软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(6):1681−1691 [doi: 10.13328/j.cnki.jos.005744]

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

拟态区块链——区块链安全解决方案*

徐蜜雪, 苑 超, 王永娟, 付金华, 李 斌

(数学工程与先进计算国家重点实验室(信息工程大学),河南 郑州 450001)

通讯作者: 苑超, E-mail: yc_xxgcdx@163.com

摘 要: 区块链起源于比特币,其核心是去中心化、去信任、防篡改、防伪造、可溯源,因此在任何高价值数据的管理、存储与流通的过程中都可以用到区块链.区块链已经在多种场景中得到应用,但是区块链的安全问题一直存在,且对用户权益影响极大.拟态防御是由中国的研究团队提出的新型网络防御技术,对新型系统的网络防御具有重要的作用.首先介绍区块链面临的安全威胁以及目前存在的应对方案,然后对拟态防御中核心的动态异构冗余(dynamic heterogeneous redundance,简称 DHR)架构进行介绍;其次,针对区块链存在的潜在安全问题,借鉴动态异构冗余架构和密码抽签的思想,结合安全性定义和参数选择规则,从动态异构共识机制以及动态异构冗余签名算法两个角度提出了区块链的安全解决方案,称为拟态区块链;最后进一步分析了拟态区块链的安全性和性能,结果显示,动态异构冗余区块链可以在多个方面得到比典型区块链更好的安全性.

关键词: 区块链;动态异构冗余;密码抽签;共识机制

中图法分类号: TP309

中文引用格式: 徐蜜雪,苑超,王永娟,付金华,李斌.拟态区块链——区块链安全解决方案.软件学报,2019,30(6):1681−1691. http://www.jos.org.cn/1000-9825/5744.htm

英文引用格式: Xu MX, Yuan C, Wang YJ, Fu JH, Li B. Mimic blockchain—Solution to the security of blockchain. Ruan Jian Xue Bao/Journal of Software, 2019,30(6):1681−1691 (in Chinese). http://www.jos.org.cn/1000-9825/5744.htm

Mimic Blockchain—Solution to the Security of Blockchain

XU Mi-Xue, YUAN Chao, WANG Yong-Juan, FU Jin-Hua, LI Bin

(State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450001, China)

Abstract: Blockchain, originated from Bitcoin, for whose core is decentralized, detrusted, tamper-resistant, unforgeable, and traceable, can be used in management, storage, and circulation of high value data. Blockchain has been applied in a variety of scenarios, but the security problems of blockchain have always existed and have great influence on users' rights and interests. Mimetic defense is a new network defense technology proposed by Chinese research team, which plays an important role in network defense of a new class of system. This paper first introduces the security threats faced by the blockchain and the existing solutions. Then the core ideas of mimetic defense, the typical dynamic heterogeneous redundance (DHR) architecture are introduced. Second, in view of the potential security problems of blockchain, combining the definition of security and parameter selection, dynamic heterogeneous consensus mechanism and DHR signature mechanism are put forward from the ideas of DHR architecture and cryptographic sortition to construct a security solution for blockchain which is called the mimic blockchain in this paper. Finally, the security and property of the mimic blockchain is further

* 基金项目: 国家重点研发计划(2016YFB0800101, 2016YF0800100); 国家自然科学基金(61521003)

Foundation item: National Key Research Program of China (2016YFB0800101, 2016YF0800100); National Natural Science Foundation of China (61521003)

本文由区块链与数字货币技术专题特约编辑斯雪明教授和陈文光教授推荐.

收稿时间: 2018-06-25; 修改时间: 2018-10-12; 采用时间: 2018-12-18; jos 在线出版时间: 2019-03-27

CNKI 网络优先出版: 2019-03-27 16:40:31, http://kns.cnki.net/kcms/detail/11.2560.TP.20190327.1640.009.html

analyzed, the result shows that the dynamic heterogeneous blockchain can provide increased security over the typical blockchain in many aspects.

Key words: blockchain; dynamic heterogeneous redundance; cryptographic sortition; consensus mechanism

区块链起源于 2008 年中本聪发表的比特币白皮书.比特币的成功促进了密码货币的发展,从莱特币开始,成百上千种密码货币出现[1].从 2013 年开始,越来越多的密码货币爱好者和研究人员开始关注支撑密码货币的区块链.随着研究的深入,区块链已经不仅应用在以比特币为代表的加密货币中,在数字存证[2]、公益募捐[3]、物联网[4]、网络安全[5]等方面都获得了很好的发展.以比特币和以太坊(Ethereum)为代表公有链[6]发展势头迅猛,以超级账本(hyperledger)[7]为代表的私有链[8]和联盟链也获得了很好的发展.区块链的核心是去中心化、去信任、防篡改、防伪造、可溯源[9],在任何高价值数据的存储、管理与分享中,区块链都有应用价值.区块链从整体上可分为以可编程货币为特征的区块链 1.0、以可编程金融为特征的区块链 2.0 和以可编程社会为代表的区块链 3.0.目前,正处于区块链 2.0 向区块链 3.0 过渡阶段[10].区块链 3.0 的核心是区块链应用落地,但是目前,区块链应用落地面临着很多的挑战,例如安全性和隐私保护的限制、吞吐率的限制、存储的限制等等.而以 IOTA[11]中采用的有向无环图(directed acyclic graph,简称 DAG)[12]为代表的新一代分布式账本技术正处于快速发展阶段,为加快区块链的应用落地提供了借鉴.在区块链快速发展的过程中,安全问题是始终需要面对的问题.私钥丢失、智能合约代码漏洞[13]、自私挖矿[14]等已经出现的安全问题都或多或少对区块链的存在与发展带来了伤害.目前,对区块链安全问题的解决方案大多集中在传统安全性防御阶段,例如算法改进[15−17]、共识算法改进[18]等,这些方案只能在一定程度上缓解区块链的安全问题,并不能从根本上解决.

