软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链性能及安全性架构调优方法*

李立中[1,2]

[1](北邮在线 数字经济研究院,北京 100876)

[2](金窝窝研究院,重庆 400010)

通讯作者: 李立中, E-mail: kvllz@163.com

摘 要: 性能及安全性架构调优是软件工程区块链领域中的一个研究热点.通过分析区块链不可能三角的业务逻辑,设计出三者相关的可信度量元;随后,通过创新的节点架构和安全方法论,旨在构建出平衡交易效率、安全性、去中心化的新模型,以可信节点、自净化及计算机体系潜在缺陷弥补程序模块,最终达到优化测试资源分配和提高软件产品质量的目的.首先,给出了研究框架并识别出区块链不可能三角的 3 个重要影响因素之间的平衡关系:度量元的设定、安全架构模型的构建方法和计算机体系缺陷弥补的相关问题;接着,依次总结了这 3 个影响因素的个人研究成果;最后,对未来研究可能面临的挑战进行了展望.

关键词: 区块链不可能三角解决;计算机体系安全缺陷弥补;区块链可信度量元;机器学习

中图法分类号: TP311

中文引用格式: 李立中.区块链性能及安全性架构调优方法.软件学报. http://www.jos.org.cn/1000-9825/ 0000.htm

英文引用格式: Li LZ. State-of-the-Art survey of static software defect prediction. Ruan Jian Xue Bao/Journal of Software, 2016 (in Chinese). http://www.jos.org.cn/1000-9825/0000.htm

Block chain performance and security architecture tuning method

LI Li-Zhong[1,2]

[1](Research Institute of Digital Economics, Beijing post online, Beijing 100876, China)

[2](Jin Wo Wo Research Institute, Chongqing 400010, China)

Abstract: Performance and security architecture tuning is a research hotspot in the field of software engineering block chains. By analyzing the business logic that block chains can not be triangulated, three related trusted metrics are designed. Then, through innovative node architecture and security methodology, a new model is designed to balance transaction efficiency, security and decentralization. Firstly, the research framework is given and the balance among the three important factors that make the block chain impossible to triangle is identified: the setting of metric elements, the security architecture. Secondly, it summarizes the personal research results of these three factors in turn. Finally, it looks forward to the challenges that the future research may face.

Key words: Block chain can not be solved by trigonometry; the security defect of computer system is made up; block chain reliability is measured; machine learning.

区块链技术的“不可能三角”问题即高效率、安全性、去中心化.也就是在区块链系统中,不可能在同一层面、同一时间在高效率、安全性、去中心化三方同时获得最优解,只能同时实现两点,这也是目前区块链无法大规模商用化的根本原因之一.如果不能够合理的解决这个“不可能三角”问题,区块链技术的落地周期就会不断被拉长,而目前提出的解决方案无论使用什么模式都无法真正的解决三者间的平衡,因此我们期望能够通过这三角的权重因子商业评估来解决这一难点问题.

对于一个商业应用技术实现来讲,高效率和安全性是第一权重因子,用金融系统的专业话术就是业务连续

* 收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos 在线出版时间: 0000-00-00
CNKI 在线出版时间: 0000-00-00

性、可用性和信息安全性、完整一致性.只有先满足这两者要求才能够真正的商业应用落地,而去中心化或多中心化的要求并不一定必须具有实时性,只要在一定时间内完成多节点的信息同步即可保障未来数据被篡改的高昂代价，进而达到区块链技术所带来的多点记账合约信任.

当前计算机安全分为三个层面：计算机体系安全缺陷[1,2]、计算机代码后门和社会工程学.计算机体系安全缺陷产生于计算机顶层设计时的认知偏差和当时对于硬件资源最大限度节省的要求，导致代码和数据在内存空间的存储方式完全一致.以至于传入的数据参数可能会通过特殊的构造方式被解释器解读为代码,注入、溢出、跨站等等攻击方法都是因此而来.这也是计算机安全脆弱性的最大风险来源,而计算机后门和社会工程学风险可以通过代码审计、逆向工程和安全管理流程进行有效规避.

本文重点对区块链技术中“不可能三角”个人的研究工作进行综述.具体来说,该类方法通过分析区块链技术落地与高效率、安全性、去中心化相关的权重因子,随后,通过区块链可信度量元来创建交易确认节点集.再通过代码异构的方式规避计算机体系安全缺陷,最后,基于上述安全可信的交易结果进行多中心或去中心的记账节点信息同步.

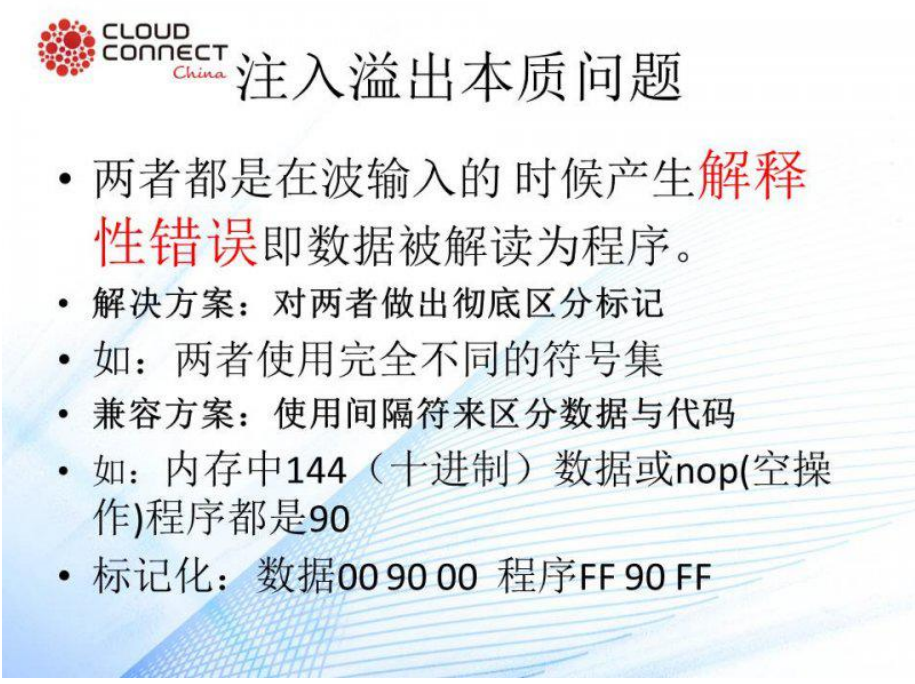
随机选出部分共识节点的可信度量元可以参考下图实现方式,我们可以通过相关交易节点的随机分层避免拜占庭将军问题,因为坏节点不知道自己所在共识节点的层级,报出不一致的错误信息就会对它的可信度量元进行降权甚至剔除出共识体系,为了平衡入侵的成本导致坏节点轻易不会发出不一致交易信息.即使偶尔发出针对交易信息的攻击,也会因为这个体系的随机性不断被自净化.

