计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20180426
55(10):2219-2232,2018

基于区块链的可监管数字货币模型

张健毅[1] 王志强[1,2] 徐治理[1] 欧阳雅菲[3] 杨 涛[4]
[1](北京电子科技学院计算机科学与技术学院 北京 100070)
[2](中国民航大学中国民航信息技术科研基地 天津 300300)
[3](北京孚链科技有限公司 北京 100190)
[4](信息网络安全公安部重点实验室 上海 200031)
(zjy@besti.edu.cn)

A Regulatable Digital Currency Model Based on Blockchain

Zhang Jianyi[1], Wang Zhiqiang[1,2], Xu Zhili[1], Ouyang Yafei[3], and Yang Tao[4]
[1](*College of Computer Science and Technology, Beijing Electronic Science and Technology Institute, Beijing* 100070)
[2](*Information Technology Research Base of Civil Aviation Administration of China, Civil Aviation University of China, Tianjin* 300300)
[3](*Beijing Fu-Link Technology Co., Ltd, Beijing* 100190)
[4](*Key Laboratory of Information Network Security, Ministry of Public Security, Shanghai* 200031)

Abstract The digital currency, represented by Bitcoin, was designed to be a decentralized system. And this property makes the regulation more difficult. However, the research of designing a regulatable digital currency is very limited. In this paper, we introduce a new digital currency model based on two chains scheme, public blockchain and consortium blockchain. As the core participant, the consortium blockchain collects and confirms every transaction, determines the status of the system, and stores the complete transaction records. The users' private information is guaranteed by the secret sharing in the consortium blockchain and also can be decrypted by the voting committee. Based on the characteristics and requirements of the consortium blockchain, we also introduce an agreement protocol based on the Credit Practical Byzantine Fault Tolerance and use the simplified agreement protocol to offer high throughput for our model and flexibility of the system. With the view-change and checkpoint protocol, we can dynamically adjust the nodes' status and authority. Extensive analysis and experimental results indicate that our proposed method is both efficient and secure. We believe that this is the first work that has the capacity of the tamper-resistant, traceability, decentralize and regulation.

Key words block chain; consortium chain; regulation; digital currency; agreement

摘 要 以比特币为代表的数字货币具有去中心化特性,造成了监管上的困难.然而,针对去中心化的数字货币可监管研究工作相对较少,还有很多问题有待解决.提出了一种可监管的数字货币模型.该模型

收稿日期:2018-06-11;**修回日期**:2018-08-02
基金项目:信息网络安全公安部重点实验室开放课题项目(C18612,C17608);中央高校基本科研业务费专项资金(328201804);中国民航信息技术科研基地开放课题基金(CAAC-ITRB-201705)
This work was supported by Open Project of the Key Laboratory of Information Network Security, Ministry of Public Security (C18612, C17608), the Fundamental Research Funds for the Central Universities (328201804), and the Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China (CAAC-ITRB-201705).
通信作者:王志强(wangzq@besti.edu.cn)

采用了双链结构设计,联盟链作为共识的核心参与者,收集和确认交易,决定系统的状态,加密存储完整的交易信息.联盟链参与者通过秘密共享保证用户交易数据的隐私性,也可以通过投票完成对交易内容的解密,以此来实现可控匿名.针对该模型,同时提出了一种基于信用的拜占庭容错机制.该机制配合简化的一致性协议以及检查点协议,让节点能够动态优化调整,促进整个模型进入良性循环.实验结果表明:该方法在保护用户隐私的前提下具有交易防篡改、可追溯、去中心化以及可监管的能力.容错性能、运行效率以及通信开销均达到设计要求.

关键词 区块链;联盟链;可监管;数字货币;共识机制

中图法分类号 TP393

作为比特币[1]的支撑技术,区块链技术为去中心化的系统提供了参与者之间的信任基础.由于区块链可以在分布式系统中的陌生节点之间建立信用,因此在比特币等新兴数字货币的系统中不再有中心化的信用实体,导致了金融监察机构和国家机关难以对数字货币系统中的参与者和他们之间的交易进行监督和管理.数字货币有可能逐渐沦为洗钱、逃税和不法交易的工具.监管的缺失也造成了用户利益的损失,有大量的资金和数字货币系统相关联或直接在系统中流动,它们也成为了黑客集中攻击的目标.以太坊[2](Etherum)众筹智能合约项目"The DAO"因为系统漏洞,导致被盗取了当时价值超过6 000万美元的以太币,以太坊最终选择了技术团队直接改变系统状态,对区块链硬分叉并取消了"The DAO"合约,但攻击者身份最终没有暴露.因此,设计出能协调保护用户隐私和可监管两者关系的系统对于区块链的长远发展具有重要意义.

本文针对数字加密货币存在的难以监管问题,提出了一种基于区块链双链结构的可监管数字货币模型.以联盟链为核心,内部成员负责交易的确认和完整交易数据的加密保存,保存的数据可以在交易追溯中作为凭据;监管机构作为联盟链的参与者加入到系统运行和维护中.以公有链为运行基础,普通用户作为公有链参与者,均能够参与和见证系统的维护.

系统借鉴了混币过程,将完整交易进行截断和混淆后存储在公有链中,作为公开可信的证据在验证交易和获取账户状态时使用.共识机制方面,根据联盟链运行场景,设计了更适合的基于信用的拜占庭容错技术.通过引入的信用评级的机制,对联盟链中节点在共识过程中的表现进行记录,以此为依据合理调节共识过程中节点的权限,优化交互过程,在长期运行中能提高系统的运行效率.经过一系列实验表明,本文设计与实现的可监管数字货币模型,简单、有效,在保证运行效率、用户交易隐私的同时,为监管提供了很好的交易追溯以及身份确定能力.

本文的主要贡献如下:

1) 提出了一种基于区块链的联盟链-公有链双链结构.保持去中心化特性的同时,通过联盟链对公有链交易溯源以及用户身份确定,实现对电子货币的监管.

2) 针对该模型,设计了一种基于信用的拜占庭容错共识机制,从而动态调整各节点的权限,优化交互过程.

3) 针对数字货币隐私保护要求,提出了一整套交易协议,通过截断、混淆、锚定等方法保护了用户交易隐私同时满足了溯源、身份确定等监管需求.

1 相关工作

早期的数字货币是由银行和政府合作构建的中心化支付、结算网络.利用密码技术为期提供安全性以及交易的隐私性.Chaum等人在1988年提出了离线交易方案[3].1995年,Brands使用基于离散对数问题的限制性盲签名设计出了更高效的单一离线电子现金方案[4],提升了系统效率.20世纪90年代,中心化信用带来的成本和效率问题促使了多种分布式的电子现金系统的出现,Back提出的"HashCash"[5]和Szabo提出的"Bit Gold"引入了可证明工作量的验证方案[6],随后逐渐发展成了比特币中的工作量证明机制.

对于区块链技术各国积极发展相关产业.从2016年开始,我国开始关注区块链技术,特别在2016年年底公布的《"十三五"国家信息化规划》的内容中专门指出要更快地推进区块链及其相关技术的创新、实现和推广,对于新时代的主导性的关键技术需要领先于对手将其掌握,取得竞争中的优势地位.央行参与并主导的基于区块链的数字票据交易平台在2017年2月的测试中取得很好的效果.

而另一方面,对于以比特币为代表的去中心化匿名数字货币,多个国家都制定了较为严厉的禁令,防止相关的违法活动的发生.为了保证安全性,数字货币采用了多种密码算法加强匿名[7-8],使得监管更加难以进行.许多研究学者也尝试实现可监管的数字货币,Sun 等人在文献[9]中提出了一种多链模型.然而链与节点间的通信较为复杂,Superchain 的设立也让该模型为了可监管而损失了去中心化特性并牺牲了交易的隐私性.

本文提出的可监管数字货币模型采用了双链结构,联盟链作为共识的核心参与者,收集和确认交易,决定系统的状态,加密存储完整的交易信息.将联盟链锚定在一个公有链上,扩大系统参与和见证群体,保证联盟链中数据的可信性,将被混淆过的交易信息存储在公有链中,作为验证交易的凭据.用户加入系统需要身份注册,联盟链参与者通过秘密共享保证用户交易数据的隐私性,也可以通过投票完成对交易内容的解密,以此来实现可控匿名.保持了数字货币去中心化、匿名性的同时,提供了可监管特性.

