



# WHITEPAPER

PERMANENT ECOLOGICAL [PEE]

PEE, A HIGHLY CUSTOMIZABLE BLOCKCHAIN INFRASTRUCTURE

VERSION: 1.3 (091319)

# 目录 [Directory]

---

- 1.0 前言摘要
- 2.0 Permanent Ecological 简明概述
- 3.0 Permanent Ecological 核心技术概述
  - 3.1 Tendermint 共识算法
    - ◇ 3.1.1 TendermintBFT
    - ◇ 3.1.2 验证人
    - ◇ 3.1.3 共识协议
    - ◇ 3.1.4 轻量化
    - ◇ 3.1.5 ABCI
  - 3.2 宪法制度
  - 3.3 区域与分散器
  - 3.4 区块链间通信-IBC
  - 3.5 分布式交换
  - 3.6 以太坊缩放
  - 3.7 多应用整合
  - 3.8 网络分区缓解
  - 3.9 桥接到其他加密货币
    - ◇ 3.9.1 将令牌发送到 Permanent Ecological 分散器
    - ◇ 3.9.2 从 Permanent Ecological 分散器提取令牌
    - ◇ 3.9.3 桥梁区的总体责任制
- 4.0 Permanent Ecological 应用生态概述
  - 4.1 云算力轻客户端
  - 4.2 分布式数字货币交易所
  - 4.3 多链区块链钱包
  - 4.4 自治商业联盟

- 4.5 去中心化金融银行
- **5.0 Permanent Ecological 发行概述**
  - 5.1 PEE 代币基础参数
  - 5.2 PET 代币基础参数
  - 5.3 PEE 代币初始分配信息
- **6.0 Permanent Ecological 免责声明**
- **7.0 Permanent Ecological 相关文献**



# 1.0

## PERMANENT ECOLOGICAL

### 前言摘要

PREFACE ABSTRACT



NOTE: 如果你能在 GitHub 上读到这篇文章 ,那么我们仍然在积极地开发这篇文章。请定期检查更新!

## **Permanent Ecological 变革未来商业新形态— PEE 全球金融自治管理会**

一种叫 “去中心化[Decentralization]” 的思想，从人类社会诞生之初与生俱来。人类渴望去掉中心，实现人与人之间直接沟通、直接交易、直接传播。人类相信总有一天，我们可能不再需要中心化的机构。在人类的发展长河中，这种思想都一再发生碰撞，与不同的组织、环境和载体相结合，进而产生不同的社会变革。站在如今的时空维度中，依然可以看到去中心化的宗教教会，也可以看到去中心化的政治制度和社会组织。

信息技术的产生与大规模使用，为去中心化的思想，带来了技术载体。追溯着这个思想和技术相结合的脉络，产生了大量人们喜闻乐见的，甚至颠覆性的创新。P2P 下载、CND（P-CND）、分布式计算（云计算）、社交媒体（自媒体）、P2P 借贷、众筹、共享、区块链、自组织 DAO 等。沿着这个创新脉络，我们会看到众多伟大的创新互联网的足迹。纵观去中心化思想的发展历史，不管区块链这条技术路线，是



否最终会赢得胜利，抑或与其他技术互相妥协、互相融合。但是，正是由于每条技术路线都感受到了来自市场的巨大压力，从而自身也催生出巨大的发展动力。我们相信，无论最终结果如何，这个世界终将被彻底改变。

Permanent Ecological 一直寻找区块链未来商业形态的全新设计，不止单单局限于单向业务的拓展，更多的在于去中心化金融、商业中心分散拓展以及区块链网络架构的创新。

Permanent Ecological 连接着许多独立区块链的网络，并且借助 Permanent Ecological BFT 共识协议以及 Tendermint 共识算法实现区块链之间的互操作性，充分的实现了区块链网络的价值潜力。

本文中 Permanent Ecological 公链将不断更新，这些更新包括但不限于关键治理和关键技术，Permanent Ecological 公链\_使命是打破传统的商业形态，从区块链技术、商业模式、经济模型和治理结构四个维度为未来重新塑造了一个新的商业形态，还创造了一个新的经济形态、新的组织形态和新的社会形态。

# 2.0

## PERMANENT ECOLOGICAL

### 简明概述

CONCISE OVERVIEW



## Permanent Ecological 永恒生态意指通过共识共建共赢来打造一个持续发展的商业生态领域。

契约关系是人类社会的基本组成部分，区块链技术的重要性在于提供一种非常有效和低成本的方式来实现可靠的契约关系。契约关系在于多方参与复杂的业务交互时达成了相对共识信任，并且在业务交互一直保持着这种关系，而这种区块链技术的契约关系又非常的低成本。也就是说区块链技术为分布式商业提供了重要的元素（以极低的交易成本提高网络效益），越来越多的人认识到区块链作为新的价值互联网影响力，并将逐步把当前的商业模式转变为更高效的分布式网络。特别是内置于大多数现代区块链中的通证机制，强调每个网络参与者的权利，并将革新商业的现有模式。

不过，区块链技术仍处于早期阶段。与其它新技术一样也存在缺点，包括有限的性能和还没有发展起来的治理机制，而且绝大多数的公链都缺乏完善的商业模式与经济模型，这些缺点使得绝大多数的公链都难以支持真实的分布式商业协作。诸如 Hyperledger Fabric 和 R3 Corda，以及以太坊企业联盟（Ethereum Enterprise Alliance）等组织都在试图通过联盟链（consortium chains）解决这些性能和治理的问题，使区块链技术更适用于企业。然而，如今的联盟链由



