、中心代理的参与，所以可以在任何时候对用户诉求进行响应，强

化了交易开展的成效，这能够降低合约履行、仲裁、强制执行过程中出现的人力成本。

2 跨境贸易区块链智能合约面临的安全问题

2.1 代码开发方面

智能合约和传统编程对比之下能够获悉，其信息应用与商业安全存在不同：

智能合约应用于跨境贸易中的时候，其具有一定商业逻辑，比如跨境贸易方、金融机构、政府监管部门的应用场景，商业机密性、数据安全性在金融机构、政府、企业来讲都非常重要，所有数据泄漏的风险、智能合约安全风险等，都会对联盟链有序运行产生影响。

联盟链中的智能合约部署是具备一致共识的，跨境贸易当中的智能合约，需要具备容错、异常终止等逻辑，同时跨境贸易的智能合约如果有安全漏洞处理机制，需要通过联盟方用约定方式予以补充和处理，规避商业层、政府层出现安全风险。

智能合约安全编程规范的制订，能够消除隐私保护、留痕以及审计方面存在的安全隐患问题[2]。

2.2 部署应用方面

伴随跨境贸易联盟链参与方的持续增加，业务链也在持续增加，商业利益、政策驱动参与方、节点会存在恶意行为，智能合约的开放性部署，会存在商业数据外泄、合约被篡改等诸多问题。同时智能合约代码并未发展成熟，实际应用中无法规避安全漏洞的产生，所以，跨境贸易联盟链在智能合约的部署与应用安全方面有严格要求。

2.3 隐私保护方面

智能合约一定要对参与者能够接触到的信息进行规划设计，比如完整接触、部分接触、无法访问等，权限需要基于代码进行明确标注。

跨境贸易区块链中如果智能合约逻辑当中需要监管者参与其中，监管者进行数据访问的权限、范围等需要明确。隐私数据的访问性质、范围等，属于静态或者是动态，怎样才能够将加密参数引入到智能合约当中，设计新参与者进行数据访问的权限与共享机制。

2.4 留痕审计方面

智能合约具有动态性，如果调用的是非确定性系统函数、外部系统非确定性数据来源、动态调用等。进行智能合约设计的时候，要尽量规避其的动态特性应用，如果系统一致性被破坏，会致使问题难度的增加，这会影响故障问题原因的理性判断。

智能合约一定是能够进行终止的，其不会对时间与资源进行无限占用。停机问题属于是逻辑数学当中可进行计算的理论问题，停机能够对程序有限时间内运行结束的相关问题进行判断，智能合约是能够终止的，否则会产生无下限的资源、时间消耗。停机问题无法预判，难以在程序不运行的情况下对其停机问题进行预判。在审计工作的实际开展中，审计者、安全专家一定要对区块链设计工作者的死循环问题进行判断，同时对基于资源管控方式对智能合约的死循环问题进行管控，针对停机问题和资源管控方面的问题，要求智能合约审计工作者进行合理判断，并且选择合理有效的措施进行处理。

3 跨境贸易区块链中智能合约的安全机制

3.1 原则

对智能合约进行合理简化，能够强化其的安全性，围绕客户这个中心，对业务与安全之间的关系进行有效协调，对智能合约复杂度进行有效简化，让复杂合约变成多个较为简单的合约内容，降低复杂性产生的风险管控障碍[3]。

智能合约的安全策略方面需要降低人工处理量，人工进行安全风险处理需要消耗大量时间，需要寻找快速扩展相关业务，以实现对安全问题进行妥善解决的目标。让安全测量更为简单、透明，研发自动化工具，自动判断风险决策，让每个参与方都可以使用安全策略，对安全决策进行持续优化。

智能合约类似于现实审过当中的账本合同，需要对其进行重复多次、严谨的审查，其中涉及业务流程、代码运行动态、测试流程、安全性以及专家的审查等。针对复杂、资金量较大的智能合约，一定要对其代码进行严格审查，基于多种方式对智能合约正确性进行验证。

跨境贸易的区块链联盟，需要给每个区块链参与方出具能够进行参照的安全管控标准，这样内容能够给让编程者、使用者、管理者等进行有效管控。

3.2 开发流程

智能合约的设计工作者、安全工作者一定要明确需求与安全风险，基于建模语言开展智能合约模型的构建，建模需要同所有智能合约参与方多次进行沟通与确认，基于此做好初步设计。

