# Be Your Own Bank

BeL2 = Bitcoin Elastos Layer 2

EF Core Team

December 1, 2023

**Abstract.**This paper explores the Bitcoin-Elastos Layer 2 solution (BeL2), enhancing Bitcoin's ecosystem by addressing scalability, programmability, and privacy. Integrating Elastos SmartWeb technology with Bitcoin, BeL2 employs zero-knowledge proofs, BTC-powered EVM smart contracts, and ELA staking mechanisms. It focuses on secure transaction verification, relayer-based fraud prevention, and gamified transaction management. Governed by the Cyber Republic's DAO, BeL2 extends Bitcoin's functionality in decentralized finance and rights markets, maintaining its core principles and leveraging its security. This BTC-powered Layer 2 solution unlocks dormant value in Bitcoin holdings, innovatively expanding its use in the SmartWeb economy.

**摘要：**本文探讨了比特币-亦来云第二层解决方案（BeL2），通过解决可扩展性、可编程性和隐私问题来增强比特币的生态系统。BeL2 将 Elastos SmartWeb 技术与比特币相集成，采用零知识证明、以 BTC 为驱动的 EVM 智能合约和 ELA 质押机制，它专注于安全交易验证、基于中继层的欺诈预防和博弈交易管理。BeL2 由 Cyber Republic 的 DAO 管理，在去中心化金融和权益市场中扩展了比特币的功能，并维护了其核心原则及充分利用了安全性。这种由 BTC 驱动的第二层解决方案释放了比特币持有量的休眠价值，创新性地扩展了其在 SmartWeb 经济中的使用。

## 1 Introduction

### 1. 序言

In 2009, Satoshi Nakamoto introduced Bitcoin, a secure and decentralized "digital gold," using the SHA-256 algorithm and proof-of-work to revolutionize financial autonomy and challenge traditional finance. Bitcoin's creation combined cryptographic innovations like Merkle trees and ECDSA to form a secure, decentralized financial network, linking miners efforts to network security and protecting against attacks. Bitcoin, more than just technology, challenges traditional authority with a new social contract based on code and computation, blending individual freedom with collective good and evolving global wealth consensus to address future economic challenges. This approach aims to help humanity overcome global debt crises as predicted by economy strategist Ray Dalio.

2009 年，中本聪推出了比特币，这被视为一种安全而去中心化的"数字黄金"，他采用 SHA-256 算法和工作证明，彻底颠覆了金融自治并对传统金融提出挑战。比特币的诞生融合了 Merkle 树和 ECDSA 等密码学创新，构建了一个安全而去中心化的金融网络，将矿工的工作与网络安全紧密相连，并提供防御攻击的保护。比特币不仅仅代表技术，更通过建立基于密码学和计算的新社会契约，挑战传统权威，将个体自由与集体利益融为一体，并形成演变中的全球财富共识，以应对未来的经济挑战。这一理念目标是帮助人类应对经济策略家 Ray Dalio 预测的全球债务危机。

In this paper, we discuss Bitcoin's scalability, programmability, and privacy challenges, and compare various Layer 2 solutions enhancing Bitcoin's functionality. We introduce the Bitcoin- Elastos's Layer2 solution, called BeL2, which focuses on integrating Elastos' SmartWeb technology to enhance Bitcoins

decentralized banking ecosystem, leveraging zero-knowledge proofs, smart contracts and implementing a staking mechanism for network security and transaction validation.

在白皮书中，我们探讨了比特币在可扩展性、可编程性和隐私方面所面临的挑战，并比较了多种增强比特币功能的 Layer 2 解决方案。我们介绍了比特币-亦来云的 Layer 2 解决方案，简称为 BeL2，该解决方案专注于整合 Elastos SmartWeb 技术，以增强比特币的去中心化银行业务生态系统，运用零知识证明、智能合约并实施用于网络安全和交易验证的博弈机制。

# 2 Pioneering the Be Layer2 from Bitcoin's Foundations

# 2. 以比特币为基础开创 Be Layer2

The Elastos SmartWeb, supported by the Bitcoin ecosystem through merged mining since its 2018 launch, aims to build BeL2 for a secure, scalable, decentralized Web3 financial ecosystem, based on the 'You Own Your Data' principle and incorporating Bitcoin's technology. This BeL2 system enables a peer-to-peer "Be Your Own Bank" environment where participants can utilize BTC assets to trade and interact with smart services. BeL2's core goals include:

自 2018 年启动以来，Elastos SmartWeb 通过联合挖矿技术得到了比特币生态系统的支持，以"You Own Your Data"为原则，为一个安全、可扩展、去中心化的 Web3 金融生态系统构建 BeL2。这个 BeL2 系统使参与者能够利用 BTC 资产进行交易并与智能服务进行互动，从而实现点对点的"Be Your Own Bank"环境。BeL2 的核心目标包括：

1. **Exchange.** Enable frictionless exchange transactions between BTC and second-layer assets, as well as with select off-chain assets, supporting smart contracts with BTC transaction fees.

1.**交易。**实现 BTC 和第二层资产以及与链外资产之间的无摩擦交易，支持使用 BTC 交易费用的智能合约。

**2. Lending.** Facilitate the use of mainnet BTC as collateral for digital asset lending (eg. USDC) within the second-layer network.

**2. 借贷**。促进主网 BTC 作为数字资产借贷（例如 USDC）的抵押物在第二层网络内的使用。

**3. Ecosystem.** Foster a developer-friendly environment, encouraging the creation of novel applications that leverage the capabilities of the BeL2 solution, such as marketplaces for digital goods and revenue generating online economies. By nurturing this smart ecosystem, we aim to catalyze innovation and expand the utility of Bitcoin technology.

