ThunderCore（TT链）白皮书

2019年10月28日

目录

第一部分：ThunderCore简介

ThunderCore（TT链） 是区块链公链，它是公开、去中心化、与以太坊虚拟机（EVM）兼容的，并且采用全球领先的权益证明共识机制（PoS），其安全性經过嚴格驗證。

ThunderCore 於2018年1月成立於美國矽谷，志在结合頂尖的学术研究及区块链技术专家，以大规模共识机制，打造出最快速、高安全、强扩展性的区块链公链。

区块链是一系列带有时间戳和具备不可窜改特性的记录，由分布式且去中心化的服务器（也称“节点”）运作。ThunderCore对所有用户开放，允许全球参与者参加保护及验证这些记录。

ThunderCore不仅是個记录交易的平台，还可执行“智能合约”。智能合约是以客观和公平的逻辑直接管控各方之间资产转移及內容分享的计算机程序。以太坊是最受欢迎的智能合约执行平台，而ThunderCore与以太坊完全兼容，部署在以太坊上的合约或应用，可仅在数分钟内部署在ThunderCore上。

这个简介的第一部分说明为什么需要区块链，什么是区块链，以及ThunderCore创新之处。第二部分概述ThunderCore协议的技术框架；第三部分则阐述ThunderCore未来的发展方向。

为什么需要区块链？

任何两个或多个实体之间的互动都需要信任，信任是依靠他人承诺并采取行动的基石。但是，信任和承诺有可能易变，造成当今社会和商业中的“信任成本”非常昂贵。然而，信任问题可以通过现代技术来解决，而不再需要个人或机构背书。信任可由代码提供保证，通过运用公私密钥对加密技术和创新的奖惩机制，新协议可以让个人和其他实体信任记录的可靠性，而无需依赖第三方监督者。人为因素有太多不确定性，原本只有通过昂贵且复杂的法律条款，甚至要通过体面的伪装才能强制执行。如今有了区块链的智能协议，上述人为因素就可以被排除，对各方而言，区块链的操作变得更高效，更可靠，更可预测，成本也更低。

初始动力

众多行业正开始认识区块链的功能和优点，其实金融行业早已关注区块链。想象一下，一个全球性去中心化的金融系统，没有边界和中介机构，而系统中的合约又是不可窜改的，全部由代码完成，那是多便捷啊！

举例来说目前全球约有17亿人口没有机会使用基本的理财产品，这极大地限制了他们选择投资和获得投资的机会。然而，由于区块链使用方便，费用价廉，耗能相当低，随着智能手机和数字素养的普及和发展，此前从未使用过理财产品的人，现在可以轻松使用区块链理财了。

深度应用

区块链从根本上改变了关于所有权、可靠性、协作和信任的设想。区块链的运用极为广泛，我们现在甚至无法想象它未来影响我们生活的深度和广度，但区块链已经改变和解决许多现有的问题，它的潜力已显而易见。

- **反欺诈**：由于区块链记录不可窜改，且永久存在，因此区块链技术可提高审计效率，降低审计成本，简单直接地解决欺诈问题。

- **众筹**：已有无数的成功项目运用区块链技术进行公开和匿名的众筹。区块链平台能处理众筹的款项，投资者则化资产为代币。

- **游戏**：从移动端休闲游戏到骰子游戏，从纸牌游戏到竞猜或桥牌拍卖游戏，都能从区块链上运作透明，成本低廉的智能合约中受益。

- **治理：**无论是私有或公共组织的章程，都可用区块链与智能合约来实现。用智能合约的代码规范及约束组织成员的行为举止。智能合约直接从利益相关者那里收集选票并执行通过的议案；智能合约同时自动执行和验证资金或资产的收支，整个过程无需任何人为的信任操作。公共机构还可以利用区块链信息不可窜改的特性，让投票流程变得更公开、安全、完整、透明。所有信息易于验证审核，无法被窜改。

- **所有权**：使用区块链解决方案，会使无论是现实世界或数字世界所持有的资产管理变得更简单，更便宜，更可信赖。

- **个人数据所有权**：使用区块链密钥共享技术，可以更安全、更完整地管理互联网浏览和其他数字浏览的历史数据。 例如，医疗记录可以存储在链上，并且可以通过私钥随时查看。 这些记录是不可窜改的，从而改善医生的工作和患者的医护质量。

