EIC
EICHAIN.IO

熵增公链白皮书

探索熵增
塑造未来的全链生态

发布日期：2024年3月1日

作者/组织信息：
比纳格基金会 & 熵增公链开发团队
联系方式：info@eichain.io
网站：www.eichain.io

目录

目录

01 | 리듬

01 引言

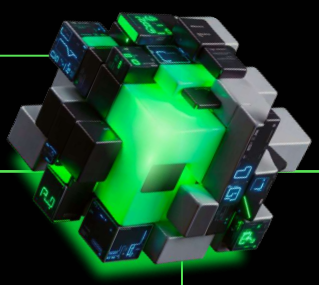
在区块链技术快速发展的当下，各类区块链平台和应用层出不穷，然而，这些平台之间缺乏有效的互操作性，严重制约了区块链技术的整体发展和应用推广。EiChain熵增公链应运而生，旨在通过其革命性的熵增技术和高度创新的区块链架构，打破现有的壁垒，实现真正的全链互通。

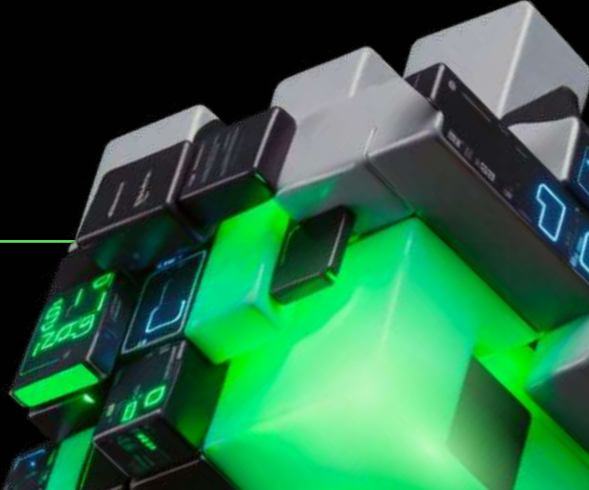
熵增公链不仅仅是一个区块链平台，它代表了一种全新的思维方式，通过 EiAlgo 熵增算法，结合先进的人工智能，为区块链世界带来前所未有的安全性、效率和灵活性。我们的目标是创建一个去中心化、高效、安全的全链生态系统，其中任何资产和信息都可以自由流动，无论它们原本属于哪个区块链。

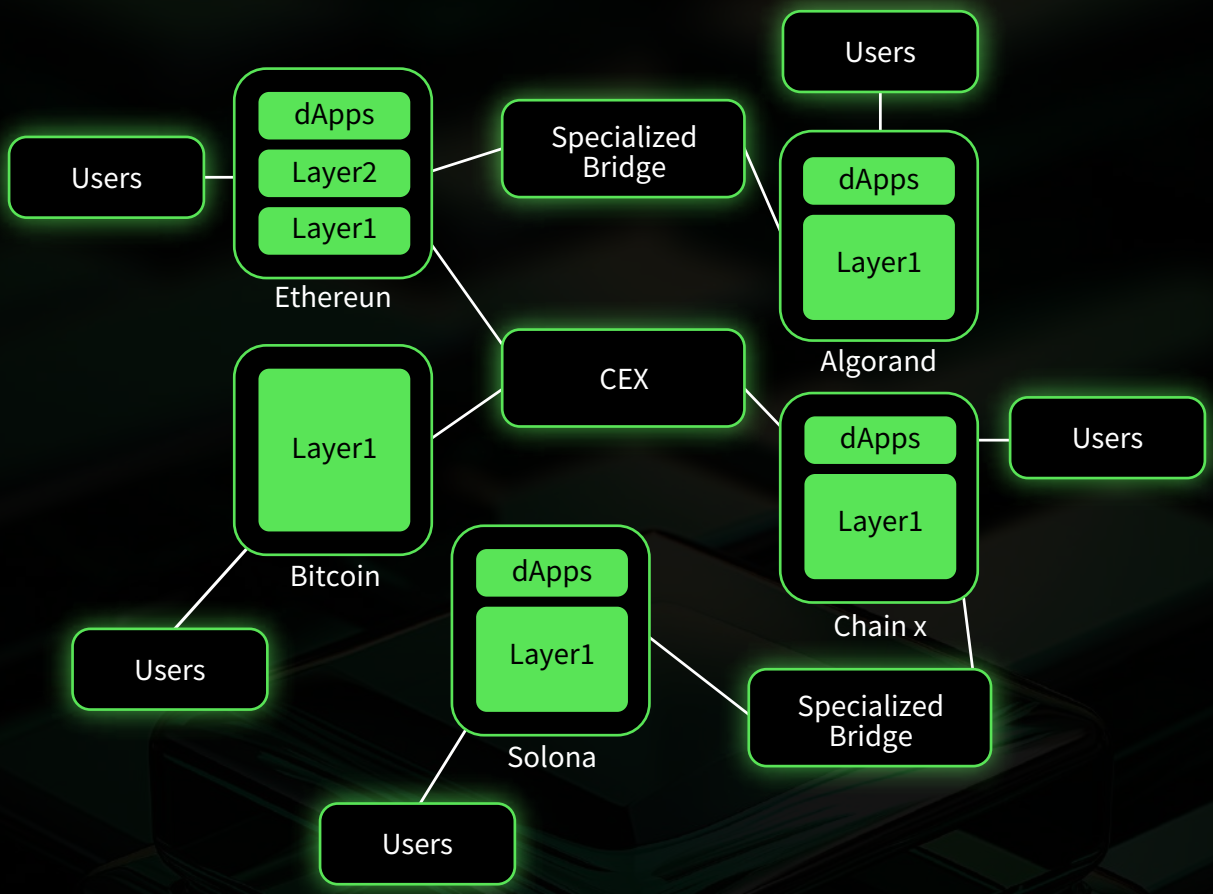
通过引入创新的观察者节点和多方阈值签名方案，熵增公链确保了跨链交易的安全与可靠，同时，我们的单一跨链Gas代币机制简化了跨链操作，为用户提供了极致的便利。熵增公链的核心在于其能够链接智能合约链和非智能合约链，包括但不限于Ethereum Chain 以太坊链、Binance Smart Chain 币安智能链, Bitcoin Chain 比特币链等，实现真正的全链互通。

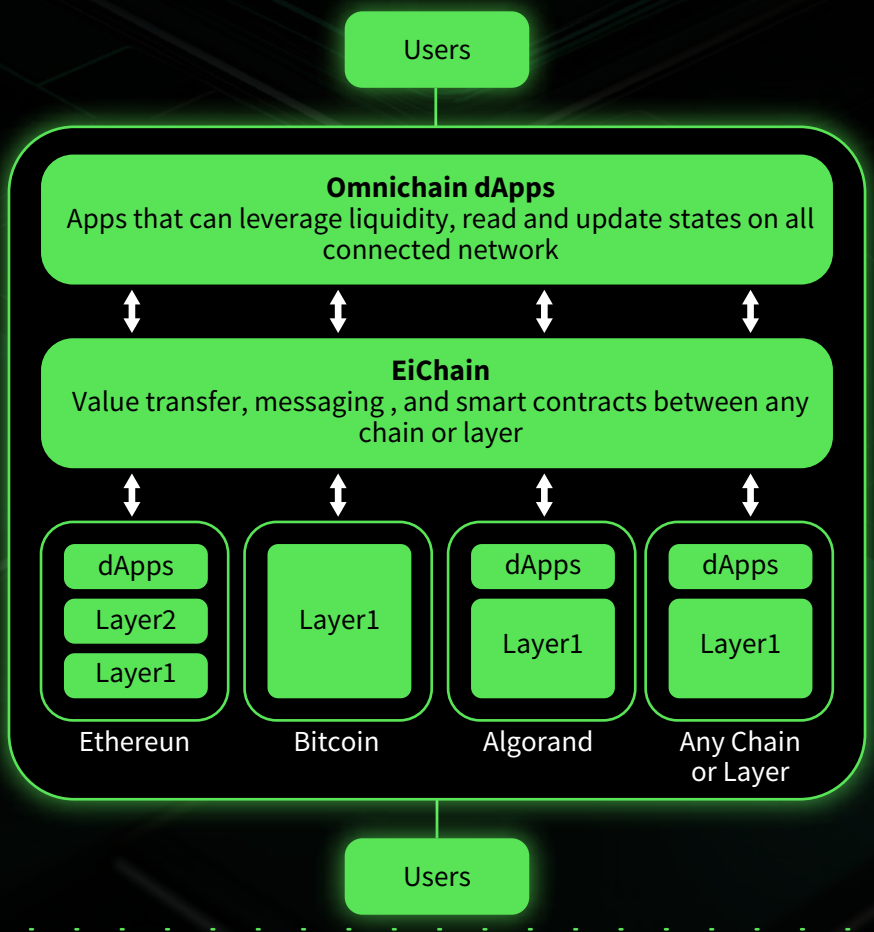
在熵增公链的设计与实现中，我们采纳了一系列前沿的区块链技术，致力于解决当前区块链生态系统中的核心挑战，特别是在互操作性、安全性和扩展性方面。熵增公链引入了权益证明（Delegated Proof-of-Stake, DPoS）共识机制，并通过创新的观察者节点和签名者节点结合多方阈值签名方案（TSS），来确保跨链操作的安全与高效。这些技术的应用不仅加强了网络的去中心化和拜占庭容错能力，还实现了对智能合约链和非智能合约链的全面支持，打开了构建跨链或"全链"去中心化应用（dApps）的大门。

熵增公链旨在成为支持真正跨区块链交易、消息传递和通用跨链智能合约的公共区块链平台，为区块链技术的未来发展开辟新的可能性。 本白皮书将详细介绍熵增公链的技术架构、核心组件、安全措施、应用场景及发展路线图，旨在为读者提供一个全面的熵增公链技术和愿景概览。






Users
dApps
Layer2
Layer1
Ethereun
Specialized Bridge
Users
dApps
Layer1
Algorand
CEX
Layer1
Bitcoin
dApps
Layer1
Chain x
Users
Users
dApps
Layer1
Solona
Specialized Bridge
Users


Users
Omnichain dApps
Apps that can leverage liquidity, read and update states on all connected network
EiChain
Value transfer, messaging , and smart contracts between any chain or layer
dApps
Layer2
Layer1
Ethereun
Layer1
Bitcoin
dApps
Layer1
Algorand
dApps
Layer1
Any Chain or Layer
Users

02 项目概览

02 项目概览

2.1. 熵增公链简介

熵增公链是一个革命性的区块链平台，旨在通过其独特的熵增技术和高度创新的区块链架构，解决当前区块链生态中存在的互操作性问题。熵增公链利用先进的人工智能和云计算技术，为区块链世界带来了前所未有的安全性、效率和灵活性。作为一个去中心化、高效、安全的全链生态系统，熵增公链使得任何资产和信息都能自由流动，无论它们原本属于哪个区块链平台。

2.2. 主要目标

熵增公链的主要目标是创建一个真正的全链互通生态系统，其中包括智能合约链和非智能合约链之间的链接。通过引入观察者节点和多方阈值签名方案，以及单一跨链Gas代币机制，熵增公链旨在简化跨链操作，提高区块链技术的可用性和用户体验。其目标是促进不同区块链之间的无缝链接和交互，从而加速区块链技术的整体发展和应用推广。

2.3. 解决的核心问题

2.3.1. 多链的出现和挑战

在区块链技术的迅速发展中，市场趋向于一个多元化的生态系统，由多个区块链构成。这些区块链在安全性、去中心化、可扩展性、速度、成本以及合规等方面各有侧重，需要做出相应的权衡。在这个多链的未来里，区块链平台通常被设计为封闭系统，这意味着它们只能处理并更新自己的状态。没有可靠的去中心化机制，外部信息很难被引入区块链中，而跨链交易则依赖于中心化实体，如交易所来执行，限制了去中心化和公共服务实现通用原子交易的能力。