**3. 生态系统。**营造一个开发者友好的环境，鼓励创造利用 BeL2 解决方案能力的新型应用程序，如数字商品市场和创收的在线经济。通过培育这个智能生态系统，我们的目标是促进创新，并拓展比特币技术的实用性。

Since BTC.com mined the first block in 2018, Elastos' merged mining with Bitcoin's Proof of Work (PoW) algorithm has enabled BTC miners to support the Elastos SmartWeb, thereby earning consistent ELA mining revenue at no additional cost in alignment with decentralized security principles. This joint venture has seen considerable growth, with BTC miners having mined over 1.31 million blocks for Elastos, providing

unrivalled security to the SmartWeb and earning 1.68 million ELA and contributing over $10 million in value to the BTC ecosystem.

自 2018 年 BTC.com 开采第一个区块以来，Elastos 将挖矿与比特币的工作证明（PoW）算法相结合，使 BTC 矿工能够支持 Elastos SmartWeb，从而遵循去中心化安全原则，无需额外成本即可获得持续的 ELA 挖矿收入。这一合作关系取得了显著增长，BTC 矿工为 Elastos 开采了超过 131 万个区块，为 SmartWeb 提供了无可比拟的安全性，并获得了 168 万 ELA，为 BTC 生态系统贡献了超过 1000 万美元的价值。

Elastos is supported by over 18 BTC mining pools, such as f2pool and Binance, contributing hash power to ELA, sometimes exceeding 50% of Bitcoin's total hash power. Before 2021, BTC miners earned over 462,000 ELA annually; following the 2025 halving, this figure stands at over 140,000 ELA per year. Total rewards have surpassed 1.68 million ELA and are projected to exceed 2 million by 2025, underscoring the successful ELA-Bitcoin mining partnership. ELA's issuance rate, similar to Bitcoin's halving process, decreases over time to control inflation and stabilize the currency, culminating in a total supply of 28.22 million coins by 2105. The goal of BeL2 is to expand the relationship with Bitcoin's hashpower, enabling programmable BTC-powered SmartWeb features and financial services.

Elastos 得到了超过 18 个 BTC 矿池支持，如 f2pool 和 Binance，为 ELA 贡献了哈希算力，有时超过比特币总哈希算力的 50%。2021 年之前，BTC 矿工的年收入超过 46.2 万 ELA；在 2025 年减半后，这一数字每年超过 14 万 ELA。总奖励已超过 168 万 ELA，预计到 2025 年将超过 200 万，证实了 ELA-BTC 联合挖矿的成功。ELA 的发行速度，类似于比特币的减半过程，随着时间的推移而降低，以控制通货膨胀和稳定货币，最终在 2105 年，达到总供应量 2822 万枚。BeL2 的目标是扩展与比特币哈希算力的关系，实现可编程的以 BTC 为驱动的 SmartWeb 功能和金融服务。

# 3 Challenges with Bitcoin Layer 1

# 3.比特币第 1 层面临的挑战

1. **Scalability.** Bitcoin's blockchain can only process about seven transactions per second due to its 1MB block size and ten-minute block interval, leading to delays and higher costs, especially compared to faster financial networks like Visa. During high demand, Bitcoin's slow confirmation times and high transaction costs, often exceeding $10 in gas, make it less suitable for users needing fast transactions, like merchants and consumers.

**1. 可扩展性。**由于比特币的 1MB 区块大小和十分钟的出块间隔，比特币的区块链每秒只能处理大约七笔交易，这导致了延迟和较高的成本，特别是与 Visa 等这样速度更快的金融网络相比。在需求高峰期，比特币确认时间慢和高交易成本，每笔交易往往超过 10 美元，使其不太适用于需要快速交易的用户，如商家和消费者。

2. **Privacy.** While Bitcoin addresses provide user anonymity, Bitcoin's transparent blockchain records all transactions publicly, allowing anyone to potentially trace addresses back to real identities, which could compromise user anonymity. To address privacy concerns, the Bitcoin community has developed technologies like CoinJoin, MimbleWimble, and ZK-SNARKs, enhancing transaction privacy while maintaining Bitcoin's transparency and verifiability.

**2. 隐私性**。虽然比特币地址提供了用户匿名性，但比特币透明的区块链公开记录所有交易，允许任何人潜在地追踪地址至真实身份，这可能会危及用户的匿名性。为了解决隐私问题，比特币社区开发了 CoinJoin、MimbleWimble 和 ZK-SNARK 等技术，增强交易隐私同时保持了比特币的透明度和可验证性。

3. **Programmability.** Bitcoin's scripting language, unlike Ethereum's Turing-complete one, is limited in functionality, restricting developers from creating complex smart contracts and advanced applications. Bitcoin was created to be a simple, secure digital currency focusing on decentralized transactions, making it highly secure but limited in handling complex applications. Ethereum's growth, aiming to overcome Bitcoin's limitations, reflects the market's demand for more extensive programmable capabilities, as shown by its market value nearing half of Bitcoin's.

**3. 可编程性。**与以太坊的图灵完备语言不同，比特币的脚本语言在功能上受到限制，这使得开发人员无法创建复杂的智能合约和高级应用程序。比特币被创建为一种简单、安全的数字货币，专注于去中心化交易，这使其具有高度的安全性，但在处理复杂应用方面有所限制。以太坊的发展旨在克服比特币的局限性，这反映了市场对更广泛可编程能力的需求，如其市值接近比特币市值的一半。

# 4 Exploring Layer 2 Innovations

# 4.探索第二层创新

• **The Lightning Network.** The Lightning Network, as a second-layer solution, enhances Bitcoin's scalability by enabling quick, low-cost transactions without recording each one on the main blockchain. The Lightning Network operates on payment channels where users create a multisignature wallet on the Bitcoin blockchain for frequent transactions, enabling numerous private and efficient exchanges without immediate blockchain broadcast. The Lightning Network offers fast payments, lower fees, better scalability, and more privacy, but faces challenges like fund immobilization, routing complexity, and maintaining sufficient liquidity.