事实上，区块链技术具有巨大的潜力，目前开发人员对它的挖掘才刚刚开始。我们现在可以通过全新的方式来存储价值，自动化流程并解决信任难题，且成本很低。区块链的前途无限，仍然还有大量工作和运用有待开发。

网络访问、电子通讯、个人计算设备等市场已成熟并饱和；目前，已有不计其数的开发人员、从业人员和用户投入区块链行业，我们相信，未来几年，区块链创新将迎来爆炸式增长，这将是我们这一代人从未见过的情景。区块链时代已经到来。

区块链是什么？

区块链是一连串带有时间戳的信息记录，这些记录由分布式服务器（又叫节点）处理并确认，它的每个块（block）记录了使用者的交易情形，又储存了前一块的稽核代吗，串成一条无法窜改的链。「共识协议」是区块链技术的核心，指参与此网络的每一台电脑一致同意链中资料内容的方法，也就是规定了节点网络如何通信以及如何将新块添加到链中。 当然，区块链协议种类繁多，每种协议都有各自不同的性能和奖惩机制。 无论是哪种类型的协议，存储在区块链上的数据都具有不可变性，这个特性可作为构建新经济体系的基础。

不可变性

经过加密算法的应用，存储在区块链的数据具有不可变性，亦即链上的数据无法被窜改或删除。区块链最大的特色是，任何试图窜改之前交易纪录的动作，會造成链上紀錄的级联效应，破坏数据的一致性，立即被检验出來。

因此，区块链上的数据是不可窜改的，非常适用于透明展现银行余额、民意调查、产品产出过程认定等信息。而更先进的区块链协议，例如ThunderCore，还具有“若P则Q”的逻辑性，可以启动被称作**智能合约**的程序。 如上所述，在特定条件下，这些智能合约可以直接管控各方之间的资产转移，而无需任何第三方。 这些管控规则通过代码实现，且能取代具強制力的法律契約，因此人们常说“**代码就是法律**”。

代码开源

有些区块链协议是**无需授权的**，允许任何计算机（又叫节点）加入；有些区块链协议是**需要授权的**，设有审查机制，仅允许“经批准”的计算机加入。但是几乎所有区块链协议的代码都是开源的, 就像ThunderCore一样，这些协议正在构建新的经济体系。从本质上讲，鲁棒性强的经济体系应允许价值的自由流入和流出。

此外，区块链允许任何开发者和参与者访问、审查、使用或改善其代码，这也将反过来推动区块链的发展。这样一来，任何消费者，开发者或企业都可以使用区块链协议，在链上搭建应用，通过部署服务来增加区块链的价值。区块链代码开源尽可能地降低准入门槛，并鼓励更多新用户参与进来，从而提高区块链系统的整体价值。

去中心化

区块链网络需要计算机（又称节点）网络来支撑，这并不是因为区块链网络需要大量的运算能力；相反地，计算机数量越多，区块链就会更加去中心化，鲁棒性更强，性能也更强大，可以抵御网络中断，合谋或腐败等故障或攻击行为。

可以说，去中心化是引发区块链革命的核心价值。 一些由政府和公司主导的中心化网站，在隐私、管控、效率方面，不可避免地需付出更高成本。而现代的经济学和密码学技术使区块链能够挑战这些问题，并提供替代方案。区块链方案将全部治理权给予用户，并具备应对审查腐败和失败的能力。

ThunderCore 区块链

区块链协议在使用上遇到了一些重大的挑战，首要是“不可能三角”的难题。众所周知，区块链无法同时实现安全性，去中心化和可扩展性，必须牺牲这三者中的一个。因此许多区块链牺牲了可扩展性，接受了低吞吐量和冗长的确认时间。

ThunderCore解决了上述“不可能三角”难题，并确信我们的共识协议是最好的权益证明共识协议。ThunderCore采用的PaLa共识协议在本文第二部份详述。此协议对任何人开放，无需授权，交易处理速度达到4,000TPS以上，1-2秒内可完成交易确认。ThunderCore作为一个无需授权的公链，ThunderCore共识协议允许任何代币持有者成为提案人（proposer）或投票者（voter），保障ThunderCore的安全性和去中心化。

