# Gaia：一种基于竞争的股权证明共识机制的区块链系统*

张仕奇[1]，宋睿[1]，宋宇波[1]，刘自明[2]，唐敏[2]

[1](东南大学 网络空间安全学院,江苏 南京 211111)

[2](Gaia World Foundation,江苏 南京 211111)

通讯作者：宋宇波, E-mail: songyubo@seu.edu.cn

摘 要: 在区块链系统中，为进行分布式记账，需要有一个所有参与者共同遵守的共识机制。在共识机制下，所有参与者就区块归属问题以及交易拟定的价值问题达成一致。目前，区块链系统主要有 PoW(Proof of Work,工作证明)以及 PoS(Proof of Stake,股权证明)两种共识机制。PoW 共识机制包含严重的资源浪费和交易速度缓慢等问题，而普通的 PoS 共识机制会降低货币流动性。本文基于锻造委员会和锻造组系统的新架构设计，提出了一种基于竞争的股权证明(CPoS)共识机制，并在此基础上实现了相应的区块链系统 Gaia。在该机制中，锻造委员首先将被按照地址的后 8 位进行分组，并获得与缴纳的保证金相关的投票权，当前锻造组中投票权最高的锻造委员当选为主锻造委员；随着区块高度的增加，投票权不断累积总投票权最高的锻造委员获得该区块所有交易费；分组再次更新，重新计算投票权。同时通过引入锻造委员会和锻造组的机制，Gaia 可以在确保分权的前提下快速去除分叉。经原型机实验分析，该机制可在较小的延迟内快速地完成出块和交易活动，较好解决了以往共识机制资源浪费、交易速度慢、流动性低等问题。

关键词: 区块链;共识机制;股权证明;锻造委员

中图法分类号：TP311

## Gaia: A Blockchain System Based on Consensus Mechanism uses Competition-Based Proof of Stake

ZHANG Shi-Qi[1], SONG Rui[1], SONG Yu-Bo[1], LIU Zi-Ming[2], TANG Min[2]

[1](School of Cybersecurity, Southeast University, Nanjing 211111, China)

[2](Gaia World Foundation, Nanjing 210023, China)

**Abstract**: In the blockchain system, for distributed accounting, a consensus mechanism is required for all participants to adhere to. Under the consensus mechanism, all participants agreed on the issue of block ownership and the value of the transaction. At present, the blockchain system mainly has two consensus mechanisms: PoW (Proof of Work) and PoS (Proof of Stake). The PoW consensus mechanism includes serious resource waste and slow transaction speeds, while the common PoS consensus mechanism will reduce currency liquidity. Based on the new architecture design of the forging committee and the forging group system, this paper proposes a

* 基金项目：国家自然科学基金(61601113)

Foundation item: National Natural Science Foundation of China (61601113)

competition-based equity certification (CPoS) consensus mechanism, and on this basis, implements the corresponding blockchain system Gaia. In this mechanism, the forging commissioner will first be grouped according to the last 8 digits of the address and obtain the voting rights related to the paid deposit. The forging commissioner with the highest voting power in the current forging group is elected as the main forging commissioner; With a high degree of increase, the forging members with the highest voting rights and the highest total voting rights receive all the transaction fees for the block; the group is updated again and the voting rights are recalculated. At the same time, by introducing the mechanism of the forging committee and the forging group, Gaia can quickly remove the fork under the premise of ensuring decentralization. Through the analysis of the prototype machine, the mechanism can quickly complete the block and transaction activities within a small delay, which better solves the problems of waste of resources, slow transaction speed and low liquidity in the previous consensus mechanism

**Key words**: Blockchain; consensus mechanisms; proof of stake; forging Committee

诞生于 2008 年的比特币作为第一个稳定运行的大规模区块链网络，被人们定义为“一种能够让整个世界就一个公共拥有的数据库的内容达成一致的机制”[1]。比特币利用对等网络来建立分类帐系统，并将其中经过记账记录验证的交易加密为区块链。在这种分散的系统下，可以在货币交易期间放弃第三方实体的信用背书[2]。通过引入密码技术，区块链系统可以在不受信任的网络中实现高稳定性和鲁棒性。在电子货币领域取得巨大成功后，研究倾向于将区块链技术应用于其他领域。Vitalik Buterin 在 2014 年建立的以太坊是最成功的尝试[3]。以太坊最大的创新是创造了一个功能完善、图灵完备的智能合约[4]。它允许用户编写具有一定复杂度的合约、自治代理和关系，以太坊的用户可以通过内置的脚本语言来实现任意交易类型，包括定制货币、金融衍生品、身份系统甚至更复杂的去中心化应用。以太坊的核心功能是所谓的“智能合约”，它最通俗的定义是“一个包含价值并且只有满足某些特定条件才能打开的加密箱子”[5]。因为图灵完备同时具备价值知晓，区块链知晓和多状态等功能，因此以太坊很容易利用智能合约来实现过去难以想象的交互行为。在分散式系统中，分布式计算架构应该使得主机之间达成状态共识。鉴于复杂网络和恶意节点的存在，应该定义容错协议和共识机制，以实现可靠的数据传输和事务协商系统[6]。