2 可监管问题与模型分析

2.1 现有数字货币系统问题

数字货币系统的信息化属性在性能上可以加快交易确认速度、提高系统的并行能力,在安全上通过密码学方法验证身份、加密保护用户隐私.虽然数字货币如今有了很多优异的性能,但在可监管上还没有提出很好的解决方案.

联盟链只允许联盟成员参与共识过程,普通用户被排斥在外,如果使用联盟链为基础建立数字货币系统,对于用户而言和现有的"客户端——服务器"模式没有任何差别,只是建立了一个金融机构间的清算汇兑平台,无法发挥区块链建立信用去中心化的优势.

基于公有链数字货币,为了保护用户隐私使用了复杂的密码技术,但复杂的运行和验证过程降低了系统的运行效率.在匿名性上不断地投入精力改进的原因是公有链的结构使每个节点都能掌握所有用户的交易信息,如果不对交易的发送者、接收者和交易数额进行很好的隐藏或混淆,现有的分析技术能轻易地找到交易之间的联系,得到用户的行为习惯甚至现实中的身份.而这些繁琐的加密和认证机制,并不适合每个用户都自己完成,当前比特币系统中用户通过频繁的改变自己的钱包地址防止分析追踪,这并不适合普通用户生活中使用.

2.2 可监管模型设计准则

本文遵循的设计准则包含 3 个方面:1)可监管数字货币模型设计的目的是为了实现将监管融入到系统运行过程中,找到一种合理的对区块链系统监管的方案,使系统内部能实现对于交易信息可以监督、追溯,实现对账户行为直接管理,从而促进各界对区块链技术的接纳和使用;2)在用户接受监管的基础上保护他们的隐私,如果作为广泛使用的数字货币系统,交易者的日常消费记录都会被记录在区块链上,保护用户隐私不被泄露也是系统应有的属性;3)在满足以上 2 个条件的基础上,尽量让用户也参与到系统共识中,充分利用区块链信用去中心化来建立系统的可信性.

区块链可以设计成不同的系统结构以适应不同的应用场景,在保证系统的易用、稳定和安全的基础上,也要考虑可扩展性.

为了实现以上目标,也为了在一定程度上改进现有模型的一些不便之处,本文提出了一种双链结构的可监管数字货币模型.以金融业为例,联盟链作为系统中的核心部分负责处理交易的收集、验证和打包记录.监管机构直接参与到联盟链的运行中来,作为共识过程的参与者.联盟链的区块中加密存储用户完整交易数据,可用来进行追溯,加密存储用来保护用户隐私.联盟链的参与者只有少数,为了提高系统的可信性可以增加公有链补充联盟链功能的不足.

公有链中存储用户状态变化信息,并将联盟链的区块摘要存储于公有链中,即锚定在公有链上.公有链的参与者可以是每个用户.完整的交易信息包括交易的起始地址、目标地址和交易数值,可以利用其生成 2 个独立的转入交易和转出交易,抹去起始地址和目标地址的关系.公有链中的记录可以用来验证账户状态,让用户在交易发起后有验证交易有效性的能力.联盟链将数据摘要存储在公有链中,防止联盟链成员串通对消息进行篡改.

在用户身份认证方面,根据中国人民银行对于数字货币后台实名制的要求,引入中心化的身份认证服务器(identity verify server, IVS).模型基本结构如图 1 所示:

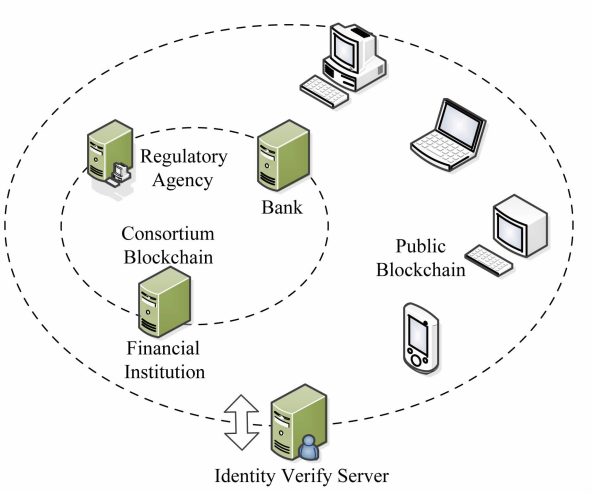


Fig. 1 The structure of the basic model

图 1 模型基本结构框图

2.3 关键数据结构

为满足可监管数字货币模型的设计,首先对必要的数据结构和名词进行约定.

定义 1. 完整交易(Txcomp). 由公有链用户生成,包括一次交易中所有的转出、转入交易和相关的密钥及参数以及标识交易的序列号. 具体结构为

$$(Sn_{\text{comp}} \parallel num_{\text{out}} \parallel \{PubKey_{\text{USOT}} \parallel PriKey\}_i \parallel num_{\text{in}} \parallel \{PubKey_{\text{new}} \parallel value\}_j \parallel Sig_{\text{user}}),$$

其中,Sn_{comp}为交易序列号,num_{out}和 num_{in}分别为完整交易中包含的转出和转入交易数,$\{PubKey_{\text{USOT}} \parallel PriKey\}_i$ 为第 i 个未花费过的转出交易地址和对应的解锁私钥,$\{PubKey_{\text{new}} \parallel value\}_j$ 为包括找零地址的转入交易中接收货币的新地址和接受金额,输出地址包括的总金额应该和 $\sum value_j$ 相等,最后为交易发起者对消息的签名.

定义 2. 转出交易(Tx_{out}). 由完整的交易截断后生成,存储在公有链上,用来验证交易有效性. 具体结构为($Sn_{\text{out}} \parallel PubKey \parallel PriKey$),其中包括交易序列号、付款地址和付款地址对应的私钥.

定义 3. 转入交易(Tx_{in}). 和转出交易同时生成,结构为($Sn_{\text{in}} \parallel PubKey \parallel value$),包括交易序列号、新生成的公钥地址和其中包含的交易金额.

定义 4. 未花费交易输出(unspend output transaction, USOT). 每一笔未经过转出的转入交易被称为 USOT,它是一个系统中合法交易的基本单位,所有交易都可以追溯到一个或多个 USOT 中,最初的 USOT 是系统外向系统内的转账,只有 USOT 地址中的交易才能执行转出,防止“双重花费”的发生.

定义 5. 联盟链数据结构. 联盟链区块体中保存的数据分 2 部分,首先是可以用来进行交易行为追溯的完整交易记录,为了防止某个节点被攻破导致交易记录泄露,它们都被加密后再打包进区块体中;第 2 部分是区块中完整交易对应的截断后交易的序列号,用来发起追溯后寻找交易存储的区块,减少解密运算工作量. 这 2 部分都经过摘要计算连接到 merkle 树中.

定义 6. 公有链数据结构. 公有链中存储独立的转出交易和转入交易,为交易有效性验证提供凭据.

定义 7. 待确认交易列表. 联盟链节点收到交易并验证正确后,将交易存储在该列表中,生成区块时根据交易加入的先后对交易进行打包,打包后的交易被标记,等待公有链区块检查到对应交易,确认已经存储在公有链后,交易将被移出列表.

系统的可监管性体现在交易追溯环节,现有的数字货币,其机制中并不包括追溯功能,区块链中存储记录的目的是为了防止篡改交易的各种攻击. 本文将可追溯作为一种安全性能加入系统,对于交易记录的分析攻击是公有链系统面临的主要安全性挑战之一,所以合理的保存记录也是系统内可监管的性能的需求,整个系统中各个功能的设计也都是为了实现这个目的.

3 基于信用的高效共识机制

去中心化的区块链系统如何高效地达成分布式系统的一致性是决定性能好坏的重要问题. 系统状态的决定权分散在每一个成员手中,成员规模越大达成共识的计算和通信成本越高. 分布式系统中如果仅存在被动错误,比如数据包丢失和延迟,可以通过 Raft 和 Paxos 等算法解决一致性问题[10];如果分布式系统中节点之间属于互相不了解的参与者,受到利益的驱使,则还可能产生拜占庭错误,即存在节点主动向其他节点发送错误信息. 在这种系统中需要使用有拜占庭容错能力的共识算法[11-12].

