区块链的安全风险评估模型

秦超霞[1],郭 兵[1],沈 艳[2],苏 红[1],张 珍[1],周驰岷[1]
(1. 四川大学计算机学院,四川成都 610065; 2. 成都信息工程大学控制工程学院,四川成都 610225)

摘 要: 随着区块链技术在社会经济领域的应用不断扩大,区块链的安全问题受到越来越多的关注. 本文提出了一种新的区块链安全风险评估方法,分别从技术架构和算力两方面量化区块链的安全风险. 我们首先根据区块链技术体系架构建立了区块链可信计算基(Blockchain Trusted Computing Base,BTCB),进而设计了一种结合层次分析(Analytic Hierarchy Process,AHP)和配对比较的安全敏感性分析方法,为每个安全风险影响因素分配权重,最终构造了一个区块链的安全风险评估模型. 在实验部分,我们采用该模型为当下 15 个常见公有链区块链项目打分,并与市场认可度较高的四家区块链评级机构的评测数据进行对比分析,实验结果表明我们的模型具有一定的可行性.

关键词: 区块链; 风险评估; 区块链可信计算基; 层次分析; 算力
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112 (2021)01-0117-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20180962

Security Risk Assessment Model of Blockchain

QIN Chao-xia[1], GUO Bing[1], SHEN Yan[2], SU Hong[1], ZHANG Zhen[1], ZHOU Chi-min[1]
(1. *College of Computer Science, Sichuan University, Chengdu, Sichuan* 610065, *China*;
2. *School of Control Engineering, Chengdu University of Information Technology, Chengdu, Sichuan* 610225, *China*)

Abstract: With the expansion of the application of blockchain technology in the socio-economic fields, increasing attention has been paid to the security of blockchain. This paper proposes a security risk assessment method for blockchain, which quantifies the security risk of blockchain from the aspects of technical architecture and hash rate. At first, we build the Blockchain Trusted Computing Base (BTCB) model based on the technology architecture. Then, we design a sensitivity analysis method combined the AHP and paired comparison to assign security weights to each security risk factor. Finally, we construct a security risk assessment model. In the experimental part, we use this model to score 15 common public-chain blockchain projects, and conducte comparative analysis with the evaluation data of four blockchain rating agencies with high market recognition. The experiment results verify the feasibility of this method.

Key words: blockchain; risk assessment; BTCB (blockchain trusted computing base); AHP (analytic hierarchy process); hash rate

1 引言

区块链起源于比特币[1],凭借去信任、防篡改、可追溯等安全优势,成为未来金融、财政等领域的重要应用技术[2]. 随着计算机计算能力的大幅提升和隐藏在应用领域背后经济利益的加大,区块链技术的安全问题[3,4]日趋显著. 因此,区块链的安全风险研究正成为国内外的研究热点.

最近几年,多种方法已经被提出用于检测和评估区块链的安全风险. 目前,大部分研究使用数学方法分析区块链中每个攻击(比如 51% 攻击、日蚀攻击[5]和物理攻击等)的影响力,从而评估区块链的安全性. 区块链中的攻击种类和数量繁多,至今还没完全被发现,因此,单独分析每个攻击的作用是不全面的. 为了全面地评估区块链的安全性,文献[6]提出了一种基于区块链状态的安全评估方法,分析每个状态变成攻击成功状态的概率,从而判断系统安全性. 根据文献查阅,现有方法没有从技术体系架构[7]和算力的角度研究区块链的安全风险,而技术组合和算力会对区块链的安全风险产生很大的影响. 因此,本文从技术体系架构和算力的角度提出了一种评估区块链安全风险的新方法.

该方法由定量影响因素和定性影响因素共同决

收稿日期:2018-11-02; 修回日期:2019-10-24; 责任编辑:王天慧
基金项目:国家自然科学基金(No. 61772352);四川省科技计划项目(No. 2019YFG0400, No. 2018GZDZX0031, No. 2018GZDZX0004)

定,定量影响因素包括区块链算力、区块链分叉深度等.定性影响因素构成了区块链的安全基础,如数字签名、共识机制、智能合约等.我们首先根据区块链技术体系架构建立区块链可信计算基,进而提出了一种结合层次分析和配对比较两种方法的安全敏感性分析方法,为每个影响区块链安全风险的因素分配权重,最后设计了一个区块链的安全风险评估模型.

2 区块链可信计算基

从区块链技术架构的角度充分揭示受评区块链项目的安全风险,需要对影响区块链安全风险的各种技术进行全面分析.基本思路是从安全风险的内涵出发,以技术的安全性为落脚点,充分考虑区块链的数据模型、加密算法、共识机制、网络设计、去中心化程度、激励机制和智能合约等安全影响因素.区块链的发展与演进大致经历了区块链1.0、2.0和3.0三个阶段,尽管在具体实现上有所不同,但基础技术架构存在许多共性,整体上可划分为六个层次:数据层、网络层、共识层、激励层、合约层和应用层,见图1.