**•闪电网络。**闪电网络作为第二层解决方案，通过实现快速、低成本的交易来增强比特币的可扩展性，且无需在比特币主区块链上记录每一笔交易。闪电网络服务于支付赛道，用户在比特币区块链上创建多签名钱包以进行频繁交易，无需立即在区块链上广播即可实现众多私密而高效的交易。闪电网络虽提供了快速支付、更低的费用、更好的可扩展性和更多的隐私，但面临着资金冻结、路由复杂性和保持足够流动性等问题。

• **The Rootstock Infrastructure Framework (RSK).** RSK, or Rootstock Infrastructure Framework, enhances Bitcoin by adding efficient functions and services like decentralized domain names and secure communication protocols to its robust foundation. However, it faces challenges in balancing added complexity with maintaining Bitcoin's core simplicity and security.

**•Rootstock 基础设施框架（RSK）。**RSK，或称为 Rootstock 基础设施框架，通过在比特币强大的基础上添加高效的功能与服务，如去中心化的域名和安全通信协议来增强比特币。然而，RSK 在平衡增加的复杂性与保持比特币的核心简单性和安全性方面面临挑战。

• **Drivechain.** Drivechain, a sidechain mechanism, enhances Bitcoin's interoperability and scalability by enabling the creation of distinct, customizable sidechains linked to the mainchain. It allows bitcoins to be transferred and verified on these sidechains through SPV. Funds can move between the sidechain and

Bitcoin's mainchain with miner consensus. However, Drivechain's implementation requires a hard fork in Bitcoin, presenting considerable coordination and consensus challenges.

• **Drivechain**。Drivechain 是一种侧链机制，通过创建与主链相连的独立、可编程的侧链，增强了比特币的互操作性和可扩展性。它允许比特币通过 SPV 在这些侧链上进行交易和验证。通过矿工共识，资金可以在侧链和比特币主链之间流动。然而，Drivechain 的实施需要比特币的硬分叉，存在着相当大的协调和共识挑战。

• **The Liquid Network.** The Liquid Network, a sidechain-based layer, connects global exchanges and institutions to speed up Bitcoin transactions and secure digital asset issuance, often settling in just two minutes. The Liquid Network prioritizes privacy, keeping transaction details confidential and supporting various assets, including L-BTC. It enables direct crypto exchanges and Bitcoinstyle security, fostering a secure and efficient digital transaction environment. Its challenge is in needing wide adoption by exchanges and institutions to be fully effective.

• **The Liquid Network**。Liquid Network 作为基于侧链的第二层，连接全球交易所和机构，以加快比特币交易并确保数字资产发行，通常只需两分钟即可结算。Liquid Network 首先考虑隐私性，对交易细节保密，并支持包括 L-BTC 在内的各种资产。它实现了直接加密交易和比特币式的安全性，促进了安全高效的数字交易环境。其挑战在于需要交易所和机构广泛采用才能充分发挥作用。

• **Rollkit.** Rollkit, initially created for Celestia, now supports Bitcoin, allowing Ethereum's Virtual Machine (EVM) applications to run on the Bitcoin network. This integration leverages Bitcoin's strong consensus and data infrastructure, enhancing application security and versatility. Rollkit includes a 'bitcoin-da' Go package for Bitcoin data interaction and supports EVM, CosmWasm, and Cosmos SDK. Its successful testing on a Bitcoin testnet marks a significant advancement in Bitcoin's cross-chain functionality. Its challenge is in integrating Ethereum's flexibility with Bitcoin's infrastructure without compromising security.

•**Rollkit**。Rollkit 最初为 Celestia 创建，现在支持比特币，允许以太坊的虚拟机（EVM）应用程序在比特币网络上运行。这一整合充分利用了比特币强大的共识和数据基础设施，增强了应用程序的安全性和通用性。Rollkit 包括一个用于比特币数据交互的"bitcoin-da"Go 包，并支持 EVM、CosmWasm 和 Cosmos SDK。它在比特币测试网上的成功测试标志着比特币跨链功能的重大进步。其挑战在于，在不影响安全性的情况下，将以太坊的灵活性与比特币的基础设施相结合。

• **RGB.** RGB is a complex smart contract system on Bitcoin and Lightning Network, turning contract states into proofs embedded in Bitcoin transactions, with dedicated nodes managing and verifying these contracts. RGB contracts on Bitcoin's Layer 2 have separate states without a shared chain, unlike Ethereum, and use Bitcoin's security but face limits in data demand and redundancy as their number grows.

•**RGB**。RGB 是比特币和闪电网络上的复杂智能合约系统，它将合约状态转化为嵌入在比特币交易中的证明，通过专用节点管理和验证这些合约。与以太坊不同的是，比特币第二层上的 RGB 合约具有独立的状态，并且拥有比特币的安全性，没有共享链，但随着数量的增长，数据需求和冗余性会受到限制。

• **ZeroSync.** ZeroSync introduces zero-knowledge proofs to Bitcoin, a significant advancement for scalability and privacy, previously mainly developed by the Ethereum community. Proving Bitcoin's entire blockchain history is demanding but results in a compact proof that lets any number of nodes quickly sync with the network, with the ability to update this proof efficiently as new blocks are added. These proof systems, compatible with Bitcoin's immutability, compress its blockchain and add new features without

changing consensus rules, giving users flexible options for blockchain interaction and enabling innovative applications.