无需授权

如上所述，区块链分为需要授权的和无需授权的，其中无需授权是指所有人可参与，也称公开性。ThunderCore坚信，无需授权是让区块链发挥最大价值的最佳方式。

区块链也被看作是创新的，基于科技的社会经济系统。因此ThunderCore坚信无需授权的系统是实现区块链真正价值的唯一方式。一个人是否能从科技进步带来的创新服务与金融工具获益，不该由任何把关者审查。此外，区块链作为一个价值转移的平台，很容易推论出：开放性是确保区块链稳健增长的基本原则。提高去中心程度，区块链系统将会得到更好的保护。ThunderCore 借由部署一个无需授权的区块链网络， 提高了去中心化程度，从而强化了整体区块链网络的安全性。

与以太坊虚拟机兼容

我们在设计ThunderCore时，已有近200,000名开发人员具有利用以太坊开发应用的经验，这是一个丰富而无法忽视的人才库。因此，为了充分利用这个人才库，ThunderCore的设计与以太坊虚拟机（EVM）完全兼容，以便开发人员仅在几分钟内，便可将去中心化应用程序（DApp）迁移到ThunderCore上，且性能、体验和可负担性都得以巨量提升。

不出所料，ThunderCore主网上线两周内，就有多个开发团队把他们在以太坊上的游戏迁移到ThunderCore上。由于ThunderCore的高效和高吞吐量，与以太坊同类游戏相比，这些被迁移到ThunderCore上的游戏迅速吸引到更多交易和玩家加入。

强扩展和高效率的共识

ThunderCore的权益证明共识机制依靠PaLa共识协议来推动。区块链的每个块包含了多笔使用者的交易纪录，又储存了前一块的稽核码，串成一条无法窜改的链。共识是指参与此网络的计算机一致同意链中资料内容的过程；此过程是任何区块链协议的核心，与其他同等级共识协议相比，PaLa共识协议是性能最先进，最高效和最简易的，其安全性经过严格验证。PaLa共识协议技术水平之高，使得ThunderCore成为强扩展，高效率的公链。

本文第二部分将会详细介绍ThunderCore技术相关内容，适合有技术背景或有兴趣的读者阅读。

第二部分：ThunderCore技术概览

比特币的迅猛发展也引起了人们对古典分布式拜占庭容错（BFT）共识协议的关注。这些协议提供了更高的性能、最终确定性，及解决当前工作量证明（PoW）区块链的扩展性问题和耗能问题的可能方向，但这些古典共识协议同时需更复杂的机制；如何利用古典协议同时实现无需授权参与网络又是另一挑战。

ThunderCore共识简介

ThunderCore最初是以Thunderella共识算法为基础设计的，该算法结合了需要授权的（permissioned）古典共识协议和去中心化的中本聪共识协议的优点。从那时起，我们的技术已再次有了显著发展。我们的研究团队发现了具有卓越性能的新共识机制。本文将着重介绍我们现用于ThunderCore公链的PaLa共识协议。我们的共识协议是由密码学和分布式共识研究领域的前沿研究人员开发的，并有严格的数学证明以保证该算法的一致性（consistency）和活跃性（liveness）。

古典共识算法[1]一般会依照轮次进行并最多可以容忍⅓的恶意节点。在每一轮中，一个提案人（proposer）将向由一组投票者（voters）组成的委员会（committee）提出新的区块。如果收到了至少⅔的委员会的支持票，则称之为公证（notarization），这表示有足够数量的节点已同意了区块链的某个状态。在正常运行时，这个过程是快速、高效且安全的。但是与此同时，我们也需要一种机制来确保可以在提案人宕机或作出恶意行为的情况下进行恢复。该过程称为提案人切换（proposer switch）。提案人宕机时，投票者必须就提案人宕机前最后确认的状态达成一致，这一任务先前是由提案人负责的。因此，经典的共识算法需要在一个区块上进行两次公证才能最终确定（finalize），即将该区块包含在区块链上不可改变的历史中。第一次公证用于确认状态，第二次公证用于确认足够的委员会成员已经认可了第一次公证。下面我们将介绍PaLa共识算法如何极大地简化切换机制并优化公证过程。

PaLa共识算法

PaLa是基于部分同步（partially synchronous）网络假设的区块链共识协议，最多可容忍1/3恶意节点。下面我们描述称为**Basic Pala**的协议简化版本来说明其简单且高效。 Basic Pala是理解完整版PaLa的基础。完整版PaLa将在本文后段概述。 对PaLa协议的详细信息有兴趣的读者可以查看PaLa研究论文。