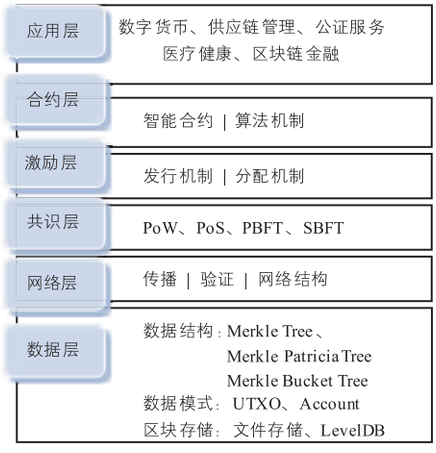

图1 区块链技术架构

为了给下文区块链安全风险的定性评估提供逻辑严密的分析过程,我们根据区块链的技术架构建立了区块链可信计算基BTCB,如图2所示.BTCB包含了影响区块链安全的所有要素,并按功能差异将它们分层分类,以便分析统计区块链的潜在安全风险或安全保护机制.

定义1 (区块链可信计算基——BTCB)区块链可信计算基表示安全区块链系统的所有安全保护机制的集合.

与区块链技术架构相比,BTCB的内容更广泛.除了技术类的安全要素外,BTCB还包含区块链行业环境、发展趋势、政策和监管措施等企业外部安全要素;企业项目、团队组成、技术实力、资本投入和运营维护等企业内部安全要素;及其他特殊安全要素.但本文的重点是从技术架构的角度量化区块链项目的安全风险,因此,我们只讨论BTCB的技术类安全要素,并将其作为区块链安全风险评估的内容.

图2 区块链可信计算基

(1)数据层:数据存储和数据加密,对应的安全保护机制分别是基于Merkle树的数据存储[8]和基于数字签名的加密算法[9].

(2)网络层:P2P网络风险、广播机制风险和验证机制风险.区块链基于P2P网络的传播、验证等机制,容易受到日食攻击、窃听攻击、BGP劫持攻击、节点客户端漏洞、拒绝服务(DDoS)等攻击.安全保护机制主要包括不断改进的网络协议、安全严谨的网络结构.

(3)共识层:共识机制的可靠性.共识机制是对一个时间窗口内的事务先后顺序达成共识的算法.区块链可支持不同的共识机制,比如PoW、PoS、DPoS、Pool验证池机制和PBFT等,面临的攻击包括女巫攻击、short-range攻击、long-range攻击、币龄累计攻击、预计算攻击等.

(4)激励层:发行机制风险和分配机制风险.分配机制将大量小算力节点集中加入矿池,易对去中心化趋势造成威胁.

(5)应用交互层:应用扩展风险、应用环境风险和市场反馈.应用扩展风险主要指对各类脚本、算法及智能合约的攻击,主要包括Solidity漏洞、短地址漏洞、逃逸漏洞、可重入性攻击、交易顺序依赖攻击、时间戳依赖攻击、堆栈溢出漏洞、整数溢出攻击等.应用环境风险包括经济形势、货币政策、企业团队背景和资本等带来的安全风险.市场反馈主要集中在与加密资产相关的领域,例如在用户节点、数字资产钱包以及交易平台的安全风险[10].

3 配对比较

配对比较[11]可以帮助领域专家更好地描述敏感性

级别,比较的内容包括敏感属性对和属性值对,表 1 是敏感属性和属性值的配对比较示例. AHP 是[12]基于配对比较的集合推断偏好,是一种决策支持工具,在一致率(Consistency Rate ,CR)小于 0.1 时有效. 配对比较和层次分析法结合,在同一级别上权衡每个值相对于其他值的重要性,然后可以通过将树中相同路径上的权重累乘来提取树中路径的重要性.

表 1　属性和属性值的配对比较

	谁更敏感?		相同	敏感程度			
属性	网络协议	网络结构	1	3	5	7	9
			√				
属性值	私有链	公有链	1	3	5	7	9
		√					√
	私有链	联盟链	1	3	5	7	9
		√			√		

注:1-相同,3-稍强,5-较强,7-非常,9-极度

在我们的例子中,我们将安全敏感性评分函数的设计定义为一个 3 级 AHP 树问题. 见图 3,顶层定义待解决的问题,该层只有一个选项且权值为 1;中间层是安全敏感属性;叶子节点表示安全敏感属性值. 我们使用配对比较,让专家先比较每个属性对,然后比较同一属性的属性值对,最后每个属性值路径上权值的累乘就是其安全敏感性评分. 本文中针对区块链安全风险相关属性的列举会有所取舍,但不影响推导过程的合理性. 例如,使用图 3 中的 AHP 树,如果想要推断“私有链”的安全风险评分,只需计算:

