Be L2 - Whitepaper

(Be=Bitcoin+Elastos)

1. 背景与问题

1.1.比特币的出现

比特币，被誉为“数字黄金”和去中心化的“互联网货币”，于2009年由神秘人物中本聪发布。其运用了SHA-256哈希算法和工作量证明（PoW）机制，实现了去中心化、不可篡改和安全的交易。比特币的出现可以视为现代康德哲学的具体体现，即康德主张的：人们应该根据理性原则自主地行动，而不是受到外部权威的强制。而比特币通过自我调节和非中心化的权力结构，挑战了传统金融体系的根基。

比特币的诞生是一次密码学和分布式共识算法的革命性突破。它将默克尔树、椭圆曲线数字签名算法（ECDSA）等技术融合在一起，构建了一个不受任何中心化组织控制的开放金融网络。比特币的共识机制是一种基于数论和概率论的复杂数学模型，它将矿工的计算能力与区块链的安全性紧密相连，Proof of Work确保了整个网络的鲁棒性和抗攻击能力。

比特币的出现不仅是技术上的创新，更是哲学和社会学上的一次深刻反思。它挑战了权威观念，提出了一种基于代码和算力的新型社会契约理论。通过去中心化博弈机制设计，比特币将个体自由和集体利益完美结合，展示了一种超越黄金、白银、银行货币等传统财富形式，在全球互联网达成新的财富共识和形成全球贸易新的清算流动性的伟大前景，从而帮助人类战胜瑞*达利欧预言的全球下一轮深重的债务危机。

1.2.比特币面临的挑战和限制

1.2.1.缺少可扩展性

比特币的区块链设计限制了其每秒处理的交易数量。目前，比特币网络每秒只能处理大约7笔交易。与传统金融系统如Visa每秒可以处理数千笔交易相比，这一限制显著降低了比特币的效率和实用性。给他们，

这一可扩展性问题的根源在于比特币的区块链结构。每个区块的大小限制为1MB，而每个区块大约每10分钟生成一次。这限制了每个区块可以包含的交易数量，从而限制

了整个网络的处理能力。此外，比特币的共识机制也需要时间来验证交易，进一步限制了交易速度。

例如，在交易高峰期，用户可能需要等待数小时甚至数天才能得到交易确认，并且交易费用GAS可能超过10美金。这使得比特币很多时候无法满足用户需求。对于那些追求即时支付的用户和商家来说，这一延迟可能是无法接受的。

1.2.2.编程能力的局限性

比特币的可编程能力相对有限，这主要体现在其脚本语言的功能限制上。比特币的脚本语言是一种堆栈式编程语言，它被用于定义交易的输入和输出条件。然而，这种脚本语言并不是图灵完备的，这意味着它无法解决所有的计算问题。相比之下，以太坊采用了一种图灵完备的脚本语言，使得开发者可以编写更加复杂的智能合约和分布式应用。

背后的原因是，比特币的设计初衷是成为一种简单、安全的数字货币，专注于实现去中心化的价值传输。因此，在设计上，比特币的目标是提供一种简单、高效的货币交换系统，而不是一个完全可编程的平台。这种设计选择加强了比特币的安全性，但也限制了其在更复杂应用领域的可应用性。

由于比特币的脚本语言不是图灵完备的，开发者在编写智能合约和分布式应用方面的能力受到了极大限制。这意味着比特币无法直接支持许多复杂的金融和商业应用，如去中心化金融（DeFi）和去中心化自治组织（DAO）等。

而为了实现更复杂的智能合约，市场催生了以太坊并且蓬勃发展，目前以太坊市值已接近比特币的一半。

1.2.3.隐私问题

虽然比特币地址是匿名的，但所有交易都在公共账本上记录。这意味着任何人都可以查看整个交易历史，并可能通过分析技术将地址与真实身份关联起来。这一特性使得比特币在某些情况下可能会暴露用户的真实身份。为了解决这一问题，比特币社区提出了许多隐私增强技术，如CoinJoin、MimbleWimble和ZK-SNARKs等。这些技术将密码学和信息论的先进理论应用到比特币的交易处理中，旨在在保护用户隐私的同时，不损害比特币的透明性和可审计性。

2. 第二层解决方案与现有技术

2.1.闪电网络

比特币闪电网络（Lightning Network）是一种二层支付协议，旨在解决比特币网络的可扩展性问题。通过在比特币区块链之上构建一个额外的层次，闪电网络允许用户在不必每次都在主链上记录的情况下进行即时、低成本的交易。

比特币闪电网络的工作原理主要是通过创建支付通道来进行交易，两个想要频繁交易的用户可以在比特币区块链上创建一个多重签名钱包，并在其中存入一些比特币。一旦通道建立，参与者就可以在通道内进行无限次数的交易。这些交易不会立即广播到比特币区块链，而是仅在通道参与者之间记录。

闪电网络的主要优势是即时支付、低成本、提高可扩展性、隐私增强。 虽然闪电网络为比特币带来了许多优势，但它也有一些挑战和限制，如通道资金的锁定、路由复杂性、网络流动性等。

2.2.RSK

RSK（Rootstock Infrastructure Framework）是一个在比特币网络上构建的二层网络项目，旨在提供更广泛的功能和更高的效率，提供了一系列基础设施服务，包括分散式域名系统、文件存储、支付协议、通信协议等。

但RIF的底层技术和协议相当复杂。虽然其目标是简化分散式应用程序的开发，但对于某些开发人员来说，理解和利用这些技术可能仍然具有挑战性。这可能会限制RSK的采用，特别是在那些缺乏区块链经验的开发人员社区中。这也增加了RSK可能需要的时间和努力来建立一个强大的用户和开发人员社区，导致其采用率并不高。

2.3.DriveChain

Drivechain 是一种允许比特币与其他区块链进行互操作的侧链解决方案。通过 Drivechain，可以创建与比特币主链相连接的侧链，这些侧链可以具有不同的特性和功能。这样可以在不改变主链的情况下实验新功能，从而增加了比特币的灵活性和可扩展性。

通过 Drivechain，开发人员可以创建具有特定规则和功能的侧链。这些侧链与比特币主链分开，但通过特殊的协议相互连接。用户可以将比特币从主链转移到侧链。这是通过一种称为“简化支付验证”（SPV）的技术实现的，该技术允许侧链验证主链上的交易。一旦资金转移到侧链，用户就可以在侧链上进行交易和操作，享受侧链提供的

特定功能和优势。用户还可以将资金从侧链转回主链。这需要主链矿工的协助，他们通过投票机制来确认转移的有效性。

DriveChain方案的实施需要Bitcoin硬分叉，这在具体操作中是一个很高的门槛。

2.4.Liquid

Liquid 是一种基于侧链的比特币第二层结算网络，连接全球加密货币交易所和机构，实现更快、更保密的比特币交易和数字资产的发行。通过 Liquid 侧链（称为“L-BTC”）移动的比特币可以在两分钟内实现最终结算。Liquid 上的交易金额和资产类型默认是隐藏的，保护用户的财务数据安全。可一次 Liquid 集成提供对 L-BTC 和发行资产的支持。所有代币基于相同的标准，允许用户利用原子交换和比特币风格的多重签名等功能。