大型企业公司主导的，他们封闭式的链上链下治理模式非常低效。联盟链可能因为缺乏公有链的通证经济模型及其开放性和激励性而缺乏活力。我们希望通过 Permanent Ecological 公链技术，让成千上万的中小企业 (Small Medium Businesses, SMBs)，甚至是个体自由职业者，可以在一个开放的网络中提供他们的服务并享受回报。

以太坊提供了图灵完备的虚拟机运行智能合约，带给人们开发分布式应用的诸多希望。然而，智能合约只能处理确定性逻辑（因此每个节点在处理完同一交易和块后都能达到相同的状态），而大量现存的业务逻辑是不确定的，在不同时间和不同环境参数下可能会发生变化。另一方面，一些真实世界的业务逻辑应该在链下运行，不应该作为诸如可重复运算的智能合约这种类型来执行。利用分布式账本集成和协同链下的服务和资源，是进一步推动区块链技术在更多真实场景中应用的关键。

使用一个公有链来处理所有用例是不可行的。每天都有不同的区块链上线，各自专注于解决问题的一个方面，比如分布式存储、资产所有权或市场预测等。据 [coinmarketcap.com](https://coinmarketcap.com) 显示，目前有超过 1000 种加密货币在不同的交易平台上活跃。构建业务应用程序时涉及处理存储以及不同数据源的来

源，我们的另一个工作动机是如何通过重用一些现有的工作，比如存储(IPFS, SIA, Storj.io 等等)、数据发送 ( Augur , Gnosis , Oraclize 等 ) 和物联网 ( IOTA 等 ) 提供的这些专用的区块链。

此外 ,有很多实时业务交易确实需要更密切的联盟链/许可链/私有链来处理性能问题、安全性和业务治理要求。因此，我们对分布式商业基础设施的愿景是要具备在多种异构链，包括公共链/联盟链/许可链/私有链之间具备互操作的能力。

跨链技术是满足这一需求非常自然的解决方案。然而目前为止，现有的跨链技术主要是为了在已有区块链中提供互操作性，并专注于通证的价值转移。Permanent Ecological 公链就是基于 Tendermint 共识引擎进行设计的，实现了互操作性和可扩展性，我们还建立多枢纽多分区模型，每个分区都是独立的区块链。另外，我们还拥有独立的治理结构，为真实商业提供了一种非常合适的体系架构，可以用 SOC ( Seperation of Concern , SOC ) 的方式对现实世界的复杂性进行建模。

# 3.0

PERMANENT  
ECOLOGICAL

核心技术概述

OVERVIEW OF CORE TECHNOLOGIES



Permanent Ecological 公链是一个独立的并行区块链网络，每个区块链都由经典的 BFT 共识算法提供支持。Permanent Ecological 公链通过新颖的区块链间通信协议连接到许多其他区块链（或区域）。并且跟踪多种令牌类型，记录每个连接区域中令牌的总数。令牌可以安全快速地从—个区域转移到另—个区域，而无需在区域之间进行液体交换，因为所有区域间硬币转移都通过 Permanent Ecological 公链进行。

这种架构解决了区块链空间当今面临的许多问题，例如应用程序的互操作性，可伸缩性和无缝可升级性。例如，可以将来自 Bitcoin，Go-Ethereum，CryptoNote，ZCash 或任何区块链系统的区域插入 Permanent Ecological 公链。这些区域使 Permanent Ecological 公链可以无限扩展以满足全球交易需求。区域也非常适合分布式交换，也将得到支持。Permanent Ecological 公链不仅是单个分布式分类帐，我们正在基于密码学原理，合理经济学，共识理论，透明度和问责制为开放式分布式账本网络设计协议，该协议可以用作未来商业系统的新基础。

### **3.1 Tendermint 共识算法**

Tendermint 是一个开源的完整的区块链实现，可以用于公

链或联盟链，其官方定位 是面向开发者的区块链共识引擎，与其他区块链平台例如以太坊或者 EOS 相比，Tendermint 最大的特点是其差异化的定位，尽管包含了区块链的完整实现，但它却是以 SDK 的形式将这些核心功能提供出来，供开发者方便地定制自己的专有区块链。

Tendermint 大致类似于两类软件。第一类包括使用非 BFT 共识的分布式键值存储，例如 Zookeeper，etcd 和 consul。第二类称为“区块链技术”，由比特币和以太坊等加密货币以及 Hyperledger's Burrow 等替代分布式账本设计组成。

### **3.1.1 TendermintBFT**

Tendermint 开源项目诞生于 2014 年，旨在解决比特币工作量证明共识算法的速度，可扩展性和环境问题。通过使用和改进 1988 年由麻省理工学院开发的经过验证的 BFT 算法，Tendermint 团队率先概念性地证明了股权证明加密货币，该加密货币解决了第一代证明所遭受的股权滥用问题，使用 NXT 和 BitShares1.0 等加密货币。

如今，几乎所有的比特币移动钱包都使用受信任的服务器为他们提供交易验证。这是因为工作量证明需要等待许多确认，然后才能将交易视为不可逆转的承诺。在 Coinbase 之



类的服务上已经展示了双花攻击。

与其他区块链共识系统不同，Tendermint 提供即时且可证明的安全的移动客户端付款验证。由于 Tendermint 的设计绝不分叉，因此手机钱包可以收到即时交易确认，这使得在智能手机上实现不信任和实用的支付成为现实。这也对物联网应用产生了重大影响。

Tendermint 中的验证人与比特币矿工具有相似的作用，但使用加密签名进行投票。验证器是负责提交块的安全专用机器。非验证人可以将他们的抵押令牌委派给任何验证人，以赚取一部分区块费和量子奖励，但是如果委托验证人被黑或违反协议，则他们将面临受到惩罚的风险。