PoW[13]在能耗方面存在巨大的浪费,大量电力被用来计算无意义的问题;出块间隔太长,导致交易确认效率低;专用芯片的出现使少数机具有构垄断区块生成的能力,记账结果的正确性和整个系统的抗攻击能力都受到影响;PoS[14]一方面解决了工作量的能耗问题,另一方面将用户更多的利益绑定进共识中,进一步提高系统稳定性. 但动态的挖矿难度会影响出块的平稳程度. 币龄的积累可以离线完成,

无法促进节点参与共识过程.鼓励用户囤积代币,减弱了系统代币的流动性;DPoS将用户分层,把交互过程参与者的范围缩小提高效率,但当被选出的见证节点存在拜占庭错误时,该共识机制没有提出很好的解决方案.

本文在提出的可监管数字货币模型中将见证节点独立出来组成联盟链,引入对联盟链成员的身份认证信息,选用更适合的方法解决拜占庭容错问题.以解决分布式系统一致性的通用方案PBFT[15]为基础,引入行为积分和分级机制,设计并实现了信用拜占庭协议(credit practical Byzantine fault tolerance,CPBFT)用于实现联盟链的共识机制.提高了对新节点加入或者剔除拜占庭节点操作的灵活性,同时将协议通信复杂度大大降低,减少了对网络带宽的要求.简化了一致性过程,提高了共识效率并降低了共识成本.

本文提出的信用拜占庭协议加入了节点的行为记录,当节点存在不能完成被分配的任务时降低对它的信用评分,甚至限制参与共识协议的权限,以此来降低错误节点比例,配合简化协议的运行,提高系统效率.在改变节点权限的过程中需要更新所有节点的网络拓扑以保持一致性,也可以允许节点的加入和离开,实现了系统的动态灵活性.新的共识机制综合考虑不同机制的特点,虽然为联盟链设计,但也可以考虑扩展到公有链系统中.

3.1 CPBFT核心协议

CPBFT借鉴基于证明的共识机制中的思想,将节点参与共识过程的历史行为作为节点可信程度的证明,和优化后的通信过程相结合,通过实现系统的良性循环提高效率,减少通信成本.联盟链要求参与者经过身份认证才能加入,可信程度和稳定性都比公有链更有保证,参与者的规模也相对较小,多项式的通信复杂度在实际中也能满足.

PBFT共识主要由一致性协议、视图更换协议和检查点协议组成.在CPBFT共识机制中,视图更换协议增加了对出块失败节点的信用分数惩罚;检查点协议中增加了节点加入退出和信用排序内容.

3.2 一致性协议和简化一致性协议

区块链系统中每隔一段时间,一定数量的交易或者账户状态变化被打包后记录进区块中.系统中节点通过一致性协议保证存储的区块信息正确并相同.协议中存在主节点(Primary)和从节点(Replica)2种身份,同一时间主节点只有一个,负责对一段时间内接收到的交易进行验证,通过验证的交易将被打包进区块.参与共识的节点会有从0到$R-1$个互不相同的编号,主节点选择公式为$p=v \bmod R$,p是被选中节点编号,v是从零开始逐渐递增的视图编号,R是参与共识的节点总数.

如图2所示,一次完整的区块生成共识发起并完成需要3个阶段的通信过程,具体步骤如下:

1)主节点生成Pre-Prepare证书,其中包括新区块、证书时间戳和主节点签名等内容.主节点将Pre-Prepare证书发送给从节点,之后主进入Prepare状态.

2)从节点收到Pre-Prepare证书后,如果是第一次收到该证书从节点进入Prepare状态,并转发该证书给其他从节点.

3)节点收到其他节点发来的证书,会校验证书内信息,包括区块内交易的正确性、区块头信息正确性和区块高度等.如果认可该区块,向发送来证书的节点回复认可反馈.一个节点收集到包括自己的$2f+1$个认可反馈,表明该区块被加入区块链尾端,这条证书进入Commit状态.

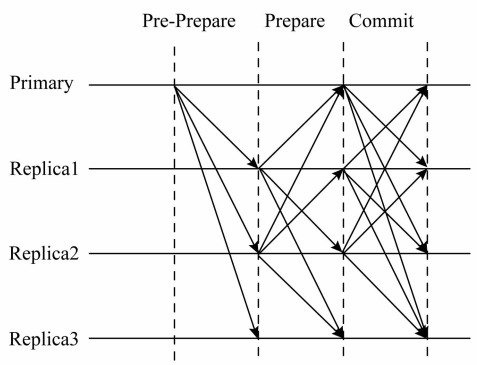


Fig. 2 The complete process of the consensus protocol

图2 一致性协议完整交互过程

图2中Primary为主节点,Replica1和Replica2为诚实且无延迟的从节点,Replica3存在被动错误,即使从节点Replica3存在拜占庭错误,根据相同的投票过程协议仍能正确执行.

完整的一致性协议需要完成2次复杂度为$O(n^2)$的通信过程,复杂度较高,所以为了简化通信过程,本文参考混合群组拜占庭容错协议对没有拜占庭错误的情况下进行优化,简化过程如图3所示,具体内容为:

1)主节点发送给所有从节点Pre-Prepare证书,从节点收到后如果认可证书内容,回复认可信息.

2)主节点如果收到超过$2f$个认可信息,将接到的反馈信息打包再发送给所有从节点,从节点可以验证其他节点的认可信息是否正确,如果正确证明

所有节点都接受该区块信息,所有节点进入 Commit 状态,将新区块加入区块链尾端.

3) 如果主节点没有收到所有的认可信息,则进入完整的一致性协议流程.

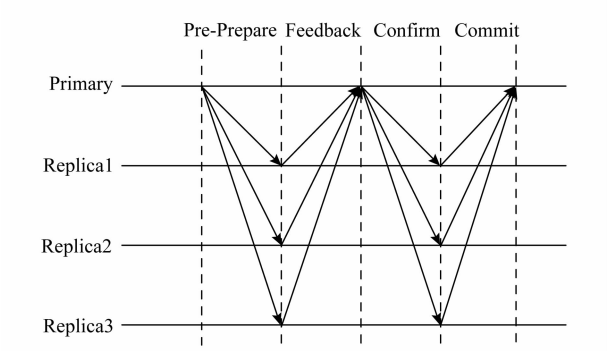


Fig. 3 The simplified process of the consensus protocol

图 3 一致性协议简化交互过程

成功完成区块生成后,将打包进区块中的交易从待确认列表中移除,视图编号增加 1,进入到下一个区块生成过程中,循环一定的周期数后会进入检查点协议更新节点信用值和节点顺序.

3.3 视图更换协议

视图是 PBFT 共识机制中节点关系的定义,视图的编号记为 v,视图中节点有不同的编号,每个视图有一个主节点. 一致性协议中主节点拥有记录交易到区块中的核心权利,主节点产生错误会导致出块停止,视图更换协议在主节点出现故障时被触发,完成变更主节点的任务,保证维持系统的运行,视图变更后视图编号增加 1.

视图更换协议由从节点发起,触发条件和等待过程如图 4 所示,以区块链中最新区块的时间戳 T 为起始时间,从节点在一致性协议运行过程中有 2 个超时情况会触发视图更换:1)在有限的时间 ΔT_1 内没有收到新的主节点 Pre-Prepare 协议;2)在有限时间 ΔT_2 内没有完成新的区块生成,其中 $\Delta T_1 < \Delta T_2$. 满足上述 2 个条件的任意一个则可以认为主节点故障,此时需要进行视图更换.

视图更换需要节点间交互通信,执行过程如下:

1) 从节点开始执行视图更换协议后进入视图 $v+1$,发送 View-Change 证书给所有节点,其中包括最新区块编号和摘要信息和新的视图编号及主节点.

2) 从节点如果收到包括自己发出在内的 $2f+1$ 条 View-Change 证书,则发送给视图 $v+1$ 中主节点 View-Change-Ack 证书. 同时清除 T 之后收到的一致性协议证书,等待新的主节点发起一致性协议.