PoW(Proof of Work,工作证明)是最初用来解决分布式系统中共识问题的方案。PoW 是基于算力的共识机制。加密货币以区块链为基础，区块链需要使用哈希函数来验证数据[7]。每个矿工解决问题的能力完全取决于他们的计算能力[8]。具体而言，分散在世界各地的主机互相竞争以找出可与原始打包数据匹配的随机数。在一个随机数被某个主机发现之后，其将与数据和哈希值一起打包到块中，然后被广播到世界各地的主机。在被大多数节点确认并认可后，矿工可以获得该块的打包权作为奖励。鉴于摩尔定律带来的性能增长，寻找随机数的难度通常会随着竞争中计算能力的提高而增加，以维持其合理的运行速度[9]。但这寻找这些随机数并无实际意义，耗费大量的资源和能源[10]，导致交易费用不断升高，却无益于提高交易速度[11]。除此之外，持币者无法参与任何决策，决策权集中在少数几个矿池手中，与去中心化理念背道而驰[12]。以以太坊为例，在以太坊区块链上进行的交易涉及的费用最终都以以太币（Ether）来结算。每笔交易必须指定一定数量的“Gas”，以及支付每单元 Gas 所需的费用[13]。在交易执行之前，将从交易发起人的账户中扣除以 Gas 价格计数的以太币。事务执行期间的所有操作（包括数据库读写，消息发送和计算）都会消耗一定量的 Gas。虽然在以太坊的设计中，每笔交易需要支付的 Gas 是固定的，但每个 Gas 单位的费用仍由用户动态设计[14]。同时，支付的交易费用越高，节点就更有积极性来打包和处理这笔交易。目前，为了进行最简单的以太转移交易，应支付 0.1 以太币作为交易费。这使得少量的以太币交易无法进行。即使在执行一些复杂的智能合约时，要支付的交易费已经超过交易本身[15]。遗憾的是，尽管付出了极为高昂的代价，基于 PoW 的区块链网络性能仍远不能满足需求。以目前最被看好的以太坊为例，以太坊网络平均每秒仅能处理 10 笔交易。这种交易速度远远无法满足现代互联网应用的要求[16]。

鉴于此，研究人员提出了一些 PoW 的替代方案。PoS(Proof of Stake,股权证明)是基于链上货币计价的共识机制[17]。PoS 用持币取代计算能力[18]。然而，采矿的难度与矿工的币天有关，PoS 鼓励用户囤积币天，这

会降低货币的流动性[19]。已有的 PoS 解决方案主要分为四种：基于拜占庭容错的 PoS，基于链的 PoS，PoW/PoS 混合,基于授权的 PoS(DPoS)。基于拜占庭容错的 PoS 容错率较低，故障节点和恶意节点不超过矿工总数的 1/3，且为了达到较短的确认时间限制了验证者的数量。基于链的 PoS 本质上是 PoW 的一个货币计价改编。PoW/PoS 混合只是一个过渡方案，最终仍会被一个纯粹的 PoS 机制所取代。基于授权的 PoS 通过选举代理人达成共识，牺牲了去中心化的概念，不适合公有链。

同时，需要关注区块链的侧链与其安全问题。侧链是基于主区块链生成的分叉，通常旨在实现某些特定目的或功能。在以太坊诞生之前，分叉通常是以硬分叉的方式进行的。以比特币为例，熟悉的比特币通常是指比特币核心（BTC）。从技术上讲，与其他新兴数字货币相比，BTC 并不具备竞争力。它的区块大小只有 1MB，而交易延迟和交易费用会越来越高[20]。在 BTC 问题上，包括 BitcoinABC，Bitcoin Unlimited 和 BitcoinXT 在内的一些团队共同开发了 Bitcoin Cash（也称为 BCH 或 BCC）。当比特币区块链长达到 478,559 时，即会自动分叉，这成为了 BTC 的第一个硬分叉货币。BCH/BCC 带来了各种升级功能，包括 8M 容量的大块，支持双向重放保护等。 2017 年 11 月 13 日，由于紧急难度调整机制（EDA）不稳定，BCH 再次进行硬分叉并引入了 DAA 难度调整机制[21]。以太坊利用智能合约的功能来设计 ERC20 令牌规范。以太坊的令牌基本上是基于在主区块链中运行的智能合约。令牌侧链在虚拟状态下运行智能合约，这与 BTC 的硬分叉不同，因为它通常意味着新硬币诞生时具有独立的区块链和节点网络。以太坊派生令牌侧链更多地用于为某些特定服务发放令牌。对于简单的令牌发放，以太坊的智能合约简单而有效。但对于一些更复杂的应用，在主区块链中运行智能合约将导致严重的安全漏洞。由于智能合约和主区块链形式的侧链不像 BTC 侧链那样被强制隔离，因此侧链设计中的缺陷可能直接影响主链[22]。导致以太坊重大损失的 DAO 事件就是一个典型的例子。DAO 指分布式自治组织(Distributed Autonomous Organization)[23]。它旨在编写用于组织规则和决策组织的代码，并消除书面文档的需求并减少管理人员，从而创建分散的管理架构[24]。DAO 在建立智能合约后开始融资，之后持币人可依赖其所有权影响 DAO 的发展。由于其侧链的安全漏洞，DAO 曾遭遇过 5500 万美元的巨大损失。