Tendermint 保证了永远都不会违背其安全性，也就是说，验证人永远不会在同一高度提交冲突块。为了达到这一点，它引入了一些锁定[Locking]的规则，这些规则对流程图中的路径进行了模块化。一旦一个验证人预提交了一个块，它就被“锁定”在了那个块上。然后，它必须为被锁定的那个块进行预投票

只有在之后的轮中，有了那个块的一个波卡，它才能够解锁，

并为一个新块进行预提交。

Tendermint BFT 共识的行之有效的安全保证，以及利益相关者（验证人和委托人）的抵押存款，为节点和轻型客户提供了可证明的，可量化的安全性。

### 3.1.2 验证人

在 Tendermint 中，每个节点具有相同的权重，并且节点具有非负的投票权，而具有正投票权的节点称为验证器。验证人通过广播密码签名或投票参与共识协议，以就下一个区块达成协议。

协议中的参与者叫着“验证人”（validator）。他们轮流对交易区块进行提议，并对这些区块进行投票。区块会被提交到链上，每一个块占据一个“高度”（height）。提交块可能会失败，如果失败，协议就会开始下一轮的提交，并且一个新的验证人会继续提交那个高度的区块。要想成功提交一个块，需要有两个阶段的投票：“预投票”（pre-vote）和“预提交”（pre-commit）。在同一轮提交中，只有超过  $2/3$  的验证人对同一个块进行了预提交，这个块才能被提交到链上。

由于一些原因，验证人可能在提交一个块时失败：当前提议

者可能离线了，或者网络非常慢。Tendermint 允许他们证实一个验证人应该被跳过。在进行下一轮的投票前，验证人会等待一小段时间从提议者那里接收一个完整的提议块。这种对于超时的依赖，使得 Tendermint 成为了一个弱同步协议，而非一个异步协议。但是，协议的剩余部分都是异步的，只有在接收到超过  $2/3$  的验证人集合时，验证人才会采取下一步操作。Tendermint 能够简化的一个原因就是它使用了同样的机制来提交一个块和跳过直接进入下一轮。注意： $2/3$ 和 like 之类的分数表示总投票权的分数，而不是验证者总数的分数，除非所有验证者的权重相同。 $> 2/3$ 表示“大于 $2/3$ ”， $\geq 1/3$ 表示“至少 $1/3$ ”。

### 3.1.3 共识协议

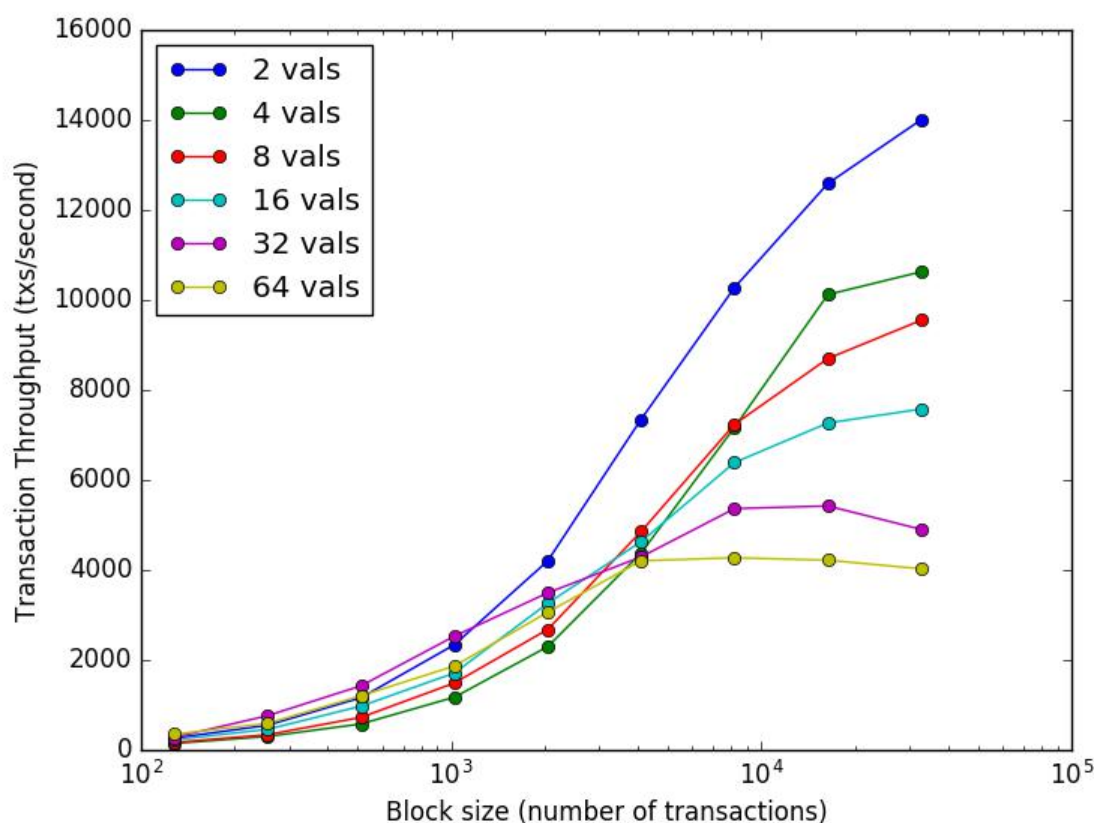
在技术方面，Tendermint 引以为傲的是其共识算法——世界上第一个可以应用于公链的拜占庭容错算法。Tendermint 以其简单性、高性能和分叉责任感而著称。该协议需要一组固定的已知验证器，其中每个验证器均由其公钥标识。验证程序尝试一次就一个区块达成共识，其中一个区块是交易列表。全面投票表决是否达成共识。每个回合都有一个圆形领导者或提议者，提议一个阻止。然后，验证人将分阶段投票决定是否接受提议的区块或进入下一轮。轮次的提议者是从验证人的有序列表中确定的，与他们的投票权成正比。