•ZeroSync。ZeroSync 为比特币引入了零知识证明，这对于可扩展性和隐私是一项重大进展，先前主要由以太坊社区开发。证明比特币整个区块历史是一项复杂的任务，但产生了一个紧凑的证明，使得任意数量的节点可以快速与网络同步，并能够在添加新块时高效更新此证明。这些证明系统与比特币的不变性兼容，通过在不改变共识规则的情况下压缩其区块链并添加新功能，为用户提供灵活的区块链交互选择，并实现创新应用。

In our analysis of BTC expansion technologies, the Lightning Network stands out for preserving decentralization, but it lacks programmability and is limited to transfers. Inspired by Ethereum's second-layer projects, we explored using zero-knowledge proofs to enable consensus transfer between networks. This led us to the ZeroSync project, which utilizes Cairo for creating proof circuits for BTC block headers. Our conclusion is that by combining zero-knowledge proofs with game theory mechanisms, we can develop a non-custodial, permissionless BTC expansion solution. This solution, which supports BTC-powered smart contracts, can enhance BTC's capabilities through a Layer 2 network without altering its mainnet consensus.

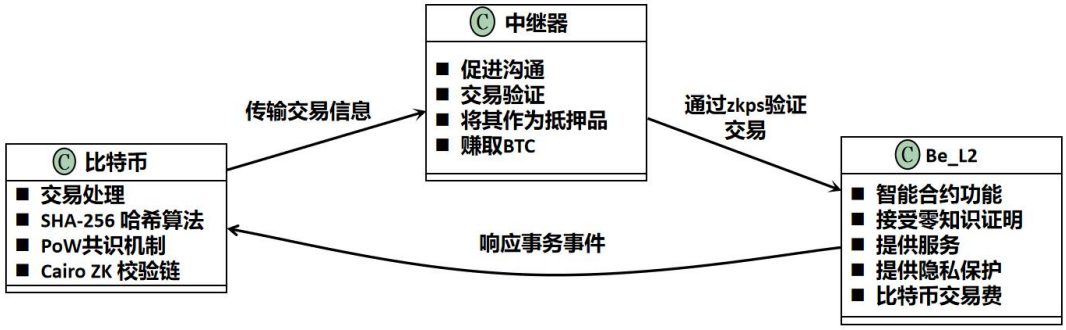
在我们对 BTC 扩展技术的分析中，Lightning Network 以去中心化而闻名，但它缺乏可编程性，而且仅限于转账。我们受以太坊第二层项目的启发，我们探讨了使用零知识证明在网络间实现共识转移的可能性。这使我们接触到了 ZeroSync 项目，该项目利用 Cairo 为 BTC 块头创建验证链路。我们的结论是，通过将零知识证明与博弈论机制相结合，我们可以开发一种非托管、无许可的 BTC 扩展解决方案。该解决方案支持以 BTC 为驱动的智能合约，可以通过第二层网络增强 BTC 的功能，而不会改变其主网共识。

# 5 An Overview of BeL2 Technology

# 5 BeL2 技术概述

Current Bitcoin Layer 2 solutions can't directly recognize transactions between their own and Bitcoin's ledgers, relying instead on error-prone multi-signature mechanisms by validators, posing risks of collusion and punishment challenges. Zero-knowledge proof (ZKP) technology enables second-layer networks to verify Bitcoin transactions without seeing their details, ensuring their authenticity and integrity alongside privacy. Information transfers in both directions, from the main network to the second layer and vice versa, is facilitated by a relayer, who, to prevent fraud, stakes a deposit that's forfeited if they act dishonestly. This self-hosted model allows independent relayer operation with just a deposit, penalizing them for malpractice or failure to prove transactional duty fulfilment.

目前的比特币第二层解决方案无法直接识别其自身和比特币账本之间的交易，而是依赖于验证者容易出错的多重签名机制，存在串通风险和惩罚挑战。零知识证明（ZKP）技术使第二层网络能够在不查看比特币交易细节的情况下验证比特币交易，从而确保其真实性和完整性以及隐私性。从主网络到第二层（反之亦然）的双向信息传输都由中继者提供验证，为了防止欺诈，如果中继者行为不端，保证金将被没收。只需提供保证金，这种自托管模式就能允许独立的中继者操作，对于渎职或未能履行证明交易义务的行为进行处罚。




## 5.1 Integration of BTC Mainnet Transactions within Layer 2 Networks

## 5.1 BTC 主网交易在第 2 层网络中的集成

Cairo, by Starkware, is a programming language designed for zero-knowledge proof circuits, especially for verifying Bitcoin transactions, and has been used in ZeroSync to optimize BTC node data synchronization. Cairo, supporting Sharknet's Ethereum Layer 2 network, creates transaction proofs verified by Ethereum's mainnet, enhancing Layer 2's reliability, as shown by Starknet's TVL exceeding 80 million US dollars. The integration of BTC mainnet transactions into the BeL2 framework is achieved through a proof circuit developed in Cairo, which facilitates the generation of multifaceted proofs to:

Cairo 是一种专为零知识证明链路设计的编程语言，特别是用于验证比特币交易，并已在 ZeroSync 中用于优化 BTC 节点数据同步。Cairo 支持 Sharknet 的以太坊第二层网络，创建由以太坊主网验证的交易证明，增强了第二层的可靠性，正如 Starknet 的 TVL 超过 8000 万美元。通过在 Cairo 中开发的证明链路，将比特币主网交易整合到 BeL2 框架中，从而实现生成了对以下多方面的证明：