2.5.Rollkit

Rollkit 是一种模块化的 rollup 框架，最近引入了对比特币的主权 rollup 的支持。Rollkit 允许开发人员使用任意执行环境创建 rollup，继承比特币的数据可用性保证和重组抵抗能力。通过新的集成，现在可以在比特币上作为 Rollkit 主权 rollup 运行 EVM。这不仅扩展了 rollup 的可能性，还有助于在比特币上引导健康的区块空间费用市场，实现更可持续的安全预算。

Rollkit 是一个模块化框架，开发人员可以插入自定义的执行层和数据可用性层。最初，Rollkit 只支持 Celestia 作为数据可用性和共识的选项。现在，比特币也是一个选项。Rollkit 可以将比特币集成为数据可用性层。在这种情况下，主权 rollup 管理自己的执行和结算，同时将共识和数据可用性卸载到比特币。Rollkit 的核心是模块化。它有一个数据可用性接口，开发人员只需实现特定方法即可添加新的数据可用性层。通过 Taproot 交易在比特币上读写数据。为此，实现了一个名为 bitcoin-da 的 Go 包，该包为比特币提供了读/写接口。Rollkit 支持自定义执行层，包括 EVM、CosmWasm 或 Cosmos SDK。通过 Rollkit 在本地比特币测试网络上运行 EVM 进行了集成测试。

3. Elastos起源于Bitcoin社区，致力于建设Be layer2

Elastos是一类WEB3信用基础设施，项目社区基于创始人陈榕的“You own your data”的基本理念，旨在打造一个安全、可扩展、去中心化的WEB3信用金融生态。

2017年8-12月，Elastos依靠Bitcoin社区资助的BTC启动，其主链在很大程度上是基于比特币的技术和思想而设计的，并一直执行和Bitcoin联合挖矿。

Elastos与Bitcoin的POW联合挖矿的初心是认同POW的去中心化安全的理念和机制，让BTC矿工将他们的算力投入到ELA网络（未来的Be layer2）中，同时ELA会给这些BTC矿工生态返还固定的挖矿收益。自2018年的8月26日开始，BTC.com矿池率先挖掘出了与ELA联合挖矿的首个区块。这一开创性的进步在接下来的五年中，得到了继续的发展，使ELA与比特币联合挖矿技术逐渐成熟。在这五年的历程中，BTC矿工们不仅成功为Elastos开采出了超过131万个区块，更产出了超过168万个ELA，占据了ELA流通量的7.8%。因此，通过这种联合挖矿机制，ELA为BTC生态贡献了超过一千万美元的价值。

目前，已有18个以上的BTC矿池，包括f2pool、antpool、btc.com、binance、ViaBTC、BTC.TOP、huobipool、OKPOOL等，纷纷加入这一行列，将其算力贡献给ELA，联合挖矿的算力峰值甚至超过了BTC全网算力的50%。

在2021年ELA减半之前，BTC矿工每年可以获得超过462,000个ELA的奖励。而在即将来临的ELA下次减半（预计在2025年12月）之前，BTC矿工每年仍有望获取超过140,000个ELA的奖励。至今，BTC矿工已累计获得了超过1,680,000 ELA的奖励；据估计，至2025年12月，BTC矿工将累计获得超过2,000,000 ELA的挖矿奖励。这标志着ELA和比特币联合挖矿的巨大成功和对比特币生态的显著贡献。。

ELA的减半节奏是一种与比特币相同的发行机制，这意味着ELA的发行速度会逐渐降低，最终将会达到一个稳定的水平。这种减半节奏与比特币相同，也是为了控制通货膨胀和保护货币的稳定性。ELA的减半节奏与BTC同频率，都是每4年减半一次。这意味着ELA的减半节奏与比特币相同，这为下一步两个社区共同建设Be layer2打下了良好的基础。

4. Be L2 技术介绍

4.1.Be L2 技术如何解决比特币的扩展问题

我们提出的比特币第二层网络技术（Be L2）由联合挖矿、zkEVM、MPC+TEE、ZKP+Taproot脚本等核心组件组成，这些组件共同构成了一个灵活、强大且安全的第二层网络架构，可以有效地解决比特币网络的扩展问题。

4.2. Be L2技术组成模块

4.2.1.Merge mining

合并挖矿（Merge Mining）最早由中本聪在2010年提出这个设想，是一种允许矿工同时挖掘两个或更多基于相同算法的区块链的过程。通过这种方式，矿工可以利用他们的哈希算力为多个网络提供安全性，而不需要分配额外的资源。

目前拥有较大BTC算力的Merge Mining的项目主要有NameCoin，RSK和Elastos。其中Elastos共享了超过50%的BTC算力，联合挖矿5年时间，总计为BTC矿工分享了超过1千万美元奖励。更重要的是Elastos采用灵活的主侧链架构，它提供一种开放性架构，允许其它网络通过它的架构继续分享BTC算力。

基于以上因素，Be L2方案采用Elastos的联合挖矿的技术方案，与Elastos一起分享BTC算力保证Be L2的共识安全。

4.2.2.zkEVM (Zero-Knowledge Ethereum Virtual Machine)

zkEVM（零知识证明以太坊虚拟机），是我们Be L2技术的基础。它利用了零知识证明（zk-SNARKs）的强大能力，使得交易可以在没有第三方验证的情况下安全执行。这种方法大大减少了交易的复杂性，并提高了处理速度，使得我们的网络能够处理大量的交易，并将证明存储在Bitcoin上，使L2更加透明且易于监控，同时还保持了Bitcoin的安全性。

1. 隐私保护： zkEVM 可以保护用户的隐私。由于交易的具体执行细节并未公开，只有执行结果，因此用户的隐私得到了更好的保护。这对于许多应用，如匿名投票、隐私交易等，都非常有用。
2. 可扩展性： zkEVM 通过零知识证明提高了系统的可扩展性。在传统的EVM网络中，所有的交易都需要被所有的节点验证，这限制了系统的处理能力。然而，在zkEVM中，一次交易的验证可以由一小部分节点完成，然后通过零知识证明技术，生成一个证明，证明这个交易已经被正确执行。这个证明可以被任何人快速验证，大大降低了系统的负载，提高了处理速度。
3. 兼容性： zkEVM 保持了与 Ethereum 虚拟机的兼容性，这意味着开发者可以无缝地将他们的 DApp 从 Ethereum 迁移到 zkEVM，无需进行大的修改。
4. 安全性： zkEVM 使用的零知识证明技术是经过严格的密码学验证的，可以确保数据的安全性和正确性。同时，由于交易的具体执行细节并未公开，攻击者无法通过分析交易数据来找到系统的弱点，进一步提高了系统的安全性。

4.2.3.MPC (Multi-Party Computation) 和 TEE (Trusted Execution Environment)