Tendermint 的安全性源于其通过超级多数 ( $> a$ ) 投票和锁定机制使用最佳的拜占庭容错功能。他们共同确保：

$\geq \frac{1}{3}$  表决权必须是拜占庭式的，以致违反安全性，其中要提交两个以上的值。

如果任何一组验证人成功违反安全性，甚至尝试违反安全性，则可以通过协议进行识别。这包括对有争议的部分进行投票和广播不合理的投票。

尽管有强有力的保证，Tendermint 仍具有出色的性能。在分布在五大洲 7 个数据中心的 64 个节点的基准中，在商业交易实例中，Tendermint 共识可以每秒处理数千个事务，而提交延迟为一到两秒钟。值得注意的是，即使在严酷的对抗条件下，验证器崩溃或传播恶意制作的选票，也能保持每秒超过一千次交易的性能。



### 3.1.4 轻量化

Tendermint 共识算法的主要优点是简化了轻客户端安全性，使其成为移动和物联网应用的理想选择。尽管比特币轻量客户端必须同步区块头链并找到工作量最大的链，但是 Tendermint 轻量客户端只需要跟上验证器集的更改，然后验证最新区块中的  $> \frac{2}{3}$  PreCommits 即可确定最新状态。简洁的轻客户端证明还可实现区块链之间的通信。

### 3.1.5 ABCI

Tendermint 共识算法在称为 Tendermint Core 的程序中实



现。Tendermint Core 是一个与应用程序无关的“共识引擎”，可以将任何确定性的黑匣子应用程序转换为分布式复制的区块链。Tendermint Core 通过应用程序区块链接口（ABCI）连接到区块链应用程序。因此，ABCI 允许以任何语言编程区块链应用程序，而不仅仅是用共识引擎编写的编程语言进行编程。此外，ABCI 使得可以轻松交换掉任何现有区块链堆栈的共识层。

ABCI 允许应用的拜占庭容错复制可以由任意一种编程语言编写。Tendermint Core（“共识引擎”）通过一个满足 ABCI 标准的 socket 协议与应用进行交流。举个大家比较熟悉的例子，比特币。比特币是一个加密货币区块链，其中的每个节点维护了一个完全经过审计的 UTXO 数据库。如果有人想要在 ABCI 之上创建一个类似比特币的系统，

Tendermint Core 将会负责：

在节点间共享区块和交易；

建立交易（区块链）的标准/不可变顺序；

而应用将会负责：

维护 UTXO 数据库；

验证交易的加密签名；

阻止花费尚未存在的交易；

允许客户端查询 UTXO 数据库；

ABCI 包含了 3 个主要的消息类型，它们由 core 发送至应用，应用会对消息产生相应的回复：

DeliverTx 消息是应用的主要部分。链中的每笔交易都通过这个消息进行传送。应用需要基于当前状态，应用协议，和交易的加密证书上，去验证接收到 DeliverTx 消息的每笔交易，。一个经过验证的交易然后需要去更新应用状态 - 比如通过将绑定一个值到键值存储，或者通过更新 UTXO 数据库。

CheckTx 消息类似于 DeliverTx，但是它仅用于验证交易。Tendermint Core 的内存池首先通过 CheckTx 检验一笔交易的有效性，并且只将有效交易中继到其他节点。比如，一个应用可能会检查在交易中不断增长的序列号，如果序列号过时，CheckTx 就会返回一个错误。又或者，他们可能使用一个基于容量的系统，该系统需要对每笔交易重新更新容量。

Commit 消息用于计算当前应用状态的一个加密保证（cryptographic commitment），这个加密保证会被放到

下一个区块头。这有一些比较方便的属性。现在，更新状态时的不一致性会被认为是区块链的分支，分支会捕获所有的编程错误。这同样也简化了保障轻节点客户端安全的开发，因为 Merkle-hash 证明可以通过在区块哈希上的检查得到验证，区块链哈希由一个 quorum 签署。

一个应用可能有多个 ABCI socket 连接。Tendermint Core 给应用创建了一个 ABCI 连接：一个用于内存池广播时的交易验证，一个用于运行提交区块时的共识引擎，还有一个用于查询应用状态。

## 3.2 宪法制度

分布式公共分类帐应具有宪法和治理制度。比特币依靠比特币基金会和采矿来协调升级，但这是一个缓慢的过程。以太坊在分叉以解决 TheDAO 黑客事件后分成了 ETH 和 ETC，这主要是因为缺乏事先的社会契约或决策机制。

Permanent Ecological 公链上的验证人和代表可以对可以自动更改系统预设参数（例如，限制气体限制），协调升级的提案进行投票，还可以对管理该政策的人类可读宪法的修订进行投票。宇宙中心。宪法允许利益相关者在诸如盗窃和错误（例如 TheDAO 事件）之类的问题上团结一致，从而可以更快，更清洁地解决问题。

每个区域也可以有自己的宪法和治理机制。例如，Permanent Ecological 公链可以具有一种强制不变性的构造（无回滚，但 Permanent Ecological 公链节点实现的错误除外），而每个区域都可以设置自己的有关回滚的策略。通过在不同策略区域之间实现互操作性，Permanent Ecological 公链网络为用户提供了最大的自由度和进行未经许可的试验的潜力。