目前的跨链策略，如侧链、中继、公证方案、哈希时间锁合约和区块链的区块链（BoB）模型，都在尝试解决这些挑战。尽管这些策略在促进互操作性方面取得了进展，但它们各自都有局限性，尤其是在去中心化和无需许可的通用交易执行方面。

2.3.2. 熵增公链的核心问题解决

熵增公链应运而生，旨在通过独特的熵增技术和创新的区块链架构，突破现有的壁垒，实现一个真正去中心化、无需许可的全链互通平台。它不仅解决了现有跨链策略的限制，还引入了以下创新解决方案：

1.去中心化的互操作性：
熵增公链通过观察者节点和多方阈值签名方案（TSS），提供一个去中心化的信任机制，使得跨链交易不再依赖于中心化实体或复杂的公证程序。

2.原子交易的通用性：
与传统的HTLC相比，熵增公链支持包含任意逻辑的原子交易，不仅仅局限于资产交换。

3.全链互通性：
通过链接各种区块链，包括智能合约链和非智能合约链，熵增公链极大地增强了跨链资产和信息的流动性。

4.智能合约的扩展性：
熵增公链支持全链智能合约，使得开发者可以构建真正意义的去中心化应用，这些应用能够在多个区块链平台上无缝运行。

在当前的多链环境中，跨链通信是区块链互操作性的基础构建块，其目的是允许一个区块链验证另一个区块链上已发生的特定交易。BTCRelay和Rainbow Bridge是旨在从比特币向以太坊建立单向桥梁的尝试，而Wormhole和LayerZero则分别依赖于验证节点集合和轻量级通信层来促进跨链信息的流动。IBC协议提供了一种端到端的通信方式，但它要求链本身内置支持IBC，这对于现有和传统的区块链构建来说是一个较高的要求。

在跨链资产转移方面，Hop、Connext和Multichain等协议通过各种机制解决了跨链交易的问题，从而使代币能够在不同区块链及其派生的Rollups之间自由流动。而对于跨链智能合约，Quant网络、ICP/Chain-Key和HyperService提出了不同的解决方案，以支持智能合约在多链环境下的执行和通信。

然而，这些现有的解决方案虽然在一定程度上提高了跨链通信和资产转移的可能性，但它们大多数还是存在局限性。特别是在去中心化、安全性、效率以及对现存和遗留系统的适应性方面。

2.4. 熵增公链的互操作性相关工作

熵增公链针对现有跨链通信和资产转移的挑战，提出了一种全新的互操作性框架。利用其先进的熵增技术，熵增公链实现了一个真正去中心化、无需许可的跨链通信和资产转移系统。

1

去中心化的互操作性：
熵增公链的跨链通信功能不依赖于中心化的验证节点或者轻量级的客户端，而是通过创新的观察者节点和多方阈值签名方案（TSS）来确保链与链之间的信息可靠传递。这种机制不仅提高了安全性，也大幅降低了操作成本，因为它不需要不断更新区块头链信息

2

跨链资产转移
熵增公链通过单一跨链Gas代币机制简化了跨链资产的转移。与传统的HTLC和AMM市场不同，熵增公链允许资产在不同的区块链间直接转移，无需通过第三方或集中化的桥梁。这种方式不仅保证了交易的原子性，还确保了过程的去中心化和无需信任。

3

跨链智能合约

借助熵增算法和高效的共识机制，熵增公链打造了一个支持跨链智能合约的平台，允许开发者在多链环境中创建和部署智能合约。与Quant网络等中心化服务不同，熵增公链提供了一个完全去中心化的环境，减少了信任假设，并提高了透明度和可验证性。

4

BoB（区块链的区块链）

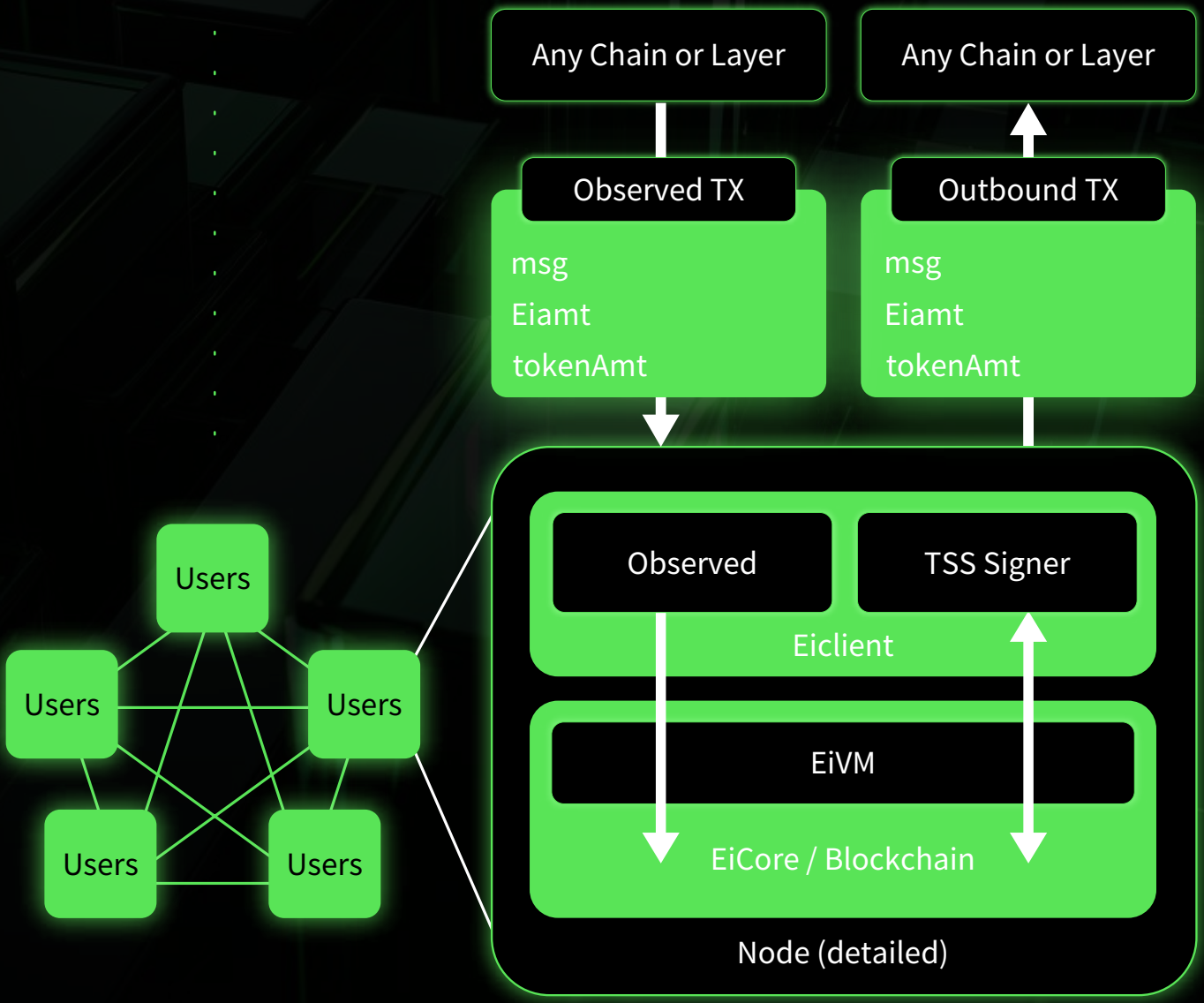
熵增公链也为BoB框架提供了支持，允许不同功能的专用链在其平台上无缝集成和互操作。与Cosmos和Polkadot不同，熵增公链不要求链在共同的基础设施上构建，它提供的互操作性对现有和传统区块链是开放的，无需对现有系统进行大规模的改造。

03 熵增公链的技术和创新

03 熵增公链的技术和创新

3.1. 熵增技术介绍

熵增公链采用了一种创新的熵增技术，它结合了区块链的分布式特性与高效的算法来优化系统的熵值，从而提高了网络的安全性和稳定性。熵增技术利用复杂性理论和最新的密码学研究，确保网络在面对各种攻击时能保持鲁棒性，同时也为跨链交易和智能合约的执行提供了高效的基础。



3.2. 核心组件

熵增公链采用了一种创新的熵增技术，它结合了区块链的分布式特性与高效的算法来优化系统的熵值，从而提高了网络的安全性和稳定性。熵增技术利用复杂性理论和最新的密码学研究，确保网络在面对各种攻击时能保持鲁棒性，同时也为跨链交易和智能合约的执行提供了高效的基础。

1 观察者节点

熵增公链的观察者节点充当外部链事件的监控者和验证者，他们负责捕捉链上的状态变化，并将信息传递到熵增公链上以便进一步处理。观察者节点的设计确保了即使在复杂的多链环境中，熵增公链也能准确、快速地反映外部链的状态。

2 签名者节点

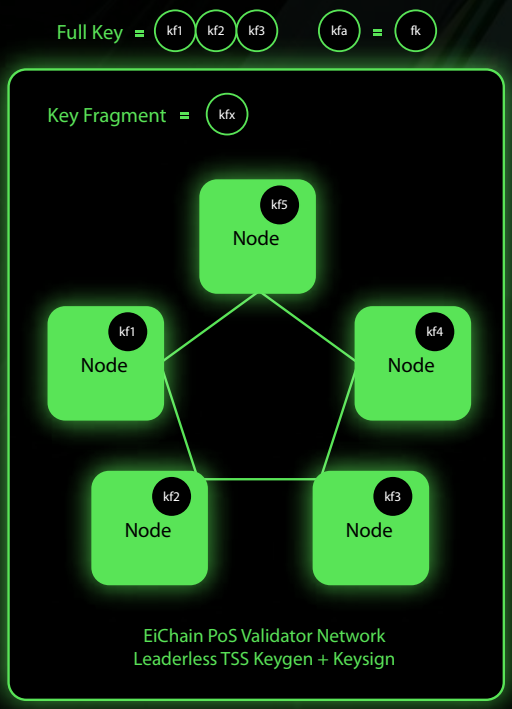
签名者节点在熵增公链中起着关键作用，它们使用多方阈值签名方案（TSS）对跨链交易进行签名，保证了交易不仅安全而且去中心化。这些节点共同持有一个分布式密钥，无单点故障，提供了网络和资产的额外保障层。

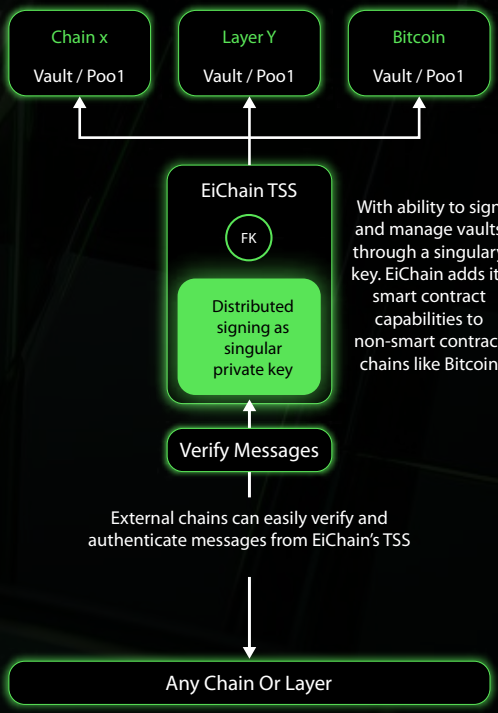
3 多方阈值签名方案（TSS）

熵增公链的TSS是一项先进的技术，允许多个节点协作产生一个单一的加密签名，这一过程无需暴露私钥的任何部分。TSS增加了对抗恶意行为者的能力，由于没有单个节点拥有完整的密钥，因此极大地增强了安全性。

4 单一跨链 Gas 币种

消除用户在进行跨链操作时需要持有和管理多种Gas币种的复杂性。用户仅需持有EIC熵增币，系统便能自动处理在不同区块链之间进行交易时所需的Gas转换，这极大地简化了用户的操作流程，降低了参与跨链活动的门槛。此外，这种机制也为熵增公链提供了一个强大的竞争优势，因为它允许熵增公链成为一个交易成本可预测且经济高效的跨链平台。通过消除在不同区块链之间进行资产转移时所需的多个步骤和交易费用，熵增公链旨在提供更为流畅和成本效益高的用户体验。在技术实现方面，熵增公链的智能合约会监控当前的Gas价格，并利用内置的价格喂价系统，确保每笔交易使用正确数量的EIC熵增币来支付相当于目标链Gas币种的费用。这种动态调整机制确保了跨链交易的高效性，同时保持了网络的稳定性和可靠性。