拟态防御[19]是一种新的网络安全防御技术,其核心是动态异构冗余,旨在为解决网络空间不同领域相关应用层次上的基于未知漏洞、后门或病毒木马等不确定性威胁.目前的区块链可以理解为简单的同构冗余,每个节点存储相同的数据,每个共识节点在每一个共识轮采用相同的共识算法,每个节点采用同样的固定的签名算法.这种同构的静态的结构为攻击者提供了便利,也是目前区块链面临安全性威胁的根本原因.本文将利用拟态防御技术核心的动态异构冗余架构(dynamic heterogeneous redundancy,简称 DHR)[20],在区块链原有的同构冗余的基础上增加动态、异构的成分,从签名机制和共识机制两个角度构建动态异构区块链,增强区块链的安全性.这种思想被认为是一种区块链的安全解决方案[21],本文对其进行了更为详细合理的阐述.

在动态异构共识机制中,每一个共识节点在每一轮共识中通过密码抽签技术确定需要采用的共识机制,并完成共识.在传播共识区块的同时,需要同时提交共识节点相应的密码抽签凭证.根据密码抽签凭证判断此轮的最终共识节点,同时,其他节点对此共识节点的共识区块和密码抽签凭证进行验证.在动态异构冗余签名机制中,采用 3 种不同体制的签名算法,这 3 种签名算法结构不同,难度不同,基于的困难问题也不同.攻击者即使能够成功伪造一种签名算法,也无法使得更改后的数据生效.同时增加了动态的特性,在动态异构冗余签名机制中,会提前部署更多的签名算法,例如基于格、基于编码的后量子签名算法,一旦有哪种签名算法被破解,可以随时更换.

本文第 1 节重点介绍动态异构冗余模型,同时对密码抽签技术进行简要介绍.第 2 节分别从安全性定义、共识机制、签名机制和节点处理算法的角度对动态异构区块链的核心内容进行介绍,并给出相应的参数选择方法,使其满足定义的安全性.第 3 节对第 2 节提出的动态异构共识机制和动态异构冗余签名机制的安全性进一步分析,并给出部分签名算法效率测试结果.第 4 节对全文进行总结.

1 准备知识

在本文中,H,H_1,H_2 和 H_3 表示 4 种不同的哈希算法,即 $H,H_1,H_2,H_3:\{0,1\}^*\to\{0,1\}^*$.如果 A 和 B 都表示二进制串,则 $A||B$ 表示 A 和 B 的级联.若 f 表示一个已知值,则 $F\leftarrow f$ 表示 F 取 f 的值.

1.1 动态异构冗余架构

动态异构冗余架构是一种基于架构技术的融合式防御方法,其核心思想是引入结构表征的不确定性,使异

构冗余架构的执行体具有动态化、随机化的内在属性,并在空间上严格隔离异构执行体之间的协同途径或同步机制.DHR 理论上要求系统具有视在结构表征的不确定性,包括非周期地从功能等价的异构冗余体池中随机地抽取若干个元素组成当前服务集,或者重构、重组、重建异构冗余体自身,或者借助虚拟化技术改变冗余执行体内在的资源配置方式或视在运行环境,或者对异构冗余体做预防性或修复性的清洗、初始化等操作,使攻击者在时空维度上很难有效地再现成功攻击的场景.

DHR 系统一般由输入代理、异构构件集、动态选择算法、执行体集和表决器组成(如图 1 所示),其中,异构元素池、异构构件集和策略调度组成执行体集的多维动态重构支撑环节.异构元素池由标准化的软硬件模块组成,这些软硬件模块按某种规则或者策略组合出 m 种功能等价、结构不同的构件体,组成异构构件集.异构构件集中的元素,即构件体,我们用 E_i 表示(i=1,2,…,m).异构构件集的构造可以采用软硬件模块的重构、重组、重建、重定义、虚拟化、策略调度等广义动态化技术措施实现.执行体集由动态选择算法从异构构件集中选出 n 个构件体组成,执行体集中的元素称为执行体,用 A_j 表示(j=1,2,…,n).任意时刻,DHR 架构系统的输入代理将输入转发给执行体集中的各执行体,不同执行体的输出结果提交给表决器进行表决,得到系统输出,DHR 典型构造如图 1 所示.

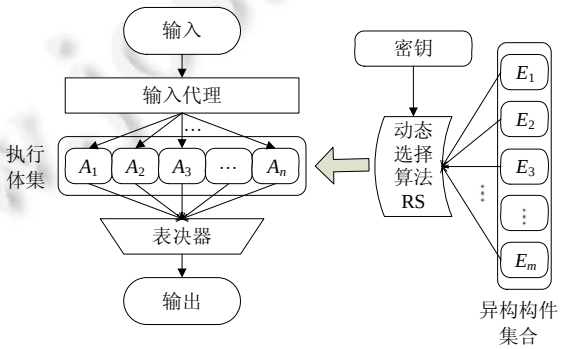

Fig.1 Typical structure of DHR

图 1 DHR 典型构造

这种 DHR 的典型构造可以用 $DHR(m,n)$来描述.

1.2 密码抽签技术

密码抽签是一种在分布式网络中,通过去中心化的方式,利用密码学技术完成可信、可认证的抽签选举的技术.图灵奖得主 Sivio Micali 的 Algorand 区块链协议将密码抽签技术运用到了区块链中.在 Algorand 中,系统需要创建并不断更新一个参数,称为种子,种子不可能被攻击者预测,也不可能被其控制.在每一轮共识过程中,Algorand 根据种子公布一个可验证的随机函数(verifiable random functions,简称 VRF).每个用户利用自己的私钥执行 VRF,得到一个对应的凭证.凭证满足一定条件的用户被认定为此共识轮的验证者,每个验证者完成一个区块,并随自己的凭证一起公布.此轮中,凭证的字典序最小的验证者被认定为领导者.最后,所有的验证者针对领导者的区块运行拜占庭协议.密码抽签在区块链中的应用主要有以下优势.