设定

[1]其他古典共识算法使用不同的术语来描述此处相同或相似的概念。本白皮书中使用的术语与PaLa研究论文中使用的术语一致。

假设一个固定的由**投票者**组成的**委员会**（稍后将详述如何选择这些节点）。每个节点都维护一个**本地时期**（local epoch）计数器*e*和区块链的本地视图（view）。每个区块包含一个时期编号、一系列交易以及其父块的哈希值。一条链的时期编号定义为其最后一个块的时期编号。每个时期都有一个唯一的提案人，网络中的所有节点都知道该提案人。在此简化版本中，每个投票者也是某些时期的提案人。

每个区块进行一次共识。提案人如果有资格在当前时期做出提案，则可以提出区块。如果满足一系列条件，投票者就对该提案人提出的区块进行投票。在一个区块中获得委员会投票数的⅔就是对该区块的**公证**。如果某个区块拥有了公证证明，则该区块已**被公证（notarized）**。每个块都有一个单调递增的时期编号。如果一个时期e的区块具有一个时期e-1的父块，则该区块称为**正常块（normal block）**，否则为**超时块（timeout block）**。如果某个区块是一个经过公证的正常块的父块，则该区块已**被最终确认（finalized）**。一个已被最终确认的区块成为区块链不可变历史的一部分并且表明已达成共识。

协议

每个节点都保持其本地的区块链处于**最新（fresh）状态**。每当节点发现一条有效区块链比其当前链**更新（fresher）**，即更新的链的时期编号高于其当前链的时期编号时，它们就会切换到该更新的链。一条有效的区块链应满足以下条件：

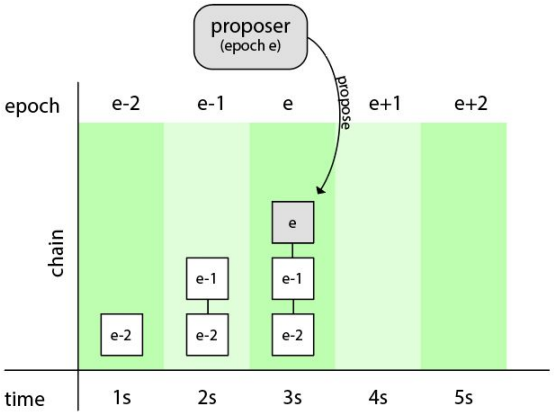
1. 所有块的时期数应严格递增
2. 区块链中的每个区块都经过公证

此外，每个节点还将执行以下操作：

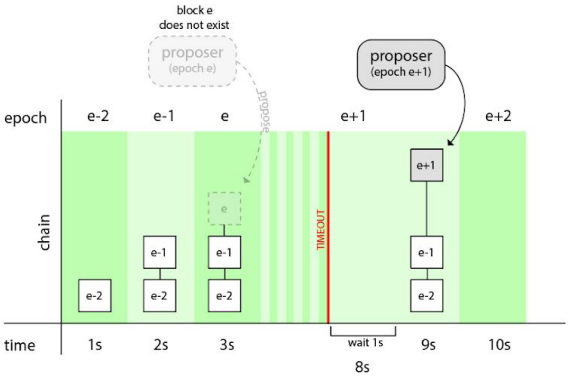
- 如果满足以下条件则将本地时期计数器增加到*e*
    - 他们当前的本地时期小于*e* 并且
        - 他们看到一条时期*e-1*的已被公证的链 或
        - 他们看到至少⅔委员会成员的有效签署的*clock(e)*消息

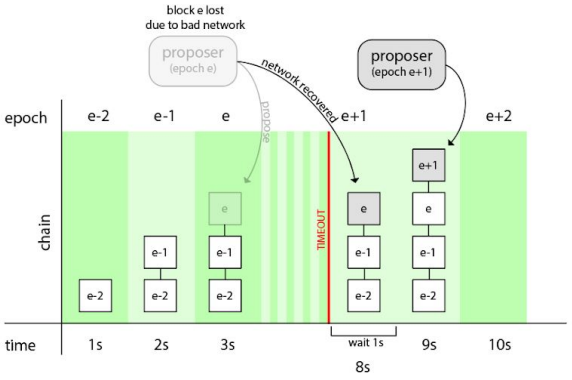
- 如果他们在时期e-1停留了足够久（一个固定数值）的时间
    - 广播*clock(e)*消息