3.3. CometBFT共识机制

CometBFT（Byzantine Fault Tolerance）是一种共识机制，旨在为分布式系统提供高度安全和高效率的共识解决方案。它允许系统在面对任何节点的恶意行为或故障时，仍能达成一致共识。CometBFT是基于经典的拜占庭容错（BFT）协议，但进行了优化以提高性能和可扩展性。

在熵增公链（EiChain）中，CometBFT共识机制可能被实施为核心的共识算法，以确保网络的安全性和稳定性。这意味着即使网络中最多有一定比例的节点表现恶意或遇到故障，熵增公链仍能正常运行，确保交易的正确性和网络的不间断运行。

实现CometBFT共识机制的步骤包括：

1.节点验证 熵增公链将验证参与共识的所有节点，确保它们是可信的和合格的。

2.消息广播 每个节点会广播其消息（如交易或区块提议），并接收来自其他节点的消息。

3.投票和确认 节点根据收到的信息进行投票，当超过三分之二的验证节点同意时，就可以确认一个区块或交易。

4.区块最终确定 节点根据收到的信息进行投票，当超过三分之二的验证节点同意时，就可以确认一个区块或交易。

通过实施CometBFT共识机制，熵增公链能够提高其网络的安全性和效率，同时确保其分布式账本的正确性和透明度。这对于建设一个稳定可靠的Web3.0平台至关重要，为用户和开发者提供一个安全、高效、去中心化的环境。

3.4. 全链互通区块链

熵增公链旨在建立一个全链互通的生态系统，这个生态系统能够无缝链接智能合约平台和非智能合约的传统区块链。它通过以下方式实现：

1 链接智能合约链

熵增公链设计了一套先进的协议，该协议能够与现有的智能合约链进行互操作，包括Ethereum及其L2扩展解决方案、Solana、Polygon和Binance Smart Chain等。该协议不仅仅局限于代币转移，它们还支持调用智能合约方法、触发事件以及执行更复杂的操作，从而实现了智能合约链之间的流畅链接和通信。

熵增公链的核心是其熵增算法和观察者节点网络，这些节点能够监控和验证跨链事件，通过TSS（多方阈值签名方案）来确保交易的安全执行。这样的设计允许智能合约的状态和逻辑能够跨链运行，为去中心化应用（dApps）开辟了跨链互动的可能性。

2 链接非智能合约链

熵增公链扩展了其互操作性到非智能合约链，如Bitcoin和Dogecoin。这些链本质上不支持智能合约或复杂的交易类型。熵增公链通过跟踪和验证其网络上的交易，并允许在熵增公链上执行相应的逻辑，从而实现了与非智能合约链的交互。

为了桥接传统区块链与现代DeFi生态系统，熵增公链引入了创新性的适配器智能合约技术。这些智能合约被设计成能够理解并执行非智能合约链，如比特币和莱特币等，上的交易逻辑和规则。这种能力使得原本无法支持复杂交互的传统链能够无缝地融入现代的去中心化金融（DeFi）应用中。

通过熵增公链的适配器智能合约，用户可以实现如下功能：

1.跨链质押

用户可以将传统区块链资产（如比特币）跨链到熵增公链，并参与质押活动，从而获得奖励或收益。

2.跨链借贷

在熵增公链上，用户不仅可以借出其传统区块链上的资产，还能在去中心化的借贷平台上借入其他资产，增加资金流动性和投资机会。

3.多链DeFi参与

利用适配器智能合约，传统区块链资产可以参与到熵增公链及其他链上的DeFi应用中，如流动性挖矿、自动化市场做市（AMM）、合成资产发行等。

这些适配器智能合约不仅极大拓展了非智能合约链的功能性，使其能够参与到丰富多样的DeFi场景中，也极大地增强了熵增公链的互操作性和灵活性。通过将传统和现代区块链世界连接起来，熵增公链正在推动一个更加开放、可互联的数字资产生态系统。

3 安全和去中心化

熵增公链的安全机制建立在去中心化的基础上。通过分布式的验证者网络和TSS，熵增公链确保了没有中心化的弱点，从而抵御潜在的攻击或故障。此外，熵增公链利用其熵增算法优化网络的熵值，增强了网络的安全性和稳定性。

4 交互的自然流动性

熵增公链的跨链Gas币种机制进一步增强了全链互通性。这一机制允许用户仅使用熵增公链的本地代币即可支付在任何链接的区块链上进行交易时所需的Gas费用，无需担心多种货币的管理，从而实现了真正的跨链经济活动

3.5. 基础的、EVM兼容公共区块链网络

熵增公链构建了一个基础的、与以太坊虚拟机（EVM）兼容的公共区块链网络，这为现有的区块链生态系统提供了一个强大的迁移和发展平台。这样的设计允许熵增公链实现以下功能：

3.5.1. 支持存量生态系统迁移

熵增公链使得存量生态系统能够无缝迁移到其平台上。通过与EVM的兼容性，它允许现有的以太坊应用程序和智能合约在不需要重写代码的情况下迁移至熵增公链，这大大简化了迁移过程。熵增公链提供了一种机制，允许开发者通过最少的配置更改，快速地将他们的服务从以太坊转移到更快、成本更低的熵增公链上。

3.5.3. 如何实现

熵增公链通过以下方式实现了这些目标：

1. **EVM兼容性：**
   熵增公链保持了与EVM的完全兼容，保证了以太坊上的智能合约和DApps可以在熵增公链上运行而无需任何修改。这一兼容性承诺确保了开发者能够利用现有的以太坊智能合约知识和资产库。

2. **迁移工具：**
   熵增公链开发了一系列迁移工具，帮助开发者轻松地将他们的应用程序和资产从以太坊移植到熵增公链。这些工具自动处理了大多数迁移任务，简化了从一个链到另一个链的过渡。

3. **开发者支持：**
   熵增公链提供了强大的开发者支持和文档，包括详细的API文档、最佳实践指南和教程，以及一个活跃的社区论坛，所有这些都是为了帮助开发者更好地利用平台。

4. **性能优化：**
   针对熵增公链的性能进行了优化，以处理高吞吐量的交易，这对于希望扩大其应用规模的开发者尤其重要。优化的共识算法和网络协议使得熵增公链能够处理比以太坊更多的交易，同时保持低延迟和低成本。

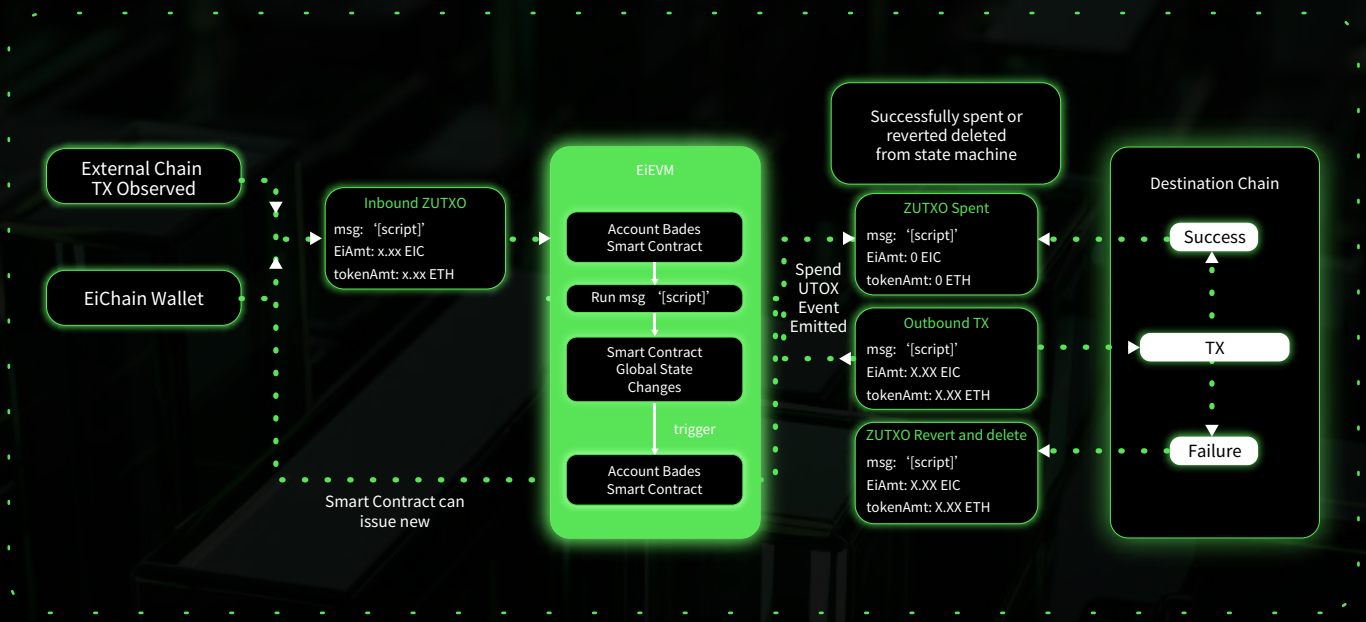
5. **资源丰富的生态系统：**
   熵增公链投资于建立一个资源丰富的生态系统，包括开发者工具、用户界面组件以及预先构建的智能合约模板，这些都旨在减少开发时间并提高用户体验。

3.6. 链间消息传递 (CCMP)

链间消息传递（Cross-Chain Message Passing，CCMP）是一种跨链通信机制，它允许不同的区块链网络之间传递和验证消息。这种机制使得一个智能合约能够调用另一个链上的智能合约，并处理跨链交易和信息的流动。CCMP是实现复杂跨链交互和资产转移的基础技术，为构建跨链应用（dApps）提供了可能。

3.6.1. EIEVM

EIEVM指的是Entropy Increment Ethereum Virtual Machine，它是熵增公链上一个与Ethereum虚拟机（EVM）兼容的执行环境。EIEVM支持执行标准的Ethereum智能合约，并通过CCMP机制，允许这些合约参与跨链操作。这意味着开发者可以使用熟悉的Solidity语言编写智能合约，并在熵增公链上部署和执行，同时实现与其他区块链的互通。



3.6.2. UTXO与EOA

UTXO（Unspent Transaction Output）

UTXO模型是比特币和一些其他区块链所采用的账户模型，每笔交易都有输入和输出，输出未被花费前都被视为UTXO。UTXO模型以其隐私性和并行处理能力而闻名。

优化的签名机制

为了提高跨链通信的效率和安全性，熵增公链采用了批量签名和并行签名机制。这些机制可以在保持高安全性的同时，减少因签名操作导致的延迟，并增加系统的吞吐量。

3.6.3. 熵增公链的实现

熵增公链通过以下方式实现了上述概念：

CCMP支持

熵增公链通过CCMP机制，建立了一个消息和价值的中继系统，允许智能合约不仅在其原生链上执行，还可以跨链调用其他链上的合约。这一系统使得EIC（熵增公链的本地代币）能够在多个链上流通，无需用户直接参与复杂的跨链操作。

1

优化的签名机制

为了提高跨链通信的效率和安全性，熵增公链采用了批量签名和并行签名机制。这些机制可以在保持高安全性的同时，减少因签名操作导致的延迟，并增加系统的吞吐量。

2

混合账户模型

熵增公链引入了一种混合UTXO和EOA账户模型，结合了UTXO模型的高并发性和EOA模型的灵活性。这种混合模型增强了系统的安全性，因为它可以结合利用两种模型的优势。

3

3.7. 全链智能合约与非智能合约链的互通性

熵增公链创造了一个全新的范例，通过引入全链智能合约，实现了对原本不支持智能合约的区块链（如Bitcoin， Dogecoin）的支持。这是通过以下几个关键组件和创新的工作方式来实现的：