本文提出了一种新的 PoS 方案：基于竞争的 PoS（CPoS）。基于锻造委员会机制，CPoS 可以解决传统 PoS 机制中富人越来越富裕的问题，提高系统的生产率和流动性。同时基于侧链的产生提出了一种平行链架构，提升了主链和侧链的运行效率以及安全性。

## 1 基于竞争的股权证明(CPoS)共识机制

Gaia 总计产生 10,000 亿 Gaia 币。在创世区块中生成并且分配 9,000 亿 Gaia 币，1,000 亿 Gaia 币作为锻造奖励预计 10 年发放完毕。短期而言，锻造者的奖励主要来源于锻造奖励和交易手续费。随着社区的发展，锻造奖励会逐渐减少直至最终取消，交易手续费会成为锻造者最主要的收益来源。之所以在项目早期设置锻造奖励，是为了防止因为前期交易过少，而导致的诚实锻造者消极出块，使得安全性降低。

### 1.1 锻造委员会

锻造委员会是一个基础底层模块，其中包括一个拥有创建区块权利的地址的集合。集合中的每一个地址都是一个锻造委员，每个锻造委员都有机会创建区块。成功锻造一个区块将会获得该区块中的所有交易费。

所有地址都可以申请加入锻造委员会，在加入锻造委员会时，会提交一个 bls 加密算法的公钥，自己保留私钥，公钥会用来验证该锻造委员产生的随机数。锻造委员会收取最少 100,000Gaia 币作为保证金，保证金和锻造者的权益值相关，如果锻造者故意作恶，保证金会被罚没。收取保证金是为了防止节点作恶，最低限度的设置是为了防止微资金地址加入锻造委员会。Gaia 认为保证金较高的地址，作恶的可能性更小。

锻造委员的职责是创建新的区块。锻造委员可以主动申请退出锻造委员会,该地址的保证金会被扣留 400,000 个区块高度。扣留保证金是一种惩罚机制，用于惩罚不能正常完成其职责的锻造委员。之所以不设置退出机制，是为了防止恶意节点，将大部分节点剔除出锻造委员会，实施长程攻击。

### 1.2 锻造组

所有人都可以查询到每个锻造委员的当前投票权。锻造委员首次将被按照地址的后 8-bit 进行分组，后两位地址即是分组编号，分组编号相同的为同一组，总共 16*16=256 个组。设当前区块高度为 H，则 H%256=N，N 号锻造组负责本轮的锻造。首次按照地址分组是为了让锻造委员尽量加入锻造委员较少的组，使得每组委员数不会相差过大。由于单一用户可以拥有无限个地址，所以即使只有一个用户也能够占满 256 个分组。

### 1.3 投票权计算

锻造委员的投票权和保证金的数值相关，设一个锻造委员缴纳的保证金为 a 个 Gaia 币，则初始投票权 K 为 $\log_{10}(a*0.01)*p$。p 为一个在[1,4]之间的随机值，在锻造委员初次获得投票权时生成，且在投票权再次初始化时重新计算。一个新申请加入的锻造委员不会立即获得投票权，需要等待 256000 个区块高度以后才会获得投票权。之后每隔 256 个区块高度(即一轮)投票权一次性增加 K。随着区块高度的增加，投票权不断累积，投票权最多增加 2560 个区块高度，即初始投票权 K 的 10 倍，之后不再增加。用投票权进行委员排序，如果有多个投票权最高的锻造委员，则比较锻造委员的地址值，地址值更大的排名更高。在当前分组中排名前 10 的锻造委员会获得额外的排名投票权，设排名为 R,则排名投票权为 $2^{(11-R)}$。总投票权为累积投票权与排名投票权之和。

每个区块都会生成一个随机值，区块高度 m 对应的随机值为 $R_{(m)}$， $H_{(x,y,z)}$ 为一个 hash 函数，让入参被唯一映射到一个[1,4]之间的值。设锻造委员地址为 l，则 $p=H_{(R(m),m,l)}$。如果一个锻造委员成功将区块添加到了区块链，则该锻造委员和当前分组中投票权更高的其他锻造委员的投票权都会被重置为初始投票权（p 值会重新计算），且都会被重新分组。分组依据为委员地址、当前区块高度、当前随机值三者 hash 的最后 8-bit 的值。之后随着区块高度的增加，投票权不断累积，直到最高为初始投票权 K 的 10 倍。之所以需要不断的更新分组和更新初始投票权，是为了防止恶意节点串通控制几个相连的节点进行双花攻击。

降低保证金数值和投票权的正相关程度是为了避免大额地址拥有过高的投票权。累计投票权随着区块高度增加而增加，是为了激励小额锻造委员也有机会成为主锻造委员。设置 10 倍的上限是为了控制小额锻造委员的数量，保证金过少的锻造委员在可信度和稳定性方面不如缴纳了大额保证金的锻造委员。排名投票权是为了降低被恶意委员联合攻击的风险。