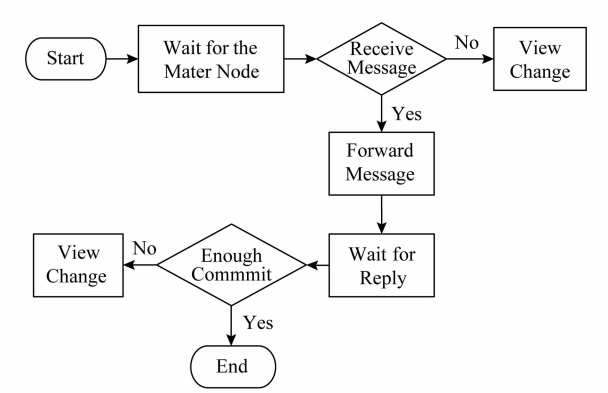


Fig. 4 The flow chart of the view-change

图 4 从节点视图更换协议触发条件

3) 新主节点根据自己存储的区块链数据开始新一轮一致性协议.

视图更换过程会造成交易确认的停止,所以需要尽量避免主节点错误,通过信用累积,多次顺利完成区块生成的节点将会有更多的机会担任主节点,提高系统效率.

3.4 检查点协议和信用分级协议

理想情况下所有节点能及时地完成系统中的各项交互任务保持一致性,但实际中部分节点可能由于本身故障或网络问题,落后于其他节点,需要一个协议周期性同步整个系统,防止节点不一致累积导致系统故障. 检查点协议在检查一致性状态后,对已经确认的区块相关的证书进行清除,减少节点存储压力. 本文还在检查点协议中扩展了动态增删节点和信用分级排序功能.

检查点协议执行时间间隔记为 CT,每次执行节点向其他节点索要区块链状态信息,一旦发现和大多数节点不一致,则主动向其他节点索要从上一个检查点开始的区块信息. 同步完成后,节点清除已经被记录的交易,更新本地交易列表,清除在最新区块时间戳之前的证书信息.

系统中根据节点行为产生信用分数,根据信用分数,把节点评级分 A,B,C 三等,3 类节点能完成的协议如表 1 所示:

Table 1 The Comparison of Right of Notes

表 1 节点权限比较

Level	Master	Slave	Checkpoint
A	√	√	√
B		√	√
C			√

刚加入系统的节点为 C 类节点,在同步完区块

后成为 B 类节点. 节点在系统中参与完成一次区块生成共识加 1 分;成为主节点成功完成区块生成会收取一定的实际收益,但该轮共识不加信用分;未能成功生成区块的主节点扣 5 分. 节点会因为自身行为在 A,B 两类节点中变化. 根据系统中节点的多少,以 n 倍 CT 为时间周期执行信用分级协议,完成信用信息的更新,A 类节点获得视图编号用来参与主节点选择. 信用分级协议也需要一次 3 阶段的通信共识,但在长期统计来看,配合简化一致性协议能大大减少通信开销,提高系统效率.

4 双链结构可监管模型

可监管模型的核心是由银行、金融机构和监管机构等参与组成的联盟链. 联盟链中根据参与者协商好的对系统的控制比例分配给各个机构不同数量的系统节点,系统节点的多少决定了在共识过程中对系统的控制权的大小.

4.1 联盟链结构设计

可监管数字货币模型的联盟链系统包括系统初始化、交易验证和转发、CPBFT 共识协议、交易混淆和交易追溯五大部分. 系统初始化完成系统参数生成和区块链最初状态;交易验证和转发是联盟链成员共享信息的过程,保证节点由同样的基础达成共识;共识过程包括 CPBFT 中节点交互的具体过程;交易混淆负责在交易被确认后处理交易在发送给公有链节点前除去交易关系信息来保护交易隐私性;最后的交易追溯是系统内部监管的过程. 联盟链内部节点间的通信使用加密信道,防止通信传明文输完整交易时造成信息的泄露.

在系统初始化阶段,根据系统安全参数 λ_1、椭圆曲线密钥生成基本参数 λ_2、联盟链参与节点总数 n 和秘密恢复门限 t 等输入,使用椭圆曲线密码算法得到区块信息加密密钥(PK_{block},SK_{block});使用秘密共享将 SK_{Block} 共享给系统中的 n 个节点,并将其销毁;随后各个节点各自生成身份认证签名($PK_{\text{com\_id}}$,$SK_{\text{com\_id}}$). 节点间交换签名密钥,防止冒充联盟链成员身份发送信息,节点间互相协商信息传递的密钥建立加密信道,防止交易信息的泄露. 完成参数初始化后,系统建立联盟链创世区块,对 CPBFT 维护的区块链状态初始化,第 1 次确认各节点状态一致性,使系统进入由共识机制保持一致性和可用性的循环.

在交易验证和转发阶段,系统通过完整交易信息验证节点收到用户发送来的交易或者其他节点转发来的交易格式是否符合规范,内容是否正确;根据交易编号 Sn_{comp} 判断用户发送的交易是否已经收到过,并根据交易有效性协议结果共同决定是否保存和转发.

CPBFT 共识协议阶段是保持系统状态一致性的核心阶段,使用基于投票的机制来验证区块信息的正确性. 如图 5 所示,协议循环的主体是一致性协议,系统开始运行后首先执行一致性协议,在一致性协议执行的过程中,从节点在执行投票反馈同时完成监督主节点的任务,主节点无法在时间阈值内完成区块生成任务,则触发视图更换协议. 进入视图更换协议后,暂时停止一致性协议运行直到新的主节点选出. 检查点协议中的区块同步部分由各个节点按照周期 T_{cp} 自行完成,n 个周期后系统停止一致性协议过程,更新信用了列表和评级,生成新的视图,一般更新间隔至少保证视图中主节点轮换完成一次循环.

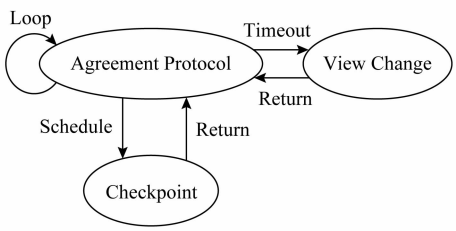


Fig. 5 The state diagram of CPBFT

图 5 CPBFT 共识协议执行状态转移图

算法 1. 区块生成算法.

输入:待确认交易列表;

输出:新区块和转入、转出交易.

① 根据发送时间选择待确认列表中靠前的交易;

② 根据完整交易生成截断的转入、转出交易,完整交易对应交易地址生成的摘要作为截断交易序列号 $\text{Hash}(Sn_{\text{comp}} \parallel PubKey_{\text{USOT}}) \rightarrow Sn_{\text{out}}$ 和 $\text{Hash}(Sn_{\text{comp}} \parallel PubKey_{\text{new}}) \rightarrow Sn_{\text{in}}$,该交易序列号作为交易归属的凭证;

③ 将截断交易序列号明文和完整交易信息密文,存入区块体中,分别生成 Merkle 树,最后共同生成一个 Merkle 根值存入区块头中;

④ 根据区块链状态,生成区块头,区块时间戳值必须大于区块中所有交易,并对区块进行签名.

算法 1 的主要功能为主节点从待确认列表中选择交易,将交易截断后生成对应的转入、转出交易,将完整交易加密后存入区块,生成 Merkle 树和区块头组成完整区块,准备在一致性协议中发送给从节点.

算法 2. 区块验证算法.

输入:接受到的新生成区块数据;

输出:验证结果.

① 验证过程中任何一步发现区块错误或者不符合要求直接返回;

② 验证区块的发送者是否是当前主节点,验证区块的完整性;

③ 验证区块的数据结构正确性:区块头和区块体不能为空,区块大小不能超过最大值 MAX_BLOCK_SIZE,区块实际大小和区块中记录一致,区块包含交易数和交易计数器一致;

④ 验证当前版本号、父区块摘要等区块头新信息的正确性;

⑤ 根据交易标号对比区块中存储的每条交易密文的正确性;

⑥ 计算 Merkle 树每层摘要值的正确性;

⑦ 确认区块正确,返回信息.

算法 2 的主要功能为节点在运行一致性协议过程中,收到主节点发来的新生成区块,在接受前对其进行检查,判断是否符合将其连入区块链的条件.

根据第 3 部分设计,CPBFT 共识协议中的一致性协议分为 2 部分:简化一致性协议和完整一致性协议,如图 6 所示. 当系统运行一致性协议部分时,如果主节点第 1 次公布区块后收到的从节点 $Accept_{\text{block}}$ 数量达到规定的门限,则只完成简化版流程;如果没有收到足够的 $Accept_{\text{block}}$ 则进入完整一致性协议. 或者,简化一致性协议运行过程中,从节点认为主节点发来的信息有误时也将进入完整一致性流程,等待主节点新的信息.

