A Network of Distributed Ledgers

**分布式账本网络**

Jae Kwon jae@tendermint.com
Ethan Buchman ethan@tendermint.com

讨论请加入 Telegram!

*注意：如果你能在 github 上阅读，我们仍然定时更新这个文档，请定期检查更新！*

# 介绍

开源的生态系统。去中心化的文件共享、以及公共的加密货币，这一系列技术的成功使人们启发和理解，去中心化的互联网协议是可以从根本上改善社会经济基础架构的。我们已经见识过个有专长的区块链应用，诸如比特币[1]（加密货币），ZCASH [2]（隐私加密货币），也看到了例如以太坊 [3] 的大众智能合约平台，还有无数基于 EVM (以太坊虚拟机)开发的分布式应用，例如 Augur（预测市场）和 TheDAO [4]（投资俱乐部）

然而，迄今为止，这些区块链已经暴露了各种缺陷，包括总体能效低下，性能不佳或受到限制和缺乏成熟的治理机制。为了扩大比特币交易吞吐量，已经研发了许多诸如隔离见证 [5]（Segregated-Witness）和 BitcoinNG [6]（一种新的可扩展协议）这样的解决方案，但这些垂直扩展解决方案仍然受到单一物理机容量的限制，以确保完整的可审计性。闪电网络 [7] 可以通过部分交易完全记录在主链账本外来扩展比特币的交易容量，这种方法十分适用于微支付和隐私保护支付通道，但是无法适用于更通用的扩展需求。

理想的解决方案是允许多个并行的区块链交互操作的同时保持其安全特性。事实证明，采用工作量证明很难做到这一点，但也并非不可能。例如合并挖矿，允许在工作完成的同时，确保母链在子链上被重复使用，但交易必须通过每个节点依次进行验证，而且如果母链上的大多数哈希算力没有积极地对子链进行合并挖矿，那么就容易遭受到攻击。关于可替代区块链网络架构的学术回顾 将在附件中展示，我们也会在相关工作中对其他（技术）方案和缺陷进行概括。

这里我们要介绍的 Cosmos，一个全新的区块链网络架构，能够解决所有这些问题。Cosmos 是由许多被称之为"分区"的独立区块链组成的网络。分区在 Tendermint Core [8]的支持下运行，Tendermint Core 是一个类似拜占庭容错安全共识引擎，具有高性能、一致性的特性，并且在严格的分叉追责 机制下能够制止恶意破坏者的行为。Tendermint Core 的拜占庭容错共识算法十分适合用于扩展权益证明(PoS)机制下的公共区块链。使用其他共识模型的区块链 包括类似基于权益证明(PoS)的以太坊，以及比特币也能够通过使用适配分区被 Cosmos 网络连接。

Cosmos 的第一个分区称之为 Cosmos 枢纽。Cosmos 枢纽是一种多资产权益证明加密货币网络，它通过简单的治理机制能够对网络进行适配和升级。此外，Cosmos 枢纽可以通过链接其他分区来实现扩展。

Cosmos 网络的枢纽及各个分区可以通过区块链间通信（IBC）协议进行通信，这种协议就是针对区块链的虚拟用户数据报协议（UDP）或者传输控制协议（TCP）。代币可以安全、快速地从一个分区转到其他分区，而无需在两个分区之间拥具有汇兑流动性。相反，所有跨分区的代币转移都会通过 Cosmos 枢纽，以此来追踪记录每个分区持有代币的总量。这个枢纽会将每个分区与其他故障分区隔离开。因为每个人都可以将新的分区连接到 Cosmos 枢纽，所以分区将可以向后兼容新的区块链技术。

利用 Cosmos 可以实现区块链间的互操作。这是一个具有潜力的有价值的互联网络，其中的资产由不同的验证人发布和控制，并可以在不依靠需要信任的第三方的情况下实现跨链资产无缝的转移和交易。

# Tendermint

在这一部分我们将阐述 Tendermint 共识协议和用于建立其应用程序的接口。 更多信息，请参见附录

### 验证人

在经典的拜占庭容错算法中，每个节点有相同的权重。在 Tendermint，节点有着不同数量（非负）的 *投票权*，而那些拥有相当数量投票权的节点称之为 *验证人*。验证人通过广播加密签名、投票或者对下一个区块表决同意来参与共识协议。