- VRF 的随机性质决定了验证者和领导者的选举过程很难被预测和操纵;
- 验证者的选举过程是秘密进行的,只有当用户公布自己的凭证时才能证明自己的验证者身份,但是此时区块信息已经公布,即使攻击者可以瞬间腐化验证者,但是公布的区块信息已经不能撤回;
- 领导者的产生是在所有的验证者公布自己的凭证后,通过比较产生的,可以认为是公共选举产生.

2 拟态区块链解决方案

目前,多数区块链可以视为一个静态同构冗余系统,区块链中的各个节点运用同样的算法,保存同样的数

据,这样可以保证单点被攻击时,整个系统还可以正常运行.但是当所有节点共同依赖的部件,比如签名算法、共识算法等被攻击时,整个系统仍然面临安全威胁.本节将从安全性定义、动态异构共识机制、动态异构冗余签名机制、共识节点处理算法等 4 个方面说明拟态区块链应该具有的性质,从而建立拟态区块链系统.

2.1 拟态区块链的安全性定义

在比特币系统中,当区块深度大于 6 时,可以被认为是大概率安全的.在 Algorand 系统中,由于采用基于 VRF 的 PoS,并结合拜占庭容错协议(Byzantine fault-tolerant algorithm,简称 BFT)[22],可以通过设置错误参数保证平均 1.9 兆年出现一次分叉.拟态区块链的共识机制可以包含传统公有链的工作量证明协议(proof of work,简称 PoW)、权益证明协议(proof of stake,简称 PoS),也可以包含小规模节点投票的代表权益证明协议(delegated proof of stake,简称 DPoS)和 BFT,拟态区块链可以使得安全性假设拓展至:存在单一共识机制的分叉攻击,也可以保证区块的不可篡改性.$state(block_r)$表示第 r 个区块产生前的总状态,定义拟态区块链的区块不可篡改如下.

区块不可篡改. 对区块链某一状态 $STATE=state(block_r)$和预先设置的可分叉参数ρ,在本区块后的ρ区块后 $STATE$ 不存在于历史状态中的概率是可忽略的.

传统区块链一旦签名算法出现问题,交易是可以伪造的.以比特币为例,如果使用的签名算法 ECDSA 被攻击成功,那么用户地址对应的比特币将全部丢失.拟态区块链的签名机制通过先执行后表决的 DHR 模型,使得在安全性假设拓展至:单一签名算法产生的签名可伪造的情况下,也可以保证交易的不可伪造.tx 表示用户的某次交易信息,$sign(\cdot)$表示用户的签名,定义动态异构区块链交易的不可伪造如下:

交易不可伪造. 对某一已经在链上的完整交易信息$(tx,sign(H(tx)))$和预先设置的可更改参数$\rho'(\rho'>\rho)$,即使某种签名算法是可伪造的,设 tx 所在区块的序列为 r,则序列大于 $r+\rho'$的区块中存在被伪造的交易的概率是可忽略的.

2.2 动态异构共识机制

目前,区块链大多只存在一种共识算法,当然也有的区块链采用两种或者多种共识算法串行运行的机制,例如 Elastico 采用工作量证明+拜占庭容错协议,2-hop 采用工作量证明+权益证明机制,Algorand 采用权益证明+拜占庭容错协议等等.共识算法是保证区块链安全的重要因素,现存的共识算法,无论是公有链中常用的工作量证明、权益证明,还是联盟链中常用的实用拜占庭容错算法等的安全性都是在某些假设下保证的.例如工作量证明的安全性要求系统中超过 50%的算力是诚实的,但是已有研究成果说明采取某些措施后,可以得到 50%以上的算力,同时在某些条件下甚至只需要 1/3 的算力,同样可以对系统造成严重的危害[23,24].

考虑到现有的单个共识机制或者多个共识机制的串行模式都会受到某些攻击威胁,本文认为,随机性、动态性是共识机制安全性的根本保证.所以借鉴拟态防御的思想,本文给出的异构共识机制中存在 3 种不同的共识算法.同时,动态异构共识机制借用了密码抽签技术,在每一共识轮中,每个共识参与者需要根据上一个区块的哈希值以及目前的区块序号形成的哈希值的签名值做一个密码抽签凭证,这里的密码抽签凭证有两个功能:一是密码抽签凭证最小的用户在某些胜选的共识算法中具有重要地位,比如 PBFT 的 leader;另外一个功能是根据密码抽签凭证确定每个节点在此共识轮中需要采用的共识算法.下面给出动态异构共识机制的具体步骤.

为了更好地描述动态异构共识机制的安全性,对一切与共识不符的行为定义为敌手做出如下假设:

假设 1:至少两种共识参与共识协议的敌手不会超过系统的 1/3.

步骤 1(确定共识节点). 假设此时的共识轮为 r,此轮共识的节点数量为 n_r,$sig_i(\cdot)$表示利用第 i 个共识参与节点用当前私钥进行的签名.

步骤 2(确定共识算法). 第 i 个共识参与节点,计算密码抽签凭证 $Ce_i^r=H(sig_i(H_1(Block_{r-1})\|r))$,根据 Ce_i^r 确定需要执行的共识算法,共识算法确定机制如下所示:

$$Co_i^r=\begin{cases}Co_1,\ Ce_i^r\equiv 0 \bmod 3\\ Co_2,\ Ce_i^r\equiv 1 \bmod 3\\ Co_3,\ Ce_i^r\equiv 2 \bmod 3\end{cases},$$

其中,Co_1,Co_2,Co_3 表示 3 种不同的共识算法,这里选定 PoW、Casper 的 PoS 和 PBFT 分别作为 3 种不同的共识算法.