1. Confirm the proper formatting of the transaction.

1. 确认交易的正确格式。

2. Validate the authenticity of the transaction's signature.

2. 验证交易签名的真实性。

3. Confirm transaction inputs are greater than outputs, maintaining financial balance.

3. 确认交易输入大于输出，保持财务平衡。

4. Verify that the referenced Unspent Transaction Outputs (UTXOs) originate from reliable sources.

4. 验证运行的交易输出（UTXO）信息来源真实有效。

5. Ascertain the functionality of the unlocking script within the transaction.

5. 确定交易中解锁脚本的功能。

A BTC transaction proof comprises raw data and a zero-knowledge proof, verifying mainnet transactions. These transactions are validated and propagated based on the BTC network consensus. Each transaction on the BTC network can generate a zero-knowledge proof and retrieve its raw data. A complete transaction proof, combining raw data and the zero-knowledge proof, confirms the transaction's validity. Therefore, it can be propagated and recorded on the blockchain. In essence, BTC mainnet transactions and their corresponding proofs are equivalent, maintaining the network's financial integrity and accuracy.

BTC 交易证明包括原始数据和零知识证明，用于验证主网交易。这些交易基于 BTC 网络共识进行验证和传播。BTC 网络上的每笔交易都可以生成零知识证明并检索其原始数据。一个完整的交易证明，结合原始数据和零知识证明，证实了交易的有效性。因此，它可以在区块链上传播和记录。从本质上讲，BTC 主网交易及其相应的证明是等效的，保持了网络的财务完整性和准确性。


## 5.2 Integration of ZKP and EVM for BTC-ELA Transactions and Relayer Mechanism

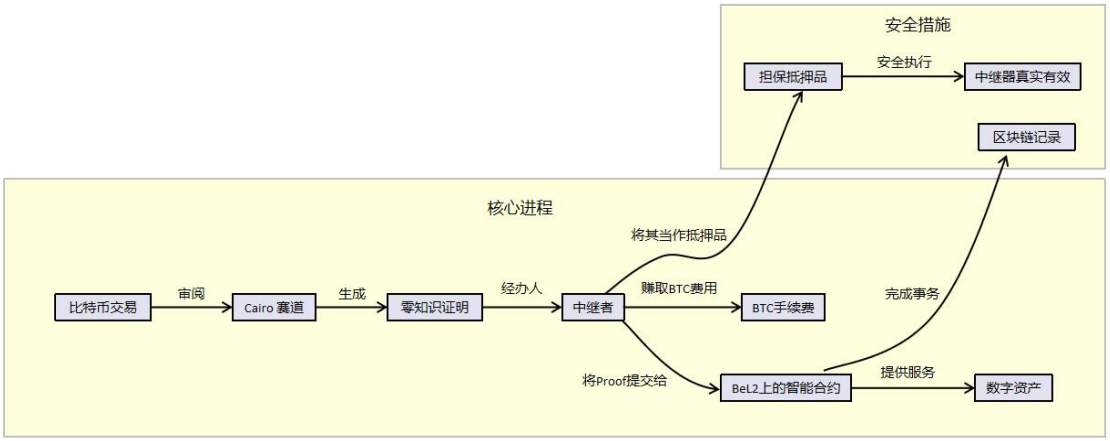
## 5.2 用于 BTC-ELA 交易及中继机制的 ZKP 和 EVM 的集成

With the advancement of Ethereum Layer 2 and zero-knowledge proof technologies, testing ZKPs in Solidity contracts has become feasible. In our initial phase using Elastos' Ethereum Virtual Machine (EVM) sidechain, we've enabled the verification of proofs generated by Cairo. Essentially, a Bitcoin user can transfer BTC on Layer 1, generate a ZKP, and submit it to a smart contract on the Elastos EVM sidechain to exchange for digital assets, thereby integrating BTC and ELA transactions.

随着以太坊第二层和零知识证明技术的进步，测试 Solidity 合约中的 ZKP 已经变得可行。在我们使用 Elastos 的以太坊虚拟机（EVM）侧链的初始阶段，我们已经实现了对 Cairo 生成的证明的验证。基本上，比特币用户可以在第 1 层交易 BTC，生成 ZKP，并将其提交到 Elastos EVM 侧链上的智能合约中，以交换数字资产，从而整合 BTC 和 ELA 交易。

In BeL2, a user wanting to trade for Layer 1 BTC deposits eg. ELA into a contract. Risks include time loss if the BTC user withdraws or doesn't transfer, especially in complex deals like mortgage loans when BTC's value falls. To streamline these transactions, a Relayer is introduced. Not a custodian but an executor, the Relayer ensures quick, efficient transaction completion. This role is vital as regular users may not be consistently online or might delay transactions. The Relayer, motivated by rewards, stays online to execute transactions promptly, reducing delays and enhancing the transaction process.

在 BeL2 中，想要交易第 1 层 BTC 的用户需将 ELA 等存入合约。风险包括如果 BTC 用户撤回或不转账，特别是在像抵押贷款这样的复杂交易中，当 BTC 的价值下降时会导致时间损失。为了简化这些交易，引入了中继程序。中继者不是托管人，而是执行者，确保快速高效地完成交易。这一角色至关重要，因为普通用户可能无法持续在线，或者可能会延迟交易。中继者在奖励的激励下使其保持在线以迅速执行交易，减少延迟并增强交易过程。




In the transaction's initial stage, the parties involved and the Relayer jointly create a Bitcoin (BTC) address requiring two out of three signatures. When executing a BTC transfer, the claimant and the Relayer together provide the necessary signatures, enabling immediate transaction execution without depending on the counterparty. This simplifies the process by reducing dependency and potential delays in transactions. The Relayer must deposit assets as collateral. If the Relayer acts maliciously, the affected party or an overseer can present proof of this misconduct, leading to the termination of the transaction and the transfer of the Relayer's deposit to the victim. This mechanism effectively deters the Relayer from any wrongdoing. Relayers are unrestricted participants who can join freely, provided they pledge assets as collateral. These assets are held in a BeL2 smart contract and can be withdrawn anytime, assuming no ongoing obligations.