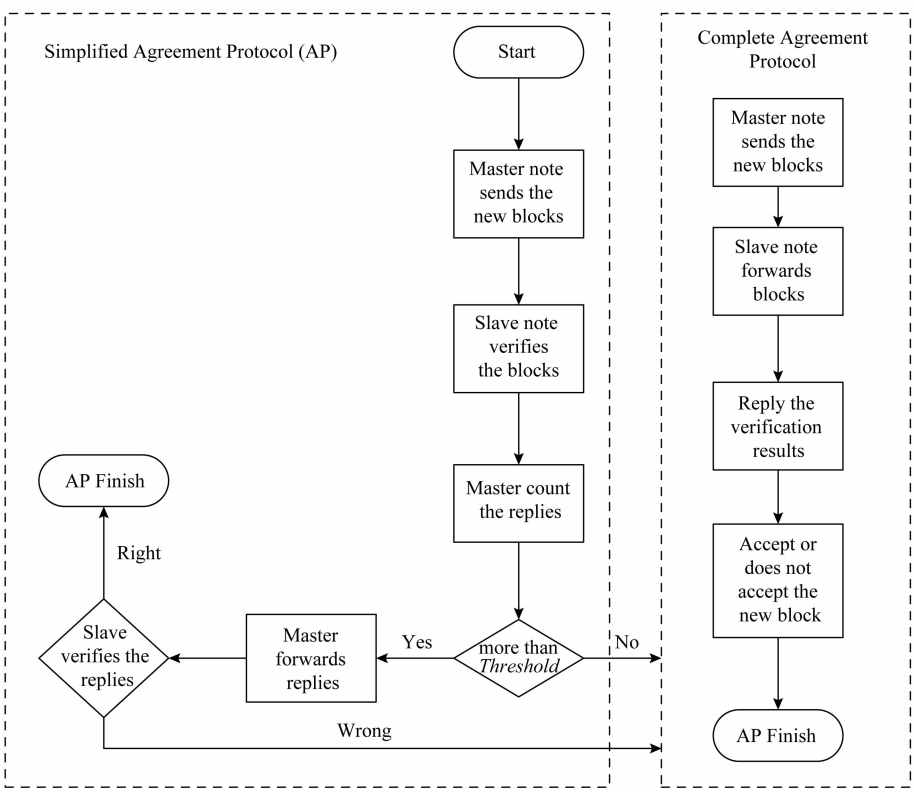


Fig. 6 The flow chart of the agreement protocol

图 6 一致性协议流程图

算法 3. 简单一致性协议算法.

输入:当前区块链系统状态、待确认交易列表;

输出:系统达成的新一致性状态.

① 主节点将待确认列表中的交易打包,生成新的区块 $Block_{\text{new}}$;

② 主节点将($Block_{\text{new}} \parallel ID \parallel Sig_i$(Hash($Block_{\text{new}}$),$ID$))发送给从节点,$Block_{\text{new}}$ 为新区块,ID 为主节点身份,Sig_i(Hash($Block_{\text{new}}$),ID)为主节点签名;

③ 从节点调用区块验证协议验证区块数据的正确性;

④ 从节点如果接受区块向主节点并回复确认信息 $Accept_{\text{block}}$,或不接受区块并回复反对信息 $Refuse_{\text{block}}$;

⑤ 主节点收到超过 $2f$ 个节点的确认 $Accept_{\text{block}}$ 消息,则进入简化一致性协议中.

⑥ 主节点将各个节点发来的 $Accept_{\text{block}}$ 集中分别转发给从节点;

⑦ 从节点验证各个节点的 $Accept_{\text{block}}$ 信息正确后接受新区块,本轮一致性协议结束;

⑧ 从节点认为主节点发送的 $Accept_{\text{block}}$ 信息中有错误或伪造的成分,则进入完整一致性协议的过程.

通过算法 3,系统保证各个节点区块生成和区块链系统状态的一致性. 新区块中包含的交易必须是待确认交易列表的子集,将对应交易信息加密后和区块内数据进行对比确认交易内容没有被篡改.

如果主节点在算法 3 步骤⑤中没有接到超过 $2f$ 个一致性协议,则进入完整一致性协议.

算法 4. 完整一致性协议算法.

①→②→③→④从节点如果验证区块内容正确向其他节点发送 $Accept_{\text{block}}$ 信息;不正确则向其他节点发送 $Refuse_{\text{block}}$ 信息;

⑤ 如果从节点收到超过包括自己 $2f+1$ 节点的 $Accept_{\text{block}}$ 信息,则向其他节点发送 $Accept_{\text{commit}}$ 信息;不接受发送 $Refuse_{\text{commit}}$ 信息;

⑥ 如果节点收到超过包括自己 $2f+1$ 节点接受区块 $Accept_{\text{commit}}$ 信息,则将区块加入区块链,主节点成功生成区块,主节点轮至下一个节点;

⑦ 在等待时间阈值 ΔT 内主节点没有成功生成区块,从节点将触发视图更换协议.

完整一致性协议算法的输入输出与算法 3 不变,只是流程需要从节点间交互.

由图 5 可知,CPBFT 共识协议中,主节点可能发生故障时该需要主动更换主节点. 即从节点向其他从节点发送视图更换验证消息,如果从节点收到包括自己的 $2f+1$ 个视图更换验证消息后,向下一个视图的主节点发送视图更换请求,如果节点收到包括自己超过 $2f+1$ 个视图更换请求后确认自己成为主节点.

由图 5 可知,CPBFT 共识协议中,系统需要按计划进入检查点对系统进行评估. 检查点协议包括 2 个部分,首先以 T_{cp} 为时间间隔确定节点间一致性,该部分由各个节点按照时间自行向其他节点发出询问请求并完成状态检查和同步;其次以 nT_{cp} 为时间间隔更新信用评级,将出现错误的节点暂时降低参与共识的权限,生成新的视图.

交易混淆阶段是保护系统数据与用户信息隐私性的重要阶段. 一个完整交易包括多个转出交易和至少 2 个转入交易,联盟链在确认完整交易正确并接收之后将完整的交易分成货币转出交易和货币转入交易,每种交易包括多个子交易,如图 7 所示. 子交易的编号可以用来作为其所属完整交易的证明,但无法通过它得到所属的完整交易,子交易编号与完整交易一起写入区块用于追溯,切分后的交易失去了货币转出和转入地址的联系从而保护用户的隐私.

将序列号为 Sn_{comp} 的交易分成多编号为 Sn 个转入、转出子交易,$Sn\in\{Sn_{\text{out\_0}},Sn_{\text{out\_1}},\cdots,Sn_{\text{out\_}i},$

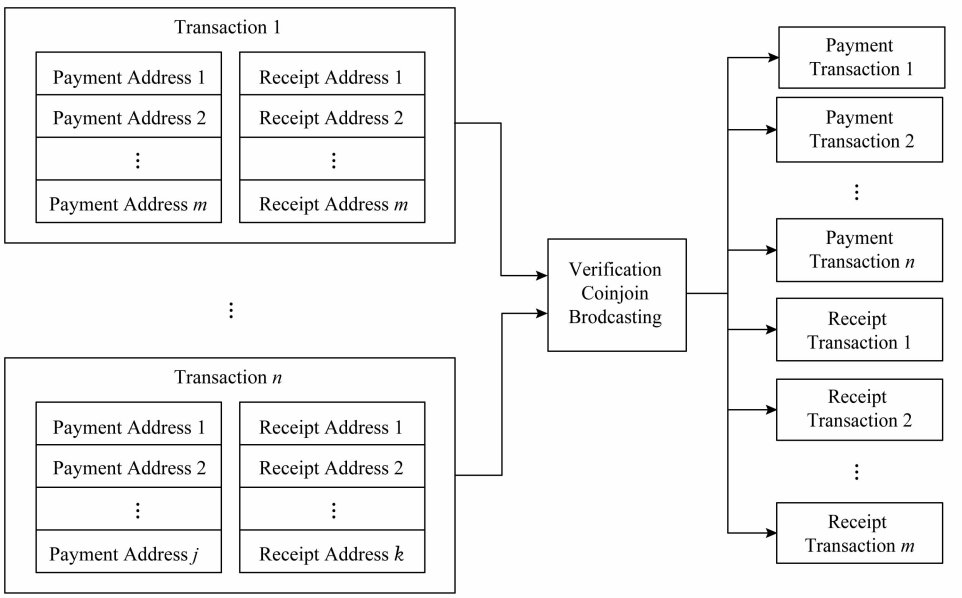


Fig. 7 Transaction confusion

图 7 交易混淆

$Sn_{in\_0}, Sn_{out\_1}, \cdots, Sn_{in\_j}\}$. 打包交易时,将子交易编号明文作为交易的一部分打包进区块,将一个区块内包含的子交易打乱后批量广播给公有链节点. 随后删除完整交易的明文,仅在区块中保留密文以供追溯.