安全风险评分(私有链) = 权重(查找安全敏感属性值的权重) × 权重(网络结构) × 权重(私有链) = 1 × 0.5 × 0.1 = 0.05

图 3 中的层次结构有一些有趣的特性:同一根节点下所有子节点的权重之和为 1;所有属性值的安全敏感性得分总和为 1. 如果一个敏感性属性有 n 个不同的属性值,则专家需要比较 $(n \times (n-1)/2)$ 次才能获得属性值的权重.[13]

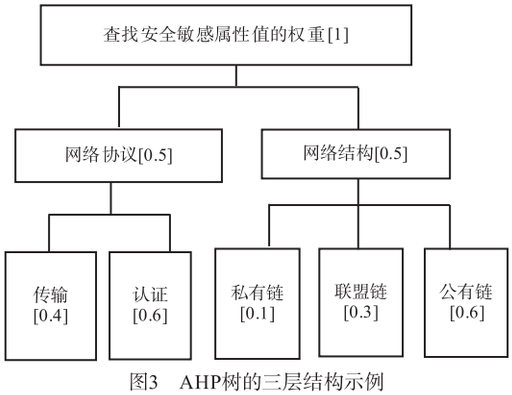

图3　AHP树的三层结构示例

4　安全风险评分函数的推导

我们首先分别讨论定量安全风险评分(算力)和定性安全风险评分(技术架构),然后确定两者的函数关系,以较全面地评估区块链安全风险. 值得注意的是,安全风险评分值越高,区块链越安全. 表 2 列出了本节涉及的主要符号及其定义.

表 2　符号说明

描述项	符号
区块链安全风险评分	S
区块链定量安全风险评分	S-quanti
区块链定性安全风险评分	S-quali

4.1　正式定义

在本节中,我们将提供本文的正式定义. 在不损失通用性的情况下,我们假设只有一个区块链系统存在,该方法可以很容易地扩展以处理多个区块链的组合系统.

定义 2　(区块链的安全敏感属性)能影响区块链安全风险程度的属性称为区块链的安全敏感属性,位于 AHP 树的中间层. 我们用集合 $\boldsymbol{A} = (A_1, \cdots, A_i, \cdots, A_n)$ 表示区块链的安全敏感属性集合,A_i 表示其中一个属性.

定义 3　(安全敏感属性的属性值)定义安全敏感属性的特定特征或参数称为安全敏感属性的属性值.

一个安全敏感属性 A_i 用集合 $\boldsymbol{P}_i = (p_{i1}, \cdots, p_{ij}, \cdots, p_{im})$ 表示,其中 p_{ij} 表示属性 A_i 的第 j 个属性值. 安全敏感属性的属性值位于 AHP 树的叶子结点.

定义 4　(安全敏感性评分函数)安全敏感性评分函数 $f[p_{ij}]: \boldsymbol{A} \times p_{ij} \in [0,1]$ 根据属性值对区块链安全风险的影响力大小为每个属性值分配安全敏感性评分. 自变量包括属性值 p_{ij} 和其对应的 AHP 路径属性集合 $\boldsymbol{A}$.

我们利用图 3 的信息举例说明安全敏感性评分函数的计算过程:

f[私有链] = 安全风险评分(私有链) = 权重(查找安全敏感属性值的权重) × 权重(网络结构) × 权重(私有链) = 1 × 0.5 × 0.1 = 0.05

4.2　定量分析

中本聪提出了比特币的原理,将诚实链和攻击链之间的竞争描述为二项随机游走,即成功事件是诚实链扩展一个块,而失败事件是攻击链扩展一个块,将差距减少 1;并计算了攻击者在不同攻击力度下成功攻击的概率.

根据区块链的设计特点,矿工所掌握的所有矿机占区块链全网总算力的百分比代表着他成功挖矿的概率. 举个例子,已知攻击节点加入之前的区块链全网算力为 M,攻击节点的算力为 A,那么诚实节点成功挖块

的概率为：

$$p=\frac{M}{M+A} \tag{1}$$

攻击节点成功挖矿概率 $q=1-p=\frac{A}{M+A}$. 目前主流的矿机算力为 14TH/s 左右，即每秒至少能做 1.4×10^{13} 次的哈希碰撞. 如果用一台算力为 14TH/s 的莱特币矿机挖莱特币（目前莱特币的全网算力大概为 390TH/s），此时，该矿机成功的概率为 $P=\frac{1.4\times10^{13}}{39\times10^{13}+1.4\times10^{13}}=0.03$.