在交易的初始阶段，参与方和中继者共同创建一个比特币（BTC）地址，需要三分之二的签名。在执行 BTC 转账时，申请人和中继者一起提供必要的签名，从而能够在不依赖交易对手的情况下立即执行交易。这通过减少交易中的依赖性和潜在延迟来简化流程。中继者必须存入资产作为抵押品。如果中继者有恶意行为，受影响的一方或监管人可以提供这种不当行为的证据，导致交易终止，并将中继者的抵押转移给受害者。这种机制有效地阻止了中继者的任何不当行为。中继者是无限制的参与者，只要他们以资产作为抵押品，就可以自由加入。这些资产被保留在 BeL2 智能合约中，不承担任何持续义务时，可以随时提取。

## 5.3 Enhanced Security through Transaction Management Gamification

## 5.3 通过交易管理博弈化增强安全性

• **Multi-Signature Management of Transaction Funds.** Transaction security on the Bitcoin mainnet is heightened through the establishment of multi-signature addresses, a collaborative effort between the transacting parties and the Relayer. To execute a transaction, at least two signatures are required, reinforcing the safeguarding of the Bitcoin involved.

**•交易资金的多重签名管理。**在比特币主网络上，通过建立多重签名地址，交易安全性得到提升，这需要交易双方和中继者共同努力。要执行交易，至少需要两个签名，以加强对所涉及比特币的保护。

• **Relayer (BeL2 Nodes) Deposit Commitment.** Relayers, acting as transaction facilitators, are obligated to place a deposit into the Layer 2 network's smart contract. This deposit must exceed the value of the transaction they intend to relay, serving as a financial guarantee of their commitment to execute the transaction faithfully.

**•中继（BeL2 节点）存款承诺。**中继者作为交易促进者，有义务将一笔押金放入 Layer 2 网络的智能合约。这笔押金必须超过他们打算中继的交易价值，作为他们忠实执行交易承诺的财务担保。

• **Initial Transaction Status Verification.** To proceed, both transaction participants must verify and agree upon the Unspent Transaction Output (UTXO) details. These confirmed UTXOs are then recorded in the Layer 2 network's smart contract, establishing the groundwork for the transaction.

**•初始交易状态验证。**为了继续交易，双方必须验证并就未花费交易输出（UTXO）的细节达成一致。这些确认的 UTXO 随后被记录在第二层网络的智能合约中，为交易奠定基础。

• **Transaction Completion and Verification.** The completion of the Bitcoin transfer is substantiated by submitting a zero-knowledge proof to the network, which validates the transaction without revealing any sensitive data.

**•交易完成和验证。**通过向网络提交零知识证明，证实了比特币转账的完成，同时不泄露任何敏感数据。

• **Proof Submission and Penalty Enforcement.** Should a Relayer act inappropriately, such as issuing an incorrect transfer certificate or attempting a double-spend, evidence of such actions triggers penalization. This safeguard ensures the integrity of the transaction process.

**•证据提交和处罚执行**。如果中继者行为不当，比如签发错误的交易证书或试图双重支出，此类行为的证据将触发惩罚。这种保护机制确保了交易过程的完整性。

• **Transactional Integrity and Assurance.** In the event Alice wishes to purchase Bitcoin from Bob and fulfills her payment obligations:

**•交易完整性和保证。**如果 Alice 希望从 Bob 那里购买比特币并履行他的支付义务：

1. If the Relayer initiates and proves a Bitcoin transfer, Bob receives the Bitcoin, completing the transaction with Alice's assets secured.

1. 如果中继者发起并证明了比特币转账，Bob 就收到比特币，从而完成了与 Alice 资产安全相关的交易。

2. Should the Relayer fail to broadcast the transaction, Bob can independently broadcast it, securing Alice's Bitcoin without any asset loss.

2.如果中继者未广播交易，Bob 可以独立广播它，保障 Alice 的比特币而不损失任何资产。

3. If the Relayer acts improperly or not at all, Bob can provide proof and claim the Relayer's deposit, protecting her assets.

3.如果中继者行为不当或根本不执行，Bob 可以提供证据并索要中继者的押金，以保护他的资产。

This process underlines the asset preservation principle inherent between first-layer (Bitcoin mainnet) and second-layer transactions, guaranteeing that assets remain unlost and transactions are faithfully executed.

这一过程强调了第一层（比特币主网）和第二层交易之间的资产保全原则，确保资产不会丢失，交易得到有效执行。

# 6 Incentivizing Blockchain Security through ELA Staking

# 6 通过 ELA 质押激励区块链安全性

In the first phase of validating the technical prototype, we will use fixed Relayers, functioning as L2 nodes, to facilitate transactions. For the second phase, our aim is to implement a permissionless, non-custodial decentralized Relayer mechanism. Relayers will back their reliability by pledging assets. Should they fail to perform, these pledged assets will be used to compensate any trading participants who suffer losses. To facilitate this, Relayers are required to stake ELA on ESC. In return for their services, Relayers will receive transaction fees in BTC.

在验证技术原型的第一阶段，我们将使用固定的中继者作为 L2 节点来促进交易。在第二阶段，我们的目标是实现一个无许可、非托管的去中心化中继机制。中继者将通过抵押资产来支持其履约行为。如果他们未能履约，这些质押资产将用于补偿任何遭受损失的交易参与者。为了促进这一点，中继需要在 ESC 上质押 ELA。作为服务的回报，中继者将以 BTC 的形式获得交易费用。

• **Become a Relayer (BeL2 nodes)** By depositing ELA in the staking contract, you can obtain a credit limit, which determines the capital limit for transactions that the Relayer can participate in. For example, if a relayer obtains a quota of 1,000 USD, it can only provide relay services for transactions with transaction amounts less than 1,000 USD. In the future, we may introduce credit services so that Relayer can achieve over-guarantee for transactions.