1.观察者和签名者的作用

在熵增公链中，观察者节点负责监控外部区块链上的活动，如比特币或狗狗币网络中的交易。这些观察者在检测到相关事件或交易时生成证据，这些证据随后被签名者节点验证。签名者节点是一群持有分布式密钥部分的节点，它们协同工作以在熵增公链上执行操作，如代币发行或合约调用，从而确保了跨链交互的安全性和有效性。

2.验证者和委托人的参与

在熵增公链中，观察者节点负责监控外部区块链上的活动，如比特币或狗狗币网络中的交易。这些观察者在检测到相关事件或交易时生成证据，这些证据随后被签名者节点验证。签名者节点是一群持有分布式密钥部分的节点，它们协同工作以在熵增公链上执行操作，如代币发行或合约调用，从而确保了跨链交互的安全性和有效性。

3.全链智能合约

熵增公链上的全链智能合约类似于以太坊上的智能合约，但它们具有任意可编程性，并且可以直接管理和被外部链调用。这意味着熵增公链上的智能合约可以直接与比特币或狗狗币这样的非智能合约链进行交互，扩展了跨链应用的可能性。这是通过在熵增公链上模拟这些非智能合约链的功能实现的，从而允许智能合约执行与这些链相关的操作，如处理比特币交易。

3.7.1. 如何实现

熵增公链实现上述功能的关键在于其创新的技术架构：

1.跨链适配器 为每个非智能合约链定制开发跨链适配器，使得熵增公链能够理解和交互这些链上的原始交易格式。

2.智能合约编程接口 提供标准化的智能合约编程接口，允许开发者编写能够响应外部区块链事件的合约逻辑。

3.高效的共识协议 运用高效的共识协议来快速验证和记录跨链交互，保证了系统的响应速度和稳定性。

4.安全的密钥管理 采用多方阈值签名技术分散密钥管理风险，即便是在执行跨链交易时，也保证了高安全标准。

5.动态链间通信 实施高度动态的链间通信协议，以适应各种区块链的特性和网络条件。

3.8. 委托权益证明 (DPoS) 共识机制

基于委托权益证明（Delegated Proof of Stake，DPoS）共识机制，结合了权益证明（Proof of Stake，PoS）的安全性和集中投票机制的效率。在DPoS系统中，代币持有者通过投票选择代表（验证人）来保护网络，这些验证人负责验证交易和创建新区块。

DPoS的主要优点在于它提高了网络的效率和可扩展性，同时还允许更广泛的参与和治理。与传统的PoS相比，DPoS通过减少直接参与共识过程的节点数量来达到这一点，从而加快决策过程并降低资源消耗。

3.8.1. 熵增公链的DPoS实现

熵增公链通过以下方式实现了DPoS共识机制：

1 选举和投票

在熵增公链生态系统内，代币持有者不仅拥有资产，还拥有决策权。这是通过一个透明且去中心化的选举和投票机制实现的，允许每一位EIC代币持有者参与到网络治理中，特别是在选举网络验证人方面。

代币持有者的角色至关重要，因为他们通过投票决定哪些候选人将成为验证人。每个持有者的投票权重与其持有的EIC代币数量成正比。这意味着每位用户都可以根据候选人的表现、信誉、提供的安全性和网络贡献等因素，来决定自己的投票。这促进了一个健康、竞争和安全的网络环境，因为验证人需要赢得社区的信任才能获得和保持其地位。

此外，这种投票机制增强了社区成员之间的互动，鼓励他们参与到网络的日常运维中来。这不仅提高了网络的去中心化程度，也确保了网络的方向和发展能够真正反映其社区的意愿。通过这种方式，熵增公链赋予了其用户真正的权力和声音，为创建一个更加公平、透明和用户驱动的区块链世界铺平了道路。

2 激励机制

验证人和委托人都会从网络维护中获得奖励。验证人因其创建区块和验证交易的工作获得奖励，而委托人则因为贡献其持有的代币以选举验证人而获得部分奖励。这一激励机制鼓励了网络的安全和活跃参与。

3 网络效率

由于选出的验证人数量相对较少，网络能够更快地达成共识，从而提高整体的交易吞吐量。这使得熵增公链能够处理大量的交易，同时保持较低的延迟。

4 安全和去中心化

尽管DPoS倾向于中心化验证人的选择，但熵增公链通过设计确保了网络的去中心化。验证人的权力受到代币持有者投票结果的限制，且验证人之间的竞争保持了网络的健康和去中心化。

5 动态调整

熵增公链可以根据网络的需要和参与者的反馈，动态调整验证人的数量和奖励机制。这种灵活性允许网络适应变化的市场条件和安全需求。

3.9. 熵增公链与工作量证明（PoW）的融合

熵增公链在设计其跨链生态系统时，创新性地将工作量证明（PoW）机制纳入其架构中。这一举措不仅允许熵增公链利用现有的硬件资源，如GPU和专用矿机，但也为区块链技术与人工智能的结合开辟了新途径。通过这种融合，熵增公链能够充分利用PoW机制的安全性和去中心化特性，同时提高其网络的处理能力和效率。

具体来说，通过将PoW机制集成到熵增公链中，该平台能够使用户利用其现有的硬件设备，如存储解决方案和计算设备，来参与网络的维护和发展。这不仅为用户提供了获得奖励的机会，还增加了网络的安全性和抗攻击能力。

此外，熵增公链的PoW机制还支持了其跨链生态系统中的各种应用，从而推动了生态应用的多元化和创新。例如，通过“X-to-Earn”模式，用户可以通过社交挖矿、交易挖矿、运动挖矿等多种方式参与到生态系统中，这不仅增加了用户的参与度和活跃度，还为整个生态系统的增长和繁荣提供了动力。

通过这种方式，熵增公链的PoW融合不仅增强了其网络的性能和安全性，还促进了新应用的开发和部署，使得熵增公链成为一个更加多元化、高效和用户友好的跨链平台。

3.9.1. 什么是工作量证明（PoW）？

工作量证明（Proof of Work, PoW）是一种加密货币共识机制，要求参与者通过执行复杂计算任务来验证交易和创建新的区块。这一过程通常被称为“挖矿”，需要大量的计算能力，以确保网络的安全和去中心化。PoW的核心思想是通过“计算工作”来证明参与者对网络的贡献，从而获得相应的奖励。

3.9.2. 熵增公链中的PoW角色

熵增公链将PoW机制作为其核心组成部分，通过以下两个创新方式实现了PoW在新时代的应用：

1 硬件链接与AI算力

熵增公链允许链接现有硬件资源（如Filecoin矿机、Ethereum矿机、GPU等）作为存储和提供AI算法所需的计算力。这种硬件的利用不仅提高了资源的使用效率，也为AI应用的发展提供了强大的后盾。

2 X to Earn模式的多样化

熵增公链通过PoW机制引入了多种“X to Earn”模式，包括社交挖矿、分享挖矿、交易挖矿、运动挖矿、骑行挖矿、消费挖矿等。这些模式通过奖励用户参与区块链网络的各种活动，不仅增强了社区的活跃度，也推动了应用生态的多样化发展。

3.9.3. 实现方式

熵增公链实现PoW的关键在于其创新的技术架构和智能合约设计，这些设计使得硬件资源能够轻松接入网络，并为不同类型的“X to Earn”活动提供支持。此外，熵增公链采用了先进的加密技术和共识算法，确保了网络的安全性和效率。

通过这种方式，熵增公链不仅解决了传统PoW面临的能源消耗和效率低下问题，也为用户提供了新的价值创造途径。熵增公链的PoW实现体现了区块链技术的创新和进步，为构建更加开放、可持续和多元化的区块链生态系统奠定了基础。

04 熵增公链架构细节

04 熵增公链架构细节

4.1. 跨链智能合约技术

熵增公链托管一个与EVM兼容的执行层，我们可以称之为EIEVM。这个执行层不仅支持EVM的所有功能，还增加了以下关键特性：

1

跨链合约调用：

EIEVM上的合约能够被外部链调用，实现了智能合约的真正跨链互动。这种互动打破了区块链之间通信的边界，允许在不同链之间自由地触发和响应智能合约事件。

2

生成出站交易：

在EIEVM上，智能合约不仅可以管理内部状态，还能生成出站交易，并在外部链上执行。这意味着熵增公链上的智能合约能够对外部区块链进行操作，扩大了其功能范围。

4.1.1 熵增公链的通用跨链交易技术

熵增公链面对通用跨链交易时，解决了两大核心挑战：异步性和原子性。

异步性的解决方案

在熵增公链中，链与链之间的通信是通过消息传递实现的，由于区块链的本质异步性，熵增公链采用了一种事件驱动的编程模型。这个模型将跨链智能合约视为一个有限状态机，其状态转换由来自其他链的消息触发。熵增公链的智能合约被设计为响应这些跨链事件，从而实现了一个分布式的事件驱动系统。这种设计使得合约能够在没有即时返回结果的情况下继续运行，同时保持了与其他链的同步。

原子性的保障

熵增公链通过内置的回滚机制来保证跨链交易的原子性。当跨链交易的某部分失败时，可以触发回滚流程，从而保证状态的一致性。熵增公链利用智能合约来监控跨链操作的状态，并在必要时执行回滚。这种方法避免了繁琐的手动回滚过程，同时确保了整个系统的健壮性。

4.1.2 混合UTXO和基于账户的方法

熵增公链结合了UTXO和基于账户的系统的优点，通过使用“合成”UTXO来跟踪和表示外部区块链交易。这些合成UTXO携带了特定数量的熵增公链代币（例如，作为燃料的EIC），以及可能的其他代币（例如，BTC、ETH），并包含一个脚本消息。当这些UTXO被花费时，熵增公链上的智能合约会触发，并产生相应的外链交易。

此外，熵增公链确保了合成UTXO的输出值等同于输入值，保持了资产的守恒。当一个交易被外链确认，相关的UTXO就被视为“花费”。若交易失败，如因燃气不足，那么这个UTXO就会被标记为“回滚”，并且任何相关的代币退款会回到原链。

这种混合模型的使用增强了熵增公链的可核算性和灵活性，同时保留了在必要时能够执行复杂操作的能力，例如在自动化做市商（AMM）中处理多个交易。

4.1.3 熵增公链跨链交易的具体实现

熵增公链将PoW机制作为其核心组成部分，通过以下两个创新方式实现了PoW在新时代的应用：

1. 跨链合约调用

用户在原链上与合约交互，触发一个带有指定消息和目标信息的事件。

2. 事件捕捉与状态触发

熵增公链观察者节点捕捉这些事件，并将其提交给智能合约处理。

3. 智能合约的自动执行

智能合约自动执行逻辑，处理合成UTXO，并生成链外交易。

4. 签名与交易广播

经过多方签名后的交易被广播至目标链，等待确认。

5. 确认与清算

一旦确认，交易被视为完成；如遇失败，启动回滚流程。

4.2. 熵增公链的跨链消息传递（CCMP）机制

在熵增公链中，跨链消息传递（CCMP）机制是一个核心组件，它使得熵增公链能够作为消息（跨链合约调用）和价值（多链代币EIC）的中继器。这种机制简化了跨链交互，并为合约之间提供了一种高效的沟通桥梁。

4.2.1. 处理交易回滚

熵增公链通过创造一个“回滚”交易来处理那些需要撤销的状态更改。这一机制的实现责任分配给了熵增公链协议和相关的应用程序合约。当回滚被触发时，熵增公链负责启动回滚交易，退还价值到原始状态，而应用程序合约则负责执行应用层面的状态回滚。这样的设计保证了即使跨链交易失败，系统也能够保持其一致性和可靠性。