步骤 3(执行共识). 经过时间 T 后,每个节点收集的凭证个数为 $T_r(T_r>2n_r/3)$,计算 $Ce^r=\min_{i=1}^{T_r} Ce_i^r$,则根据 Ce^r 执行对应的共识.

(1) 以 PoW 胜选为例,若第 i 个共识参与节点公布的 $block_i^r$ 区块满足难度要求,就可以作为第 r 轮最终的区块,即 $Block_r \leftarrow block_i^r$;

(2) 以 Casper 的 PoS 胜选为例,假设参与投票的 PoS 权益为 rig_r,则超过 $2rig_r/3$ 投注率的区块 $block_r$ 即作为第 r 轮最终的区块,即 $Block_r \leftarrow block_r$;

(3) 以 PBFT 胜选为例,com_r 个共识算法为 PBFT 的 Ce_i^r 对应节点组成委员会,而对应 Ce^r 的节点将作为 leader 打包 $block_r$ 并开始 PBFT 协议,只有超过 $2com_r/3$ 个节点的确认消息被收到,才会得到第 r 轮最终的区块,即 $Block_r \leftarrow block_r$.

步骤 4(生成区块). 所有共识节点对 $\{Ce_i^r, sig_i(H_1(Block_{r-1})\|r)\}_{i=1}^{T_r}$ 和 $Block_r$ 进行验证,按照共识算法,用 $Block_r$ 中的公钥验证相应 $\{sig_i(H_1(Block_{r-1})\|r)\}_{i=1}^{T_r}$ 的子集,且对区块中的数据进行验证,如果验证通过,加入自己的区块链中,并进行第 r+1 轮共识,重复步骤 1~步骤 3.

图 2 给出了动态共识过程.

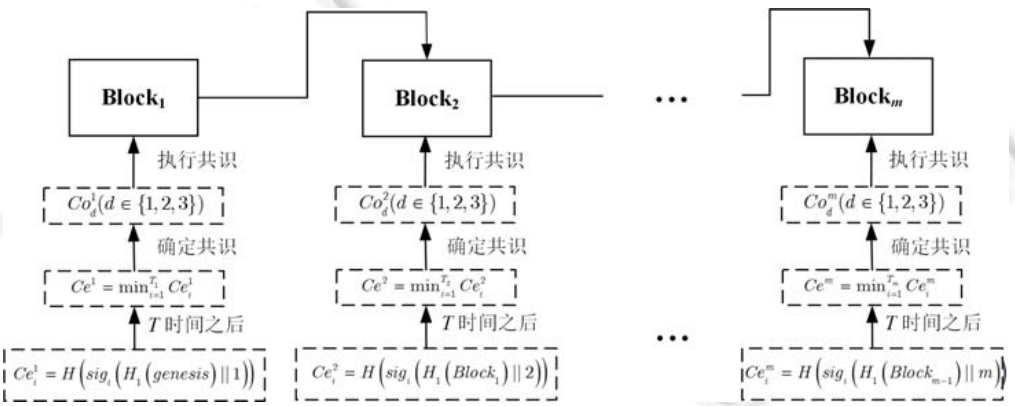

Fig.2 Dynamic heterogeneous consensus mechanism

图 2 动态异构共识机制

根据 Decker 等人的测试结果[25],比特币中 1KB 消息的传播至 95%的节点只需要 1s,1MB 消息传播到 95%的节点不超过 1m.而比特币在线用户数量超过 150 万,根据 gossip 协议规模和传播效率的关系,动态异构共识节点在千级时,1MB 消息传播到 95%节点不超过 6s.

为了给出区块可分叉参数ρ的值,首先考虑共识协议都至多 1/3 敌手可以参与节点共识,若区块共识权益总量为 d,设事件 X 是该区块共识中敌手的数量,对事件离散化处理后,根据二项分布 $B(d,1/3)$可知:

$$\Pr\{X \geqslant l\} = C_d^l \left(\frac{1}{3}\right)^l \left(\frac{2}{3}\right)^{d-l}.$$

如果区块共识是 PoW,则敌手生成区块的平均成功概率满足:

$$S_1 > \sum_{l=1}^{d} \frac{l}{d} C_d^l \left(\frac{1}{3}\right)^l \left(\frac{2}{3}\right)^{d-l}.$$

如果区块共识是 PoS 或 PBFT,将 d 看做整数处理,d 的值越大,表示离散化程度越高,则敌手生成区块的平均成功概率满足:

$$S_2 > \sum_{l=2/3d}^{d} C_d^l \left(\frac{1}{3}\right)^l \left(\frac{2}{3}\right)^{d-l} = \sum_{l=0}^{d/3} C_d^l \left(\frac{1}{3}\right)^{d-l} \left(\frac{2}{3}\right)^l.$$

然后考虑如果存在某个共识算法是可以完全被控制的,即其敌手成功生成区块的概率为 1,设置一个足够小的安全参数ε并认为其可以忽略,如果认为共识算法的出现是均匀的,则可分叉参数ρ满足如下条件:

$$\begin{cases} S_2^{\frac{2\rho}{3}} < \varepsilon \\ S_1^{\frac{\rho}{3}} S_2^{\frac{\rho}{3}} < \varepsilon \end{cases}.$$

所以,

$$\begin{cases} \rho > \dfrac{\log \varepsilon}{2\log S_2/3} \\ \rho > \dfrac{\log \varepsilon}{\log S_1/3 + \log S_2/3} \end{cases}.$$

设置可分叉参数ρ是满足条件的最小整数,则得到如下计算结果(见表 1).