• **成为中继者（BeL2 节点）。**通过在质押合约中存入 ELA，您可以获得信用额度，该额度决定了中继者可以参与的交易的资金限额。例如，如果中继者获得 1000 美元的配额，则只能为交易金额低于 1000 美元的交易提供中继服务。未来，我们可能会推出信贷服务，使中继者能够实现交易的超额担保。

• **Relay transactions** When users need to trade, they can manually or automatically select the Relayer for the trade. Relayer assists transaction participants in completing BTC multisignature transaction signatures so that transactions can proceed smoothly. At the same time, it is the responsibility to ensure that the BTC transaction content comes from the content in the transaction contract, and to use appropriate technical means so that the transaction can be packaged by the BTC main network as soon as possible.

**•中继交易。**当用户需要交易时，他们可以手动或自动选择交易的中继者。中继者协助交易参与者完成 BTC 多重签名交易签名，使交易顺利进行。同时，中继者也有责任确保 BTC 交易内容来源于交易合约，并使用适当的技术手段，使 BTC 主网络能够尽快打包交易。

Once the Relayer is involved in the transaction between Alice and Bob, they cannot cancel their pledge until the transaction is completed. When staking ELA, a buffer is maintained. For example, pledging ELA valued at 130 US dollars might cover a transaction worth 100 US dollars. There are additionally two potential solutions to address under-collateralization caused by changes in the price of ELA or BTC:

一旦中继者涉及 Alice 和 Bob 之间的交易，在交易完成之前无法取消他们的质押。在质押 ELA 时，将会维持一个缓冲区。例如，质押价值 130 美元的 ELA 可能覆盖价值 100 美元的交易。此外，还有两种潜在的解决方案可以解决 ELA 或 BTC 价格变化引起的抵押不足问题：

1. Implement CreDA's credit system and regulate relayers through this system, rather than solely relying on asset pledges.

1.实施 CreDA 的信贷系统，并通过该系统规范中继者，而不仅仅依赖于资产质押。

2. Employ cryptographic technology to obscure the relationship between transactions and the relayer. This would prevent the relayer from knowing which transaction they are signing for, thereby inhibiting any collusion with transaction participants for malicious purposes.

2.利用加密技术来掩盖交易和中继者之间的关系。这将阻止中继者知道他们正在为哪笔交易签名，从而防止与交易参与者为恶意目勾结的可能性。

• **Rewards and penalties.** By being a relayer for transactions, you can get transaction fees (BTC). BTC rewards are derived from transaction fees. For instance, the Relayer deposits ELA for transaction facilitation and reward earning. Bob offers 20K ELA for 1 BTC over 3 months, transferring 20K ELA to the BeL2 smart contract and agreeing to a 1% BTC fee to the facilitating Relayer. Alice sends 1 BTC as collateral to borrow 20K ELA. The Relayer finalizes the transaction, claiming the 1% fee to cover BTC mainchain fees, ESC gas, and a reward. The 1 BTC is held in a 2/3 multisig address requiring signatures from Alice, Bob, and the Relayer. With a 12% annual interest rate, Alice's three-month interest on 20K ELA is 600 ELA, totaling a 20,600 ELA repayment. At term end, Alice retrieves 0.99 BTC, minus the 0.01 BTC Relayer fee. Without this fee, the contract rejects the transfer. Handling fee calculations are based on set terms. The handling fee calculation follows the agreed terms. Calculation of handling fee:

**•奖励和惩罚。**作为交易的中继者，您有机会获得交易费用（BTC）。BTC 奖励来源于交易费用。例如，中继者为促进交易和奖励而存入 ELA。Bob 在 3 个月内为 1 个 BTC 提供 2 万个 ELA，将 2 万个 ELA 转移到 BeL2 智能合约，并同意支付中继者 1%的 BTC 费用。Alice 发送 1 个 BTC 作为抵押品来借款 2 万 ELA。中继者最终完成交易，要求索取 1%的费用，以支付 BTC 主链费用、ESC gas 和奖励。1 BTC 保存在 2/3 多重签名地址中，需要 Alice、Bob 和中继者的签名。按照 12%的年利率，Alice 对 2 万 ELA 的三个月利息为 600 ELA，共计 20600 ELA 还款。交易周期结束时，Alic 收回 0.99 BTC，扣除 0.01 BTC 中继费。如果没有这笔费用，合约将拒绝转账。手续费的计算基于设定的条款，遵循约定的计算方式。手续费计算公式为：

$$\text{Handling Fee} = \text{TIME} \times \text{RATE} \times \text{AMOUNT}$$

$$\text{手续费} = \text{时间} \times \text{费率} \times \text{金额}$$

The "RATE" is the service quotation set by Relayer itself, but it must be greater than 0 and less than 50%. If during the service period, it is proven that the responsibilities are not properly performed, including service timeout and incorrect transaction submission, the mortgage assets will be deducted and the transaction will be ended. In the future, this information will also be submitted to credit services as a blacklist where they will no longer cooperate.

"RATE"是中继者自己设置的服务报价，但必须大于 0 且小于 50%。如果在服务期内，证明未正确履行责任，包括服务超时和提交的错误交易，质押资产将被扣除，并结束交易。将来，这些信息也将作为黑名单提交给信贷服务机构，届时他们将不再合作。

• **Exit mechanism** When Relayers are idle and not servicing any transactions, they can exit the Relayer role and, if they have not been penalized, retrieve all their staked ELA.