4.2.2. CCMP交易的工作流程

1. 用户在原链（链A）上与合约（C1）互动，产生一个事件或事务备忘录，包含必要的目标信息如链ID、合约地址和消息。
2. 熵增公链的观察者节点捕获这个事件或备忘录，并将信息传递给核心处理模块（eicore），以验证传入的交易。
3. 核心处理模块使用OutboundTxParams来修改跨链事务（CCTX）的状态，指示TSS签名者（在熵增公链的客户端中）构建、签名和广播外部交易。
4. 一旦广播的交易被链上确认，熵增公链的客户端会将此确认报告给核心处理模块，以更新CCTX的状态。
5. 如果交易成功，CCTX标记为OutboundMined，交易完成。如果交易失败，CCTX的状态会更新为需要回滚或中止。
6. 如果需要回滚，熵增公链会创建并广播一个还原交易到原链，并调用应用合约的回滚功能。
7. 回滚交易确认后，CCTX状态更新为Reverted或Aborted，标志着该交易的处理结束。

4.2.3. 启动CCMP的接口定义

```solidity
interface EICInterfaces {
    struct SendInput {
        uint256 destinationChainId;
        bytes destinationAddress;
        uint256 destinationGasLimit;
        bytes message;
        uint256 eicValueAndGas;
        bytes eicParams;
    }
}

interface EICConnector {
    function send(EICInterfaces.SendInput calldata input) external;
}
```

在熵增公链上，发送方可以是直接的用户EOA或通过应用合约间接地指定目标链和合约。接收方的合约需要实现相应的接口来处理接收到的消息：

```solidity
interface EICInterfaces {
    struct EICMessage {
        bytes eicTxSenderAddress;
        uint256 sourceChainId;
        address destinationAddress;
        uint256 eicValue;
        bytes message;
    }
}

interface EICReceiver {
        function onEICMessage(EICInterfaces.EICMessage calldata
eicMessage) external;
}
```

这个接口允许熵增公链的智能合约接收跨链消息，并处理附带的EIC熵增币和数据。

通过这些技术和机制的集成，熵增公链确保了跨链交易的高效执行和安全回滚，为构建复杂的跨链应用提供了坚实的基础。这一全新的CCMP机制体现了熵增公链在处理跨链交互方面的创新和领先，展现了其强大的技术实力和对未来区块链互联互通的深刻洞察。

4.3. 熵增公链的全链智能合约机制

熵增公链为了减少跨链应用的复杂性，引入了全链智能合约机制，它允许在单一平台上管理和操作跨多个区块链的资产和逻辑。这个机制允许熵增公链的智能合约直接与外部链上的资产互动，并能被外部链直接调用，提供了一种全新的多链应用程序开发方式。

4.3.1. 全链智能合约的功能

1.任意可编程性 与EIEVM上的常规智能合约相似，熵增公链的全链智能合约可以编写复杂逻辑，并直接在熵增公链上执行.

2.管理外部资产 全链智能合约能够管理来自外部链的资产，比如比特币或以太坊上的代币，而不需要用户在不同链之间进行复杂的资产转移操作。

3.外部链调用 这些合约可以接收外部链的直接调用，允许外部链资产在没有中间人的情况下与熵增公链上的合约进行交互。

4.3.2. 全链智能合约的实现流程

1 用户向外部链的TSS地址发送资产，并附带一个指向熵增公链上合约地址和消息的备注。

2 熵增公链的核心系统检测到该调用并验证，然后调用SystemContract的`depositAndCall()`函数，它进而调用用户指定的全链智能合约的`onCrossChainCall()`函数。

3	全链智能合约接收外部资产，并根据用户提供的消息执行预定的业务逻辑。
4	如果需要，合约可以生成新的跨链交易，将资产或其结果发送回外部链或到另一个目标地址。
5	如果全链智能合约的执行失败，熵增公链将自动创建一个回滚交易，以恢复到交易之前的状态，并将资产退还给用户。

4.3.3. 全链智能合约与CCMP的对比

相比于传统的CCMP，全链智能合约提供了一个更集中的解决方案，将应用状态和逻辑集中在熵增公链上，简化了不同链之间状态的同步和通信。这种集中式的处理方式减少了跨链交互的延迟，降低了开发和运维的复杂性，同时也简化了回滚处理。

附注

资产类型的扩展

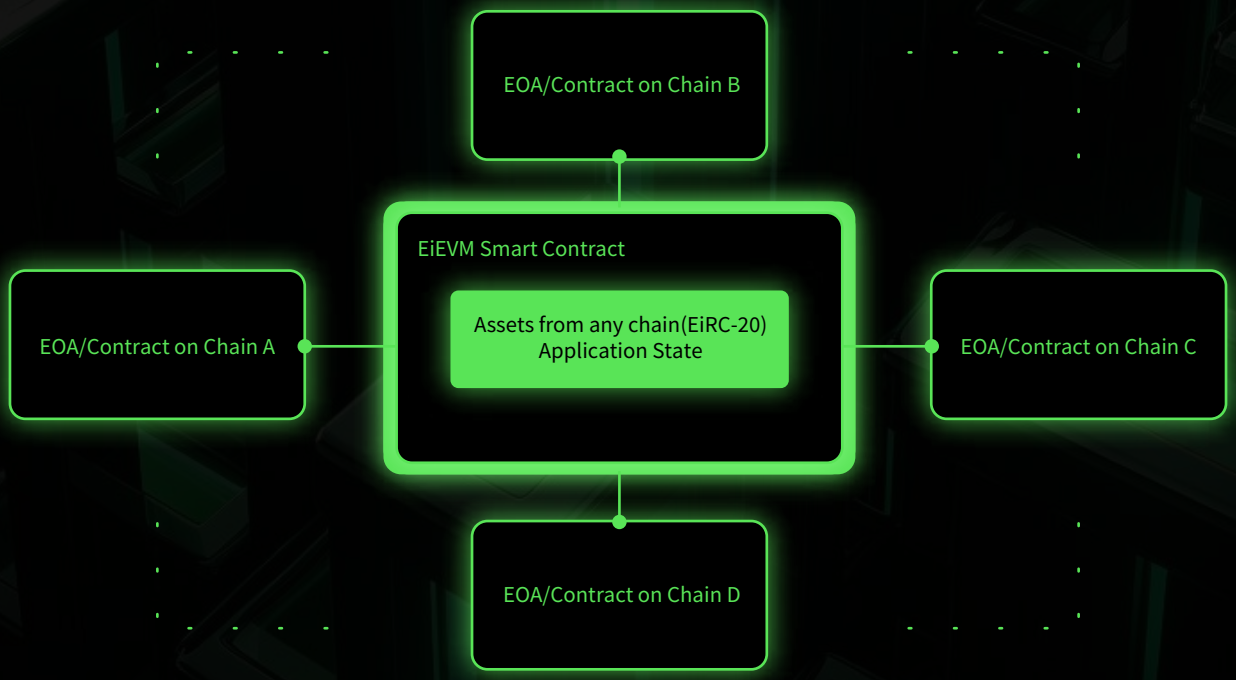
熵增公链的全链智能合约能够支持各种类型的资产，包括非可交换代币、不可转让代币、数字身份等，提供了强大的扩展性。

非智能合约链的支持

由于全链智能合约在熵增公链上执行所有操作，因此它们可以支持那些原本不支持智能合约的区块链，如比特币网络，为这些链提供了智能合约的功能。

4.4. 全链智能合约与跨链信息传递的比较

全链智能合约和跨链信息传递是实现跨链交互的两种机制，它们各有优势和局限，适用于不同类型的区块链应用程序。下面介绍全链智能合约如何为开发人员和用户提供一个更加统一和简化的跨链交互体验。

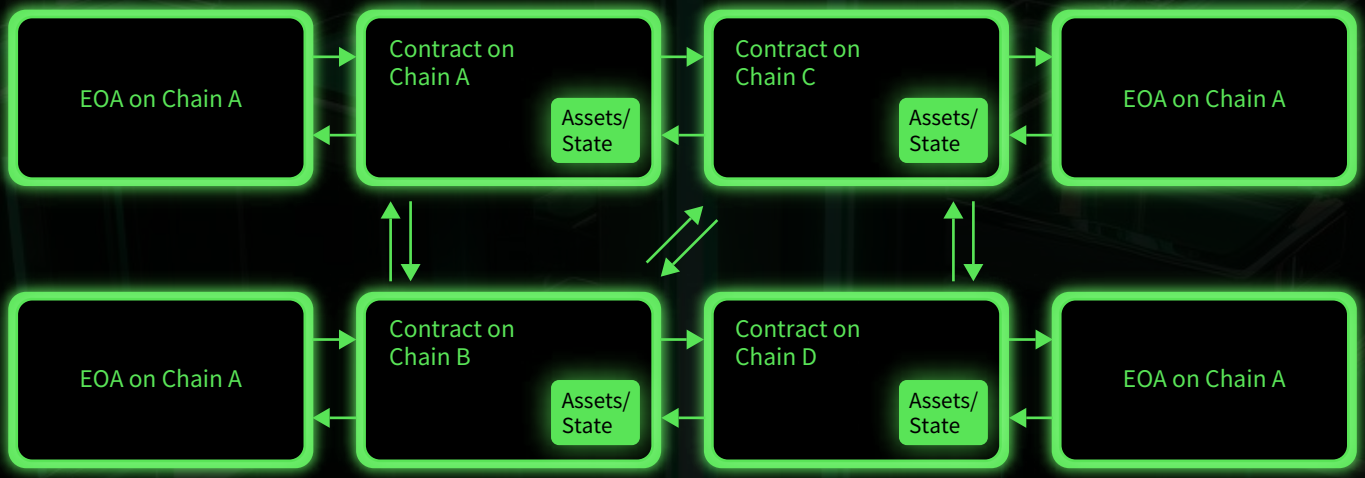


4.4.1. 全链智能合约的优势

全链智能合约将所有逻辑和状态集中在一个地方，为开发者提供了一种所有资产和逻辑都在单一链上操作的体验。这种集中化的架构降低了跨链应用的复杂性，并显著减少了因状态不一致而导致的安全风险和额外的Gas费用。更复杂的dApp，如去中心化金融（DeFi）平台，可以直接在全链智能合约上实现，而无需为了同步状态和逻辑而跨多个链广播消息。

4.4.2. 跨链信息传递的局限

与全链智能合约相比，跨链信息传递要求应用的状态和逻辑分布在多个链上，使得开发和运维变得更加复杂。在同步状态和逻辑时需要更多的消息传递和Gas费用，尤其是在涉及多个链的情况下。例如，跨链的资产管理和借贷协议的复杂性可能会随着链的数量呈指数级增长。



4.4.3. 全链智能合约在实际应用中的表现

实际上，已经在EVM上审计并经过实战测试的应用程序，如Uniswap、Curve等，可以通过最小的更改部署到全链智能合约平台上。这为用户提供了与在以太坊上相同的单步交互体验，即使是在跨链环境中。此外，由于全链智能合约的集中式特性，它们可以支持在那些原生不支持复杂智能合约的链上启动和结算交易，如比特币网络。

4.5. 熵增公链的单一跨链Gas币种机制

熵增公链通过其创新的单一跨链Gas币种机制，极大地简化了跨链交易的复杂性，确保了用户在进行跨链操作时的便利性和经济效率。此机制通过使用EIC熵增币作为统一的Gas支付手段，自动处理跨链交易中所需的Gas费用转换，从而消除了用户需要管理多种Gas币种的需求。

4.5.1. 功能优势

1. 简化操作流程

用户只需持有EIC熵增币，即可无缝进行跨链交易，无需担心不同链上的Gas费用问题，大大降低了跨链交易的操作复杂度。

2. 降低跨链活动门槛

通过消除多种Gas币种的管理需求，熵增公链使得用户更容易参与跨链活动，特别是对于非技术用户来说，这一点尤为重要。

3. 提高经济效率

熵增公链根据目标链上的实时Gas价格，自动计算并使用EIC熵增币支付等价的Gas费用，确保跨链交易的成本效益。

4.5.2. 技术实现

1. 智能合约监控

熵增公链的智能合约能够实时监控各个目标链上的Gas价格变化，确保跨链交易费用的准确性和及时性。

2. 价格喂价系统

熵增公链集成了先进的价格喂价系统，提供准确的跨链Gas费用兑换率，保证了EIC熵增币支付的公正性和市场相关性。

3. 动态调整机制

此机制确保了跨链交易在不同区块链上始终以最优化的成本进行，同时维持了网络的高效运行和稳定性。

4.5.3. 竞争优势

熵增公链的单一跨链Gas币种机制不仅优化了用户体验，还提高了平台的竞争力。它解决了传统跨链平台在费用管理上的痛点，使得熵增公链成为一个更加吸引用户和开发者的跨链解决方案。此外，这种机制还有助于促进更广泛的区块链生态系统的互联互通，推动区块链技术的进一步发展和应用。