在我们的比特币二层技术框架Be L2中，多方计算（MPC）和可信执行环境（TEE）是两大核心技术，他们共同赋予了系统卓越的安全性和隐私保护能力。

多方计算（MPC）

多方计算是一种允许网络中的多个节点在不需要公开全部输入的情况下，共同计算一个函数结果的安全协议。MPC在分布式系统中的应用，可实现安全的计算和决策。

1.安全性：MPC协议保证了即使存在一部分恶意节点，只要数量不超过预定阈值，整个系统仍能保持安全性和正确性。

2.隐私性：MPC协议可确保每个参与计算的节点的输入信息都保持私密，其他节点无法获得这些具体信息，从而保证了隐私。

3.广泛应用：MPC协议在多个场景中均有应用，如在不可信环境中进行安全计算，保护用户隐私，实现分布式密钥管理等。

可信执行环境（TEE）

可信执行环境为代码和数据提供了一个安全的执行环境。即使在存在恶意软件的主机环境中，TEE也能保证代码的完整性和数据的保密性。

1. 安全执行：TEE可以防止运行中的程序被外部恶意软件修改或窥探，从而确保代码的安全执行。
2. 数据保护：TEE保护其内部处理的数据不被外部恶意软件获取，保障了数据的隐私性。
3. 远程认证：TEE提供了远程认证的功能，确保了系统的可信度。

在我们的节点服务器中，使用TEE运行节点服务程序，生成不可导出的节点私钥，确保节点只能执行预定义的代码逻辑，防止任何恶意行为。利用TEE操作节点可以显著提升安全性，即使节点的所有者也无法获取私钥，大大增加了执行恶意操作的难度。

综合运用MPC和TEE，我们的比特币二层技术框架Be L2在提供高效服务的同时，最大限度地保护了用户的隐私和交易安全。

4.2.4.基于见证人验证Be L2交易的机制

在Be L2技术中，我们引入了一种基于见证人的机制来验证二层网络中的交易。这种机制的工作原理如下：

1. 交易生成：在Be L2网络中，一旦生成一个新的交易，其信息将在整个网络中进行广播。
2. 见证人角色：见证人节点在网络中起到了重要的角色。他们监视Be L2网络中所有的交易，并对其有效性进行验证。验证包括检查交易的签名、确认交易的输入和输出是否平衡，以及核实交易是否符合网络的其他规则。
3. 挑战非法交易：如果有人篡改了交易，操作者或其它参与者都可以作为见证人挑战非法交易。挑战成功后，作弊者会受到惩罚，其押金将被没收，部分押金将作为奖励给予成功的挑战者。
4. 共识机制：所有的见证人节点都必须运行相同的共识机制，以确保对有效交易和无效交易的认定保持一致。

当前，在尚未实现BTC一层网络验证二层交易的情况下，我们采用见证人的方式解决二层交易的验证和冲突裁决作为过渡期解决方案。见证人服务运行在TEE+MPC的环境下，即便见证人自己也无法接触到私钥，所有代码行为都来自被审计过的软件包，这大大增强了见证人的可信性。这种验证机制为Be L2网络提供效率与安全之间的折衷方案。

4.2.5.混合ZKP和Taproot脚本验证Be L2交易的机制

这是我们的终极方案，我们希望借助零知识证明技术和比特币的Taproot脚本编程，共同实现在一层网络验证二层交易的真实性。

零知识证明（ZKP）

零知识证明（ZKP）是一种密码学工具，可以在不泄露任何实质信息的情况下验证声明的正确性。在我们的Be L2网络中，我们使用ZKP来验证交易的有效性。

1. 交易生成：在Be L2网络中，一旦生成一个新的交易，交易发起者会生成一个零知识证明，证明这个交易是有效的。这个证明会与交易一起广播到整个网络。
2. 交易验证：其他节点可以通过验证这个零知识证明来确定交易的有效性，而无需知道交易的具体内容。这不仅加速了交易验证的过程，还保护了用户的隐私。

Taproot脚本

Taproot是比特币网络中一种新的脚本类型，它将条件检查与普通的支付结合在一起，从而实现了灵活且高效的交易验证机制。

1. 交易生成：在Be L2网络中，交易发起者可以使用Taproot脚本来生成交易。Taproot脚本将交易的条件和支付信息编码在一起，这使得交易更加紧凑，且更加难以分析。
2. 交易验证：其他节点可以通过执行Taproot脚本来验证交易的有效性。由于Taproot脚本将条件检查和支付结合在一起，这种验证过程非常高效。

通过将零知识证明（ZKP）和Taproot脚本结合起来，我们的Be L2解决方案可以提供一种既快速又安全的交易验证机制。这种机制可以提高Be L2网络的性能，同时保护用户的隐私。

4.2.6. 在L2的BTC的强制撤离机制

我们的Be L2技术还包含了一个强制撤离机制。在这个机制中，如果在过渡阶段，二层网络的见证人无法达成共识导致一直无法完成二层的出块，那么用户在强制广播他的提款交易，在经历过一个漫长的延迟（14天）过程之后，就可以撤出资金。从而让用户不必持续等待L2恢复。这是一种弱中心化的解决方案，节点只是协助加速，这才是保底方案，让用户不会丢失资产。

5. 比特币和Be L2网络的协同效应

在我们的设计中，比特币与第二层网络（Be L2）不是独立存在的，而是互相支持、互相加强的。以下是比特币与Be L2网络间的几种主要的协同效应。

5.1.同步一层交易到Be L2网络

为了让Be L2网络能够最大限度地利用比特币网络的算力，我们设计了一种机制，使得一层的比特币交易可以在Be L2网络中得到同步。每当在比特币网络中发生一次交易时，Be L2网络会生成一个对应的交易，使得在BeL2网络中可以看到所有在比特币网络中发生的交易。

这种设计可以使Be L2网络实时地反映比特币网络的状态，使得用户可以随时查看和验证他们在比特币网络中的资产状态。

一个潜在的用例是在二层网络上与比特币一层的Ordinals资产互动。比如，用户在一层网络Mint出一个Ordinals资产，可以在二层感知这个事件，并做出反应，比如给用户发送某个ERC20的token作为奖励。

5.2.为L1提供BTC价格种子

比特币的价格是由市场决定的，而市场价格的波动直接影响了比特币网络的安全性和稳定性。因此，我们设计了一种机制，使得Be L2网络可以为比特币网络提供价格种子。

在这个设计中，Be L2网络会周期性地获取比特币的市场价格，并将这个价格、时间，共同签名并作为种子加入到比特币一层网络的UTXO中。当比特币网络需要获取价格信息时，可以在脚本中设置判断条件，例如，当BTC价格低于3万美元时，就可以解锁这个UTXO，这可以用于抵押BTC借款时解锁并清算BTC抵押品。

6. 路线图

项目路线图是我们实现目标和愿景的关键路径。在这个部分，我们将详细介绍我们的路线图，以及每个阶段的目标和计划。

6.1.第一阶段：原型验证以及生态基础设施建设

在第一阶段，我们将在测试网实现兼容Ethereum虚拟机（EVM），并通过和BTC联合挖矿和权益证明（PoS）保证共识。同时也将建设跨链桥、预言机等生态基础组件。还会引入跨链Swap、Dex、借贷等基础dApps，以方便更多类型的生态应用加入到二层网络。

6.2.第二阶段：去中心化与跨链

第二阶段的目标是通过Ordinals和BRC20数据索引合约解决集中化问题。基于Ordinals资产进行跨链，并根据二层网络上的Ordinals铸造一层网络的资产，提供类似于以太坊DeFi的一层网络资产的衍生服务，如发行、交换和铸币。