Table 1 Example of parameters selection

表 1 参数选取示例

共识权益度量	二项分布	S_1	S_2	ε	ρ
180	B(60,1/3)	0.168 2	0.582 0	10^{-4}	26
				10^{-8}	52
				10^{-12}	76
300	B(100,1/3)	0.161 8	0.547 0	10^{-4}	23
				10^{-8}	46
				10^{-12}	69
1 000	B(333,1/3)	0.180 3	0.576 9	10^{-4}	26
				10^{-8}	51
				10^{-12}	76

由表 1 可知,PoS 和 PBFT 敌手攻击成功概率与共识权益总量分割细度几乎无关.共识节点数量足够的大时,可分叉参数ρ的取值只与安全参数ε相关.当ρ设置为 52 时,分叉出现的概率即可以忽略不计,所以只需要 52 块后,即可确认区块不可篡改.

2.3 动态异构冗余签名机制

签名算法的安全性是区块链发展过程中面临的重要问题.防篡改、防伪造是区块链最重要的特征,但是这些特征的前提是区块链中签名算法、私钥生成算法等是安全的.但是现在认为安全的椭圆曲线算法、RSA 算法、哈希算法等随着密码分析技术、计算技术、量子计算机等的发展,可能会变得不够安全.IBM 和 Google 等公司不断宣布关于量子计算机研究的最新进展,2017 年,IBM 宣布 50 比特的量子计算机原型机也已研制成功,在 2018 年的美国物理学会上,Google 实验室的公布了最新一代量子处理器 Bristlecone,这是一款 72 位量子位处理器,错误率只有 1%.最为重要的是,Google 实验室谨慎且乐观地认为:如果一切运行良好的话,量子霸权将在未来几个月到来.因此,考虑到未来区块链的安全性,采用抗量子的签名算法是十分必要的.但是抗量子的签名算法比基于公钥的签名算法复杂度高很多,目前在椭圆曲线算法相对安全的时期换用抗量子的签名算法会带来较高的代价.但是一旦量子计算机的性能达到攻击椭圆曲线算法的能力,将瞬间对区块链系统带来致命的打击,因此我们要事先对抗量子签名算法进行部署准备.

除了量子计算机的威胁外,计算技术、密码分析技术的发展也对目前的签名算法带来威胁,并且一旦某种签名算法被攻破,则与其采用相同体制,或者基于相同计算难题的签名算法都将受到威胁.受到拟态防御思想的启发,对异构冗余系统攻击的难度大于对同构冗余系统的攻击难度,同时,对同构冗余系统的攻击难度又大于对单一系统的攻击难度.本文认为:目前的区块链系统在系统级是单一系统,虽然从用户级来看是同构冗余的,为了达到更高的安全等级,本文考虑将单一系统调整为异构冗余系统.这里考虑的异构冗余部分主要集中在签名

算法方面,当然考虑的不是对单一算法的改进,例如环签名、聚合签名、门限签名、多重签名等,一旦某一种密码体制受到攻击,在此密码体制之上的签名变种都会受到致命的打击.本文主要考虑的是采用不同密码体制的异构冗余.

本文给出了异构签名算法,其思想简单,主要是采用 3 种签名算法代替之前的单一的签名算法.如果考虑对于每一个消息,消息发出者分别利用自己的 3 个私钥形成 3 个签名,消息的大小为现有系统的 3 倍,这会影响每个区块容纳消息的数量,进一步影响区块链系统的吞吐率.因此,本节决定采用先执行后表决的 DHR 模型,进行交易的输入脚本中只有一个签名和该签名对应的公钥哈希,输出脚本中包含 3 个签名对应的公钥哈希,使得每个消息的大小与现有消息的大小基本相同.在动态异构区块链中的每个节点都拥有 6 种签名算法的公私钥对,其中 3 个公私钥对{(Pk_1,Sk_1),(Pk_2,Sk_2),(Pk_3,Sk_3)}在现行区块链系统中使用,另外 3 个公私钥对{(Pk_4,Sk_4),(Pk_5,Sk_5),(Pk_6,Sk_6)}作为备用.

为了更好地叙述先决策后表决的 DHR 模型,需要对交易做出假设.

假设 2:公钥是一次性公钥;交易类型是 1 对 1 交易,且交易后发送方对应地址无余额.

假设是合理的:首先,前向安全的签名体制公钥或者 Monero 中的一次性公钥都可以满足公钥的一次性;另外,其他交易模型可以根据 1 对 1 交易推出.

这里的交易结果采用比特币中的 UTXO 模式表示(可与余额模式互相转换),对每一个消息,需要交易发送者 S 用一个私钥 Sk_1^S 进行签名,同时发送消息中携带交易接收者 R 的 3 个公钥信息 $\{H_1(Pk_1^R),H_2(Pk_2^R),H_3(Pk_3^R)\}$;交易额外的信息 Q^s,包括上笔交易的哈希和输出序数等;交易对应的 *token* 值 tx_s_value.对一笔消息进行验证时,仅需要该签名算法通过验证.而交易接收者 R 想要作为发送方时需要提供另外一种签名,比如基于 Sk_3^R 的签名 $sign(Sk_3^R,tx)$.图 3 给出了异构签名算法的实施过程.其中,虚线表示的部分不会被记录在区块上,而在签名和验证过程中是需要计算的.当矿工将第 2 笔交易纳入区块时,当系统参与方更新到该交易所在区块时,矿工和系统参与方都将作为验证者 *Verifier* 检查签名.