交易追溯阶段是系统实现监管目的的手段,系统通过对交易的追溯、对交易参与者身份的揭示,实现监管的目的. 这里引入一个安全性假设,系统中的监管节点是可信的,由监管节点完成秘密共享份额的收集和解密密钥的恢复,在完成追溯任务后,监管节点会诚实的完成对相关信息的删除. 交易追溯的结果并不直接作用到区块链系统中,不会发生系统内对系统状态的修改,如果要追回资金或者封禁账户均由系统外的监管机构完成.

追溯发起时,由联盟链参与者发起对某项交易的追溯请求 $Review_{req}$,全体成员投票决定是否执行. 同意发起追溯的节点将保存的秘密共享信息 $Share_i$ 发送给联盟链中的监管节点,当超过秘密恢复门限 t,监管节点恢复出密钥 SK_{Share}. 信息揭示时,根据提供的被截断后的交易编号,查找联盟链中相匹配的交易,对交易进行恢复,得到交易者的身份. 当完成对一次完整交易的追溯就会得到与其相关的属于其他完整交易的转出和转入交易,因此可以通过逐步递进完成对所有交易信息的揭示. 交易追溯结束后监管机构销毁解密密钥等相关信息.

4.2 公有链结构设计

在可监管数字货币中加入公有链的部分,一方面是为了增加系统的可信性,将联盟链每个区块的摘要数据存储在公有链中起到锚定的作用,通过用户监督数据防止篡改. 另一方面联盟链上存储的是加密数据,公有链上存储了截断联系的交易数据明文,在保护用户隐私的基础上为整个系统中的节点提供验证交易的依据. 公有链中的参与者是系统中的用户,采用公有链的结构方便系统的扩展,促使更多的人参与到系统共识和维护中,提高系统的稳定性. 公有链中的用户加入系统要向身份认证服务器注册,配合交易追溯过程. 整个公有链包含 5 个阶段:

1) 用户身份认证阶段. 用户向身份认证服务器提交身份信息 Msg_{ID}. 身份验证服务器检查用户身份,如果存在问题则拒绝身份申请. 如果接收用户申请,用私钥 SK_{IVS_id} 对用户提供的信息进行签名生成证书 $Cer\_user = sig^{SK_{IVS\_id}}(id\_msg, PK_{user\_id})$,并存档后发送给用户.

2) 交易生成阶段. 交易付款方获取收款方新生成的付款地址 $\{PubKey_{new}\}_i$,付款方生成交易找零地址 $\{PubKey_{new}\}_j$. 将付款 USOT 和其解锁密钥以及付款地址加入交易中,随后统计交易中包含的地址个数,验证交易金额是否收支是否平衡,生成交易编号,对交易进行签名.

3) 公有链区块生成阶段. 公有链节点接收到联盟链发来的混淆后交易的广播,广播中包括大量付款交易和收款交易. 支付交易对应一个已经存在的 USOT,包括该 USOT 的编号、解锁密钥. 收款交易会生成新的 USOT. 验证信息发送者的身份签名和消息签名后,对验证付款交易的正确性进行判断,以及对应的支付交易是否为 USOT 交易,提供的支付密钥是否正确. 最后将正确的交易打包进区块中,生成 Merkle 根和区块头.

4) 区块验证阶段. 对收到的区块判断是否合规正确. 其中包括验证区块的发送者是否是当前主节点,验证区块的完整性;验证区块的数据结构正确性;区块头新信息是否正确;根据交易标号对比区块中存储的每条交易密文的正确性;最后计算 Merkle 树每层摘要值的正确性. 验证过程中任何一步发现区块错误或者不符合要求直接返回 $Refuse_{block}$.

5) 公有链共识阶段. 采用 DPoS 共识协议,其中包括见证节点的选举和见证节点完成区块生成. 因为公有链节点规模较大,可以将见证节点的选取的间隔时间设置的较长,减少通信成本. 公有链节点都可以申请成为见证节点,但如果存在出块延迟甚至生成错误区块,则会在之后的选举过程中被其他节点替代.

在选举出公有链中负责生成区块的见证节点时,首先注册过的用户节点根据自己选择的见证节点生成投票信息 $(\{Node_i\} \parallel ID \parallel Sig_i(\text{Hash}(\{Node_i\}), ID))$,其中 $\{Node_i\}$ 为节点选择的见证节点集合,ID 为投票节点身份. 节点对消息进行签名广播给其他节点. 随后公有链用户验证收到的投票的完整性和正确性,对超过 2/3 的选票选择的节点进行统计,并广播得票前 101 位的候选节点作为确认信息,根据得票数确定见证节点顺序. 最后,公有链用户收到相同的确认信息超过总信息数的 2/3,则确认其中的节点为下一周期共识的见证节点.

在选举得到见证节点之后,区块的生成和验证由见证节按顺序轮流完成,其他用户通过监督见证节点区块生成过程的行为,决定是否在下一次投票中是否选择对应的节点成为见证节点.

4.3 双链结构的可监管数字货币模型系统设计

本文实现了双链可监管模型的验证原型.系统中包括3个模块:用户钱包、联盟链节点(含监管)和公有链节点.系统中节点间使用P2P通信,除了节点担任的任务不同,不存在服务器和客户端的定位区别.用户钱包是在系统中交易的发起者,帮助用户管理着所拥有的USOT对应的公私钥和交易,方便用户查询和使用.联盟链完成交易接收、确认、混淆和打包记入区块的功能.公有链存储的转入、转出交易作为验证交易和用户钱包获得账户状态的凭据.

可监管数字货币系统的交易流程如图8所示,系统中公有链节点和联盟链节点之间是对等的关系只是处理消息的工作不同,这2部分合起来可以视为服务器,用户钱包是客户端,向服务器发送操作请求.

系统发起追溯的流程如图9所示,整个流程只发生在联盟链节点间,追溯发起节点向包括监管节点的其他联盟链节点发起请求,图9中的其他联盟链节点包括不止一个节点,分别对请求做出判断,监管节点恢复出密钥后获取用户身份.