为了进一步增强节点的安全性,我们可以使用 CN201810565810.X 基于区块链的交易信息确认方法及装置,通过随机同步三个或奇数个交易确认集来避免单一可信节点集的半数节点拜占庭攻击问题.

采用随机的部分可信节点完成交易共识,结束交易后再把相关信息同步到外部交易信息披露节点.交易记账节点完成记账后,当次交易可以视作完成,而交易信息同步节点可以等待后续的调度程序慢慢同步,这样记账就可以大幅提升交易的效率,又保障了后面的去中心化或多中心化的结果.

上面的方法只能解决商业交易效率问题和部分安全性问题,但是对于之前提到的计算机体系安全缺陷还需要新的防范手段,我们可以通过 CN201510537379.4 一种语句预处理方法、装置以及语句的解释方法、装置,

把代码和数据从源头上区隔开来,让两类信息永远鸡同鸭讲.最有效的方法就是在硬件层面就区分数据和代码的指令集,但是为了现有计算机体系的兼容性我们可以在内存构造区隔符号,所有的程序代码在初始化的时候就由 FF 间隔,而数据方式的写入就都是 00 间隔,这样不管是堆溢出还是栈溢出都是数据方式覆写的内存,内存表现形式都是 00 的,这样溢出后程序远跳到对应位置识别为当前信息是数据结构就会立刻报错,进而解决相关溢出问题.而注入跨站等问题也可以参考 2015 年我在全球云计算大会发表的演讲 PPT.



CLOUD CONNECT China

```
0:000> kb
ChildEBP RetAddr  Args to Child
WARNING: Frame IP not in any known module. Following frames may be wrong.
0012fbb8 41414141 41414141 41414141 41414141 0x41414141
0012fbbc 41414141 41414141 41414141 41414141 0x41414141
0012fbc0 41414141 41414141 41414141 41414141 0x41414141
0012fbc4 41414141 41414141 41414141 41414141 0x41414141
0012fbc8 41414141 41414141 41414141 41414141 0x41414141
0012fbcc 41414141 41414141 41414141 41414141 0x41414141
0012fbd0 41414141 41414141 41414141 41414141 0x41414141
0012fbd4 41414141 41414141 41414141 41414141 0x41414141
0012fbd8 41414141 41414141 41414141 41414141 0x41414141
0012fbdc 41414141 41414141 41414141 41414141 0x41414141
0012fbe0 41414141 41414141 41414141 41414141 0x41414141
0012fbe4 41414141 41414141 41414141 41414141 0x41414141
0012fbe8 41414141 41414141 41414141 41414141 0x41414141
0012fbec 41414141 41414141 41414141 41414141 0x41414141
0012fbf0 41414141 41414141 41414141 41414141 0x41414141
0012fbf4 41414141 41414141 41414141 41414141 0x41414141
0012fbf8 41414141 41414141 41414141 41414141 0x41414141
0012fbfc 41414141 41414141 41414141 41414141 0x41414141
0012fc00 41414141 41414141 41414141 41414141 0x41414141
0012fc04 41414141 41414141 41414141 41414141 0x41414141
```

如果间隔符数据为00，程序为FF

CLOUD CONNECT China

- FF 41 FF 41 溢出后 00 41 00 41 跳过去解析程序就会报错
- 溢出Shellcode执行的方法和破解技术中的SMC方法非常相似
- Shellcode是实时修改， SMC是预先修改Shellcode只要执行一般不会管后面的运行而SMC要跳回原有的流程。
- 本方法只能阻挡实时修改

综上所述,通过合理的技术架构,把商业应用的高效率和安全性优先权前置,去中心化或多中心化的共识算法后置,通过 CN201510537379.4 一种语句预处理方法、装置以及语句的解释方法、装置 CN201810565810.X 基于区块链的交易信息确认方法及装置 CN201610501761.4 基于本地节点随机指令分布式认证方法,系统及装置这三项发明创新保障系统及节点的安全性,再通过 CN201610479798.1 一种区块链共识及同步方法,系统及装置来保障商业应用交易的高效率,这样就可以有效的解决不可能三角问题.

附中文参考文献:

[1] CN201510537379.4 一种语句预处理方法、装置以及语句的解释方法、装置

[2] CN201810565810.X 基于区块链的交易信息确认方法及装置

[3] CN201610501761.4 基于本地节点随机指令分布式认证方法,系统及装置

[4] CN201610479798.1 一种区块链共识及同步方法,系统及装置