6.3.第三阶段：增强安全性与效率

在第三阶段，我们计划增强比特币主网存证和共识，将zkEVM移植到二层网络，支持交易证明和二层网络比特币余额的Merkle树生成。基于可信执行环境（TEE）实施可信赖的节点运营环境，基于多方计算（MPC）/阈值签名实施节点资产管理服务模块，实施二层网络的共识机制，包括交易打包、证明生成、多方签名证明交易到一层网络的公证机制等。实现一层和二层之间的比特币跨链机制，基于二层网络的比特币余额Merkle树，实现到一层网络的非托管提现方式。

6.4.第四阶段：混合技术解决方案

在第四阶段，我们将探索混合技术解决方案，包括探索基于现有Bitcoin OP Code实施zk验证证明算法的可行性，探索一层网络上有限证明验证的混合技术解决方案，跟踪潜在的二层网络应用场景的最新技术解决方案。并且，将以非托管方式支持比特币在一层和二层网络之间的单向桥接。即使二层网络不再运作，用户也可以将比特币提现到自己的钱包。

6.5.第五阶段：比特币超级链BL Stack

在第五阶段，我们的目标是建立BL Stack，是将孤立的各类BTC L2整合成一个单一的超级链（Superchain），这一愿景不仅具有前瞻性，还具有实际的战略价值。

随着比特币网络的复杂性增加，出现了许多孤立的L2解决方案。这些解决方案虽然在某些方面有效，但缺乏统一和互操作性。BL Stack的目标是通过整合这些孤立的L2，创建一个统一的超级链，从而消除碎片化，提高整个网络的效率和可用性。

BL Stack的超级链不仅整合了现有的L2，还强调了互操作性和组合性。这意味着不同的L2可以无缝交互，共享资源和功能。这种组合性使得开发人员可以灵活地构建复杂的应用，同时保持系统的一致性和可维护性。

BL Stack的另一个重要目标是简化L2的部署过程。通过提供统一的框架和工具，BL Stack使得启动L2就像今天将智能合约部署到以太坊一样简单。这大大降低了开发门槛，吸引了更多的开发人员和项目加入比特币生态系统。

BL Stack的超级链是开放和可扩展的。任何人都可以参与和贡献，新的L2可以轻松地集成到现有的超级链中。这确保了BL Stack能够适应未来的需求和挑战，持续推动比特币网络的创新和增长。

7. Token经济

（正式发行的白皮书中可能不包含本部分内容，token计划在第3、4阶段发行，大约在2025年年中，将视技术开发进度和市场情况调整。）

$Be2 是 Be Layer2 network 的原生 ERC-20 治理代币。启动时的代币属性：

Initial supply cap	**100 billion**
Inflation	Max 2% per year
Minting/burning mechanism	L2 smart contract
Bridgeable to Bitcoin L1?	Yes
Tokens launch on	Bitcoin Layer 2
On-chain governance (voting) happens on	Bitcoin Layer 2
Airdrop snapshot	计划于第3阶段（测试网转主网后）发行token，对参与共识的节点、参与生态建设的dApp和用户进行空投，时间预计在2025年年中。

Initial token allocation & airdrop distribution

Percentage of initial supply	**Number of tokens**	**Allocated to**
45%	45 billion	DAO treasury
25%	25 billion	开发团队和顾问
15%	15 billion	Investors
15%	15 Billion	空投给用户、共识节点、生态应用

8. 质押ELA挖$Be2

从Be L2建设的第一阶段到第三阶段，Elastos社区将负责建设其测试网络，并开放Be L2的共识节点，每个节点至少需质押10,000ELA或者0.5个BTC，所有节点在18个月内一共可获得$Be2 总量10%的代币奖励。

8.1.代币奖励数量

$Be2 发行总量的10%将空投给测试网节点，分18个月平均分配。

8.2.节点质押

8.2.1.质押数量

1. 每个共识节点需至少质押10,000 ELA或0.5个BTC。
2. 节点所有者和投票人共同凑够质押所需的ELA或BTC。

8.2.2.质押时间

1. 节点所有人在创建节点时需选择节点质押时间。
2. 投票人在投票时需选择投票节点和投票质押时间，投票质押时间不能大于节点剩余的质押时间。
3. 质押时间结束后质押资金自动释放，质押期结束前无法取回质押Token。

4. 节点所有人和投票人可以在质押期结束前选择延长质押期，新的质押期将在第二天0:00生效；无法缩短质押期。
5. 投票人在质押期结束前可以变更投票节点。更新后的投票信息在第二天0:00生效。

8.3.节点类型

1. 节点分为共识节点和候选节点。
2. 满足最少质押Token数量要求且算力排名前108名的测试节点为测试网共识节点，其他节点为测试网候选节点。
3. 共识节点和候选节点都将获得空投奖励。

8.4.算力计算

1. 上线时10,000 ELA与0.5个BTC算力相同；上线后以每周一0:00的ELA和BTC的30日均线价格为基准价格，计算未来一周的测试节点算力。
2. 算力公式：

   算力(质押ELA) = ELA基准价格 * 质押ELA的数量 * 质押数量系数 * 质押时间系数

   算力(质押BTC) = BTC基准价格 * 质押BTC的数量

   节点算力 = [节点所有人算力 + sum(节点投票人算力)] * 节点系数

3. 每天0:00计算节点算力并更新节点算力排名。
4. 按照节点算力占所有节点总算力的比例，计算每天的代币奖励。
5. 投票人可以给节点投票，节点所有人和投票人分别获得投票算力对应代币奖励的20%和80%。
6. 质押数量系数

ELA质押数量	系数	备注
1～1000	1	
1001～10000	1.05	1.01^5
10001～20000	1.34	1.015^20

20000以上	1.5	

7. 质押时间系数

ELA质押时间	系数	备注
7天	1	
30天	1.04	1.01^4
90天	1.21	1.015^(90/7)
180天	1.50	1.016^(180/7)
360天	2.38	1.017^(360/7)
540天	3.96	1.018^(540/7)

8. 节点系数

节点	条件	系数
共识节点	排名≤108且质押ELA≥10000	5
候选节点	节点排名>108或质押ELA<10000	1

8.5.节点投票

1. 节点所有人和投票人在质押时需选择质押时间，质押时间结束后质押资金自动释放。质押期结束前无法取回质押Token。
2. 投票时选择的质押时间不能大于节点剩余的质押时间。
3. 节点所有人和投票人可以在质押期结束前选择延长质押期，新的质押期将在第二天0:00生效；无法缩短质押期。
4. 投票人在质押期结束前可以变更投票节点。更新后的投票信息在第二天0:00生效。

8.6.质押NFT

1. 节点所有人和投票人质押后将获得“质押NFT”和“权益NFT”。
2. 质押NFT和权益NFT支持在NFT平台交易。
3. 持有质押NFT的地址在质押期结束后，将获得质押的ELA或BTC。
4. 持有权益NFT的地址可以在空投时领取与权益对应数量的$Be2。

Be L2 - Whitepaper

(Be=Bitcoin+Elastos)

1 Background and problems

1.1 The emergence of bitcoin

Bitcoin, known as "digital gold" and a decentralized "Internet currency", was released in 2009 by the mysterious Satoshi Nakamoto. It uses the SHA-256 hash algorithm and proof-of-work (PoW) mechanism to realise decentralized, tamper-proof and secure transactions. The emergence of Bitcoin can be regarded as a concrete manifestation of modern Kant's philosophy , which Kant advocated: people should act autonomously according to rational principles, rather than being compelled by external authorities. Bitcoin challenges the foundations of the traditional financial system through its self-regulating and decentralized power structure.