### 3.3 区域与分散器

Permanent Ecological 公链是由 Tendermint 支持的许多区块链的网络。现有建议旨在创建一个具有整体全球交易顺序的“单个区块链”，而 Permanent Ecological 公链允许许多区块链在保持互操作性的同时并发运行。在这里，我们描述了分散和可扩展性的新型模型。

Permanent Ecological Disperser 管理着许多独立的区块链，称为“Zones”（有时称为“碎片”，参考称为“碎片”的数据库扩展技术）。来自发布在分散器上的区域的持续不断的最新块提交流使分散器能够跟上每个区域的状态。同样，每个区域都与分散器的状态保持同步（但区域之间不是通过分散器间接地保持同步）。然后，通过发布 Merkle 证明作为信息发送和接收的证据，将信息包从一个区域传递到

另一个区域。这种机制称为区块链间通信，简称 IBC。

### 3.4 区块链间通信-IBC

现在我们看一下分散器和区域之间如何通信。例如，如果有三个区块链 “ Zone1 ” ， “ Zone2 ” 和 “ Disperser ” ，我们希望 “ Zone1 ” 产生发往 “ Zone2 ” 的数据包，并通过 “ Disperser ” 。为了将数据包从一个区块链移动到另一个区块链，在接收链上发布证明。证据表明，发送链发布了所谓目的地的数据包。为了使接收链能够检查此证明，它必须能够跟上发送方的块头。这种机制类似于侧链所使用的机制，侧链需要两条相互作用的链通过双向的存在证明数据报（事务）流来相互了解。

自然可以使用两种类型的交易来定义 IBC 协议：一种 IBCBlockCommitTx 交易，允许区块链向任何观察者证明其最近的哈希值；另一种 IBCTransferTx 交易，允许区块链向任何观察者证明给定的数据包确实是由发件人的应用程序通过对最近的区块哈希的 Merkle 证明发布的。

通过将 IBC 机制拆分为两个独立的交易，我们允许接收链的本钱市场机制确定提交（即确认）的数据包，同时允许发送链完全自由地允许允许多少个出站数据包。



### 3.5 分布式交换

就像比特币通过成为分布式的，大规模复制的账本来提高安全性一样，我们可以通过在区块链上运行交易所来减少交易所受到外部和内部黑客的攻击。我们称其为分布式交换。

如今，加密货币社区所谓的去中心化交易所是基于一种称为“原子跨链”（AXC）交易的东西，Permanent Ecological 公链定义为量子跨链[QXC]。使用 QXC 事务，两个不同链上的两个用户可以进行两个在两个分类帐上一起提交的转移事务，或者根本不提交（即量子）。例如，即使比特币和以太坊没有相互连接，两个用户也可以使用 QXC 交易将比特币换成以太币（或两个不同分类账中的任意两个代币）。在 QXC 交易上运行交换的好处是用户都不需要互相信任或交易匹配服务。缺点是双方都必须在线才能进行交易。

分散式交换的另一种类型是在其自己的区块链上运行的大规模复制分布式交换。进行这种交易的用户可以提交限价单并关闭其计算机，并且交易可以在用户不在线的情况下执行。区块链代表交易者匹配并完成交易。

Tendermint 共识提供了更快的事务提交的其他好处。通过在不牺牲一致性的情况下优先考虑快速确定性，Permanent Ecological 公链中的区域可以快速完成交易-对于交换订单

交易以及 IBC 令牌往返其他区域的转移。

鉴于当今的加密货币交换状态，Permanent Ecological 公链的一个重要应用是分布式交换（又名 Permanent Ecological DEX）。事务吞吐能力以及提交延迟可以与集中式交换媲美。交易者可以提交限价单，无需双方在线即可执行。借助 Tendermint，Permanent Ecological 枢纽和 IBC，交易者可以快速将资金进出交易所到其他区域。

### 3.6 以太坊缩放

解决扩展问题是以太坊的一个开放问题。当前，以太坊节点处理每个单笔交易并存储所有状态。由于 Tendermint 可以比以太坊的工作量证明更快地提交区块，因此由 Tendermint 共识支持并在桥接醚上运行的 EVM 区域可以为以太坊区块链提供更高的性能。此外，尽管分散器和 IBC 数据包机制本身不允许任意执行合约逻辑，但它可用于协调在不同区域上运行的以太坊合约之间的令牌移动，从而通过分片为以令牌为中心的以太坊缩放提供基础。

### 3.7 多应用整合

Permanent Ecological 公链区域运行任意应用程序逻辑，该逻辑在区域生命周期的开始就定义，并且可能会随着时间

的推移而通过治理进行更新。这种灵活性允许 Permanent Ecological 公链区域充当与其他加密货币（如以太坊或比特币）的桥梁，并且还允许使用相同的代码库但具有不同的验证器集和初始分布的那些区块链衍生产品。这使得许多现有的加密货币框架（例如以太坊，Zerocash，比特币，CryptoNote 等）可以与 Tendermint Core 一起使用，Tendermint Core 是一个性能较高的共识引擎，可以在通用网络上使用，这为跨平台的互操作性提供了巨大的机会。此外，作为多资产区块链，单个交易可能包含多个输入和输出，其中每个输入可以是任何令牌类型，使 Permanent Ecological 公链可以直接用作去中心化交易的平台，尽管假定订单是通过其他平台匹配的。或者，区域可以用作分布式容错交换（带有订单簿），这可以对现有的集中式加密货币交换进行严格的改进，而随着时间的流逝，该交换中心通常会遭到黑客入侵。