### 1.4 主锻造委员

当前锻造组中投票权最高的锻造委员当选为主锻造委员，后续锻造组都倾向于验证和认同主锻造委员锻造的区块。本组内所有的锻造委员都可以创建区块并且全网广播，其他节点收到区块后将进行验证。第 N 个区块的投票权等于主锻造委员在锻造该区块时的总投票权，区块链的总投票权为单个区块的总投票权之和。因为主锻造者的投票权极高，所以区块将会在极短的区块高度就达成共识，分叉将迅速被消除。

为了优化不必要的计算和网络广播和建设分叉，如果主锻造委员在上一个区块产生 N 秒之后仍然没有全网发送新区块，则当前锻造组中投票权第 2,3 高的锻造委员则会立即锻造区块并广播。如果再过 1S 仍未产生区块，则投票权第 4,5 高的锻造委员则会立即锻造区块并广播。以此类推，直到锻造出新的区块。这个策略可以降低分叉的可能性，同时兼顾区块创建速度。

### 1.5 锻造过程

为了便于理解，此处只描述最高投票权锻造者和次高投票权锻造者的锻造过程和选择策略。

在区块高度 255,999,所有组编号为 0 的锻造委员均有机会创建 256,000 号区块，其他分组无法创建区块。R1 地址为 0xdab12...00,缴纳了 10,000Gaia 币保证金,随机值 P=1.5，总共累计了 2,304 个区块高度(即 9 轮)，累积投票权为 27，排名投票权为 1024，总投票权为 1051，设其创建的区块为 B1。R2 地址为 0xd12e9...00,缴纳了 1,000,000,000Gaia 币保证金,随机值 P=1,总共累计了 768 个区块高度(即 3 轮)，累积投票权为 21，排名投票权为 512，总投票权为 533，设其创建的区块为 B2。虽然 R2 缴纳的保证金为 R1 的 100,000 倍，但是 R1

却获得了更高的投票权,避免了富者对投票权的垄断。所有组编号为 0 的锻造委员都可以将自己创建的 256,000 号区块进行全网广播。只有组编号为 1 的锻造委员们可以继续创建 256,001 号区块。由于总计投票权最高的链会成为主链，组编号为 1 的锻造委员们在理智的情况下都会在 B1 的基础上继续创建 256,001 号区块。

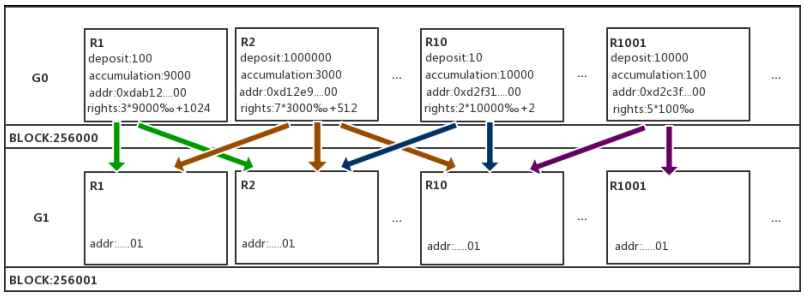


Fig.1 Act of a Forging Group in Ideal Environment.

图 1 理想情况下的锻造组行为

现实世界的网络环境极为复杂，投票权最高的投票委员有可能没有向下一个锻造分组发生新的 256,000 号区块。G1 分组锻造委员的最优策略是：等待 G0 分组 R1 一段时间，如果仍无响应，则接受 R2 创建的区块。愿意等待的时间和 G1 分组锻造委员自身的总投票权相关。自身总投票权越低的节点愿意等待的时间越长，因为这是在 256,001 区块高度打败同组更高投票权投票委员的唯一方法。G1 分组中 R1 会等待一段相对较短的时间，然后接受 G0 分组 R2 创建的区块。因为自身投票权最高，即使接受了投票权较低的区块，仍然有较大机会胜出。

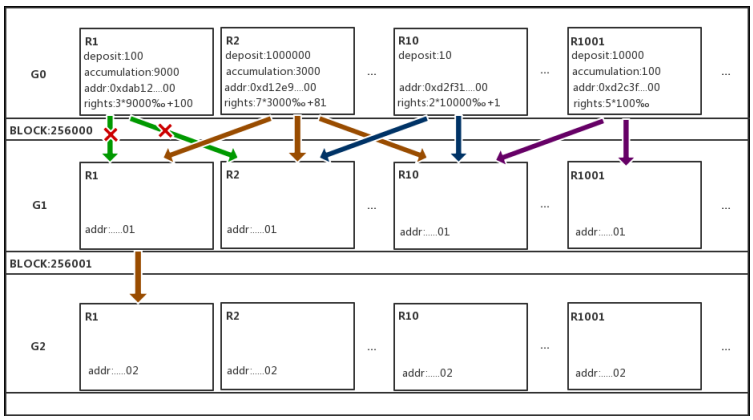


Fig.2 Act of a Forging Group When Broadcast is not Accepted.