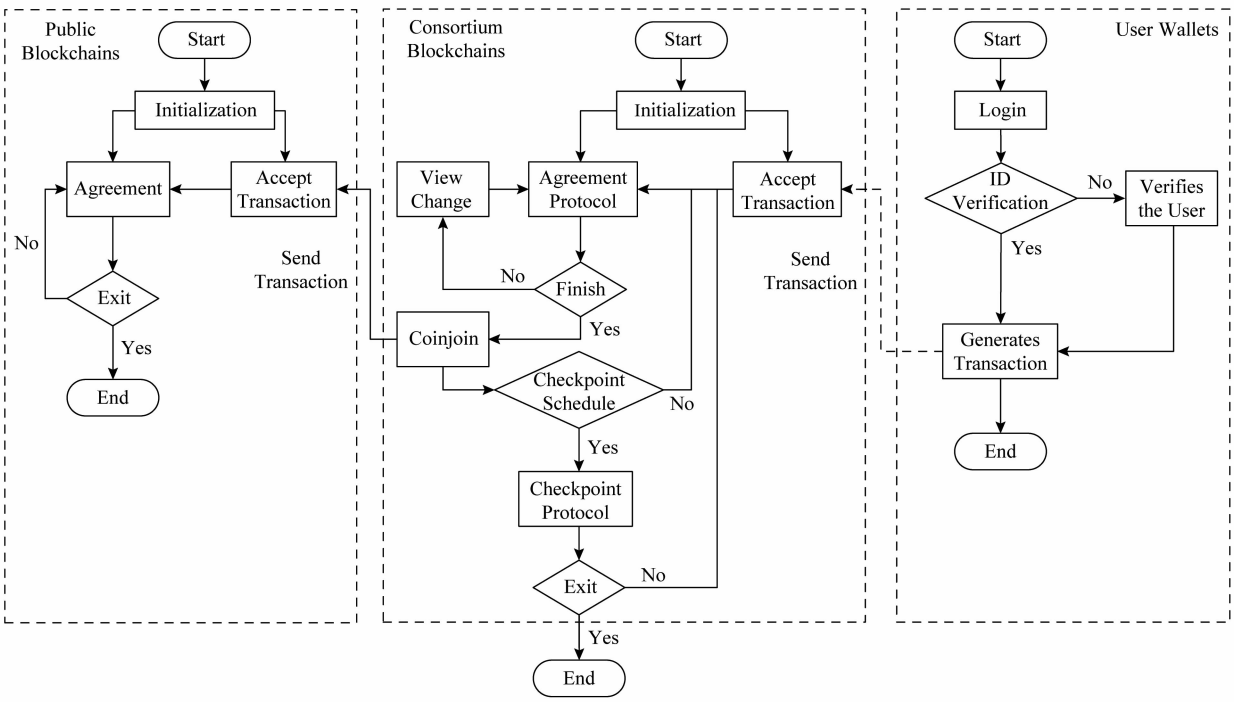


Fig. 8 The flowchart of the transaction

图8 交易流程图

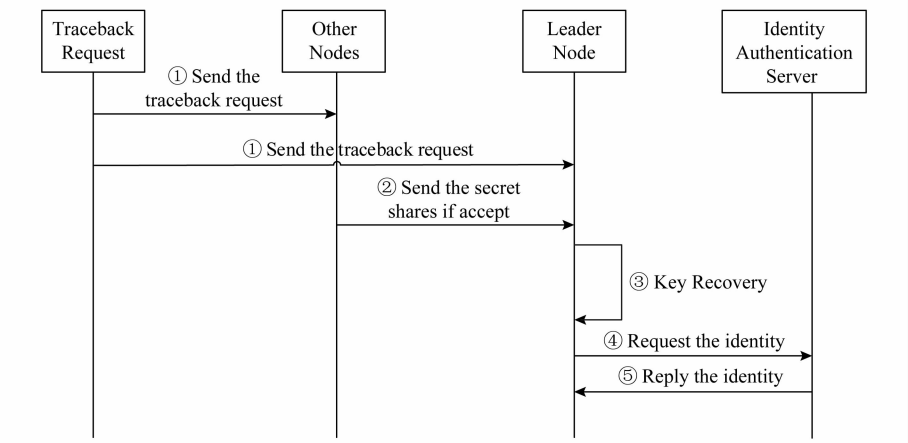


Fig. 9 The flowchart of the tracing back

图9 联盟链追溯过程通信流程图

4.4 安全性分析

可监管数字货币模型的安全性主要从模型安全性和交易安全性 2 个方面进行分析.

1) 模型安全性是由共识机制的安全性进行保障. 本文采用的基于信用的拜占庭容错机制作为共识机制,其本质仍然是一种状态机副本复制算法. 算法保证了活性(liveness)和可证明安全性(safety),并提供了一部分容错性. 文献[16]给出了具体的证明过程. 对于区块链的隐私保护机制,本模型所采用的混币技术、加解密技术等网络层、交易层的防御机制均为已证明安全的技术进行支撑. 具体分析可参考文献[17].

2) 交易安全性是由监管机制进行保障. 数字货币交易一般分为铸币交易与流转交易. 铸币交易是系统作为激励给用户或是系统外资金流入,而流转交易就是用户间交易. 当用户账户发生资金被盗时,监管机构首先通过投票或秘密共享进行交易追溯. 虽然监管机构无法转走他人资金,但其完成取证后,可以通过产生新交易、同时冻结偷盗者账号和未花费交易的方式弥补用户损失. 以以太坊为例,其通过投票将黑客地址冻结,系统对黑名单中的公钥地址交易不进行处理. 用于监管的联盟链其区块摘要则被锚定在公有链中,防止联盟链数据被篡改.

5 实验与结果

本节中,通过 Matlab 以及 Python 编写的原型系统实际运行过程对文章所提出的模型方法进行测试.

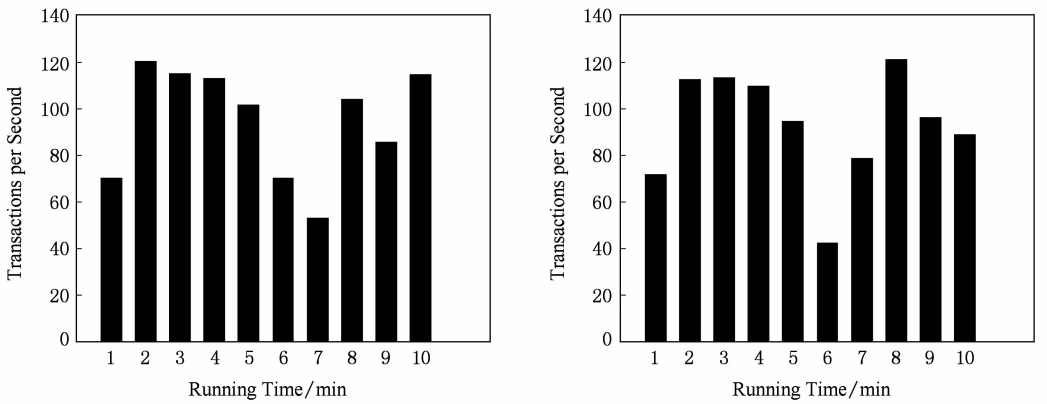
5.1 共识机制性能分析

本节对比 PBFT 和 CPBFT 共识机制的运行效率,以交易确认速率为评价指标,测试在拜占庭错误节点占总节点中不同比例和不同运行时间下 2 个算法的性能差异. 交易确认速率为单位时间能打包进区块的交易数量平均值,计算方法为 $transcations/\Delta t$. 其中 $transcations$ 为一段时间内包含进区块链的交易数,Δt 为记录时间,一般为区块生成时间的整数倍. 本文主要从 3 个方面进行分析.

1) 容错性能方面. 系统中拜占庭错误节点所占比例是对系统性能影响最大的因素,CPBFT 并没有引入更严格的情景假设,所提供的拜占庭节点占所有参与共识节点的比例阈值和 PBFT 相同,总节点数目为 n 时最大错误节点数目为 $f=\lceil n/3\rceil$. 图 10 分别为使用 PBFT 共识机制和 CPBFT 共识机制的系统运行 10 min,在运行过程中平均每分钟交易确认速率情况,系统中总共设置 301 个节点,最大 100 个错误节点环境中,系统中错误节点随机变化但不会超过最大值. 对比可以看到,在相同的系统环境中,短时间内 CPBFT 和 PBFT 能达到相同的效率.

2) 运行效率方面. CPBFT 设计的目的之一就是提高系统长期运行效率. 随着系统运行,高错误率节点的低信用信用分使其成为主节点频率降低,低主节点错误率和简化一致性协议及激励相配合,CPBFT 能比 PBFT 更高效的完成区块生成、确认,提高系统的交易吞吐率. 图 11 为一段较长时间的 PBFT 和 CPBFT 的交易确认速率变化,系统采用共 301 个节点,最大 100 个错误节点环境. 可以看到随着系统运行,主节点错误率下降后系统的交易吞吐量有明显增加.