一个攻击链能够追上诚实链的概率如式（2）所示：

$$q_z=\begin{cases}(q/p)^z, & p>q\\ 1, & p\leqslant q\end{cases} \tag{2}$$

q_z 是攻击者最终消弭 z 个落后区块并改变当前区块交易内容的概率. 根据 51% 攻击观点，当 $q>0.5$ 时，攻击者一定能够追赶上诚实者. 假设诚实节点将耗费平均预期时间产生一个区块，那么攻击者的攻击进展就是一个泊松分布，分布的期望值为：$\lambda=z\times(q/p)$[14]. 我们将攻击链扩展第 k 个区块的概率密度，乘以在 k 长度链下攻击者依然能够成功的概率，最终求和得到攻击者追赶上 z 个区块的总概率：

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\times\begin{cases}(q/p)^{(z-k)}, & k\leqslant z\\ 1, & k>z\end{cases} \tag{3}$$

为了避免对无限数列求和，式（3）可以转化为式（4）的形式：

$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\times(1-(q/p)^{(z-k)}) \tag{4}$$

区块链安全性与成功攻击概率成反比关系，因此 S-quanti 函数可以设计为：

$$\text{S-quanti}=\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\times(1-(q/p)^{(z-k)})$$
$$\text{S-quanti}\in[0,1] \tag{5}$$

详细的 S-quanti 逻辑设计见算法 1.

算法 1　计算 S-quanti 函数值

输入：诚实矿工成功挖矿概率 p，攻击链区块落后差距 z
输出：S-quanti 函数值
1. 计算攻击者成功挖矿概率 q，$q=1-p$
2. 计算 $\lambda=z\times(q/p)$
3. 令 $sum=0$
4. for 攻击者取得进展区块数量 $k=0$ 到 z
5. 计算 $poisson=\text{pow}(\lambda,k)\times\exp(-\lambda)$
6. 如果 $k\leqslant1$，$mul\_k=1$；否则 $muk\_k\times=k$
7. $poisson=poisson/mul\_k$
8. $sum+=poisson\times(1-(q/p)^{(z-k)})$
9. end for
10. 返回 sum

表 3 给出了部分 S-quanti 值，从概率层面分析，当 $p<0.5$ 时，攻击者一定能够追赶上诚实者. 因此，我们只讨论 $p\geqslant0.5$ 时 S-quanti 值的变化规律. 根据图 4 我们发现固定 p 值，S-quanti 值随 z 值非线性增大，表示攻击链离攻击成功的目标越远，此时区块链越安全；固定 z 值，S-quanti 值随 p 值非线性增大（见图 5），表示诚实链算力越大，此时区块链越安全.

表 3　S-quanti 函数值

S-quanti		z										
		0	1	2	3	4	5	6	7	8	9	10
p	0.5	0	0	0	0	0	0	0	0	0	0	0
	0.6	0	0.1711	0.2636	0.3358	0.3966	0.4494	0.4960	0.5377	0.5752	0.6092	0.6400
	0.7	0	0.3723	0.5543	0.6754	0.7609	0.8226	0.8679	0.9013	0.9261	0.9445	0.9583
	0.8	0	0.5841	0.7961	0.8968	0.9470	0.9726	0.9857	0.9926	0.9961	0.9980	0.9989
	0.9	0	0.7954	0.9490	0.9868	0.9965	0.9991	0.9998	0.9999	1	1	1

4.3　定性分析

已存在共识算法可以部分解决 51% 攻击问题，比如 PoS、DPoS，这说明仅从定量上分析区块链的安全风险是不足的，我们还需要定性分析区块链的安全风险.

基于安全敏感属性 AHP 树的定义和函数推导的需要，我们先做如下假设和定义.

（1）位于 AHP 树倒数第二级的安全敏感属性数量为 p，因此安全敏感属性值可以分为 p 组.

（2）每组安全敏感属性值的数量为 $q_1,q_2,\cdots,q_p$.

（3）每组安全敏感属性值的深度分别为 $n_1,n_2,\cdots,n_p$.

（4）每组安全敏感属性值表示为：

第一组安全敏感属性值分别为：$s_{11},s_{12},\cdots,s_{1q_1}$；

第二组安全敏感属性值分别为：$s_{21},s_{22},\cdots,s_{2q_2}$；

……

第 p 组安全敏感属性值分别为：$s_{p1},s_{p2},\cdots,s_{pq_p}$.

记 $\boldsymbol{S}=(s_{11},s_{12},\cdots,s_{1q_1};\cdots;s_{p1},s_{p2},\cdots,s_{pq_p})$.