图 2 广播未被接受时的锻造组行为

由于总投票权和分组、保证金、累积区块高度、排名投票权、地址五者相关，使得锻造委员难于串通作弊，但不排除由于网络原因或者其他未知原因导致的，最高投票权锻造者接受了上一个区块的次高投票权的锻造者创建的区块，如图所示。

G1 分组中的 R1 接受了 G0 分组 R2 创建的 256,000 号区块，而 G1 分组中的 R2 接受了 G0 分组 R1 创建的 256,000 号区块。G1 分组中的 R1 和 R2 都会向 G2 分组的锻造者提交区块。G2 分组中的 R1 选择总投票权最高的链继续锻造。

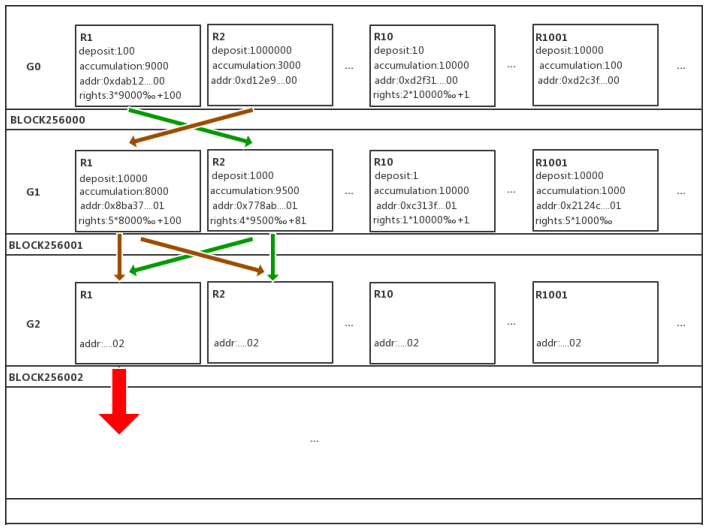


Fig.3　The second highest voting forge created a new block.

图 3　次高投票权的锻造者创建新区块

基于 CPoS 机制，分叉总是能在较短的区块高度被消除，如图所示。在区块高度 256,000 和区块高度 256,001 产生了分叉，而 G2 分组的最高投票权锻造者选择了其中一条链，该链的总投票权显著增大，有极高概率胜出。G3 分组的锻造者会基于该链继续创建区块。

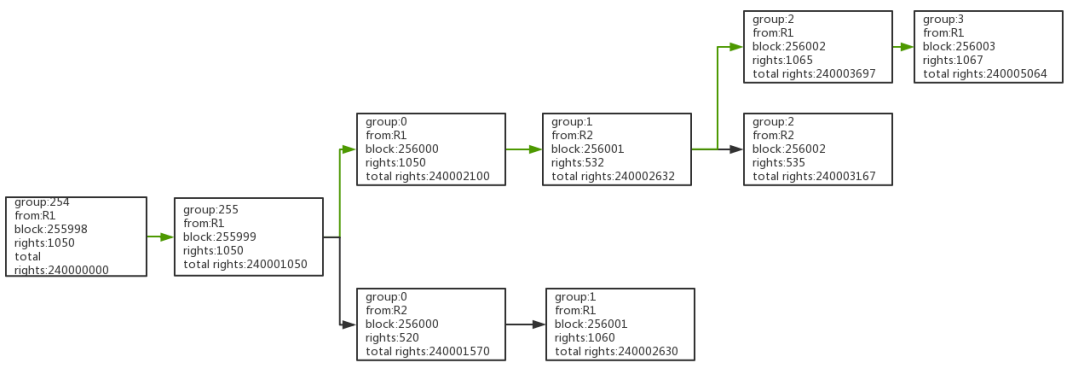


Fig.4　Fork are Removed.

图 4　分叉被消除

### 1.6　平行链

为了提高区块链的可扩展性和分散主链的网络压力，Gaia 设计了平行链架构。平行链由主链和侧链两部分组成。侧链代码和主链相同，使用相同的共识算法（CPoS），有自己独立的区块链。和传统的 PoW 共识机制不同，PoS 占用的系统资源较少，使得侧链和主链可以共享网络节点资源，侧链从创建初就获得了较高的安全性。同时，侧链也能吸引更多的节点加入网络，主链的安全性也会得到加强。