05 熵增币（EIC）：熵增公链的能量核心

05 熵增币 (EIC)：熵增公链的能量核心

熵增币 (EIC) 作为熵增公链生态系统中的多功能实用代币，是实现跨链基础设施功能的关键。它不仅作为网络运行的基础，还确保了跨链交易的流畅执行和网络的安全性。EIC熵增币的核心用途包括但不限于以下几点：

1. **网络共识和安全性**
   质押/委托/惩罚机制：EIC熵增币支持熵增公链的DPoS共识机制，通过代币质押、委托给验证者以及对恶意行为的惩罚，确保网络的去中心化和安全运行。

2. **资源使用的公平性和效率**
   防止垃圾交易：EIC熵增币通过支付交易费用来防止网络的滥用，确保计算和存储资源的高效利用。

3. **跨链Gas支付**
   通用Gas资产：EIC作为统一的Gas支付手段，简化了跨链交易过程，用户无需关心各链的具体Gas费用细节，从而降低了跨链操作的复杂度。

4. **价值转移**
   跨链价值转移：EIC熵增币可以自由在不同的区块链之间转移，实现价值的快速流通。

5.1. EIC熵增币的核心作用

全链智能合约和跨链信息传递是实现跨链交互的两种机制，它们各有优势和局限，适用于不同类型的区块链应用程序。下面介绍全链智能合约如何为开发人员和用户提供一个更加统一和简化的跨链交互体验。

确保交易安全

质押系统：通过EIC熵增币的质押，参与者（包括验证者和观察者节点）需要锁定代币作为网络参与的保证金，增加网络的信任度和安全性。

1

激励机制

网络活跃性和效率：通过对EIC熵增币的激励，鼓励更多的网络参与者积极维护网络的稳定和安全，同时促进了网络去中心化程度的提升。

2

简化跨链操作

跨链Gas代币功能：EIC熵增币的这一角色极大地简化了跨链交易和智能合约操作的复杂度，用户无需为每次跨链操作准备不同链上的Gas费用，从而降低了参与跨链活动的门槛和成本。

3

5.2. 熵增公链发行机制与代币经济学

熵增公链采用综合的代币经济模型，旨在通过精心设计的发行机制、奖励算法、销毁模式和再生模式，推动生态系统的健康成长和持续创新。

5.2.1. 发行机制与模型

实际上，已经在EVM上审计并经过实战测试的应用程序，如Uniswap、Curve等，可以通过最小的更改部署到全链智能合约平台上。这为用户提供了与在以太坊上相同的单步交互体验，即使是在跨链环境中。此外，由于全链智能合约的集中式特性，它们可以支持在那些原生不支持复杂智能合约的链上启动和结算交易，如比特币网络。

总供应量

总供应量设定根据 EIC 交易量，以确保保持稀缺性。

销毁模式

为了防止通货膨胀并增加代币的稀缺性，熵增公链将实行代币销毁机制，部分交易手续费将被永久销毁。

再生模式

通过智能合约和链上活动，如特定任务完成或社区贡献，新的EIC熵增币可以按照设定的算法和条件生成，以奖励对生态系统有贡献的行为。

5.2.2. 代币分配与激励机制

种类分配	百分比	锁仓
用户增长池	10%	发布时为 4.5%。第一个月后 5 个月内每月解锁 0.2%。从上线后 6 个月开始，剩余代币的 1/36 将在 36 个月内每月解锁。
生态系统增长基金	12%	1.5% 在发布时。从发布后 6 个月开始，剩余代币的 1/42 每月解锁，持续 42 个月。
验证者	8%	通过4年的区块排放进行分配。
利宾金库	25%	发布时为10%，为期6个月，剩余的将在24个月解锁完毕。
算力贡献者	25%	发布时为10%，为期6个月，剩余的将在24个月解锁完毕。
流动池	5.5%	发布时为 3%。从发布开始，每月剩余解锁的 1/48。
采购商与技术	14.5%	从发布后 6 个月开始，为期 6 个月，每月解锁 1/18。12 个月后，1/36 将每月解锁 24 个月。

熵增公链代币分配与激励机制细分如下，旨在通过透明、公平的方式奖励网络的各类参与者，同时保持生态系统的健康和可持续发展：

用户增长池

专门设立以奖励参与熵增公链网络活动的用户，如交易、投票、社交互动等。目的在于鼓励更多用户加入和参与熵增公链生态系统，进而促进网络的增长和用户基础的扩大。

生态系统增长基金

旨在支持熵增公链生态系统内项目的发展，涵盖去中心化应用（dApps）开发、社区建设、营销推广等方面。通过提供必要的资金和资源，助力生态内项目成长，增强生态系统的整体实力和多样性。

验证者激励

为了保证网络的安全和高效运行，熵增公链通过区块奖励的形式，激励那些参与网络维护、处理交易和保持网络稳定的验证者。这种激励机制鼓励更多的验证者加入，增加网络的去中心化程度和安全性。

流动性激励

针对为网络提供流动性的用户，比如参与流动性挖矿或质押，熵增公链提供奖励，以促进市场的健康和稳定发展，确保资产的流通性和交易的活跃度。

礼宾金库

为未来生态系统的关键投资和战略合作留存资金。该金库将被用于支持那些能够为熵增公链带来长期价值和创新的项目和合作伙伴。

核心贡献者

对那些对熵增公链有重大贡献的团队成员和早期支持者提供奖励，以认可他们的工作和努力，并鼓励他们继续为网络的发展和成长做出贡献。

采购商和顾问

为项目提供重要指导和帮助的顾问和合作伙伴设置奖励。这些奖励旨在吸引和留住高质量的专业人士，以帮助熵增公链实现长期的成功和发展。

06 熵增公链和熵增币（EIC熵增币）应用场景

06 熵增公链和熵增币（EIC熵增币）应用场景

构建全面的跨链生态系统，旨在解决当前区块链世界中存在的隔离和互操作性问题。以下是熵增公链及其原生代币EIC在实践中的一些革新应用场景和案例：

1. **全链抽象账户智能合约钱包**

   熵增公链通过全链抽象账户智能合约钱包实现了用户资产的统一管理。用户可以在一个界面中管理和交易跨多个区块链的资产，无需为每个链分别设置钱包。这不仅提高了用户体验，还大大提高了资产管理的安全性和效率。

2. **多链NFT**

   在熵增公链上，NFT可以跨链流通和使用。艺术家和创作者可以在一个链上铸造NFT，并在另一个链上销售或展示，扩大了NFT市场的可达性和流动性，同时也为NFT带来了更广泛的应用场景，如跨链游戏和数字艺术收藏。

3. **全链DeFi**

   熵增公链使得去中心化金融（DeFi）服务可以在多个区块链之间无缝集成，用户可以访问跨链借贷、流动性池、自动做市商（AMM）等服务，不受单一区块链限制。这促进了DeFi生态系统的增长和多样性，同时也为用户提供了更多的选择和更好的收益机会。

4. **多链或多签保险库**

   熵增公链支持创建跨链的多签名保险库，为企业和高净值个人提供了高安全性的资产管理方案。这些保险库可以配置为要求多个签名者批准才能执行跨链交易，增加了资产保护的层次。

5. **通用支付**

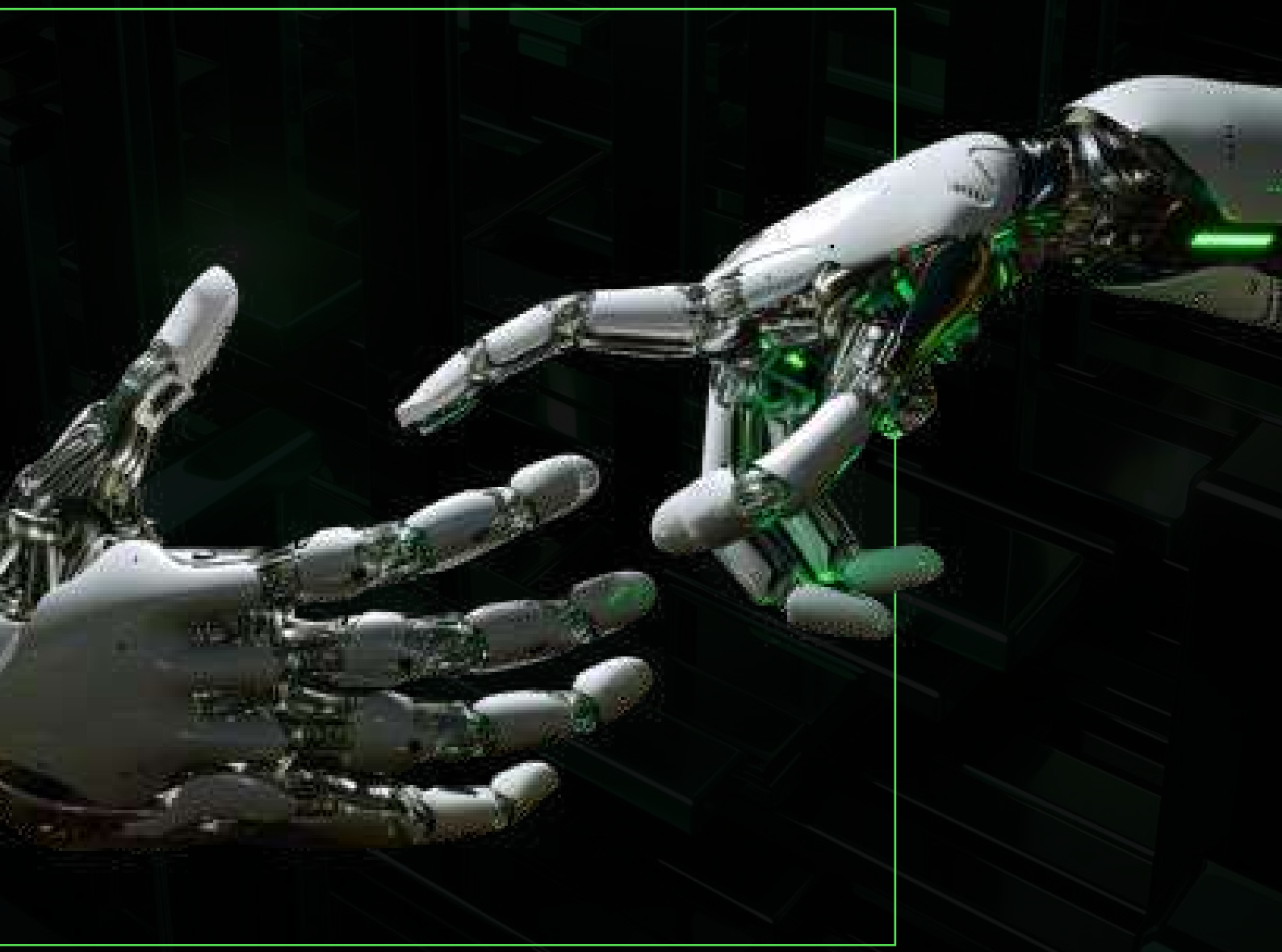
   熵增币（EIC）作为通用的跨链支付手段，用户可以在不同的区块链上使用EIC进行交易和支付。这极大地简化了跨链交易，使得跨链电子商务和服务变得更加可行和便捷。

6 链DAO

熵增公链支持创建跨链的去中心化自治组织（DAO），使得全球社区成员可以共同管理跨不同区块链的项目和资金。这为全球协作和共识决策提供了新的可能性，推动了去中心化治理的发展。

7 通用身份和资产

熵增公链提供了一个跨链身份认证框架，允许用户在不同的区块链应用和服务中使用同一个身份进行认证和访问。这不仅提高了用户体验，也为数字身份和资产的全球互联互通奠定了基础。