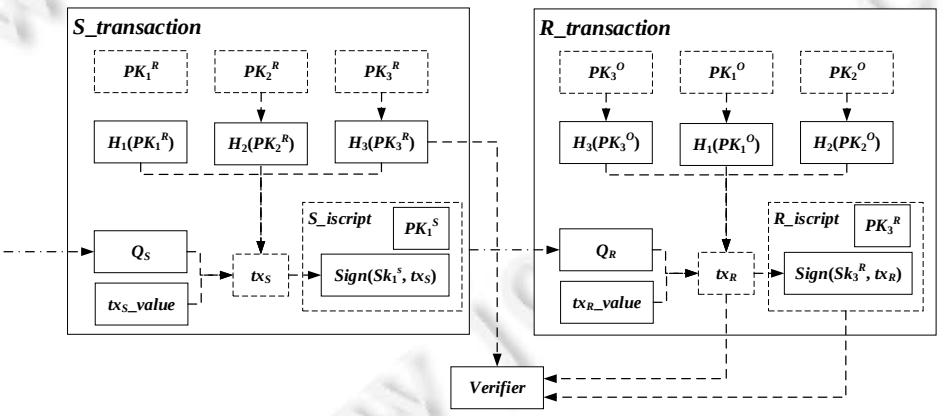

Fig.3 Dynamic heterogeneous redundance signature mechanism

图 3 动态异构冗余签名机制

我们假设可以容忍某种签名算法可伪造,一旦某种签名算法伪造,例如(Pk_3,Sk_3)对应的签名算法受到攻击,由于在交易未花费时用户只有公钥哈希在链上,而且假设没有余额的交易模式,所以攻击者只能通过分叉并双花对用户进行攻击.假设图 3 的 *R_transaction* 所在区块的序列为 t,区块中的 $sign_{Sk_3^R}(tx')$ 是由攻击者产生的,且其所在的区块序列为 $r(r\geqslant t)$,则系统允许用户在 $r+\rho'$ 区块内,用对应的备用签名算法 $sign_{Sk_1^R}(tx'),sign_{Sk_2^R}(tx')$ 取消交易,若 $state(tx)$表示某次交易前的所有账户状态,则默认将状态回退至 $state(tx')$.图 4 给出了取消交易的决策机制.

由于 $r\geqslant t,\rho'\geqslant\rho$,可知 $r+\rho'\geqslant r+\rho$,即在确认攻击者已经完成攻击后可以进行决策,这是一种变形的 *DHR*(6,3)构造.不妨设置ρ'为 60,则要求用户在提交交易后 110 个块内最好保持可提示状态,以便于监督是否有敌手通过双花和分叉对其进行攻击.动态异构冗余签名机制还带来了一个天然的优点,即在交易发布的 60 个块内可以撤销交易,这种撤销不是通过更改原有数据,而是通过共识添加一个操作,使得撤销是可以追溯的.

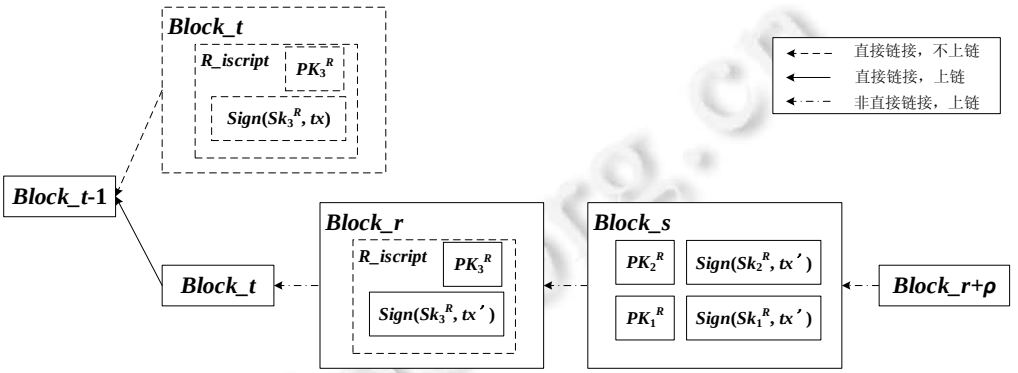

Fig.4 Decision-making mechanism

图 4 决策机制

2.4 共识节点处理算法

根据动态异构共识机制要求,共识算法产生速度要基本一致,可以通过调整难度参数 *diff* 来改变共识的时间,使其保持在稳定状态;*txs* 是在该阶段节点收集到的交易集合.下面结合第 2.2 节和第 2.3 节中对于动态异构共识机制和动态异构冗余签名机制的描述,形成动态异构区块链共识节点处理算法(见表 2).

Table 2 Node processing algorithm

表 2 节点处理算法

节点处理算法

输入:$Block_{r-1}$,*diff*,*txs*;
输出:$Block_r$.
算法:
$Ce_i^r = H(sig_i(H_1(Block_{r-1})\|r))$;
$Block_r$={};
for *tx* in *txs*:
if *tx* is valid://即符合异构签名机制描述
$Block_r=Block_r\|tx$;
else continue;
endif;
endfor;
switch($Co_i = Ce_i^r$ mod3)
Case 0: $Block_r$←*PoW*($Block_{r-1}$,*diff*);
return $Block_r$;
Case 1: $Block_r$←*PoS*($Block_{r-1}$,*diff*);
return $Block_r$;
Case 2: $Block_r$←*PBFT*($Block_{r-1}$,*diff*);
return $Block_r$;
endswitch;

3 拟态区块链安全性和性能分析

3.1 拟态区块链安全性分析

- 1/*n* 攻击

1/*n* 攻击是指如果攻击者能够获得超过 1/*n* 的共识权力,就会导致网络振荡、系统崩溃.攻击者可以通过 DoS

攻击来阻止诚信的节点进行正常共识,从而降低自身所需要的共识权重.在拟态区块链中存在 3 种不同的共识算法,在动态异构区块链中,共识节点的形成是通过密码抽签完成的,且每个共识节点在每个共识轮中要完成的共识任务是不确定的,因此与之前的 1/*n* 攻击相比,在拟态区块链中只拥有单一共识权力的 1/*n* 是无法完成攻击任务的,因此,拟态区块链可以有效地抵御 1/*n* 攻击.