The birth of Bitcoin was a revolutionary breakthrough in cryptography and distributed consensus algorithms. It integrates Merkle tree, Elliptic Curve Digital Signature Algorithm (ECDSA) and other technologies to build an open financial network that is not controlled by any centralized organization. Bitcoin's consensus mechanism is a complex mathematical model based on number theory and probability theory, which closely connects the computing power of miners with the security of the blockchain. Proof of Work ensures the robustness and attack resistance of the entire network.

The emergence of Bitcoin is not only a technological innovation, but also a profound reflection on philosophy and sociology. It challenges authority and proposes a new social contract theory based on code and computing power. Through the design of the decentralized game mechanism, Bitcoin perfectly combines individual freedom and collective interests, showing a way to surpass traditional forms of wealth such as gold, silver, and bank currency, and to reach a new wealth consensus on the global Internet and form a new settlement of global trade The great prospect of liquidity will help mankind overcome the next deep debt crisis in the world predicted by Ray Dalio.

1.2 Bitcoin's Challenges and Limitations

1.2.1 lack of scalability

Bitcoin's blockchain design limits the number of transactions it can process per second. Currently, the Bitcoin network can only process about 7 transactions per second. This limitation significantly reduces Bitcoin's efficiency and usefulness compared to traditional financial systems such as Visa, which can process thousands of transactions per second.

The root of this scalability problem lies in Bitcoin's blockchain structure. The size of each block is limited to 1MB, and each block is generated approximately every 10 minutes. This limits the number of transactions each block can contain, thereby limiting the processing power of the entire network. Additionally, Bitcoin’s consensus mechanism also takes time to verify transactions, further limiting transaction speed.

For example, during peak transaction periods, users may have to wait for hours or even days for transaction confirmation, and the transaction fee may exceed $10 in gas. This makes Bitcoin unable to meet user needs in many cases. For users and merchants looking for instant payments, this delay may be unacceptable.

1.2.2 Limitations of Programming Capabilities

Bitcoin's programmability is relatively limited, which is mainly reflected in the functional limitations of its scripting language. Bitcoin's scripting language is a stacked programming language that is used to define the input and output conditions of transactions. However, this scripting language is not Turing complete, which means it cannot solve all computing problems. In contrast, Ethereum uses a Turing-complete scripting language that allows developers to write more complex smart contracts and distributed applications.

The reasoning behind this is that Bitcoin was originally designed to be a simple, secure digital currency focused on enabling decentralized value transfer. Therefore, by design, the goal of Bitcoin is to provide a simple and efficient currency exchange system, rather than a fully programmable platform. This design choice strengthens Bitcoin's security, but also limits its applicability to more complex applications.

Since Bitcoin's scripting language is not Turing complete, developers are greatly limited in their ability to write smart contracts and distributed applications. This means that Bitcoin cannot easily support many complex financial and business applications, such as decentralized finance (DeFi) and decentralized autonomous organizations (DAO).

In order to implement more complex smart contracts, the market gave birth to Ethereum and it has flourished, with the current market value of Ethereum approaching half of Bitcoin’s.

1.2.3 Privacy Issues

Although Bitcoin addresses are anonymous, all transactions are recorded on the public ledger. This means that anyone can view the entire transaction history and possibly link addresses to real-world identities through analytical techniques. This feature makes it possible for Bitcoin to expose the user's real identity in certain situations. To address this problem, the Bitcoin community has proposed many privacy-enhancing technologies, such as CoinJoin, MimbleWimble, and ZK-SNARKs, etc. These technologies apply advanced theories of cryptography and information theory to Bitcoin transaction processing, aiming to protect user privacy without compromising the transparency and auditability of Bitcoin.

2 Layer 2 Solutions vs. Existing Technologies

2.1 Lightning Network

The Bitcoin Lightning Network (Lightning Network) is a second-layer payment protocol designed to solve the scalability issue of the Bitcoin network. By building an additional layer on top of the Bitcoin blockchain, the Lightning Network allows users to conduct instant, low-cost transactions without the need to record them on the main chain every time.

The working principle of the Bitcoin Lightning Network mainly involves creating payment channels for transactions. Two users who want to trade frequently can create a multi-signature wallet on the Bitcoin blockchain and deposit some Bitcoins in it. Once a channel is established, participants can conduct an unlimited number of transactions within the channel. These transactions are not immediately broadcast to the Bitcoin blockchain, but are only recorded between channel participants.

The main advantages of the Lightning Network are instant payments, low cost, improved scalability, and enhanced privacy. Although the Lightning Network brings many advantages to Bitcoin, it also has some challenges and limitations, such as the lock of channel funds, routing complexity, network liquidity, etc.

2.2 RSK

RSK (Rootstock Infrastructure Framework) is a two-layer network project built on the Bitcoin network, aiming to provide a wider range of functions with higher efficiency, and a series of infrastructure services, including decentralized domain name system, file storage, payment protocol, communication protocol, etc.

However, the underlying technology and protocols of RIF are quite complex. Although its goal is to simplify the development of decentralized applications, understanding and utilizing these technologies may still be challenging for some developers. This may limit the adoption of RSK, particularly in developer communities that lack blockchain experience. This also increases the time and effort RSK may need to establish a strong user and developer community, resulting in a relatively low adoption rate.

2.3 DriveChain

Drivechain is a sidechain solution that allows Bitcoin to interoperate with other blockchains. With Drivechain, it is possible to create sidechains connected to the Bitcoin main chain, and these sidechains can have different characteristics and functions. This allows experimentation with new features without changing the main chain, increasing Bitcoin's flexibility and scalability.

With Drivechain, developers can create sidechains with specific rules and functions. These sidechains are separate from the Bitcoin main chain, but are connected to each other through special protocols. Users can transfer bitcoins from the main chain to the side chain. This is achieved through a technology called Simplified Payment Verification (SPV), which allows sidechains to verify transactions on the mainchain. Once the funds are transferred to the side chain, users can conduct transactions and operations on the side chain and enjoy the specific functions and advantages provided by the side chain. Users can also transfer funds from the sidechain back to the main chain. This requires the assistance of the main chain miners, who confirm the validity of the transfer through a voting mechanism.

The implementation of the DriveChain proposal requires a hard fork of Bitcoin, which is a significant barrier in terms of specific operations.

2.4 Liquid

Liquid is a sidechain-based Bitcoin second-layer settlement network that connects global cryptocurrency exchanges and institutions to enable faster and more secure Bitcoin transactions and digital asset issuance. Bitcoins moving through the Liquid sidechain (called "L-BTC") can achieve final settlement within two minutes. Transaction amounts and asset types on Liquid are hidden by default to protect users' financial data. One Liquid integration provides support for L-BTC and issued assets. All tokens are based on the same standard, allowing users to take advantage of features such as atomic swaps and Bitcoin-style multi-signatures.