07 熵增公链未来展望与人工智能结合

07 熵增公链未来展望与人工智能结合

7.1. 人工智能在熵增公链中的应用

随着区块链技术和人工智能（AI）的飞速发展，熵增公链致力于探索二者的融合，以引领区块链技术的下一步革新。熵增公链计划在以下几个方面应用人工智能技术：

1. 智能合约自动优化

利用AI技术分析智能合约的性能和安全性，自动优化合约代码，减少漏洞和不必要的计算成本。

2. 交易模式识别

通过AI分析交易数据，识别潜在的欺诈行为和不正常交易模式，提高系统的安全性。

3. 跨链数据分析

使用AI技术对跨链数据进行深入分析，为用户提供更精准的市场预测、投资建议和风险评估。

4. 用户体验优化

通过机器学习了解用户行为，自动调整熵增公链平台的UI/UX设计，提供更个性化、更友好的用户体验。

5. 去中心化自治组织（DAO）的AI决策辅助

为DAO提供AI决策支持，帮助其更高效地管理社区资源和投票决策，实现自治组织的智能化管理。

7.1. 人工智能在熵增公链中的应用

随着区块链技术和人工智能（AI）的飞速发展，熵增公链致力于探索二者的融合，以引领区块链技术的下一步革新。熵增公链计划在以下几个方面应用人工智能技术：

1. 提高效率

AI的引入能自动化处理大量重复性工作，如智能合约的审核和优化，大大提高了熵增公链网络的运行效率。

2. 增强安全性

AI技术能够实时监控网络状态，识别并防范安全威胁，增强熵增公链的安全防护能力。

3. 市场预测和资产管理

AI分析工具可以为用户提供基于大数据的市场预测，帮助用户做出更明智的投资决策，优化资产配置。

4. 用户体验革新

通过AI技术实现的个性化服务将极大提升用户体验，吸引更多用户参与到熵增公链生态系统中。

5. 智能化DAO治理

AI辅助的决策工具将使DAO治理更加高效和公正，推动去中心化自治组织向更高级别的智能化演进。

7.3. 熵增币如何应用在AI人工智能

熵增币（EIC）在人工智能（AI）领域的应用，展现了区块链与AI技术融合的创新潜力。EIC作为熵增公链的原生代币，不仅在跨链交易、网络治理和激励机制中发挥核心作用，还可以在支持AI应用的发展和运营中起到重要角色。以下是熵增币在人工智能中应用的几种方式：

1. 激励AI开发与创新

- 开发激励：EIC可以用作奖励机制，鼓励开发者在熵增公链平台上创建和部署AI驱动的应用和服务。通过财务激励，促进AI技术的创新和发展。
- 贡献奖励：对于贡献算力或数据以支持AI训练和操作的用户，EIC可以作为奖励发放，激励更多用户参与到AI生态系统的建设中。

2. 交易和运营费用

- AI服务费用：EIC可以用于支付AI服务的使用费，如AI模型的训练、推理和API调用等。用户通过支付EIC获得AI服务，简化了支付流程并降低了交易成本。
- 数据交易：在EiChain上，EIC可用于购买和销售AI需要的数据集，促进数据的流通和共享，为AI训练提供高质量的数据资源。

3. AI治理和投票

- 网络治理：EIC持有者可以利用代币进行投票，参与到AI应用的治理决策中。例如，决定哪些AI项目应该获得资金支持，或对AI应用的道德和安全标准进行投票。
- 模型治理：在某些AI驱动的应用中，EIC可以用于对AI模型的更新和迭代进行投票，确保模型的发展方向符合社区的利益和价值观。

4. 质押和安全保障

- 模型质押：AI开发者可以通过质押EIC作为信用保证，提高其AI服务的可信度。如果服务未能达到预期效果或违反了服务协议，质押的EIC可以被扣除作为惩罚。
- 安全保障：利用EIC作为保证金，为AI服务提供安全保障。这可以应用于保护用户数据隐私、确保AI服务的可靠性和安全性。

08

熵增公链无缝链接 WEB 3.0

08 熵增公链无缝链接 WEB 3.0

作为一个旨在实现多链互操作性和去中心化应用（DApp）发展的区块链平台，自然而然地融入了WEB 3.0的愿景。WEB 3.0强调的是一个去中心化、开放且更加智能的互联网，这不仅仅是关于信息的自由流动，还涉及到价值的自由流动和互操作性，这些正是熵增公链努力实现的目标。

8.1. 熵增公链进入WEB 3.0的途径

1.互操作性与多链集成

熵增公链通过提供一个无缝链接不同区块链网络的框架，使得价值和数据可以自由地在不同的区块链系统间流动，为WEB 3.0的建设提供了基础设施。这种互操作性允许不同区块链的DApps和服务无缝交互，打破了区块链孤岛，促进了一个统一而多元的去中心化网络的形成。

2.去中心化金融（DeFi）和去中心化自治组织（DAO）

熵增公链支持DeFi和DAO的发展，这些应用是WEB 3.0的重要组成部分。通过利用熵增公链的技术，可以创建无需中介机构的金融服务和自主管理的组织，这些都是构建去中心化互联网的关键步骤。

3.支持创新的DApp开发

熵增公链为开发者提供了一个灵活、高效和安全的平台，使他们能够构建和部署创新的DApps。这些应用可以覆盖从游戏到社交媒体，再到在线市场和更多，推动了WEB 3.0生态系统的多样化和繁荣。

8.2. 熵增币在人工智能中的应用

1.数据市场和激励机制

在人工智能和机器学习项目中，数据是至关重要的资源。熵增币可以用作在去中心化数据市场中购买、销售或交换数据的媒介，为数据提供者提供激励，促进高质量数据的共享和利用。

2.AI算法和模型的交易

熵增公链可以支持一个去中心化的AI算法和模型市场，开发者和公司可以使用熵增币购买或许可使用先进的AI技术，加速AI应用的开发和部署。

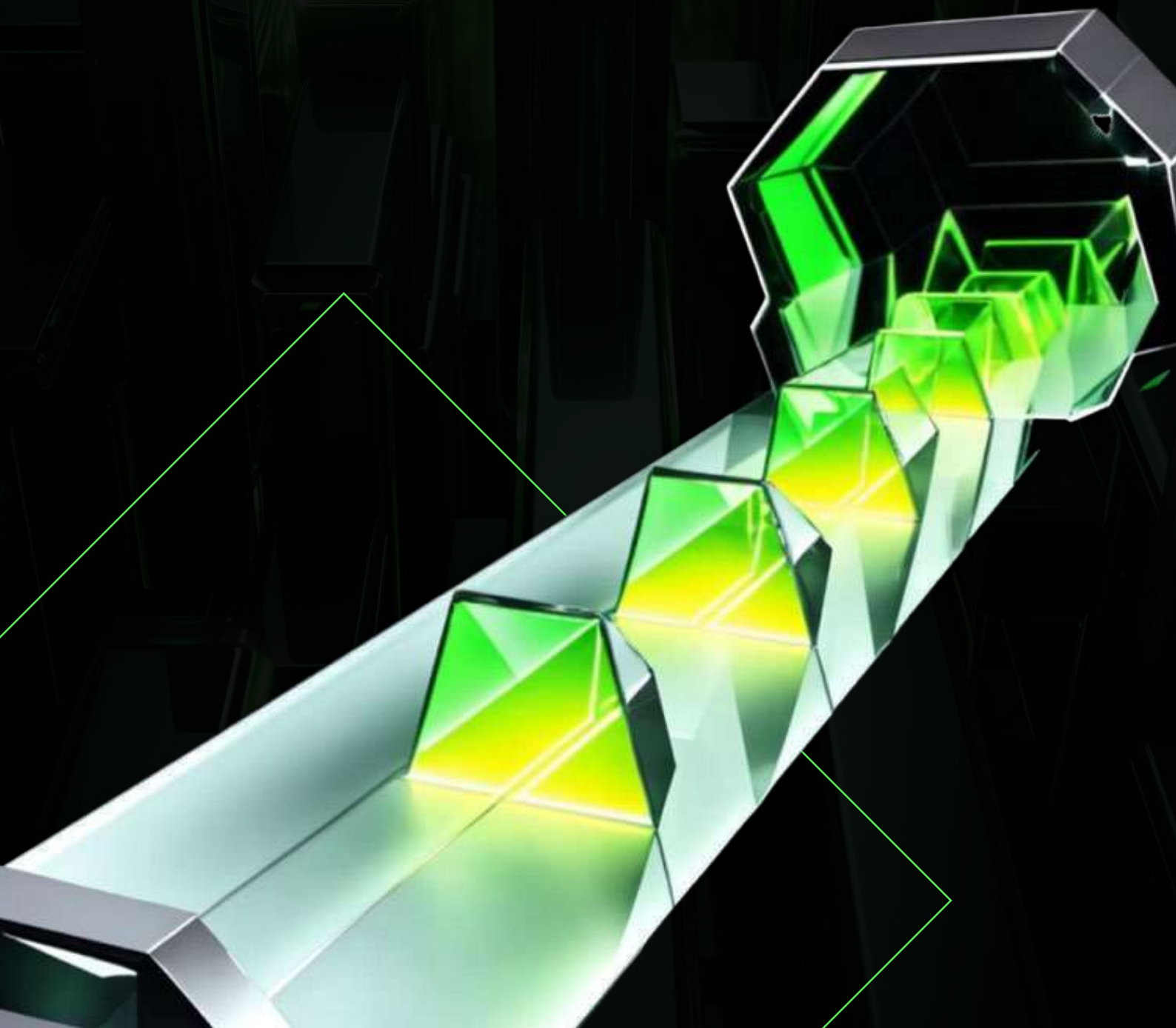
3.智能合约自动执行

熵增公链的智能合约功能可以自动执行基于AI决策的合约条款，例如，基于预测市场变动自动调整保险费率或执行复杂的金融交易策略。这些智能合约可以使用熵增币作为执行和交易的货币。

4.去中心化AI服务

通过熵增公链，可以创建去中心化的AI服务网络，其中服务如计算能力、数据存储和AI模型都可以用熵增币支付。这不仅降低了进入门槛，还促进了资源的有效分配和利用。

熵增公链和熵增币在推动WEB 3.0的发展和应用人工智能方面拥有巨大的潜力。通过提供一个去中心化、互操作和灵活的平台，它们能够支持新一代互联网的建设，使得更多的创新和价值创造成为可能。



09 熵增公链 发展路线图

09 熵增公链架构细节

9.1. 短期目标 (2024年 - 2025年)

2024年Q1

- 完成熵增公链的概念验证和初步设计，重点关注跨链资产转移和智能合约的应用场景。
- 启动社区建设，与早期开发者合作探索初步的应用案例。

2024年Q2

- 发布熵增公链的测试网，邀请开发者和用户进行测试和反馈，特别是针对NFT市场和跨链支付解决方案的测试。
- 开展跨链合作伙伴关系，拓展生态系统，推动多链游戏和社交媒体平台的早期开发。

2024年Q3

- 实现熵增币的初始发行和分配，启动基于熵增公链的去中心化自治组织（DAO）的试点项目。
- 完成关键基础设施的建设，并推出支持跨链DeFi应用的框架和API。

2024年Q4

- 正式启动熵增公链主网，并推出面向消费者的跨链钱包和支付应用。
- 开始实施去中心化治理模型，激励社区参与公链的治理和应用开发。

2025年

- 深化跨链互操作性，推出全面支持多链NFT和游戏资产交换的平台。
- 推出熵增公链的开发者激励计划，促进更多创新应用的开发和部署，如全链供应链解决方案和去中心化身份认证系统。去中心化金融（DeFi）平台和跨链交易所。

9.2. 长期目标 (2026年及以后)

2026年

- 成为领先的跨链平台，支持广泛的区块链生态系统互操作，并确保全链DeFi、游戏和社交应用的广泛应用和流畅体验。
- 实现熵增公链与人工智能、物联网等前沿技术的深度融合，探索和推动智能城市和智能合约自动化决策等新兴应用场景。