（5）安全敏感属性值的路径权重为：

s_{11} 的路径权重：$t_{111},t_{112},\cdots,t_{11n_1}$；

s_{12} 的路径权重：$t_{121},t_{122},\cdots,t_{12n_1}$；

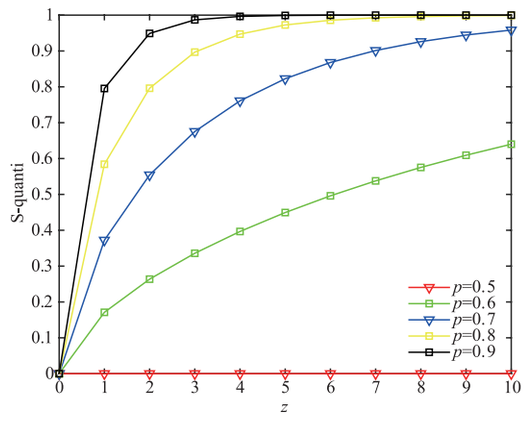

图4　S-quanti值随z值变化趋势

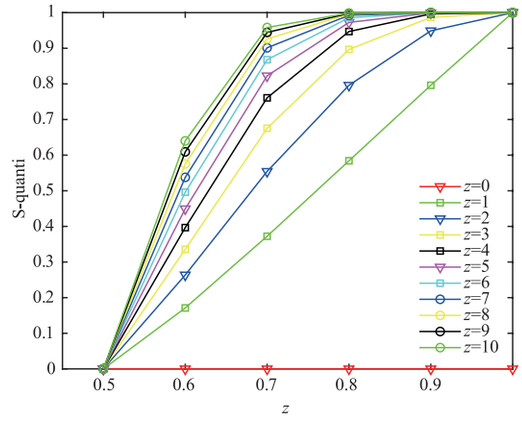

图5　S-quanti值随p值变化趋势

……

s_{1q_1}的路径权重:$t_{1q_1 2}, t_{1q_1 2}, \cdots, t_{1q_1 n_1}$;

s_{21}的路径权重:$t_{211}, t_{212}, \cdots, t_{21n_2}$;

……

s_{pq_p}的路径权重:$t_{pq_p 1}, t_{pq_p 2}, \cdots, t_{pq_p n_p}$.

记 $\boldsymbol{T} = (t_{111}, \cdots, t_{11n_1}; \cdots; t_{pq_p 1}, \cdots, t_{pq_p n_p})$.

(6)用 $\boldsymbol{X}$ 表示输入变量的集合,记 $\boldsymbol{X} = ((x_{11}, x_{12}, \cdots, x_{1q_1}); \cdots; (x_{p1}, x_{p2}, \cdots, x_{pq_p}))$,如果该区块链包含 s_{ij},$i \in [1, p]$,$j \in [1, \max(q_1, q_2, \cdots, q_p)]$,则相同下标的 x_{ij} 取值为 1,否则为 0.

我们将输入与其路径权重的乘积求和得到式(6):

$$\text{S-quali} = \sum_{i=1}^{p} \sum_{j=1}^{q_i} (x_{ij} \times t_{ij1} \times \cdots \times t_{ijn_i}) \tag{6}$$

又因为安全敏感性评分函数:

$$f[s_{ij}] = t_{ij1} \times t_{ij2} \times \cdots \times t_{ijn_i} \tag{7}$$

所以式(6)可以写成式(8)的形式:

$$\text{S-quali} = \sum_{i=1}^{p} \sum_{j=1}^{q_i} (x_{ij} \times f[s_{ij}])$$
$$\text{S-quali} \in [0,1] \tag{8}$$

4.4　安全风险评分函数的计算

如上所述,区块链定量安全风险评分(S-quanti)和定性安全风险评分(S-quali)共同影响了区块链安全风险评分(S),调整前二者的影响因子,使其满足下列限制:

$$\alpha + \beta = 1 \tag{9}$$

$\alpha, \beta \geqslant 0$. 我们将 S 与 S-quanti、S-quali 的函数关系设计为:

$$\text{S} = \alpha \times \text{S-quanti} + \beta \times \text{S-quali}$$
$$\text{S} \in [0,1] \tag{10}$$

4.5　复杂度分析

在本节中,我们分析区块链安全风险评分函数的计算复杂性. 为此,我们将 z 表示为攻击者落后的区块个数,n 表示为安全敏感属性值的 AHP 层次数量,p 表示安全敏感属性的数量,q 表示各个安全敏感属性值的数量.

定理　区块链安全风险评分函数的计算复杂性是 $o(z) + o(n \times p \times q)$.

证明　区块链安全风险评分函数计算的复杂性主要受三个因素的影响:定量安全风险评分 S-quanti;每个属性值的安全敏感性评分 $f[s_{ij}]$;定性安全风险评分 S-quali.