2.5 Rollkit

Rollkit is a modular rollup framework that recently introduced support for Bitcoin's sovereign rollup. Rollkit allows developers to create rollups using arbitrary execution environments, inheriting Bitcoin's data availability guarantees and reorganization resistance. With the new integration, it is now possible to run the EVM on Bitcoin as a Rollkit sovereign rollup. Not only does this expand the rollup possibilities, but it also helps steer a healthy block space fee market on Bitcoin, enabling a more sustainable security budget.

Rollkit is a modular framework where developers can plug in custom execution and data availability layers. Initially, Rollkit only supported Celestia as an option for data availability and consensus. Now, Bitcoin is also an option. Rollkit can integrate Bitcoin as a data availability layer. In this case, the sovereign rollup manages its own execution and settlement, while offloading consensus and data availability to Bitcoin. At its core, Rollkit is modular. It has a data availability interface and developers can add new data availability layers simply by implementing specific methods. Read and write data on Bitcoin through Taproot transactions. To this end, a Go package called bitcoin-da is implemented, which provides a read/write interface to Bitcoin. Rollkit supports custom execution layers including EVM, CosmWasm or Cosmos SDK. Integration testing was done with Rollkit running the EVM on a local Bitcoin testnet.

3 Elastos originated from the Bitcoin community and dedicated to building Be layer2

Elastos is a type of WEB3 credit infrastructure. The project community is based on the basic concept of "You Own Your Data" of the founder Chen Rong, aiming to create a safe, scalable and decentralized WEB3 credit financial system.

From August to December 2017, Elastos was launched with fund from the Bitcoin community. Its main chain is largely designed based on Bitcoin technology and concepts, and has been implementing merged mining with Bitcoin.

The original intention of Elastos and Bitcoin's POW merged mining is to acknowledge the decentralized security concept and mechanism of POW, allowing BTC miners to contribute their computing power to the ELA network (future Be layer2). At the same time, ELA will provide these BTC miners with a fixed mining income.

Starting from August 26, 2018, the BTC.com mining pool was the first to mine the first block for joint mining with ELA. This pioneering progress has continued to develop over the next five years, gradually maturing the merged mining technology between ELA and Bitcoin. In this five-year journey, BTC miners have successfully mined over 1.31 million blocks for Elastos, producing over 1.68 million ELA, accounting for 7.8% of ELA's circulation. Therefore, through this merged mining mechanism, ELA has contributed over $10 million in value to the BTC ecosystem.

Currently, there are more than 18 BTC mining pools, including f2pool, antpool, btc.com, binance, ViaBTC, BTC.TOP, huobipool, OKPOOL, etc., joining the ranks and contributing their computing power to ELA. The peak computing power of merged mining even exceeds 50% of the total computing power of the entire BTC network.

Before the halving of ELA in 2021, BTC miners could receive over 462,000 ELA rewards per year. And before the upcoming next halving of ELA (expected in December 2025), BTC miners are still expected to receive over 140,000 ELA rewards per year. So far, BTC miners have accumulated over 1,680,000 ELA rewards. It is estimated that by December 2025, BTC miners will have accumulated over 2,000,000 ELA mining rewards. This signifies the great success of joint mining between ELA and Bitcoin and their significant contribution to the Bitcoin ecosystem.

The halving mechanism of ELA is the same as Bitcoin, which means that the issuance speed of ELA will gradually decrease and eventually reach a stable level. This is also to control inflation and protect the stability of the currency. The ELA halving occurs every 4 years as well, which lays a good foundation for both Bitcoin and ELA communities to jointly build Be layer2.

4 Be L2 Technology Introduction

4.1 How Be L2 Technology Can Solve Bitcoin’s Scaling Problem

The Bitcoin Layer 2 (Be L2) technology consists of core components such as merged mining, zkEVM, MPC+TEE, ZKP+Taproot scripts, which together form a flexible, powerful and secure second-layer network architecture. This architecture effectively addresses the scalability issue of the Bitcoin network.

4.2 Be L2 technology components

4.2.1 Merge mining

Merged Mining was first proposed by Satoshi Nakamoto in 2010. It allows miners to simultaneously mine two or more blockchains with the same algorithm. In this way, miners can use their hash power to provide security for multiple networks without additional resources.

Currently, projects with a significant BTC computing power in Merged Mining are mainly NameCoin, RSK, and Elastos. Among them, Elastos shares over 50% of the BTC computing power and has been merged mining for 5 years, resulting in over $10 million in rewards shared with BTC miners. What is more significant is that Elastos adopts a flexible mainchain-sidechain architecture, which provides an open architecture that allows other networks to continue sharing BTC computing power through its framework.

Based on these factors, the Be L2 solution adopts Elastos' joint mining technical solution to share BTC computing power and ensure the consensus security of Be L2.

4.2.2 zkEVM (Zero-Knowledge Ethereum Virtual Machine)

zkEVM (Zero-Knowledge Proof Ethereum Virtual Machine), is the foundation of our Be L2 technology. It leverages the power of zero-knowledge proofs (zk-SNARKs), allowing transactions to be executed securely without third-party verification. This method greatly reduces transaction complexity and improves processing speed, enabling our network to handle a large number of transactions and store proofs on

Bitcoin, making L2 more transparent and easy to monitor, while maintaining the security of Bitcoin sex.

1. **Privacy protection:** zkEVM can protect the privacy of users. Since the specific execution details of the transaction are not disclosed, only the execution results are available, so the user's privacy is better protected. This is very useful for many applications, such as anonymous voting, private transactions, etc.
2. **Scalability:** zkEVM improves the scalability of the system through zero-knowledge proofs. In the traditional EVM network, all transactions need to be verified by all nodes, which limits the processing capacity of the system. However, in zkEVM, the verification of a transaction can be completed by a small number of nodes, and then through zero-knowledge proof technology, a proof is generated to prove that the transaction has been executed correctly. This proof can be quickly verified by anyone, which greatly reduces the load on the system and improves the processing speed.
3. **Compatibility:** zkEVM maintains compatibility with the Ethereum virtual machine, which means developers can seamlessly migrate their DApps from Ethereum to zkEVM without major modifications.
4. **Security:** The zero-knowledge proof technology used by zkEVM has undergone strict cryptographic verification to ensure data security and correctness. At the same time, since the specific execution details of the transaction are not disclosed, the attacker cannot find the weakness of the system by analyzing the transaction data, which further improves the security of the system.

4.2.3 MPC (Multi-Party Computation) and TEE (Trusted Execution Environment)

In our Bitcoin two-layer technical framework Be L2, multi-party computing (MPC) and trusted execution environment (TEE) are two core technologies, which together endow the system with excellent security and privacy protection capabilities.

Multi-Party Computation (MPC)

Multi-party computation is a secure protocol that allows multiple nodes in a network to jointly compute the result of a function without disclosing all the inputs. The application of MPC in distributed systems enables secure computation and decision-making.

1. **Security:** The MPC protocol ensures that even if there are some malicious nodes, as long as the number does not exceed the predetermined threshold, the entire system can still maintain security and correctness.

2. **Privacy:** The MPC protocol can ensure that the input information of each node participating in the calculation remains private, and other nodes cannot obtain the specific information, thus ensuring privacy.

3. **Wide application:** The MPC protocol is applied in many scenarios, such as performing secure computing in an untrusted environment, protecting user privacy, and realizing distributed key management.