区域还可以用作企业和政府系统的区块链支持版本，其中传统上由一个组织或一组组织运行的特定服务的某些部分作为 ABCI 应用程序在某个区域上运行，这使它可以继承 Permanent Ecological 公链公共网络的安全性和互操作性，而不会牺牲对基础服务的控制。因此，对于希望利用区块链技术但对将控制权完全放弃给分布式第三方的组织而言，

Permanent Ecological 公链可能提供两全其美的方法。

### 3.8 网络分区缓解

有人声称，像 Tendermint 这样的有利于一致性的共识算法的一个主要问题是，任何导致没有投票权大于（的单个网络分区（例如， $\geq \text{offline}$  下线）的任何网络分区都将完全终止共识。Permanent Ecological 公链体系结构可以通过使用具有区域自治区的全球枢纽来缓解此问题，在该自治区中，每个区域的投票权均基于共同的地理区域来分配。例如，一个通用范例可能是让各个城市或地区在共享一个公共分散器（例如 Permanent Ecological 分散器）的同时操作自己的区域，从而在分散器由于临时网络分区而停止时，使市政活动得以持续。请注意，这允许在设计健壮的联合容错系统时考虑真实的地质，政治和网络拓扑特征。

### 3.9 桥接到其他加密货币

特权区域可以充当另一种加密货币的桥接令牌的来源。桥梁类似于 Permanent Ecological 公链枢纽与区域之间的关系。两者都必须跟上另一个的最新块，以验证令牌已从一个移到另一个。Permanent Ecological 公链网络上的“桥接区域”与集线器以及其他加密货币保持同步。通过桥接区域的间接允许分散器的逻辑保持简单，并且与其他区块链共识

策略（例如比特币的工作量证明挖掘）无关。

### 3.9.1 将令牌发送到 Permanent Ecological 分散器

每个桥区验证器都将运行带有 Tendermint 的区块链，一个特殊的 ABCI 桥应用程序，以及一个“起源”区块链的完整节点。

当在原点上挖掘新块时，桥接区域验证器将通过签署并共享其对原点的区块链技巧的本地视图来就已提交的块达成协议。当桥接区域在原点上收到付款时（对于以太坊或比特币这样的 PoW 链，已经确认已经确认了足够的确认），就会在桥接区域上创建一个具有该余额的对应帐户。

在以太坊的情况下，桥接区域可以与分散器共享相同的验证器集。在以太坊方面（起源），桥接合同将允许以太坊持有者通过将以太币发送到以太坊上的桥接合同来将醚传送到桥接区域。一旦桥接合同接收到以太，除非桥接合同从桥接区域接收到适当的 IBC 数据包，否则无法提取以太。桥梁合同跟踪桥梁区域的验证人集，该验证者集可能与分散器的验证人集相同。

就比特币而言，此概念类似，不同之处在于，每个 UTXO 都



将由阈值多重签名 P2SH 发布来控制，而不是一个单一的桥梁合同。由于 P2SH 系统的限制，签名者不能与分散器验证器集相同。

### 3.9.2 从 Permanent Ecological 分散器提取令牌

桥接区域上的以太坊（“桥接的以太坊”）可以在分散器之间来回传输，然后通过将其发送到以太坊上特定提款地址的交易进行销毁。可以将 IBC 数据包证明交易发生在桥接区域上，然后将其发布到以太坊桥接合同中，以允许以太币被提取。

就比特币而言，受限制的脚本系统使镜像 IBC 硬币转移机制变得困难。每个 UTXO 都有其自己独立的发布，因此，当比特币托管签名者的集合发生变化时，每个 UTXO 必须迁移到新的 UTXO。一种解决方案是根据需要压缩和解压缩 UTXO 集，以减少 UTXO 的总数。

### 3.9.3 桥梁区的总体责任制

这样的缩水合同的风险在于流氓验证者。 $\geq \frac{1}{3}$  拜占庭投票权可能会导致叉子，将以太币从以太坊上的桥合约中撤出，同时将以太保持在桥区上。更糟的是， $> \frac{2}{3}$  拜占庭投票权可能会偏离桥带的原始桥接逻辑，从而从那些将其发送到桥牌合同的人那里彻底窃取以太币。

通过设计完全负责的桥梁可以解决这些问题。例如，来自分散器和始发地的所有 IBC 数据包都可能需要桥接器区域进行确认，以使分散器或始发者的桥接器可以有效地挑战 and 验证桥接器区域的所有状态转换合同。分散器和源应允许桥接区域验证程序过帐抵押品，并且应延迟将令牌从桥牌合约中转移出去（并且抵押品无担保期限足够长），以允许独立审核员提出任何挑战。我们将规范的设计和该系统的实现作为 Permanent Ecological 公链未来的改进建议开放，以供 Permanent Ecological 公链分散器的治理系统通过。



# 4.0

**PERMANENT  
ECOLOGICAL**

应用生态概述

OVERVIEW OF APPLIED ECOLOGY



我们一直努力从区块链技术、商业模式、经济模型和治理结构四个维度来构建 Permanent Ecological 公链 ,商业模式、经济模型也是 Permanent Ecological 公链核心关键。本文章为技术白皮书 , 重要阐述 Permanent Ecological 公链技术基础设施 ,应用生态的阐述主要在 Permanent Ecological 公链经济黄皮书内容中。

## 4.1 云算力轻客户端

在区块链领域 , 客户端是一种以点对点的方式连接到其他客户端的软件。由于所有客户端相互通信 , 它们一起组成了一个网络 , 在该网络中每一个客户端都是一个网络节点。这种网络节点负责验证以及转发网络上的交易和区块。由于无需信任的环境 ( 开放的网络 ) 以及区块链本身的性质 , 每个全节点都需要下载并验证所有的区块 , 因此所有区块中的所有交易信息都需要经过网络节点的验证 , 这里称为全节点。不幸的是 , 多数情况下运行全节点是极其昂贵和迟缓的 , 并且与目前用户使用的智能手机终端是不兼容的。