- 如果他们是时期e的提案人
    - 如果他们当前的链以时期e-1结束，则立即为时期e提出一个新的区块以扩展自己当前的链



- 如果其当前链的时期数为e（由于超时），则等待一段固定的时间（为了收到更新的链），并为时期e提出一个新的区块以扩展自己当前的链。





- 从时期e的提案人收到时期e的区块提案后，如果满足以下条件，则签署该提案并广播签名：
  - 他们已经看到了提案的父块的公证
  - 该区块至少与时期e开始时的当前链一样新
  - 他们没有为时期e的任何其他块签名

通过这些简练的规则，PaLa共识协议可实现活跃性和一致性。PaLa协议简洁且经过严格证明。PaLa是基于部分同步网络的假设而设计的，因此从本质上是分区容忍（partition tolerant）和响应积极的（responsive）。如果存在网络分区，则活跃性只会暂时中断。当分区恢复，它将恢复进度且不会产生任何状态冲突。

委员会重新配置和双流水线PaLa

在现实中的权益证明区块链中，我们希望随着权益在系统中的易手而定期更换委员会成员。PaLa共识算法支持高速流畅的委员会切换。完整的机制在此不详述。基本思想

是，上一任委员会必须最终确认一个特殊的**重新配置区块（reconfiguration block）**后，下一任委员会才能開始運作，以确保一致连续性。

ThunderCore将部署研究论文中描述的完整PaLa协议，该协议也称为双流水线PaLa（Doubly Pipelined PaLa），它支持**流水线化提案（proposal pipeline）**功能。此版本允许共识每次前进*k*个区块（*k*是协议设置参数）。提案流水线可以实现让较新的块在较旧的块仍在进行投票时被缓存。根据我们的测试发现，当网络延迟相对于区块时间而言较高时，更高的*k*值可以提高吞吐量。

小结

从性能的角度来看，PaLa是对先前古典共识协议的一项重大改进，古典共识协议要求每个块进行两轮投票、传送 $O(n^2)$ 个消息。PaLa参考了流水线式BFT（pipelined BFT）[2]算法中第二轮投票附带在下一个区块的第一轮投票中的这一想法。当期的提案人使用BLS多重签名来收集投票并分发公证。 PaLa与轴辐式网络拓扑结构（hub and spoke network topology）结合时可以仅传送 $O(n)$ 个消息便达成共识。

Tendermint，FBFT，Casper FFG和Hotstuff等较新的BFT共识算法虽与PaLa有些类似的创新，但是都不及PaLa简练、优雅和最优化。

PaLa相较BFT共识就像Kademlia相较分布式哈希表（DHT）一样具有开创性意义

ThunderCore还致力于提供最佳的资源以帮助大家进一步了解PaLa。 PaLa共识协议的参考实现代码已经发布，其中包含完整的文档和更多教程材料。

权益证明（PoS）[3]

有了PaLa，我们有了一种可以进行可靠的委员会重新配置和提案人切换的机制。完整方案还需要一种激励相容（incentive compatible）的用于选举共识节点的权益证明（

[2] 双流水线PaLa的第一条流水线是 BFT 流水线，第二条流水线是上述的 *K* 个区块。
[3] 权益证明最初是一种中本聪共识算法，该算法使用矿工权益的哈希值代替随机数来决定区块选择的特权。更常见的是，权益证明一词是指依赖于权益抵押来选择共识的任何区块链。我们遵循这种普遍使用的术语。

PoS）设计。我们选择了一种简洁的按照会话[4]（session）进行的前*K*位投票者选举设计。每场会话持续3个小时。在每届任期中，进行成为下届任期的共识节点的竞标。

一个竞标包含以下参数

1. 权益额
2. 签名公钥
3. 奖励地址
4. 期望GAS价格
5. 拥有签名私钥的证明

在会话结束时，所有有效的竞标会被收集并按权益额大小排序。前32名成员构成下届的新委员会，新一轮会话将在PaLa重新配置区块最终确定后开始。为了限制硬盘空间的骤增和网络带宽的使用，我们将GAS价格设置为全部委员会期望GAS价格的2/3高值以保证有2/3的投票者会对设定的GAS价格或更高的价格感到满意。