根据计算 S-quanti 函数值的算法,我们用变量存储 $k-1$ 次的计算结果,则每一次循环的计算复杂度为 $O(1)$,S-quanti 函数的计算需要循环 z 次,因此其复杂度为 $O(z)$. 根据定义 4 计算每个属性值的安全敏感性评分 $f[s_{ij}]$. 当属性值的 AHP 层次数量为 n 时,$f[s_{ij}]$ 的计算复杂度为 $O(n)$;p 个属性共 $p \times q$ 个属性值,即 S-quali 的计算复杂度为 $o(n \times p \times q)$. 因此,区块链安全风险评分函数的计算复杂性是 $o(z) + o(n \times p \times q)$.

5　实验

5.1　实验说明

目前全球有 30 多家代表性区块链评级/评测机构:RatingToken、Weiss、赛迪区块链研究院、数链、链塔智库等. RatingToken 是一个基于大数据分析的区块链评级网站,根据各种因素评估区块链项目的安全风险程度,包括白皮书内容,社交媒体热度,技术实力,团队成员,行业顾问,投资者和合同扫描共 81 个指标. TokenInsight 是一家区块链数据研究公司,做一些币圈项目评级,专注于区块链项目的风险与资质评级,帮助投资者规避风险、提高收益. Weiss Ratings 是美国领先的金融机构独立评级机构,主要从匿名程度、内部治理能力、升级能力、可扩展性、市场渗透力、网络安全性、去中心化程度方面判断区块链的技术实力级别. 赛迪公有链技术评估主要考虑公有链的基础技术水平、应用层级和创新能力,其中基础技术水平主要评估公有链的实现功能、基础性能、安全性和去中心化程度.

为了验证本模型的可行性,我们选取了当下 15 个一

线公有链区块链项目作为实验对象,评估内容主要包括技术安全性、去中心化程度、机制可靠性和算力四个维度共12个指标,模型计算结果与其他权威机构的评测数据见表5. 在实验中,我们尝试回答以下研究问题:

(1)区块链安全风险评估模型是否实现了区块链安全风险的量化目标?

(2)区块链安全敏感属性和属性值的权重从何而来?

在下一小节,我们解释了实验的过程,并给出了所使用的问卷样例.

5.2 实验问卷

我们的评估模型根据区块链可信计算基BTCB评估区块链项目的安全风险,因为受限于区块链白皮书、技术开发报告、安全检测报告等信息的开放程度,想要逐一分析区块链的每一个安全敏感属性几乎不可能. 为了让模型计算尽量囊括BTCB各个层面,我们分别在数据层、网络层、共识层、激励层和应用交互层各选了一到三个代表性安全敏感属性作为安全评分要素. 本实验中安全敏感性权重调查问卷共发放35份,实际收回35份. 鉴于我们为受访人提供统一的评估维度、评估规范、评估资料且受访人必须有专业知识背景,因此,我们认为该问卷样本数目基本满足了我们研究的需要. Harel A 等[15]证明了配对比较评分方法是最受专家欢迎和精确度最高的评分方法,因此在问卷填写中,受访人统一运用配对比较的评分方法. 表4展示了安全敏感权重的部分内容.

表4 安全敏感权重问卷样例

属性类别/权重		属性值/权重
数据层0.1216	数据模式0.5	基于交易0.25
		基于账户0.75
	数据结构0.5	Merkle 树0.2378
		Merkle Patricia 树0.6953
		Merkle bucket 树0.0669
网络层0.0309	网络协议0.5	TCP-based P2P 0.25
		HTTP/2-based P2P 0.75
	网络结构0.5	私有链0.0463
		联盟链0.1552
		公有链0.7985
共识层0.4785	共识机制(算法)1.0	
激励层01216	激励机制1.0	(分配、验证机制)
应用交互层0.2475	应用扩展0.25	(智能合约)
	应用领域0.25	(行业分析)
	应用环境0.25	(环境分析)
	市场反馈0.25	(活跃度、市值)

5.3 实验结果

我们根据式(5)计算区块链系统的S-quanti值,根据式(8)计算区块链系统的S-quali值,根据式(10)计算区块链系统的S值,计算结果见表5. 表中空白处代表无评测数据. 统计检验得出如下结论.

表5 实验结果与权威机构评测数据($\alpha=0.1$,$\beta=0.9$,攻击算力$=7\times14$T)

加密货币公有链	S-quanti $Z=6$	S-quali	S(区块链安全风险评分0-1,0最劣)	RatingToken安全风险评分0-5(0最劣)	TokenInsight安全风险评级D-AAA(D最劣)	Weiss(技术/采用)评级E-A(E最劣)	赛迪(基础技术)评分0-?(0最劣)
Bitcoin	1.00	0.65	**0.69**	4.90	AA	A	43.20
Ethereum	0.18	0.60	**0.56**	4.60	AA	A	76.60
Bytom	0.00	0.55	**0.50**	4.10	BB	C-	
Litecoin	0.94	0.55	**0.59**	4.00	BBB	B+	45.80
Monero	0.00	0.59	**0.53**	4.00	BB	B	60.70
Dash	1.00	0.54	**0.59**	4.00	BB	B	55.30
Zcoin	0.00	0.54	**0.49**	4.00	B	D+	
Decred	1.00	0.53	**0.57**	3.90	BB	B	49.90
Sia	1.00	0.49	**0.54**	3.80	CCC	C	59.20
Bytecoin	0.00	0.52	**0.47**	3.70	CCC	D+	60.90
Bitcoin SV	1.00	0.54	**0.59**	3.60		C-	
Komodo	0.00	0.55	**0.49**	3.30	B	B-	69.90
Bitcore	0.00	0.47	**0.43**	3.20			
ETC	0.00	0.51	**0.46**	3.10	BB	B	69.00
ETN	0.00	0.48	**0.43**	3.00	CCC	E	