- 类自私挖矿攻击

自私挖矿攻击是指共识节点完成共识任务后,并不在第一时间内公布自己的共识区块,而在此基础上继续进行下一轮的共识任务,然后在适当的时候,同时公布自己的多个共识区块,达到自己获利以及使其他用户工作无效的目的.目前,在原始的自私挖矿攻击的基础上发展出了多种更加有效的攻击方法.在拟态区块链中,由于每个共识轮中共识节点的产生是通过密码抽签的形式产生,需要大部分共识节点的密码抽签凭证的比较.因此,共识过程具有更强的随机性与不可预测性,而且遇到PoS类和PBFT类的共识,自私挖矿产生的区块不能被超过2/3 共识节点认可,所以可以有效抵御类自私挖矿攻击.

- 日蚀攻击

日蚀攻击通常与 51%攻击相结合,攻击者首先发送代币给接收方,等待交易上链后,通过非正常途径产生大量节点与想要隐瞒的接收方节点链接,然后通过强大的共识权力造成区块分叉,新的区块包含将原本代币发送给其他接收方的交易以多次获利.拟态区块链的下一轮共识与密码抽签结果一起公布,只拥有某种强大共识权力的攻击者不一定会成为下一轮共识节点,而且分叉需要公布大量连续区块,在难度调节机制中,某类共识块的连续出现将会提升该类共识块的出块难度.因此,拟态区块链可以使得日蚀攻击更加困难.

- 量子计算机威胁

传统区块链用的传统非对称签名体系对于量子计算中的 shor 算法是不安全的,随着量子计算机的可计算能力提高,如果不提供一种可以抵抗量子计算的实用策略,区块链上的高价值数据会有很大的安全隐患.但是现有较为安全的后量子非对称签名体制公钥长度过长、签名速度过慢,对于区块链的性能和存储都有不利影响.动态异构冗余签名机制通过将后量子签名算法公钥哈希 $H_2(Pk_2)$存放在区块上,直到出现问题和需要修改的个例才使用后量子签名算法,同时实现不安全的签名算法的快速替换,将可能存在问题的区块迅速固化.这样做的好处是:在没发生问题时,不会使区块的性能和存储下降过多.

3.2 动态异构冗余签名机制性能分析

初始使用的 3 个签名机制是 SM2 算法、基于编码的 CFS 签名算法[26]和传统 RSA 算法.其中,本节对 SM2 算法嵌入了 openssl 进行了测试,并与比特币中使用的 ECDSA 算法做了比较,测试环境见表 3.

Table 3 Test environment

表 3 测试环境

CPU	Intel(R) Core(TM) i7-4510U@2.00GHz 2.60GHz
内存	8GB
操作系统	Windows 7
开发环境	VS 2015

得到如下测试结果,见表 4.

Table 4 Test result

表 4 测试结果

	ECDSA 算法	SM2 算法
预处理	对签名消息不作处理	
预处理速度	0	4ms
计算	计算随机数和签名第 1 项	计算随机数,计算椭圆曲线点的横坐标,计算签名第 2 项的第 1 个乘数
签名速度	2 889ms	2 935ms
验证速度	1 790ms	2 013ms

根据各算法的验证速度可知,拟态区块链快速处理能力受限于 SM2 算法的验证时间和共识算法时间.

4 总 结

区块链的安全问题是影响区块链发展的重要问题.从网络密码分析的角度看,在算法、协议、实现、使用与系统的各个方面,区块链都存在安全问题.而区块链逐渐被应用在金融、网络安全等其他核心环境中,在这些环境中,安全性要求都特别高,因此要使得区块链能够真正得到实际应用,解决其安全性是首要条件.本文从拟态防御的角度出发,分别设计了动态异构共识机制和动态异构冗余签名机制,从而搭建了拟态区块链架构.对拟态区块链的安全性进行了定义和分析,提出了参数选取方案,并且对签名机制进行了效率测试.目前,我们的拟态区块链架构的动态异构共识机制还属于动态异构阶段,未来将进一步考虑动态异构冗余架构,增强区块链的安全性.另外,动态异构冗余签名机制还需要解决后量子密码算法公钥量大、算法速度慢的问题,未来会考虑有效的部署方案.

References:

[1] Gandal N, Halaburda H. Competition in the cryptocurrency market. Social Science Electronic, 2014,10:14−17. [doi: 10.2139/ssrn.2506463]

[2] Korpela K, Hallikas J, Dahlberg T. Digital supply chain transformation toward blockchain integration. In: Proc. of the 50th Hawaii Int'l Conf. on System Sciences. Honolulu: University of Hawaii, 2017. 4182−4191. [doi: 10.24251/HICSS.2017.506]

[3] Chen PW, Jiang BS, Wang CH. Blockchain-based payment collection supervision system using pervasive bitcoin digital wallet. In: Proc. of the Int'l Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob). Rome: IEEE, 2017. 25−28. [doi: 10.1109/WiMOB.2017.8115844]

[4] Dorri A, Kanhere SS, Jurdak R. Towards an optimized blockchain for IoT. In: Proc. of the IEEE/ACM 2nd Int'l Conf. on Internet-of-Things Design and Implementation. Pittsburgh: IEEE, 2017. 173−178. [doi: 10.1145/3054977.3055003]

[5] Bozic N, Pujolle G, Secci S. A tutorial on blockchain and applications to secure network control-planes. In: Proc. of the 2016 3rd Smart Cloud Networks & Systems. Dubai: IEEE, 2017. 1−8. [doi: 10.1109/SCNS.2016.7870552]

[6] Sato M, Matsuo S. Long-term public blockchain: resilience against compromise of underlying cryptography. In: Proc. of the IEEE European Symp. on Security and Privacy Workshops. IEEE, 2017. 1−8.