平行链支持把指定的侧链作为主链，继续分叉成新的侧链，最后形成一个侧链树，如图 5 所示。

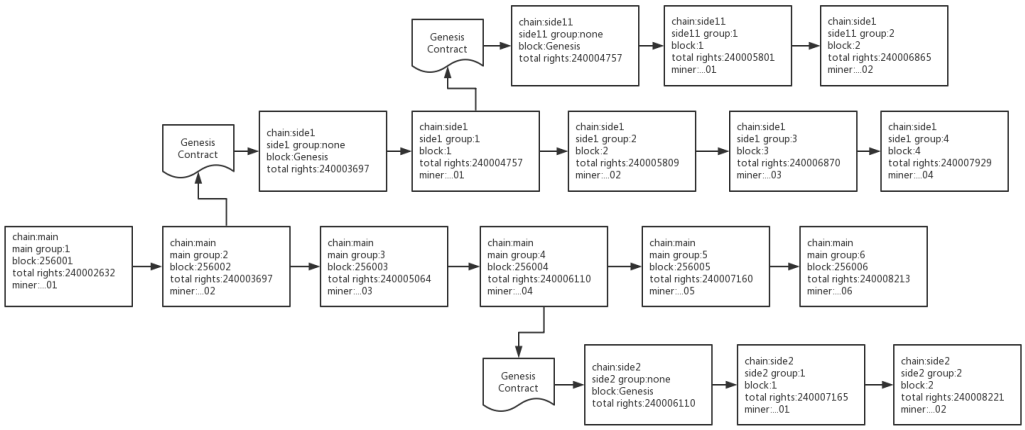


Fig.5 sidechains fork.

图 5 侧链分叉

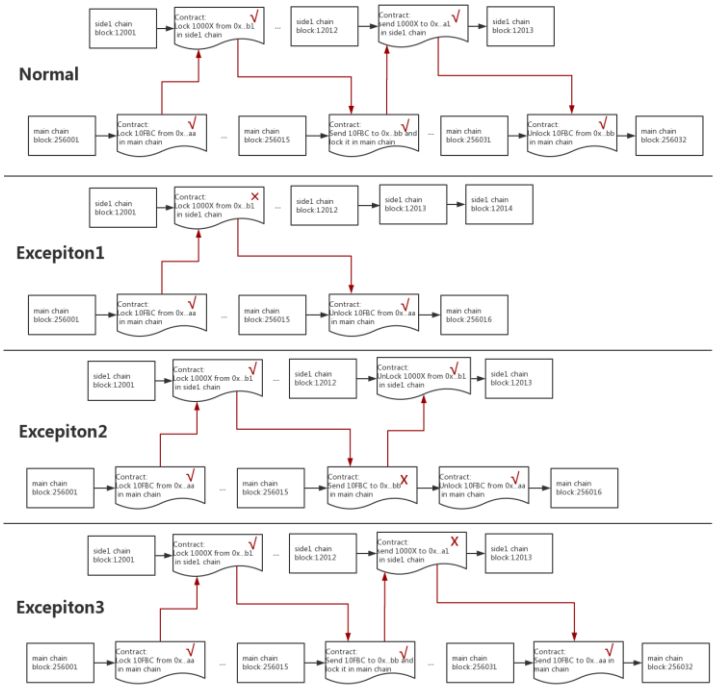


Fig.6 Cross-chain transaction specification.

图 6 跨链事务规范

在每条链上，智能合约或交易都是一个完整事务。由于侧链和主链处在不同的节点网络中，各自区块链的生成者、速度和规则都不一样，无法完成一个完整事务。因此我们制定了一个跨链事务规范来保证侧链和主链可以运行一个完整事务，如图 6 所示。

主链与侧链之间是互惠互利的关系，主链为侧链提供基础设施，侧链则可以为主链补充更多的节点和开发者，以壮大整个系统。侧链的开发者不需要提供机器，可以利用已经存在的主链节点，只需要节点拥有该

货币。另外，主链和侧链可以用系统提供的跨链事务规范进行价值交换，相当于为侧链的资产提供了一种价值的媒介。

## 2 安全性能分析

目前互联网安全中，区块链的攻击大多数分为贿赂攻击(The Bribing Attack)、自私采矿攻击(Selfish Mining Attack)，日蚀攻击(EclipseAttack)、扣块攻击(Block withholding attack)、双花攻击(Double Spending Attack)这五种常见的攻击方式。

(1) 贿赂攻击，指一个区块链协议以外的贿赂者通过收买现有节点（代币或者算力），以攻击原有区块链的恶意行为。CPoS 引入了锻造委员会机制中的保证金和惩罚措施，较好地解决了这个问题。保证金和锻造者的投票权相关，贿赂者的恶意行为会导致保证金罚没的损失。

(2) 自私采矿攻击，是指在个人算力的提高陷入瓶颈时，矿池作为个体矿工的组合进行挖矿活动。而矿池在发现块时不进行发布，从而创建一个可供自身私下挖掘而诚实矿工不知情的私人分叉，在此种情况下继续进行挖掘，当私人分叉较公共链更长时进行发布，诚实矿工保有的公共链将被丢弃。这种攻击在 PoW 共识机制中较为常见，PoS 机制中摒弃了对算力的极度追求，从而使得矿池的自私采矿攻击行为失效。

(3) 日蚀攻击，攻击者不断向受害节点发出请求, 并且发送大量无用的信息, 使得受害节点所有信息的接收与发送在一个隔离的网络中被恶意节点控制，从而阻止其他合法节点的连接请求。以太坊已在 geth1.8.0 修复此问题，通过最大化其作恶代价，使得攻击一个节点需要上千个节点进行操作。