2027年

- 扩大全球社区，建立更多国际合作，推动熵增公链在全球范围内的应用，特别是在数字版权管理、供应链跟踪和跨境支付等领域。
- 推动熵增公链技术的迭代升级，提高系统的可扩展性、安全性和用户友好性，以适应不断增长的市场需求和应用场景。

2028年及以后

- 不断优化和升级熵增公链技术，维持其在跨链技术领域的领先地位。
- 推动熵增公链在金融、游戏、社交、物联网和人工智能等多个行业的广泛应用，实现价值互联网的愿景，并促进数字经济的全面发展。

10 熵增公链 核心团队

10 熵增公链核心团队

[illegible] 能的互联网，这不仅仅是关于信息的自由流动，还涉及到价值的自由流动和互操作性，这些正是熵增公链努力实现的目标。

10.1. 核心团队成员

Scott Hendricks - 比纳格首席执行官

Scott Hendricks，英籍企业家，熵增公链的创办人，曾是英伟达的重要成员。他带领一个由QuantConnect和Hanson Robotics的前成员组成的专家团队。这支团队在技术创新和人工智能领域有着卓越的贡献，其中包括历史上首个获得公民身份的索菲亚Sophia机器人项目。Scott在区块链、人工智能和机器人技术方面拥有深厚的专业知识和丰富的实战经验。在熵增公链项目中，他不仅是战略规划的核心驱动力，还负责引导团队解决技术难题，确保项目的创新性和实用性。

David Botic - 比纳格研发工程师

David Botic是一位资深的软件工程师，拥有计算机科学学士学位和10年以上的软件开发经验。在加入比纳格基金会之前，David曾在多个国际项目中担任关键开发角色，专注于区块链技术、智能合约和分布式系统的研发。在熵增公链项目中，David主要负责核心区块链技术的研发和优化，以及新功能的实现和集成。

Raymond Huang - 比纳格研发工程师

Raymond Huang是一位经验丰富的区块链工程师，持有软件工程硕士学位。他在加密货币、智能合约安全性和区块链架构方面具有丰富的研究和开发经验。Raymond在熵增公链项目中负责设计和实施安全框架，确保平台的安全性和稳定性。他的工作对于保护用户资产和数据，以及防范潜在的安全威胁至关重要。

Sri Gurupatham - 比纳格研发工程师

Sri Gurupatham是一位区块链解决方案专家，具有强大的技术背景和跨文化团队合作经验。Sri在区块链应用开发、跨链技术和去中心化金融（DeFi）解决方案方面具有深入的专业知识。在熵增公链项目中，Sri专注于开发友好的开发者工具和API，以便于第三方开发者和项目方能够轻松地构建和部署跨链应用，推动生态系统的多样化和成长。

11 安全措施

11 安全措施

在熵增公链的设计和实施中，安全是核心考虑之一，特别是在去中心化和交易安全保护方面。以下是熵增公链如何解决安全问题、保护内外部交易、对抗任意铸币，并应对外部链被攻击时可能出现的情况的优化描述：

11.1. 去中心化与安全性

熵增公链通过其去中心化的架构设计来避免单点故障，增强系统的容错性和抗攻击能力。该公链由分布在全球的各个未经许可的节点组成，确保了高度的去中心化。通过使用无领导的门限签名方案（TSS），熵增公链实现了密钥的分布式管理，任何单一节点或个体在任何时刻都无法访问完整的私钥信息，从而提高了跨链消息签名的安全性。

11.2. 内外部交易的安全保障

熵增公链利用其EiCore和EiClient节点监控外部链上的事件，并通过共识机制在内部达成一致，以触发状态更改并执行跨链交易。所有交易和决策均在区块链上记录，确保了不可变性、完全的透明度和可验证性。

11.3. 防御任意铸币

熵增公链采用了全面的措施来防止非法铸币行为，确保EIC熵增币的总供应量保持不变。包括在启动代币铸造前检查跨链总供应量，并利用Chainlink等去中心化的喂价机制来提供跨链总供应量的数据。这些措施共同作用，有效防止了未经授权的代币铸造。

11.4. 应对外部链攻击

当与熵增公链链接的外部链遭受攻击时，熵增公链能够通过其设计来减轻部分损害或限制损害的扩散。例如，总供应量检查可以阻止由于外部链攻击而导致的代币无限制铸造。此外，熵增公链可以进入紧急停机状态，以评估情况并协调恢复工作。

在构建熵增公链及其生态系统时，我们充分考虑到了跨多个司法管辖区运营的法律和监管挑战。熵增公链项目由新加坡注册的比纳格基金会负责执行，旨在确保项目的全球合法合规性，并保障用户和投资者的利益。以下是我们在法律和监管方面的重点考虑：

12 法律和监管框架

12 法律和监管框架

12.1. 全球合规策略

熵增公链项目认识到，不同国家和地区对于区块链技术和数字资产有着不同的法律法规要求。为此，比纳格基金会采取了全面的合规策略，确保熵增公链及其衍生应用在全球范围内的合法运营。

12.2. 合作与监督

1.法律顾问团队

比纳格基金会与全球范围内的法律顾问团队合作，确保熵增公链项目符合各个司法管辖区的法律法规要求。这包括了解和遵守反洗钱（AML）、反恐怖融资（CFT）、数据保护等相关法规。

2.审计合作

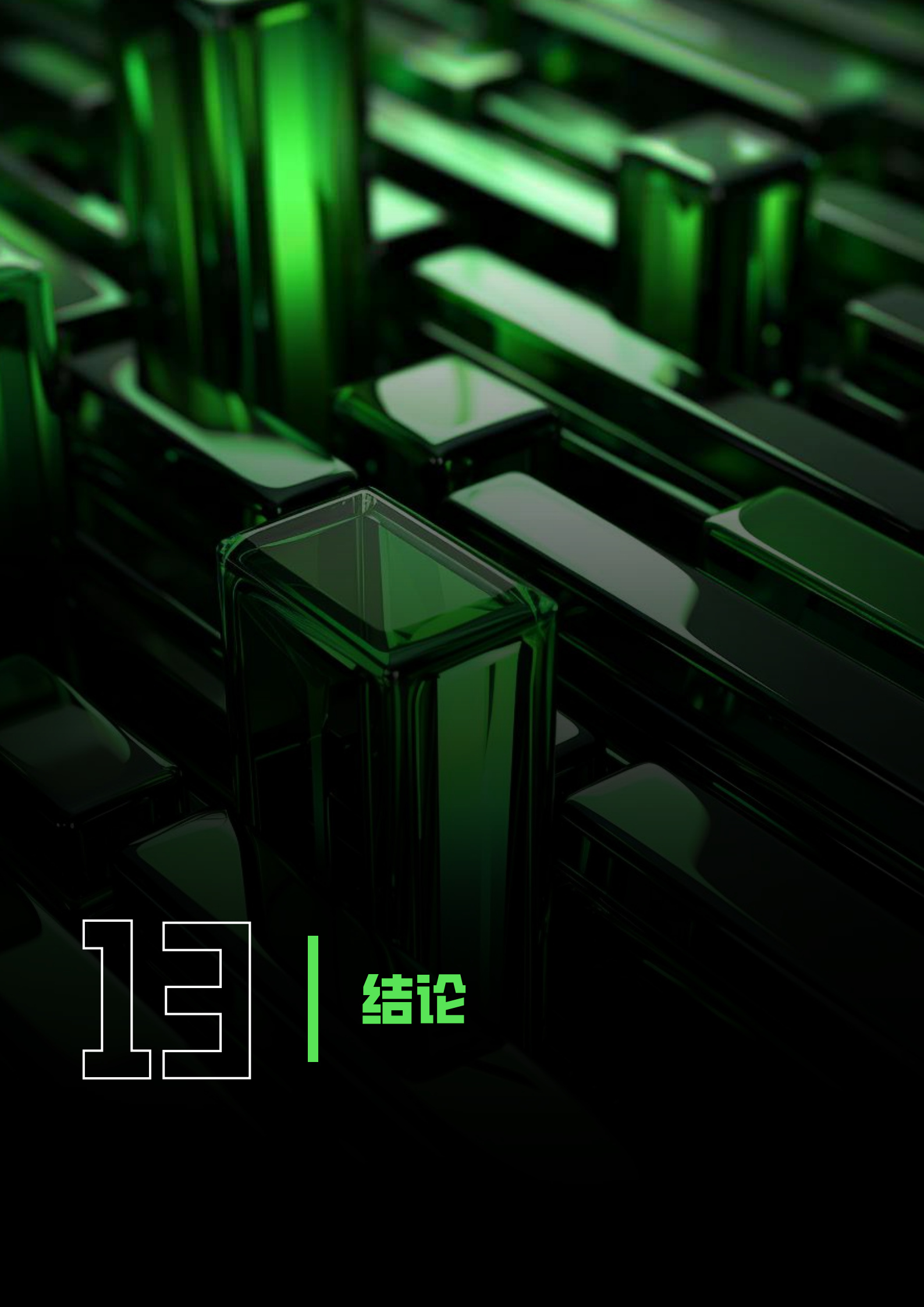
为了增加项目的透明度和安全性，熵增公链选择了全球权威的区块链安全审计公司CERTIK对其智能合约、代币经济以及所有衍生应用进行定期的安全审计。这一措施旨在保障熵增公链生态系统的稳定性和用户资产的安全。

12.3. 去中心化与安全性

虽然熵增公链项目由比纳格基金会在新加坡注册并执行，但其核心理念是去中心化，力求在全球范围内构建一个安全、透明、去中心化的区块链生态系统。通过采用去中心化的共识机制和分布式的节点运营模式，熵增公链确保了网络的高度安全性和容错性。

12.4. 适应监管变化

熵增公链项目团队持续监测全球监管环境的变化，以便及时调整策略和操作，确保项目始终处于合法合规的状态。我们认识到，区块链和数字资产领域的法律法规是不断发展的，因此比纳格基金会承诺将持续与全球监管机构合作，确保熵增公链生态系统的长期稳定发展。



13 结论

13

结论

熵增公链项目代表了区块链技术的下一代进步，致力于构建一个去中心化、安全和用户友好的跨链生态系统。通过其创新的技术框架和熵增币（EIC）的应用，熵增公链旨在解决当前区块链生态面临的互操作性问题，为全球用户和开发者提供一个无缝链接各种区块链网络的平台。

13.1. 项目的独特价值提案

1

全面的跨链解决方案

熵增公链通过提供一个统一的跨链通信协议，使得不同的区块链网络之间的互操作成为可能，进而促进了区块链应用的多样化和创新。

2

安全与合规

熵增公链项目重视安全和合规性，通过与全球权威的审计机构CERTIK合作，确保智能合约和网络协议的安全性，同时遵守全球各地的法律法规，保障用户资产安全。

3

去中心化与用户驱动

熵增公链采用去中心化的网络架构，通过质押和激励机制鼓励社区参与，确保了网络的去中心化和高效运行，同时为用户提供了参与网络治理的机会。

4

高性能与可扩展性

熵增公链设计了高效的共识机制和网络架构，确保了交易的快速处理和低延迟，同时保持了良好的可扩展性，能够支持未来区块链应用的需求增长。

13.2. 呼吁行动

熵增公链项目诚邀全球的开发者、企业和区块链爱好者加入我们的生态系统，共同探索和创造更多的跨链应用场景，推动区块链技术的发展和应用。无论您是区块链技术的开发者，还是寻求区块链解决方案的企业，或者是对区块链技术充满热情的个人，熵增公链都欢迎您的加入。

1. 开发者

我们提供丰富的开发工具和资源，帮助您轻松构建和部署跨链应用。

2.企业

通过熵增公链的跨链解决方案，您可以实现业务的去中心化，提高效率和安全性。

3.区块链爱好者

加入熵增公链社区，参与到项目的讨论和治理中来，共同塑造熵增公链的未来。

熵增公链项目致力于成为链接不同区块链网络、促进价值流通和信息交换的关键桥梁。让我们携手共创一个更加开放、安全和高效的区块链世界。立即加入熵增公链，共同开启跨链技术的未来之旅。

让我们共同构建跨链技术的未来。加入熵增公链，一起开启新的区块链时代。