[7] Sukhwani H, Martínez JM, Chang X, *et al*. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). In: Proc. of the 2017 IEEE 36th Symp. on Reliable Distributed Systems (SRDS). Hong Kong: IEEE, 2017. 253−255. [doi: 10.1109/SRDS.2017.36]

[8] Dinh TTA, Wang J, Chen G, *et al*. BLOCKBENCH: A framework for analyzing private blockchains. In: Proc. of the 2017 ACM Int'l Conf. on Management of Data. Chicago: ACM Press, 2017. 1085−1100. [doi: 10.1145/3035918.3064033]

[9] Melanie. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.

[10] Ulieru M. Blockchain 2.0 and Beyond: Adhocracies. Springer Int'l Publishing, 2016. 297−305. [doi: 10.1007/978-3-319-42448-4_15]

[11] Red VA. Practical comparison of distributed ledger technologies for IoT. In: Proc. of the Society of Photo-Optical Instrumentation Engineers (SPIE) Conf. Series, 2017. [doi: 10.1117/12.2262793]

[12] Bender MA, Farach-Colton M, Pemmasani G, *et al*. Lowest common ancestors in trees and directed acyclic graphs. Journal of Algorithms, 2005,57(2):75−94. [doi: 10.1016/j.jalgor.2005.08.001]

[13] Delmolino K, Arnett M, Kosba A, *et al*. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer-Verlag, 2015. [doi: 10.1007/978-3-662-53357-4_6]

[14] Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in bitcoin. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer-Verlag, 2016. 515−532. [doi: 10.1007/978-3-662-54970-4_30]

[15] Aitzhan NZ, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. on Dependable & Secure Computing, 2016,15:840−852. [doi: 10.1109/TDSC.2016.2616861]

[16] Yuan C, Xu MX, Si XM. Research on a new signature scheme on blockchain. In: Proc. of the Security and Communication Networks. 2017. 1−10. [doi: 10.1155/2017/4746586]

[17] Yuan C, Xu M, Si X, *et al*. A new aggregate signature scheme in cryptographic currency. Int'l Journal of Performability Engineering, 2017,13(5):754−762. [doi: 10.23940/ijpe.17.05.p18.754762]

[18] Gilad Y, Hemo R, Micali S, *et al*. Algorand: Scaling Byzantine agreements for cryptocurrencies. In: Proc. of the 26th Symp. on Operating Systems Principles. Shanghai: ACM Press, 2017. 51−68. [doi: 10.1145/3132747.3132757]

[19] Si XM, Wang W, Zeng JJ, Yang BC, Li GS, Yuan C, Zhang F. A review of the basic theory of mimic defense. Strategic Study of CAE, 2016,18(6):62−68 (in Chinese with English abstract). [doi: 10.15302/J-SSCAE-2016.06.013]

[20] Wu JX. Research on cyber mimic defense. Journal of Cyber Security, 2016,1(4):1−10. (in Chinese with English abstract)

[21] Yuan C. Research on key technology of privacy protection in blockchain [MS. Thesis]. Zhengzhou: Information Engineering University, 2018. (in Chinese with English abstract)

[22] Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proc. of the 3rd Symp. on Operating Systems Design and Implementation. New Orleans: ACM Press, 1999. 173−186. [doi: 10.1145/571637.571640]

[23] Nayak K, Kumar S, Miller A, *et al*. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In: Proc. of the IEEE European Symp. on Security and Privacy. Saarbrucken: IEEE, 2016. 305−320. [doi: 10.1109/EuroSP.2016.32]

[24] Zhang R, Preneel B. Publish or perish: A backward-compatible defense against selfish mining in bitcoin. In: Proc. of the Topics in Cryptology (CT-RSA 2017). San Francisco: Springer-Verlag, 2017. 277−292. [doi: 10.1007/978-3-319-52153-4_16]

[25] Decker C, Wattenhofer R. Information propagation in the Bitcoin network. In: Proc. of the IEEE P2P 2013. Trento: IEEE, 2013. [doi: 10.1109/P2P.2013.6688704]

[26] Courtois NT, Finiasz M, Sendrier N. How to achieve a McEliece-based digital signature scheme. In: Proc. of the ASIACRYPT 2001, Vol.2248. 2001. 157−174. [doi: 10.1007/3-540-45682-1_10]

附中文参考文献:

[19] 斯雪明,王伟,曾俊杰,等.拟态防御基础理论研究综述.中国工程科学,2016,18(6):62−68. [doi: 10.15302/J-SSCAE-2016.06.013]

[20] 邬江兴.网络空间拟态防御研究.信息安全学报,2016,1(4):1−10.

[21] 苑超.区块链隐私保护关键技术研究[硕士学位论文].郑州:信息工程大学,2018.

徐蜜雪(1993－),女,山东莱州人,硕士生,主要研究领域为区块链隐私与安全,对称密码攻击.

付金华(1980－),男,博士生,CCF 学生会员,主要研究领域为区块链,大数据.

苑超(1992－),男,硕士生,主要研究领域为区块链隐私与安全.

李斌(1955－),男,博士,教授,博士生导师,主要研究领域为计算机辅助几何设计,计算机图形学,科学计算可视化,医学图像处理.

王永娟(1982－),女,博士,副教授,CCF 专业会员,主要研究领域为密码算法设计与分析.