(4) 扣块攻击为双花攻击的变种，本文中将其作为双花攻击的一种进行分析。

(5) 双花攻击为如下描述的主要攻击模式。如果用户首先启动第一笔交易，而在确认第一笔交易之前进行相互矛盾的第二笔交易，这意味着此时第一笔交易尚未打包到块中。然后，欺诈者故意将第一笔交易广播到网络的一半，并将第二笔交易分别广播到网络的另一半。巧合的是，网络两侧的两名矿工同时获得了簿记权，分别构建他们的块并将其块发布给网络中的每个人。这时，原来的统一分类账发生了分叉。

由于 PoS 共识机制本身对前三种区块链攻击行为抵抗性较好，而对双花攻击与其变种抵抗性较差，因此 CPoS 着重设计了对双花攻击的抵抗机制，如下所述。

在双花攻击中，欺诈者将采取以下步骤来最大化其非法利益。如果其中一个分叉获得批准，这意味着相应的交易由区块链确认，并且欺诈者获得加密货币购买的货物，他们立即作为矿工参与另一个分支机构的下一个记账权的竞争。如果他们在第二个分支上构建一个新的区块，并使第二个分支的总权限高于第一个分支，则第二个分支将被批准为主链，而第一个分支将被放弃。但此交易的货物已经交付给欺诈者。因此，双花攻击是成功的。

为防止这种攻击，应审查锻造委员会的规则以加强该系统。锻造成员的投票权与持币的价值有关。成员的初始投票权可用公式（1）表示：

$$K = p \times [\log_{10} d - 2] \tag{1}$$

其中 d 代表存款金额，p 是 1 至 4 之间的随机值，当锻造成员首次获得投票权时产生该随机值，并且当投票权再次初始化时将重新计算。新申请的锻造成员不会立即获得投票权，在获得投票权之前需要等待 256,000 个街区。之后，该成员的投票权在每 256 个块高度（即，一个回合）之后增加 K,但是，为了降低恶意成员共同攻击的风险，投票权将在 2,560 个区块高度后停止增加。因此，总投票权可以通过公式（2）评估：

$$T = p \times [\log_{10} d - 2] \times acc \tag{2}$$

其中 acc 代表最高为 10 的轮次的高度积累。然后根据他们的投票权 T 对锻造成员进行排名，并且一组中

的前 10 名成员将获得额外的排名投票权 R，其可以通过公式（3）计算：

$$R=2^{11-r} \tag{3}$$

其中 r 代表锻造成员的等级。因此，前十名成员的总投票权可以表示为：

$$T_r = p\times[\log_{10} d-2]\times acc+2^{11-r} \tag{4}$$

为了执行双花攻击，欺诈者应该使得在总投票权中排名第二的区块的总投票权超过区块链分叉之后的第一个。为了实现这一目标，欺诈者应该使他的 T 超过第一和第二等级成员之间的附加投票权的差 $R_1$-$R_2$。因此，我们可以得到不等式（4）：

$$p\times[\log_{10} d-2] > R_1 - R_2 = 512 \tag{5}$$

解不等式，我们可以得到当随机值 p 的最大值为 4 时，持币 d 应不小于 $10^{14.8}$，而当 p 得到其最小值为 1 时，它将不小于 $10^{53.2}$。因此，要实现这种攻击，应该至少支付 $10^{14.8}$ 作为持币，这几乎是不可能的。因此，在 Gaia 系统中实施双花攻击极其困难。

## 3 实验及结果

使用 rust 语言实现了一个 Gaia 的原型。使用了 50 台商用 PC 机(CPU:Intel i5-7500;内存:DDR4 2666 8g)。

每台 PC 机启动 1-30 个不等的节点，每个节点可同时使用 1-100 个不同的地址，用以模拟最多 1,500 个节点，150,000 个地址的情况。每个节点分配 20Mbps 的内网带宽，为了模拟真实的网络环境，每个节点设置了 200ms 的信息传输延迟,每个节点最多链接 125 个其他节点。创世区块中设置的默认出块速度为 1000ms。

图 7(a)中模拟了每个节点使用 2 个区块地址的情况下，用户从发出交易到获得第一次确认所需的平均时间和区块的平均出块速度。图 7(b)中模拟了 1,500 个节点不同数量区块地址的情况下，用户从发出交易到获得第一次确认所需的平均时间和区块的平均出块速度。图 7(c)中模拟了 1,500 个节点，150,000 地址，不同交易数量情况下，用户从发出交易到获得第一次确认所需的平均时间和区块的平均出块速度。

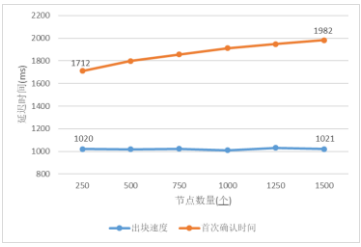


Fig. 7(a)

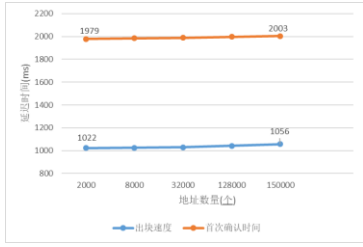


Fig. 7(b)