Permanent Ecological 公链通过 Tendermint 共识算法为用户提供了轻量级的替代方案 :

云算力轻客户端[CloudHash&Light Client]，它允许云算力轻客户端与全节点在最小化信任的情况下进行交互，并不需要同步 Permanent Ecological 公链全节点区块数据，只需同步验证器集的更改以及验证最新区块中的  $> \frac{2}{3}$  PreCommits 即可确定最新状态。这种简化使其成为移动以及物联网用例的理想选择，并且，云算力轻客户端证明还可实现区块链之间的通信。

## 4.2 分布式数字货币交易所

数字货币交易所为区块链市场的资产代币化发展提供了全球化、全天候的充足流动性，然而这些交易所是中心化的，中心化的模式存在一些显著的风险和问题。中心化交易所一般都提供账户体系、KYC、资产充值、资产托管、撮合交易、资产清算、资产兑换等业务模块，在技术实现上已经有相对成熟的解决方案，但在面对突发状况时往往没有很好的应对措施，比如交易系统防篡改性较差，且基于中心化的运营模式存在宕机的可能性，当服务器无法承载超负荷的流量，中心化平台有可能会出现宕机的情况。早期的 Mt.Gox 被盗事件，到 bitfinex 和 coincheck 等交易所被盗事件，在损害用户利益和交易所声誉的同时，也对整个行业造成震荡性影响。

传统交易所撮合交易的流程：

1. 收到数字货币来发行 IOU（欠条）；2. 收取法币来发行 IOU；3. 处理订单撮合；4. 赎回 IOU，以上每一个步骤都需要基于高度的信任，并且将直接面临对手风险（对手风险：交易中对方不履行其金融义务而产生的风险），因为用户所交易的其实是来自交易所发布的 IOU。而去中心化交易所具有去中心化、信息不可篡改、匿名安全等特性，在去中心化交易所的所有交易都是在链上直接交换，数字货币会直接保存在区块链上的智能合约。Permanent Ecological 公链基于 Tendermint 共识引擎开发了去中心化数字货币交易所。Permanent Ecological 公链的去中心化交易所采用了订单簿和 Uniswap 协议构建了混合式 DEX 撮合模型，给用户提供一个安全，快速，便捷的数字货币交易环境。

### 4.3 多链区块链钱包

对于普通用户来说，传统的多链钱包不解决私钥管理的问题，用户因不能妥善管理私钥而造成资产丢失的事件层出不穷。此外，不同区块链采取了不同的计费模型，也增加了用户使用区块链的门槛。Permanent Ecological 公链基于 Tendermint 共识引擎，采用 Tendermint BFT 以及桥接非 Tendermint 链服务等创建了多链区块链钱包。Permanent Ecological 公链多链区块链钱包可以满足只需要一个钱包就

可以方便地管理多条的加密资产。为用户提供极大的便利，减轻了管理多链资产的负担。多链区块链钱包采用一个数字身份，然后根据不同链的编号，为用户生成各种链的私钥和账户，并且用户只需要备份好一套助记词，就可以控制多链资产。由于 Tendermint 跨链的属性，在多链区块链钱包中经过跨链映射的资产，就可以在新链或侧链内，享受不同的链服务了，比如 Permanent Ecological 公链使 BTC 变成了 PBTC，同时让 PBTC 摆脱了缓慢昂贵的 BTC 主链，获得了快速支付能力。

#### 4.4 自治商业联盟

区块链自治商业联盟是未来互联网商品贸易新的时代，它将是更好的选择。在如今的商业形态中，全球中小企业及实体经济一直面临着严峻的考验，如何利于区块链技术帮助他们度过这个寒冬成为了当下极具讨论下的话题，资金链断链、库存产品滞销、产品研发效率低能、商品质量溯源等问题一直困扰着他们的发展。区块链技术的日渐成熟让分布式存储、点对点传输、共识机制等特点给这些痛点的解决提供了一条可行的思路。Permanent Ecological 公链为未来商业形态提供了新的自治商业联盟模式，在电商自身环节供应链管理、中心化带来的信息不对称等一直限制着商品贸易进一步发展，Permanent Ecological 公链通过打破这一瓶颈环



节，来逐步改变现有商业形态。

## 4.5 去中心化金融银行

Permanent Ecological 公链去中心化金融银行旨在解决中心化服务不能解决的两个主要问题：不平等金融服务；金融审查。不平等金融服务，这主要是指个人能够获得贷款、抵押贷款和保险等金融服务的机会。那些难以或无法获得金融服务的人常被称为“没有银行账号的人”（“unbanked”）。去中心化金融应用旨在改善这个问题，确保人们可以无障碍地使用这些应用；所需要的只是一台智能手机和互联网连接。金融审查，为了特定利益，政府、金融机构或第三方机构会关闭个人或公司的账户并限制他们交易。例如，如果有公司敢于公开表达对政府政策的不同意见，政府可以限制这家公司获得基本的金融服务，从而使他们保持沉默。拿银行账户服务来说，公司需要通过银行账户来支付员工以及其他费用，如果没有这些服务，会导致公司的破产。而 Permanent Ecological 公链去中心化金融银行通过有效的区块链应用来打破这两个问题。例如，中小企业及实体经济链改化以及链改 Token 债券化，或者 C.D.P.S 抵押债务头寸智能合约来实现 Permanent Ecological 公链去中心化金融银行的价值。