在编写智能合约代码的时候，要求专业智能合约编写工作者参照智能节约的安全规范开展编写作业，基于审计工具分析存在的漏洞问题。智能合约发布以前需要进行全面、深入的代码设计工作，确保审计完成之后的代码就是用户所实际应用的智能合约内容。

智能合约测试工作者于测试链中部署智能合约，同时测试智能合约，比如边界、业务逻辑以及漏洞的测试，测试工作者一定要同业务、安全专家明确设定测试边界，根据测试结果对安全结果进行分析，审计、安全专家联合出具审计报告。报告内容当中涉及漏洞攻击方面的测试，合约内容已经存在或者潜在可能的漏洞情况，合约出现漏洞之后需要怎样响应、终止与更换。智能合约代码报告中能够明确其通用性，也就是说合约场景能够重复使用，其是否可以应用在其他智能合约中，同时需要把修复情况报送给各个参与方。所有参与方基于审计报告、漏洞修复等诸多问题达成共识、认可，这份智能合约才具备进行发布的条件[4]。

3.3 安全规范

跨境贸易链当中智能合约需要对所有权进行规范，基于数字化证书的形式，明确智能合约对应的所有权，基于对函数、状态变量可见性的明确标记，来明确具体谁能够对智能合约进行调用，谁具备合约变量访问的权限。跨境贸易中有些智能合约会被外部所调用，要求调用的数据必须保证安全，能够被信任与依赖。对外部调用进行规范的时候必须谨慎，所有外部调用都要设定成潜在的安全隐患，设计智能合约的时候，安全风险的级别参数无关信息需要设定到发生结果中，以备审计与留痕的时候进行合理应用。

在对外部调用存在的错误问题进行处理时，需要对返回值进行检查，如果使用的是匹配、模式验证，需要对调用不成功的返回值进行调用处理，于合约代码中兼顾所有调用不成功的可能性进行合理处理。调用规范的约定，不能使用外部调用的返回值进行逻辑管控判断，因为外部调用结果存在危险性与不确定性，在重要的逻辑判断中不能调用外部函数结果进行逻辑判断，以免出现双重攻击的风险问题。基于外部资源调用的智能合约，其在输入、出的时候都会存在留痕以及审计等诸多操作设计，比如是金融场景，智能合约应用层一定要进行回滚提供与访问管控，保证智能合约可以进行重新限制，规避安全漏洞问题的产生。

基于智能合约的代码对函数等诸多标识进行命名，以此对编码规范性进行满足，在同外部合约交互的时候，代码层面需要于方法、合约接口、变量上进行规范命名，对审计不明确的外部合约、外部依赖等，需要进行明确标识，基于明确明示与数据、智能合约进行交互的时候存在安全风险。

快速失败原则，其说的就是在执行智能合约核心逻辑以前，要对合约录入数据进行全面检查，数据内容如果无法满足合约校验的规则，要快速返回到失败结果处，以免智能合约实际执行中出现异常。快速失败原则能够降低智能合约实际执行的时间，以免因为未知异常而导致的堆栈溢出等风险问题。设计过程中要意识到数据检验如果失败，会应用到一个默认值，让合约得以继续执行。尽快找到不成功的执行，比如区块链的脚本语言通常基于 try 语法机制，对失败原因进行快速定位与捕获。以免不一致、不稳定的状态对其他调用者、状态等产生影响。

智能合约中如果需要对多个不同函数、智能合约进行调用，会出现顺序依赖的问题，要先将内部函数工作完成，之后再进行外部函数调用。同时，有一些智能合约基于锁定机制对调用依赖问题进行调用，互斥锁能够对代码块进行锁定，基于锁定对资源访问的权限进行有效保护。

在智能合约的实际执行中，交易处理会因为交易顺序不同而出现截然不同的情况，交易状态不同会致使输出结果的不同。智能合约问题也就是交易顺序的依赖合约，恶意参与方会对智能合约执行顺序进行故意修改，对合约合法性产生在破坏影响，所以，在设计跨境区块链的智能合约时，需要对交易顺序进行严格设计、验证。

智能合约依赖于区块时间戳，或者是遵照时间戳进行随机数提供，在网络节点时间戳出现偏差的时候，会影响执行智能合约的结果。攻击者基于区块链时间节点中的时间戳，对智能合约的执行结果进行改变，让结果有利于自己。所以，跨境贸易区块链中的智能合约如果只依靠时间戳，需要对合约时间错的范围进行校验，多个参与方于时间戳时间范围层面上达成共识，以此对智能合约进行有序执