3) 通信开销方面. PBFT 及其衍生的共识机制存在的问题就是共识过程需要大量的节点间通信,



(a) PBFT (b) CPBFT

Fig. 10 Transaction throughput

图 10 交易吞吐量对比

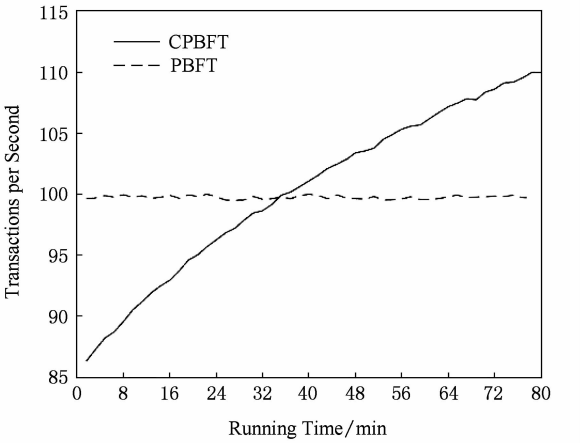


Fig. 11 The TPS between PBFT and CPBFT

图 11 PBFT 与 CPBFT 长期运行吞吐率比较

CPBFT 中检查点协议由于加入了信用评分,需要额外的通信过程对信用评分达成一致,系统开始运行的短时间内或者系统中错误节点较少时,会增加传输数据量,但在错误节点较多的场景中,能减少视图更换协议的调用,在另一方面降低了数据量. 图 12 为在图 11 的系统设置下,节点间数据传输量的比较,图中横轴为系统持续运行时间,纵轴为生成一个区块需要的复杂度为 $O(n^2)$ 的点对点通信次数. PBFT 没有运行中的优化机制,生成区块平均通信量没有变化,CPBFT 随着主节点错误率下降,通信效率逐渐提高.

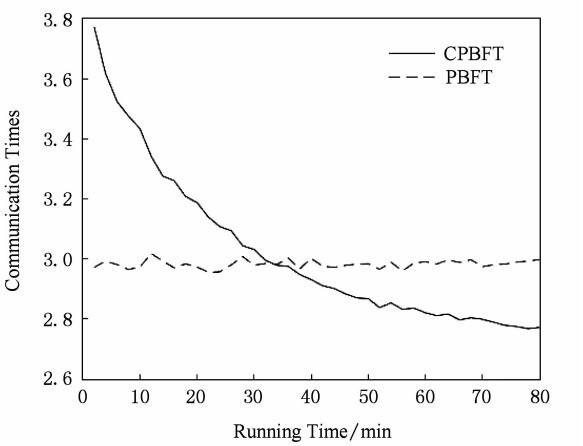


Fig. 12 The traffic of one unit block generation

图 12 生成单位区块的通信量

5.2 数字货币系统整体分析

本节将可监管的数字货币系统部署于测试环境中,实验硬件配置为 Dell 的 R730 服务器. 由 Intel Xeon E5-2630,12 核 2.4 GHz 主频、32 GB 内存、500 GB SSD 硬盘,1 Gbps 网络.

系统运行压力测试如表 2 所示. 系统性能平均在 300TPS 附近,最大性能到 440TPS. 系统总体 CPU 占用率持续为 100%.

Table 2 Performance of the Two Chains Scheme

表 2 双链模型性能

Transaction Batch Size	Maximum Throughput/TPS	Average Throughput/TPS	CPU Usage/%
300	435	295	100
100	440	298	100
50	438	402	100

功能方面,用户可以进行转账操作,发送交易后等待联盟链节点和公有链节点执行一系列操作最终将相关的转入、转出交易存入公有链区块中,钱包保存了完整交易并可以通过对比公有链中存储的数据来检查自己发起的交易是否已经被写入区块并且经过多个区块确认.

公有链和联盟链节点可以正常运行,联盟链节点按 30 s 的间隔生成新的区块,当节点在 30 s 内无法完成区块生成,会轮换至下一个节点. 公有链中也实现了类似的规则,传递生成区块权利维护系统运行.

追溯交互过程运行正常,最终可以看到对交易追溯的结果. 查找交易时根据查询的交易序列号,遍历区块中保存的交易信息明文,找到包含相同的序列号的区块,对其中交易解密,最终找到交易,将交易中的完整记录显示出来.

6 总 结

本文针对目前数字加密货币存在的难以监管问题,提出了一种基于区块链的可监管模型. 通过双链结构构成便于监管的数字货币体系. 其中,作为核心的联盟链结构中,内部成员负责交易的确认和完整交易数据的加密保存,保存的数据可以在交易追溯中作为凭据;监管机构作为联盟链的参与者加入到系统运行和维护中. 公有链的参与者可以是普通的用户,让每个用户都能参与和见证系统的维护. 系统借鉴了传统数字货币为了增强匿名性而采用的混币过程的思路,将完整交易进行截断和混淆后存储在公有链中,作为公开可信的证据在验证交易和获取账户状态时使用. 共识机制方面,根据联盟链运行场景,设计了更适合的基于信用的拜占庭容错技术. 通过引入的信用评级的机制,对联盟链中节点在共识过程中的表现进行记录,以此为依据合理调节共识过程中节点的权限,优化交互过程,在长期运行中能提高系统的运行效率.

系统使用2条链的结构是为了将完整的交易信息和验证用的信息分开存储和访问,实现用户隐私安全和便于监管2种属性的平衡.同时,为了增强信用去中心化,联盟链通过被锚定在公有链上来保证数据的可信性,以此让系统能通过代码和运行过程来建立自己的信用.实验结果表明:本文提出的双链可监管数字货币模型运行正常,共识机制以及总体性能均符合设计要求.

参 考 文 献

[1] Natamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. 2008 [2018-07-27]. https://zoo. cs. yale. edu/classes/cs426/2017/bib/bitcoin. pdf

[2] Buterin V. A next-generation smart contract and decentralized application platform [EB/OL]. (2018-6-13) [2018-07-27]. https://github. com/ethereum/wiki/wiki/White-Paper

[3] Chaum D, Fiat A, Naor M. Untraceable electronic cash [C] //Proc of the Conf on Theory and Application of Cryptography. Berlin: Springer, 1988: 319-327

[4] Brands S A. Off-line electronic cash based on secret-key certificates [C] //Proc of the 2nd Int Symp of Latin American Theoretical Informatics (LATIN'95). Berlin: Springer, 1995

[5] Back A. Hashcash-A Denial of Service Counter-Measure [EB/OL]. 2002 [2018-07-27]. http://www. cypherspace. org/hashcash/hashcash. pdf

[6] Peck M E. The cryptoanarchists' answer to cash [J]. IEEE Spectrum, 2012, 49(6): 50-56

[7] Chaum D. Blind signatures for untraceable payments [C] // Proc of Crypto82, Advances in Cryptology. Berlin: Springer, 1983: 199-203

[8] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from bitcoin [C] //Proc of the 35th IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2014: 459-474

[9] Sun He, Mao Hongliang, Bai Xiaoming, et al. Multi-blockchain model for central bank digital currency [C] //Proc of the 18th Int Conf on Parallel and Distributed Computing, Applications and Technologies (PDCAT). Piscataway, NJ: IEEE, 2017: 360-367

[10] Lamport L. Paxos Made Simple [J]. ACM Sigact News, 2001, 32(4): 18-25

[11] Lamport L, Merz S. Specifying and verifying fault-tolerant systems [C] //Proc of the 3rd Int Symp on Formal Techniques in Real-Time and Fault-Tolerant Systems. Berlin: Springer, 1994: 41-76

[12] Castro M, Liskov B. Practical Byzantine fault tolerance [C] //Proc of the Operating Systems Design and Implementation. Berkeley, CA: USENIX Association, 1999: 173-186

[13] Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: Analysis and applications [C] //Proc of the 34th Int Conf on Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 281-310

[14] King S, Nadal S. PPCoin: Peer-to-peer crypto-currency with proof-of-stake [EB/OL]. 2012 [2018-07-27]. http://bitcoin. peryaudo. org/vendor/peercoin-paper. pdf

[15] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery [J]. ACM Trans on Computer Systems (TOCS), 2002, 20(4): 398-461

[16] Castro M, Liskov B. A Correctness proof for a practical Byzantine-fault-tolerant replication algorithm, MIT/LCS/TM-590 [R]. Cambridge: MIT Laboratory for Computer Science, 1999

[17] Zhu Liehuang, Gao Feng, Shen Meng, et al. Survey on privacy preserving techniques for blockchain technology [J]. Journal of Computer Research and Development, 2017, 54(10): 2170-2186
(祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10): 2170-2186)

Zhang Jianyi, born in 1982. PhD, associate professor. His main research interests include Internet security, data security, privacy protection and digital currency.

Wang Zhiqiang, born in 1985. PhD, associate professor. His main research interests include system security and network security.

Xu Zhili, born in 1991. MSc, researcher. His main research interests include digital curreny and blockchain.

Ouyang Yafei, bron in 1985. Received her MSc degree from the University of East Anglia, UK. Her main research interests include digital curreny and blockchain.

Yang Tao, bron in 1976. PhD. His main research interest is cybersecurity.