Trusted Execution Environment (TEE)

A trusted execution environment provides a secure execution environment for code and data. TEE guarantees code integrity and data confidentiality even in host environments where malware is present.

1. **Secure Execution** : TEE can prevent running programs from being modified or snooped by external malware, thus ensuring safe code execution.
2. **Data protection** : TEE protects its internally processed data from being obtained by external malware, ensuring data privacy.
3. **Remote authentication** : TEE provides the function of remote authentication to ensure the credibility of the system.

In our node server, use TEE to run the node service program to generate a non-exportable node private key to ensure that the node can only execute predefined code logic and prevent any malicious behavior. Using TEE to operate nodes can significantly improve security, even the owner of the node cannot obtain the private key, which greatly increases the difficulty of performing malicious operations.

Using MPC and TEE comprehensively, our Bitcoin two-layer technical framework Be L2 maximizes the protection of user privacy and transaction security while providing efficient services.

4.2.4 Verifying Be L2 transactions based on validators

In Be L2 technology, we have introduced a Validators-based mechanism to verify transactions in the two-layer network. This mechanism works as follows:

Transaction generation : In the Be L2 network, once a new transaction is generated, its information will be broadcast throughout the network.

Validators role : Validators nodes play an important role in the network. They monitor all transactions in the Be L2 network and verify their validity. Validation includes checking the signature of the transaction, confirming that the inputs and outputs of the transaction are balanced, and verifying that the transaction complies with other rules of the network.

Challenge illegal transactions : If someone tampers with the transaction, the operator or other participants can challenge the illegal transaction as a Validator. After the challenge is successful, the cheater will be punished and his deposit will be confiscated, and part of the deposit will be given to the successful challenger as a reward.

Consensus mechanism : All validator nodes must run the same consensus mechanism to ensure consistent identification of valid and invalid transactions.

Currently, in the absence of BTC's first-layer network to verify second-layer transactions, validators are to verify transactions and resolve conflicts in the second-layer as a transitional solution. The validators service runs in the TEE+MPC environment. Even the validators themselves cannot access the private key. All codes are audited, which greatly enhances the credibility of the validators. This verification mechanism provides a balance between efficiency and security for the Be L2 network.

4.2.5 Combined ZKP and Taproot scripts to verify Be L2 transactions

This is our ultimate solution. We expect to use zero-knowledge proof technology and Bitcoin's Taproot script programming to jointly verify the authenticity of the second-layer transaction on the first-layer network.

Zero Knowledge Proof (ZKP)

Zero-knowledge proof (ZKP) is a cryptographic tool that can verify the correctness of a statement without revealing any substantive information. In our Be L2 network, we use ZKP to verify the validity of transactions.

Transaction generation : In the Be L2 network, once a new transaction is generated, the transaction initiator will generate a zero-knowledge proof to prove that the transaction is valid. This proof is broadcast to the entire network along with the transaction.

Transaction verification : Other nodes can verify the validity of the transaction by verifying this zero-knowledge proof without knowing the specific content of the transaction. This not only speeds up the verification of the transaction, but also ensures the privacy of users.

Taproot script

Taproot is a new type of script in the Bitcoin network, which combines condition checks with ordinary payments, enabling a flexible and efficient transaction verification mechanism.

Transaction generation : In the Be L2 network, transaction initiators can use Taproot scripts to generate transactions. Taproot scripts encode the conditions and payment information of a transaction, which makes the transaction more compact and harder to analyze.

Transaction verification : Other nodes can verify the validity of transactions by executing Taproot scripts. This verification process is very efficient thanks to the Taproot script that combines condition checks and payments.

By combining zero-knowledge proofs (ZKP) and Taproot scripts, Elastos Be L2 solution provides a fast and secure transaction verification mechanism. This mechanism can improve the performance of the Be L2 network while protecting the privacy of users.

4.2.6 The forced withdrawal mechanism of BTC in L2

The Be L2 technology also incorporates a forced evacuation mechanism. During the transition period,in the case that the validators of the second-layer network cannot reach a consensus and cannot complete the second-layer block generation, the user can broadcast his withdrawal transaction, and after a period of time (14 days), the funds can be withdrawn. This allows users to avoid continuously waiting for the recovery of Layer 2. It is a light centralized solution where nodes only assist in speeding up the process, serving as a backup plan to ensure that users do not lose their assets.

5 Synergy of Bitcoin and the Be L2 Network

In our design, Bitcoin and the second layer network (Be L2) are not independent. They support and strengthen each other in the following aspects.

5.1 Synchronize layer-1 transactions to the Be L2 network

In order to allow the Be L2 network to maximumly leverage the Bitcoin network's computing power, we have designed a mechanism so that Bitcoin transactions on the first layer can be synchronized in the Be L2 network. Whenever a transaction occurs in the Bitcoin network, the Be L2 network will generate a corresponding transaction, so that all transactions that occur in the Bitcoin network can be seen in the BeL2 network.

This design enables the Be L2 network to reflect the status of the Bitcoin network in real time, allowing users to view and verify the status of their assets in the Bitcoin network at any time.

A potential use case is the interaction between the second layer network and the first layer of Bitcoin's Ordinals asset. For example, a user mints an Ordinals asset on the first layer network, and this event can be detected on the second layer, prompting a reaction such as sending the user a certain ERC20 token as a reward.

5.2 Provide BTC price seed for L1

The price of Bitcoin is determined by the market, and fluctuations in market prices directly affect the security and stability of the Bitcoin network. Therefore, we designed a mechanism so that the Be L2 network can provide price seeds for the Bitcoin network.

In this design, the Be L2 network will periodically obtain the market price of Bitcoin, and add this price, time, and co-signature as a seed to the UTXO of the Bitcoin layer 1 network. When the Bitcoin network needs to obtain price information, it can set conditions in the script, for example, when the BTC price is below $30,000, the UTXO can be unlocked. This can be used to unlock and liquidate BTC collateral when borrowing against BTC.

6 Roadmap

Project roadmap is critical to achieve our goals and vision. In this section, we will detail our roadmap, with goals and plans for each stage.

6.1 Stage 1: Prototype verification and ecological infrastructure construction

In this stage, we will implement compatibility with the Ethereum Virtual Machine (EVM) on the test network, and ensure consensus through merged mining with BTC and Proof of Stake (PoS). At the same time, ecological basic components such as cross-chain bridges and oracles will also be built. Basic dApps such as cross-chain Swap, Dex, and lending will also be introduced to facilitate the introduction of more types of ecological applications to the second-layer network.

6.2 Stage 2: Decentralization and cross-chain

The goal of the second stage is to solve the centralization problem through Ordinals and BRC20 data index contracts. Cross-chain based on Ordinals assets, and mint the assets of the first-layer network based on Ordinals on the second-layer network, providing derivative services similar to Ethereum DeFi's first-layer network assets, such as issuance, exchange, and minting.

6.3 Stage 3: Enhancing Security and Efficiency

In the third stage, we plan to enhance the Bitcoin network deposit certificate and consensus, transplant zkEVM to the second-layer network, support transaction proof and Merkle tree generation of the second-layer network Bitcoin balance. Implement a reliable node operating environment based on the Trusted Execution Environment (TEE), implement a node asset management service module based on multi-party computing (MPC)/threshold signatures, and implement a consensus mechanism on the second-layer network, including transaction packaging, proof generation, and multi-party signature certification The notarization mechanism for transactions to the first-layer network, etc. Realize the Bitcoin cross-chain mechanism between the first layer and the second layer, based on the Bitcoin balance Merkle tree of the second layer network, realize the non-custodial withdrawal method to the first layer network.