行，以免智能合约的无法得到有序执行[5]。

智能合约不同于传统编程，在智能合约的编程设计中，需要在合约当中写入容错、异常终止等逻辑。智能合约回退的时候要尽量简单，所有智能合约都需要设置回退功能，函数回退一定要对回退动作进行记录，如果需要更为繁琐的回退功能，要先进行测试评估，以免回退太过复杂。

设计智能合约的代码时，想要确保合约实现就要对边界条件进行考量，准备好应对智能合约实际运行中可能会产生的不良情况，智能合约如果有漏洞问题存在，对恢复方法、流程等进行有效规范，让智能合约能够尽快、安全地恢复，跨境贸易领域中的容错方案，能够给所有智能合约提供备用方案，备用方案能够对智能合约的漏洞问题进行紧急处理。容错可使用合约停止机制，合约管理工作者可使用冻结方式进行应急处理，合约停止的时候，需要使用线下、合约修正等方式补偿业务逻辑。在对合约进行设计、优化的时候，要对影响合约的节点进行考量，兼顾怎样对合约数据进行处理，如果新合约和旧合约所使用的数据相同，与旧合约、新合约并行了一段时间之后，可将旧合约关闭或者废止。

3.4 存证审计

对智能合约的安全审计工作机制进行完善，其中包含代码、存证流程、执行记录等方面的审计验证，跨境区块链中的智能合约，可使用超级账本、分布式账本等进行解决。如果区块链外部应用程序需要对账本进行访问，就会进行调用，基于多种编程语言达成目标。

3.5 隐私保护

智能合约可以基于中心化身份进行身份管理，其中包含很多功能，身份认证，比如在 LDAP 中进行信息注册，担保证书的发行，交易证书的发行等，确保平台交易相关信息数据的安全性，同时要求证书可以进行更新与撤销。

跨境交易场景有很多，所有场景都会有对应的智能合约，并且基于通道将其隔离开来，所有通道都有一部分授权参与者，其能够对通道合约带帽、交易数据等进行查看。通道中基于可见性对力度可见性进行限制。在对合约中间数据、结果进行处理的时候，可基于加密方式予以上链与存储。链上存储介质当中的数据要基于国密算法予以加密，确保数据信息的安全性。

3.6 资产保护方面

基于区块链技术为数字资产的安全提供保证，本身数据的加密技术能够请确保数据真实性与可追溯性。基于存证合约确保数字资产出现争议时候能够基于取证与仲裁，对数字资产安全相关问题进行有效解决。智能合约实际运行中的数字资产，需要持续健康交易行为，并且进行快速预警，确保数字资产不会遭遇攻击、出现漏洞，或者在遭遇攻击、出现漏洞的时候能够及时被发现和处理，以免产生严重的经济损失。智能合约本身具备更新、暂停机制，对运行范围进行限制，确保数字资产产生经济情况的时候，可以有紧急方式进行制动与止损。

4 结束语

综上所述，智能合约对应的安全技术创新发展，配套技术、规则等也在持续完善，其能够对智能合约高效运行提供安全保证。

参考文献

[1] 曾丽.基于区块链的跨境电商大数据智能处理传输方法及平台:,CN111461840A[P].2020.

[2] 王东,谢珍贞.区块链技术在跨境电商协同发展中的应用路径与法律规制框架[J].新疆财经大学学报,2020(3):8.

[3] 林斌晖.区块链技术对传统跨境贸易结算方式的影响研究[J].2020.

[4] 李晓风,许金林.一种基于区块链的跨境贸易隐私数据管理系统及方法:,CN112417512A[P].2021.

[5] 陆昉.跨境贸易领域中区块链智能合约安全机制研究[J].网络安全技术与应用,2021(07):161-164.

收稿日期：2022 年 4 月 22 日
出刊日期：2022 年 5 月 25 日
引用本文：袁瑞瑞，跨境贸易领域中区块链智能合约安全机制分析[J]. 现代工商管理, 2022, 2(1):36-39
DOI: 10.12208/j.jmba.20220010

检索信息：RCCSE 权威核心学术期刊数据库、中国知网（CNKI Scholar）、万方数据（WANFANG DATA）、Google Scholar 等数据库收录期刊