验证者的投票权是一开始就确定好了，或者根据应用程序由区块链来决定修改投票权。例如，在像 Cosmos 枢纽的权益证明应用里，投票权可由绑定为押金的代币数量来决定。

注意：像 ⅔ 和 ⅓ 这样的分数指的是占总投票权的分数，而不是总验证人，除非所有验证人拥有相同权重。而>⅔ 的意思是"超过 ⅔ "，≥⅓ 则是"⅓ 或者更多"的意思。

### 共识

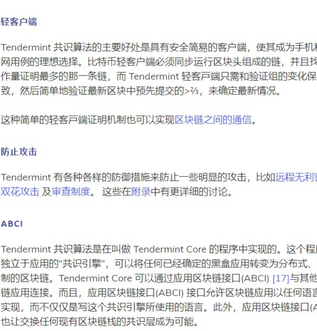
Tendermint 是部分同步运作的拜占庭容错共识协议，这种协议源自 DLS 共识算法 [20]。Tendermint 以简易性、高性能以及分叉问责制而著称。协议要求这组验证人固定且被熟知，并且每个验证人都有其公钥验证身份。这些验证人试图同时在一个区块上达成共识，这些区块是一系列的交易记录。每个区块的共识轮流进行，每一轮都会有个领头人，或者提议人，由他们来发起区块。之后验证人分阶段对是否接受该区块，或者是否进入下一轮做出投票。每轮的提议人会从验证人顺序列表中按照其投票权比例来选择确定。

更多协议的全部细节，请点击这里.

Tendermint 采用了使用大多数投票（超过三分之二）和锁定机制的最优拜占庭容错，来确保其安全性。这些能够保证：

- 蓄意破坏者想要造成安全性问题，必须有三分之一以上的投票权，并且要提交超过两份以上的值。
- 如果有一组验证人成功破坏了安全性，或者曾试图这么做，他们会被协议识别。协议包括对有冲突的区块进行投票和广播那些有问题的投票。

除了其超强的安全性外，Tendermint 还具备杰出的性能。以商用型云平台为例，Tendermint 共识以分布在五大洲七个数据中心的 64 位节点为基准，其每秒可以处理成千上万笔交易，订单提交延迟时间为 1-2 秒。而值得关注的是，即使是在极其恶劣的敌对环境中，比如验证人崩溃了或者是广播恶意破坏的投票，也能维持这种每秒超过千笔交易的较高性能。详见下图。




### 轻客户端

Tendermint 共识算法的主要好处是具有安全简易的客户端，使其成为手机和物联网用例的理想选择。比特币轻客户端必须同步运行区块头组成的链，并且找到工作量证明最多的那一条链，而 Tendermint 轻客户端只需和验证组的变化保持一致，然后简单地验证最新区块中预先提交的>⅔，来确定最新情况。

这种简单的轻客户端证明机制也可以实现区块链之间的通信。

### 防止攻击

Tendermint 有各种各样的防御措施来防止一些明显的攻击，比如远程无利害关系双花攻击 及审查制度。 这些在附录中有更详细的讨论。

### ABCI

Tendermint 共识算法是在叫做 Tendermint Core 的程序中实现的。这个程序是独立于应用的"共识引擎"，可以将任何已经确定的黑盒应用转变为分布式、可复制的区块链。Tendermint Core 可以通过应用区块链接口(ABCI) [17]与其他区块链应用连接。而且，应用区块链接口(ABCI) 接口允许区块链应用以任何语言编程实现，而不仅仅是写这个共识引擎所使用的语言。此外，应用区块链接口(ABCI) 也让交换任何现有区块链栈的共识层成为可能。

我们将其与知名加密货币比特币进行了类比。在比特币这种加密币区块链中，每个节点都维持着完整的审核过的 UTXO（未使用交易输出）数据库。如果您想要在应用区块链接口(ABCI)基础上，创建出类似比特币的系统，那么 Tendermint Core 可以做到：

- 在节点间共享区块及交易
- 创建规范或不可改变的交易顺序（区块链）

同时，ABCI 应用也可以做到：

- 维护 UTXO 数据库
- 验证交易的加密签名
- 防止出现不存在的余额被交易
- 允许客户访问 UTXO 数据库