提案人选举

身为完全无需许可（permissionless）的协议，我们需要一个公平的提案人选举政策。我们预期任何提案人也可以充当投票者，因为提案人的硬件要求严格高于投票者的硬件要求。因此选举中，任何投票者都可以表示是否希望成为提案者。

我们蒐集表达过愿意当提案者的委员会当选人的名单，构成提案人清单，再以权益额排序。

要成为提案人，共识节点必须在竞标中包含以下附加内容：

1. 公开URI（统一资源标志符）
2. 提案公钥
3. 自选消息

目前，提案人按权益大小进行排序并轮流提案，在每次会话中，每个提案人仅被允许提议与其权益额成正比的区块个数。因此，每个诚实且网络连接良好的提案人每届任期将至少服务一次。由于提案人强制切换的设计，即使是一个由恶意节点组成的的占多数联盟也只能在短时间内暂停活跃性或限制交易。只要保证至少有一个行为举止良好的诚实的提案人，就可以确保所有有效交易都将最终被包括在链中。

奖惩机制

本节介绍ThunderCore的权益证明奖惩制度。设计上我们希望有一个能够实现以下目标的系统：

- 激励相容性：我们的激励机制应奖励诚实和高效的参与。
- 对攻击具有经济稳健性（Economically robust）：在均衡状态下，有足够的权益保护区块链从而使攻击成本与货币的重要性成比例。

[4]一场会话，即委员会的一届任期

因此我们通过过激励措施与诱因设计来确保节点遵循规则。我们的设计为任何试图破坏一致性的拜占庭式节点带来了极高的攻击成本。对于试图破坏活跃性的故障节点或拜占庭节点将给予一定的惩罚，并且不会给予任何奖励。

奖励

ThunderCore将使用区块奖励补贴交易费以激励参与。区块奖励是从我们现有的委员会奖励池中分配的。分配区块奖励不会铸造新的代币，ThunderCore会将奖励池交给链的协定来控制。

进行分配时，提案人首先获得一部分奖励，剩余的奖励将按权益比例分配给参与投票的投票者。提案人的奖励会依照收集到的票数佔委员会全员的比例调整，以激励提案人不要只收集满足公证条件的⅔数量的票。投票人只有在有确实投票的情况下才能拿到奖励。依以上规定不该有人领取的奖励会返回至奖励池。

为遵守EVM标准，ThunderCore使用1秒的区块时间。我们认为1秒的出块时间足以负荷广泛使用情境。因此，投票者有1秒的时间将投票提交给当期的提案人以获取奖励。

惩罚

投票者会话结束后，已抵押的资金将被冻结在智能合约中24小时，在这段时间内，如果记录到不良行为的证据，则扣除部分抵押资金作为惩罚。

如果某投票者在冻结其权益的期间对两个相互冲突的提案投票，这一恶意行为的加密证据如果被发现并被举报提交给区块链，其冻结资金的10%将被返回给奖励池，其中一小部分将作为报酬提供给举报者。剩余的资金将被冻结一百万（1000000）个区块。已冻结的资金无法再用于该投票者的权益抵押。为了防止“无成本作恶”（nothing-at-stake attacks）攻击，在线节点还必须拒绝父块不在冻结期内的区块。

鉴于无意掉线的节点不会自动在下一个会话中竞标，因此ThunderCore不会因其投票失败而给予惩罚。由于ThunderCore仅向参与投票的投票者提供奖励，不投票的机会成本很高。如果发现活跃性攻击的威胁超过了机会成本，ThunderCore将对不投票行为实施惩罚。

第三部分：下一步发展方向

作为一家技术公司，我们有许多令人振奋的想法，仍在積極探索、研發，包括：

- **Thunderella**仍是个杰出且独特的共识协议。它具有同步算法的容错边界和异步单轮投票的最终确认时间这两大优势。这意味着它比任何其他协议快两倍。我们认为，Thunderella如果不是作为第1层区块链的独立协议，则可能会非常适合用在第2层的侧链。提供一个生产就绪的Thunderella参考实现仍在我们的未来规划图中。