数据统计日期:2019年6月17日

(1)高安全:大部分评级机构对 Bitcoin 和 Litecoin 评价较高,这与我们的模型评估结果一致.

(2)适中安全:大部分评级机构都认为 Dash、Decred 和 Sia 安全性适中,这与我们的模型评估结果一致.

(3)低安全:大部分评级机构都认为 Komodo、Bytecoin、Bitcore 和 ETN 安全性较低,这与我们的模型评估结果一致.

(4)区别 1:尽管四家机构都认为 Ethereum 安全性极高,但由于其全网算力较低,因此我们的评分是适中.

(5)区别 2:尽管两家机构都认为 Bitcoin SV 安全性较低,但由于其全网算力极高,因此我们的评分是高.

图 6 是实验计算结果与 RatingToken 评分的图形化对比分析. 经观察,我们发现两个不同的评分模型计算的结果在安全级别上大体一致. 我们以 Dash 项目为例,详细介绍我们评估模型的计算原理. Dash 项目的定性安全风险评分 S-quali 为 0.5,在这 15 个区块链项目中属于偏低级别,但他的全网算力较高,为 3190.88T H/s,位居第四. 根据前文介绍的挖矿概率计算公式,Dash 的挖矿概率 p 为 $\frac{3190.88\text{TH/s}}{3190.88\text{TH/s}+7\times14\text{TH/s}}=0.97$(本实验的攻击算力统一设置为 7×14TH/s),进而计算出定量安全风险得分 S-quanti 为 1. 综合评估得出 Dash 项目的安全风险得分 S 为 0.55,属于中等安全级别,这与客观事实相符合.

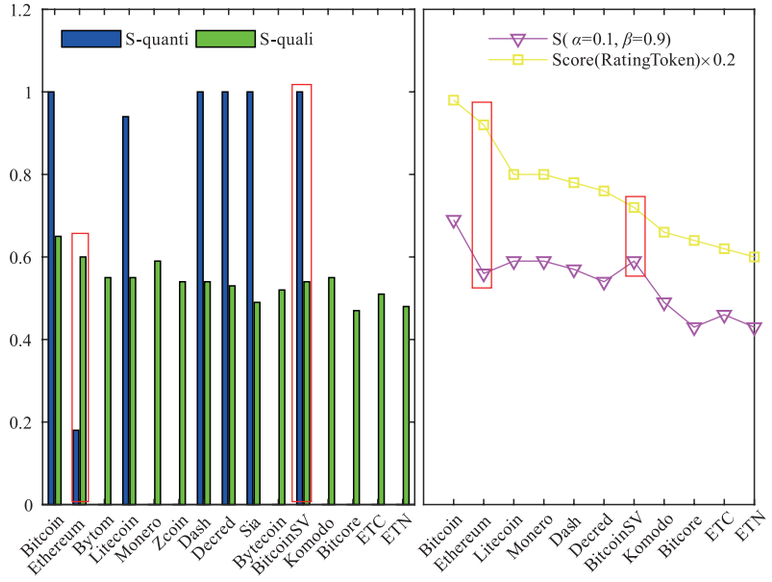

图6　实验结果与RatingToken评分的对比分析

6　总结与讨论

本文从区块链的技术体系和算力入手,提出了一种新的区块链安全风险评估模型,并通过实验验证了它的可行性. 然而,与任何安全风险评估模型一样,本文模型有较高的应用门槛,评估人员必须要专业的知识背景,掌握全面的区块链技术检测信息和权威的安全权重信息,才能得到最真实的评估结果.

参考文献

[1] Grinberg R. Bitcoin:An Innovative Alternative Digital Currency[J]. Hastings Science & Technology Law Journal, 2011,(4):160 – 210.

[2] 侯云春. 防范金融风险要有金融技术加持[J]. 中国商界,2017,(9):24 – 25.
HOU Yun-chun. Financial technology to prevent financial risks [J]. Business China,2017,(9):24 – 25. (in Chinese)

[3] Nayak K,Kumar S,Miller A,et al. Stubborn mining:Generalizing selfish mining and combining with an eclipse attack[A]. Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS \ &P)[C]. USA:IEEE,2016. 305 – 320.