# 5.0

## PERMANENT ECOLOGICAL

### 发行概述

RELEASE OVERVIEW



Permanent Ecological 公链总共发行 2 款代币，是一种双代币系统。主网发行的代币为 PEE；侧链发行的代币为 PET（稳定代币）。

## 5.1 PEE 代币基础参数

|         |                      |
|---------|----------------------|
| 总发行量    | 3,33,0000,000 PEE    |
| 权益证明方式  | POS 基于 Tendermint 引擎 |
| 区块出块间隔  | 6 Seconds            |
| 出块奖励量   | 40 PEE               |
| 减产周期（块） | 2635200 Blocks       |
| 减产幅度    | 3%                   |

## 5.2 PET 代币基础参数

|        |                 |
|--------|-----------------|
| 总发行量   | 56,0000,000 PET |
| 区块出块间隔 | 21 Seconds      |
| 出块奖励量  | 2 PET           |

## 5.3 PEE 代币初始分配信息

PEE 总发行量共计 3,33,0000,000 PEE，初始分配类型分为量子发生器、轻挖算力服务 1.0 挖矿阶段、轻挖算力服务 2.0 挖矿阶段、轻挖算力服务 3.0 节点质押挖矿阶段、技术维护、

生态贡献、社区维护、全节点奖励、激励机制。Permanent Ecological 公链采用的是 POS 挖矿机制，在创世阶段每个类似的分配将直接映射到各个类型的超级节点中，通过智能合约进行自动触发，所有数据将在区块浏览器中对 PEE 共识者公开监管。并由 Permanent Ecological 公链智能 ECO AI 进行监管监督。

| 去中心节点属性             | 分配比例 | 分配数量      |
|---------------------|------|-----------|
| 量子发生器               | 10%  | 333000000 |
| 轻挖算力服务 1.0 挖矿阶段     | 10%  | 333000000 |
| 轻挖算力服务 2.0 挖矿阶段     | 15%  | 499500000 |
| 轻挖算力服务 3.0 节点质押挖矿阶段 | 25%  | 832500000 |
| 技术维护                | 10%  | 333000000 |
| 生态贡献                | 5%   | 166500000 |
| 社区维护                | 10%  | 333000000 |
| 全节点奖励               | 10%  | 333000000 |
| 激励机制                | 5%   | 166500000 |

# 6.0

PERMANENT  
ECOLOGICAL

免责声明

DISCLAIMER



## 6.1 本文介绍的为一个开发中的项目

本黄皮书及其相关文档用于 Permanent Ecological 公链的开发和应用。仅做信息传播之用并可能更改。

本文所设想的 Permanent Ecological 公链在开发中，并将不断更新，这些更新包括但不限于关键治理和关键技术。开发使用 Permanent Ecological 公链或与之相关的测试平台以及技术，可能无法实现或无法完全实现本白皮书所述的目标。

如果 Permanent Ecological 公链得以完成，可能与本文所述有所不同。本文不对未来的任何计划、预测或前景的成功性或者合理性做出陈述或保证，本文的任何内容都不应被视为对未来的承诺或陈述。

## 6.2 并非监管类产品的要约

Permanent Ecological 公链不代表任何一种司法监管下的产品。本文不构成对任何受监管产品的出价要约或询价邀请，也不构成以投资为目的的促销、邀请或询价。其购买条款并非提供金融服务的文件或任何类型的招股说明书。



## 6.3 并非建议

本黄皮书不构成任何对 PEE 的购买建议。请不要依赖本黄皮书去达成任何购买的决策。

## 6.4 风险警告

购买 PEE 并参与 Permanent Ecological 公链伴随着极大的风险。在购买 PEE 之前，您应该仔细评估并考虑风险。

## 6.5 您必须获得所有必要的专业建议

您有必要在决定是否购买 PEE 或参与 Permanent Ecological 公链项目之前，必须咨询律师、会计师和/或税务专业人员，以及其他专业顾问。



# 7.0

## PERMANENT ECOLOGICAL

### 相关文献

RELATED LITERATURE



比特币：[bitcoin.org/bitcoin.pdf](https://bitcoin.org/bitcoin.pdf)

以太坊：[github.com/ethereum/wiki/wiki/White-Paper](https://github.com/ethereum/wiki/wiki/White-Paper)

TheDAO：[download.slock.it/public/DAO/WhitePaper.pdf](https://download.slock.it/public/DAO/WhitePaper.pdf)

BitcoinNG：[arxiv.org/pdf/1510.02037v2.pdf](https://arxiv.org/pdf/1510.02037v2.pdf)

闪电网络：

[lightning.network/lightning-network-paper-DRAFT-0.5.pdf](https://lightning.network/lightning-network-paper-DRAFT-0.5.pdf)

Tendermint：[github.com/tendermint/tendermint/wiki](https://github.com/tendermint/tendermint/wiki)

PBFT：[pmg.csail.mit.edu/papers/osdi99.pdf](https://pmg.csail.mit.edu/papers/osdi99.pdf)

Interledger：

[interledger.org/rfcs/0001-interledger-architecture](https://interledger.org/rfcs/0001-interledger-architecture)

侧链：[blockstream.com/sidechains.pdf](https://blockstream.com/sidechains.pdf)

ABCI：[github.com/tendermint/abci](https://github.com/tendermint/abci)

DLS：[groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf](https://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf)

瘦客户端安全性：[en.bitcoin.it/wiki/Thin\\_Client\\_Security](https://en.bitcoin.it/wiki/Thin_Client_Security)

以太坊 2.0 淡紫色论文：[vitalik.ca/files/mauve\\_paper.html](https://vitalik.ca/files/mauve_paper.html)