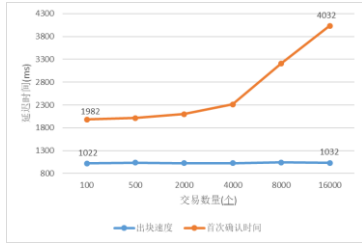


Fig. 7(c)

Fig.7 Transaction confirmation time and block speed

图 7 交易确认时间及出块速度

由图 7 结果中可得，当发出交易的节点数量由 250 个增加至 1500 个时，首次确认时间的延迟时间仅从 1712ms 提升至 1982ms，表明节点数目的增多对系统运作情况影响较小；当发出交易地址数目从 2000 个增加至 150000 个时，首次确认时间延迟几乎不变，表明 Gaia 系统可支持大批地址数目的交易请求；当用户发出交易数目从 100 个增加至 16000 个时，延迟时间先是缓慢增加，在交易数目达到 4000 个之后增加较快，由 4000 交易量时的 2300ms 延迟提升至 16000 交易量时的 4032ms 延迟。表明在 1,500 个节点，150,000 地址条件下，同时 4000 个交易数目为 Gaia 系统良好程度支持的限额，比起以太坊系统提升较大。而对于节点数量、地址数量、交易数量，出块速度的延迟都较低，说明 Gaia 系统可承载较大的用户使用量下的区块链计算任务。

## 4 结论

本文基于锻造委员会和锻造组系统的新架构设计，提出了一种基于竞争的股权证明(CPoS)共识机制，并在此基础上实现了相应的区块链系统 Gaia。经原型机实验分析，该机制可在较小的延迟内快速地完成出块和交易活动，较好解决了以往共识机制资源浪费、交易速度慢、流动性低等问题。同时，Gaia 系统针对分叉和安全问题设计了平行链架构和抗双花攻击机制，保障了区块链系统的有效运行。

**References**:


[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[2] Ron D, Shamir A. Quantitative Analysis of the Full Bitcoin Transaction Graph[M]// Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2013:6-24.

[3] V. Buterin et al., “Ethereum white paper,” GitHub repository, 2013.

[4] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, pp. 1–32, 2014.

[5] V. Buterin et al., “A next-generation smart contract and decentralized application platform,” white paper, 2014.

[6] Vukolić M. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication[M]// Open Problems in Network Security. Springer International Publishing, 2015.

[7] Biryukov A, Pustogarov I. Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay[M]// Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015:445-455

[8] Aste T. The Fair Cost of Bitcoin Proof of Work[J]. Social Science Electronic Publishing, 2016

[9] Shi N. A new proof-of-work mechanism for bitcoin[J]. Financial Innovation, 2016, 2(1):31

[10] Gilboa A, Shteingart Z, Levin K, et al. METHOD AND SYSTEM FOR REDUCING POWER CONSUMPTION IN BITCOIN MINING VIA DATA INPUT HOPPING:, US20170300875[P]. 2017

[11] Gervais A, Karame G O, Glykantzis V, et al. On the Security and Performance of Proof of Work Blockchains[C]// ACM Sigsac Conference on Computer and Communications Security. ACM, 2016:3-16

[12] Natoli C, Gramoli V. The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example[J]. 2016

[13] Chen T, Li X, Wang Y, et al. An Adaptive Gas Cost Mechanism for Ethereum to Defend Against Under-Priced DoS Attacks[J]. 2017:3-24

[14] Kim T. On the transaction cost of Bitcoin[J]. Finance Research Letters, 2017, 23

[15] Berg C. Populism and Democracy: A Transaction Cost Diagnosis and a Cryptodemocracy Treatment[J]. Social Science Electronic Publishing, 2017

[16] O'Dwyer K J, Malone D. Bitcoin mining and its energy footprint[C]// Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies. IET, 2014:280-285

[17] Rosenfeld M, Rosenfeld M, Rosenfeld M, et al. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]y[J]. Acm Sigmetrics Performance Evaluation Review, 2014, 42(3):34-37

[18] T. Duong, L. Fan, and H.-S. Zhou, “2-hop blockchain: Combining proof-of-work and proof-of-stake securely,” Cryptology ePrint Archive, Report 2016/716, 2016. https://eprint. iacr. org/2016/716, Tech. Rep., 2016

[19] King S, Nadal S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake[J]. 2012

[20] Pilkington M. Blockchain Technology: Principles and Applications[J]. Social Science Electronic Publishing, 2015

[21] Back A, Corallo M, Dashjr L, et al. Enabling Blockchain Innovations with Pegged Sidechains[J]. 2014

[22] Y. Omran, M. Henke, R. Heines, and E. Hofmann, “Blockchain-driven supply chain finance: Towards a conceptual framework from a buyer perspective,” 2017

[23] Swan M. Blockchain Thinking : The Brain as a Decentralized Autonomous Corporation [Commentary][J]. IEEE Technology & Society Magazine, 2015, 34(4):41-52

[24] Norta A. Creation of Smart-Contracting Collaborations for Decentralized Autonomous Organizations[C]// International Conference on Business Informatics Research. Springer, Cham, 2015:3-17