- **Pili**[5] 是一个非常独特的具有异步级别性能的同步共识协议。我们相信，一个生产就绪的参考实现对区块链社区具有巨大的价值。

- **无需信任的随机数生成**使在链上易于实现不可预测的随机行为。我们将使用与PaLa协议相同的假设，研究基于多方计算（MPC）的实现。

- **无需信任的跨链通信**可实现跨越独立的区块链之间的无信任信息交换。

- **Paella**将慢链回落方案整合到PaLa中，以实现½活跃度的容错能力和抗审查能力。这个协议的特性另述如下。

- **亚秒级的出块时间**可最大程度地提高吞吐量，并充分利用双流水线PaLa的全部潜力。

- 解决长期困扰区块链磁盘使用问题的**存储费**机制。

- 通过EVM优化和乐观并发处理（optimistic concurrent processing ）以及提案流水线化解决网络瓶颈，实现**100,000+ TPS**。目前，4,000 TPS足以满足所有区块链使用。 ThunderCore将持续不断优化协议，以满足用户需求。

- **分片技术**突破了单台机器的吞吐量和存储限制，从而将可扩展性提升至另一个数量级。 PaLa和我们的PoS方案可以轻松扩展到分片链。我们可以在单个信标链（beacon chain）上选举出一个大型委员会。每个分片与委员会池中随机分配的投票者和提案人一起运行PaLa共识协议。

Paella

PaLa的研究论文概述了选举提案人的“有利于稳定”和“有利于民主”的选举方法。后一种方法要求更频繁的强制切换，以使得更多节点担当提案人角色。 ThunderCore将在

[5] https://eprint.iacr.org/2018/980.pdf

PaLa中选择“有利于稳定性”的方法，这意味着较少的提案人切换。此方法最适用于稳定提供高吞吐量。

为了增加系统的去中心化程度，我们引入了Thunderella协议中的yell消息。yell消息是另一个区块链上的交易，在其数据字段中包含具有有效签名的ThunderCore交易。这些交易应被包含在ThunderCore区块链中。诚实的投票者不会投票给不包含yell信息的区块（将造成强迫提案人切换）。诚实的完整节点应拒绝不包含有效yell消息的区块。

yell消息还提供了一种新的后备机制，可以从委员会不工作的状态中实现恢复。如果没有提案人能够收集⅔的票数来公证下一个区块，交易仍可以通过一定会在未来某时刻被包含在链上的yell消息处理；此未来时刻将由协议定义。。特别重要的是节点运营者仍可以发送新的竞标并选举一个新的提案人来重新配置参与共识的节点，从而使其可以再次正常运行。

Thunderella需要在慢链上定期发布alive消息以使共识节点协调回退和恢复。而使用PaLa时，共识节点可以直接协调它们之间的提案人切换，因此不再需要alive消息。alive消息仍可被用于防止远程攻击（long range attacks），如果我们确定远程攻击会对区块链安全性构成威胁，则它们可能是ThunderCore协议的一部分。

我们亲切地将此修改称为“PaLa **Paella”**。

第四部分：发展理念

ThunderCore是个具有使命感的技术团队。 最后，我们想分享推动我们不断前进的核心理念。

我们坚信：

區塊鏈將從根本上改變人們的生活。
我们正处于人机交互之新时代的初始阶段。区块链技术将从根本上改变人类与技术的互动方式。大量中心化的营利性机构已达到其发展潜力的极限，但区块链的潜力才刚刚开始发挥。

人们将越来越依赖并使用区块链服务。
在日常交互中，人们开始质疑与大型中心化服务提供商的信任问题。随着时间推进，人们开始越来越倾向通过代码，去中心化服务和机构来解决信任问题。区块链就是建立在这些基本原则上的，我们相信区块链很快会被大规模采用。

不受限制地获得技术创造的利益和价值是一项全民权利。
区块链有助于实现全球性的平等，意义十分重大。去中心化和开放性是实现平等公正必需的条件，因为ThunderCore是公开的，无限制的，因此，全世界的人都能使用我们的平台，享受我們服务的利益，同时，這些参与者也能将他們的价值带到我们的平台上。

未来是开放的，去中心化的和透明的。
未来充满挑战。 我们正处于历史上最奇妙的时刻，未来充满可能性，我们拥有让自我书写未来的机会。ThunderCore始终不渝地坚信并追求：区块链技术会实现更开放，更去中心化，更透明的未来。