[4] 程丽辰,刘吉强. 区块链技术及其安全问题[J]. 信息通信技术,2017,11(3):39 – 45.
CHENG Li-chen,LIU Ji-qiang. Technology and security of blockchain[J]. Information and Communications Technologies,2017,11(3):39 – 45. (in Chinese)

[5] Heilman E,Kendler A,Zohar A,et al. Eclipse attacks on bitcoin's peer-to-peer network[A]. Proceedings of the 24th USENIX Security Symposium (USENIX Security 15)[C]. USA:USENIX,2015. 129 – 144.

[6] 叶聪聪,李国强,蔡鸿明,等. 区块链的安全检测模型[J]. 软件学报,2018,29(05):1348 – 1359.
YE Cong-cong,LI Guo-qiang,CAI Hong-ming,et al. Security detection model of block chain[J]. Journal of Software,2018,29(05):1348 – 1359. (in Chinese)

[7] 邵奇峰,金澈清,张召,等. 区块链技术:架构及进展[J]. 计算机学报,2018,41(05):969 – 988.
SHAO Qi-feng,JIN Che-qing,ZHANG Zhao,et al. Blockchain technology: Architecture and progress[J]. Chinese Journal of Computers,2018,41(05):969 – 988. (in Chinese)

[8] 李赫,孙继飞,杨泳,等. 基于区块链 2.0 的以太坊初探[J]. 中国金融电脑,2017(6):57 – 60.
LI He,SUN Ji-fei,YANG Yong,et al. Preliminary exploration of Ethereum based on block chain 2.0[J]. Financial Computer of China,2017(6):57 – 60. (in Chinese)

[9] 吴涛,景晓军. 一种强不可伪造无证书签名方案的密码学分析与改进[J]. 电子学报,2018,46(3):602 – 606.
WU Tao,JING Xiao-jun. Cryptanalysis and improvement of a strong non-forgeable certificateless signature scheme[J]. Acta Electronica Sinica,2018,46(3):602 – 606. (in Chinese)

[10] 孙君,熊关. SCMA mMTC 系统中基于联盟区块链的无线电资源交易的信用支付[J]. 电子学报,2019,47(8):1677 – 1684.
SUN Jun,XIONG Guan. Credit payment of radio resource transaction based on alliance blockchain in SCMA mMTC system[J]. Acta Electronica Sinica,2019,47(8):1677 – 1684. (in Chinese)

[11] Saaty T L. A scaling method for priorities in hierarchical structures[J]. Journal of Mathematical Psychology,2000,15(3):234 – 281.

[12] Saaty T L. How to make a decision:The analytic hierarchy process[J]. European Journal of Operational Research,1994,24(6):19 – 43.

[13] WANG D,GUO B,SHEN Y. Method for measuring the privacy level of pre-published dataset[J]. IET Information Security,2018,12(5):425 – 430.

[14] Nakamoto S. Bitcoin:A peer-to-peer electronic cash system. bitcoin. org[J/OL]. https://bitcoin. org/bitcoin. pdf (accessed:21. 05. 2019),2008.

[15] Harel A,Shabtai A,Rokach L,et al. M-Score:A misuseability weight measure[J]. IEEE Transactions on Dependable & Secure Computing,2012,9(3):414 – 428.

作者简介

秦超霞 女,1995 年生,重庆忠县人,2018 年毕业于四川大学获得学士学位,现为四川大学计算机学院博士研究生,主要研究区块链安全与关键技术.
E-mail:scuqcx@163. com

郭 兵 男,1970 年生,四川成都人,2002 年毕业于成都电子科技大学获得博士学位,现为四川大学计算机学院教授,博士生导师,主要从事个人大数据管理和区块链等相关研究.
E-mail:guobing@scu. edu. cn

沈 艳 女,1973 年生,四川成都人,2004 年毕业于成都电子科技大学获得博士学位,现为成都信息工程大学控制工程学院教授,博士生导师,主要从事智能终端及仪器等相关研究.
E-mail:shenyan02@163. com

苏 红 男,1979 年生,四川成都人,2006 年毕业于四川大学获得硕士学位,现为四川大学计算机学院博士研究生,主要研究区块链理论与关键技术.
E-mail:suguest@126. com

张 珍 女,1982 年生,四川成都人,2010 年毕业于西华大学获得硕士学位,现为四川大学计算机学院博士研究生,主要研究区块链理论与关键技术.
E-mail:zhangzhen@stu. scu. edu. cn

周驰岷 男,1975 年生,四川成都人,2006 年毕业于西华大学获得硕士学位,现为四川大学计算机学院博士研究生,主要研究区块链理论及形式化验证.
E-mail:1955946@qq. com