6.4 Stage 4: Hybrid Technology Solutions

In the fourth stage, we will explore hybrid technology solutions, including exploring the feasibility of implementing the zk verification proof algorithm based on the existing Bitcoin OP Code, exploring hybrid technology solutions for limited proof verification on the first-layer network, and tracking potential second-layer networks The latest technology solutions for application scenarios. In addition, it will support the one-way bridging of Bitcoin between the first-layer and second-layer networks in a non-custodial manner. Users can withdraw bitcoins to their wallets even if the Layer 2 network is no longer functioning.

6.5 Stage 5: Bitcoin super chain BL Stack

In the fifth stage, our goal is to build BL Stack, which is to integrate all kinds of isolated BTC L2 into a single superchain (Superchain). This vision is not only forward-looking, but also has actual strategic value.

As the complexity of the Bitcoin network increased, many isolated L2 solutions emerged. These solutions, while effective in some ways, lack uniformity and interoperability. The goal of BL Stack is to create a unified super chain by integrating these isolated L2s, thereby eliminating fragmentation and improving the efficiency and availability of the entire network.

BL Stack's super chain not only integrates the existing L2, but also emphasizes interoperability and composition. This means that different L2s can seamlessly interact and share resources and functions. This compositionality allows developers the flexibility to build complex applications while maintaining system consistency and maintainability.

Another important goal of BL Stack is to simplify the deployment process of L2. By providing a unified framework and tools, BL Stack makes launching L2 as easy as deploying smart contracts to Ethereum today. This greatly lowers the development barrier and attracts more developers and projects to join the Bitcoin ecosystem.

BL Stack's super chain is open and scalable. Anyone can participate and contribute, and the new L2 can be easily integrated into existing hyperchains. This ensures that BL Stack can adapt to future needs and challenges, and continue to promote the innovation and growth of the Bitcoin network.

7 Tokenomics

(This part of the content may not be included in the officially released white paper. The token is planned to be issued in the third and fourth phases, around the middle of 2025, and will be adjusted depending on the progress of technology development and market conditions.)

$Be2 is the native ERC-20 governance token of the Be Layer2 network. Token properties at launch:

Initial supply cap	**100 billion**
Inflation	Max 2% per year
Minting/burning mechanism	L2 smart contract
Bridgeable to Bitcoin L1?	Yes
Tokens launch on	Bitcoin Layer 2
On-chain governance (voting) happens on	Bitcoin Layer 2
Airdrop snapshot	It is planned to issue tokens in the third phase (after the test network is transferred to the main network), and airdrop to the nodes participating in the consensus, dApps and users participating in the ecological construction, and the time is expected to be in the middle of 2025.

Initial token allocation & airdrop distribution

Percentage of initial supply	**Number of tokens**	**Allocated to**
45%	45 billion	DAO treasury

25%	25 billion	Development Team and Consultants
15%	15 billion	Investors
15%	15 Billion	Airdrop to users, consensus nodes, and ecological applications

8 Staking ELA to mine $Be2

From the first stage to the third stage of Be L2 construction, the Elastos community will be responsible for building its test network and opening the consensus nodes of Be L2. Each node needs to stake at least 10,000ELA or 0.5 BTC, and all nodes will be within 18 months A total of 10% of the total amount of $Be2 tokens will be rewarded.

8.1 Number of Token Rewards

10% of the total issuance of $Be2 will be airdropped to the test network nodes, which will be distributed evenly in 18 months.

8.2 Node Staking

8.2.1 Staking amount

1. Each consensus node needs to stake at least 10,000 ELA or 0.5 BTC.
2. Node owners and voters collectively contribute ELA or BTC required for staking.

8.2.2 Staking time

1. The node owner needs to choose the node staking time when creating the node.
2. Voters need to choose the voting node and voting staking time when voting, and the voting staking time cannot be greater than the remaining staking time of the node.
3. The staked funds will be released automatically after the stake period ends, and the staked Token cannot be retrieved before the stake period ends.

4. Node owners and voters can choose to extend the stake period before the end of the stake period, and the new stake period will take effect at 0:00 the next day; the stake period cannot be shortened.
5. Voters can change voting nodes before the end of the stake period. The updated voting information will take effect at 0:00 the next day.

8.3 Node type

1. Nodes are divided into consensus nodes and candidate nodes.
2. The test nodes that meet the minimum number of staked Tokens and rank among the top 108 in computing power are testnet consensus nodes, and other nodes are testnet candidate nodes.
3. Both consensus nodes and candidate nodes will receive airdrop rewards.

8.4 Calculation

1. 10,000 ELA has the same computing power as 0.5 BTC when it goes online; after going online, the 30-day moving average price of ELA and BTC at 0:00 every Monday is used as the benchmark price to calculate the computing power of the test node for the next week.
2. Calculation formula:

   Computing power (staking ELA) = ELA benchmark price* Amount of staked ELA* stake Quantity Coefficient * stake Time Coefficient

   Computing power (staked BTC) = BTC benchmark price * amount of staked BTC

   Node computing power = [node owner computing power + sum(node voter computing power)] * node coefficient

3. Calculate node computing power and update node computing power ranking at 0:00 every day.
4. Calculate the daily token rewards according to the ratio of node computing power to the total computing power of all nodes.

5. Voters can vote for nodes, and the node owner and voter receive 20% and 80% of the token rewards corresponding to the voting computing power respectively.
6. Stake Quantity Coefficient

Amount of ELA staked	coefficient	Remark
1 ~ 1000	1	
1001 ~ 10000	1.05	1.01^5
10001 ~ 20000	1.34	1.015^20
More than 20000	1.5	

7. Staking Time Coefficient

ELA stake time	coefficient	Remark
7 days	1	
30 days	1.04	1.01^4
90 days	1.21	1.015^(90/7)
180 days	1.50	1.016^(180/7)
360 days	2.38	1.017^(360/7)
540 days	3.96	1.018^(540/7)

8. node coefficient

node	condition	coefficient
consensus node	Rank ≤ 108 and stake ELA ≥ 10000	5
candidate node	Node rank > 108 or staked ELA < 10000	1

8.5 Node voting

1. Node owners and voters need to choose the stake time when staking, and the staked funds will be released automatically after the stake time ends. The staked Token cannot be retrieved before the end of the stake period.
2. The stake time selected during voting cannot be greater than the remaining stake time of the node.
3. Node owners and voters can choose to extend the stake period before the end of the stake period, and the new stake period will take effect at 0:00 the next day; the stake period cannot be shortened.
4. Voters can change voting nodes before the end of the stake period. The updated voting information will take effect at 0:00 the next day.

8.6 stake NFT

1. Node owners and voters will obtain "staking NFT" and "stake NFT" after staking.
2. Stake NFT and equity NFT support transactions on the NFT platform.
3. The address holding the staked NFT will get the staked ELA or BTC after the stake period ends.
4. Addresses that hold equity NFT can receive the amount of $Be2 corresponding to the equity during the airdrop.