**•退出机制。**当中继者处于空闲状态且不为任何交易提供服务时，他们可以主动退出中继角色，并在未受到惩罚的情况下取回其所有抵押的 ELA。

## 6.1 Interoperability and Financial Services Integration

## 6.1 互操作性与金融服务集成

The assurance of transactional integrity allows for seamless interoperability between the network layers.

交易完整性的保障实现了网络层之间的无缝互操作

• **Zero-knowledge proofs.** A zero-knowledge proof submitted following a first-layer transaction prompts the second layer's smart contract to execute the corresponding action.

**•零知识证明。**在第一层交易后提交的零知识证明促使第二层的智能合约执行相应的动作。

• **Relayer.** Conversely, the Relayer is compelled to perform the relevant first-layer transaction after a second-layer event, under penalty of forfeiture.

**•中继者。**相反，中继节点在第二层事件发生后，面临没收惩罚的威胁，被迫执行相关的第一层交易。

This foundational trust enables the development of marketplace transactions and collateralized lending services on the Bitcoin mainnet. With Relayer services ensuring timely execution, marketresponsive triggers from oracle-provided prices can initiate transfer transactions—be it for fulfilling open buy/sell orders of Bitcoin or for managing collateral liquidation in lending agreements.

这种基础信任使比特币主网上的市场交易和抵押贷款服务得以发展。通过中继者服务确保及时执行，来自预言机提供价格的市场响应触发可以启动转账交易——无论是用于完成比特币的公开买卖订单，还是用于管理贷款协议中的抵押品清算。

## 6.2 Power everything with BTC

## 6.2 用 BTC 驱动万物

The Ethereum Account Abstraction (AA) wallet enables operations to be performed with zero gas. In this system, the wallet holder initiates and signs a request. Subsequently, a third party submits this request for execution on the blockchain, earning rewards in the process. This allows users to perform on-chain operations without needing any tokens beforehand, making it more user-friendly for newcomers to a blockchain, as they don't need to acquire gas in advance.

以太坊账户抽象（AA）钱包允许在零 gas 的情况下执行操作。在该系统中，钱包持有者发起并签署请求。随后，第三方提交此请求以在区块链上执行，并在此过程中获得奖励。这使得用户在不需要任何代币的情况下执行链上操作，使区块链新手更容易使用，因为他们不需要提前获取 gas。

In a 2/3 multi-signature wallet, the first signer provides a signature, and the second signer both signs and broadcasts the transaction. Similarly, a Bitcoin user sets up a transaction contract with an agent, transferring 0.01 Bitcoin for gas fees for 100 ESC transactions. The agent submits these signed transactions to the AA wallet, which executes only with the Bitcoin user's valid signature, ensuring security. Once 100 transactions are complete, the agent can withdraw 0.01 BTC, aided by a relayer.

在 2/3 多重签名钱包中，第一个签署者提供签名，第二个签署者对交易进行签名和广播。同样，比特币用户与代理人签订交易合约，为 100 笔 ESC 交易转账 0.01 比特币作为 gas。代理将已签名的交

易提交给 AA 钱包，只有在比特币用户的有效签名下执行，以确保安全。一旦 100 笔交易完成，代理可以在中继层的帮助下提取 0.01 BTC。

We can integrate the BeL2 mechanism with the AA wallet. BTC users can create a trading contract with EVM chain users and transfer BTC to a co-managed address as compensation. The EVM user then covers the AA wallet's gas fees on behalf of the BTC user and executes the necessary operations. This arrangement enables BTC users to use their BTC as gas for activities on any chain, enhancing the overall experience for BTC users.

我们可以将 BeL2 机制与 AA 钱包集成。BTC 用户可以与 EVM 链用户创建交易合约，并将 BTC 转账到共同管理的地址作为补偿。然后，EVM 用户代表 BTC 用户支付 AA 钱包的 gas，并执行必要的操作。这种安排使得 BTC 用户可以将他们的 BTC 用作任何链上活动的 gas，提升了 BTC 用户的整体体验。

## 6.3 Leveraging Zero-Knowledge Proofs to Broaden Application Domains

## 6.3 利用零知识证明拓展应用领域

The innovative use of smart contracts on the second-layer network, powered by zero-knowledge proof (ZKP) technology, significantly broadens the scope of interoperability across various domains. This versatility transcends traditional second-layer network transactions, facilitating extensions into diverse fields. Here are some examples.

通过零知识证明（ZKP）技术在第二层网络上智能合约的创新使用，显著拓宽了在各个领域之间的互操作性范围。这种通用性超越了传统的第二层网络交易，促进拓展进入多样领域。以下是一些例子。

• **zkEmail Technology.** zkEmail stands as a proof to the power of ZKP technology, validating email signature authenticity, decoding email content, and ultimately generating a zero-knowledge proof for the email, thereby ensuring the integrity and confidentiality of the transactional information.

**•zkEmail 技术。**zkEmail 作为对 ZKP 技术威力的证明，验证电子邮件签名的真实性，解码电子邮件内容，并最终为电子邮件生成零知识证明，从而确保交易信息的完整性和保密性。

• **Bridging BTC and Traditional Banking.** Using the zkEmail solution, Alice can buy Bitcoin from Bob by transferring $1,000; a zero-knowledge proof of the bank transfer email confirms the transaction, allowing the Relayer to execute the Bitcoin transfer on the second-layer network. Using the zkEmail project, this process creates irrefutable proof for bank transfer emails, ensuring transaction legitimacy and enabling flexible Bitcoin transactions on platforms like Elacity, a digital asset marketplace for trading access, distribution and royalty NFT rights.

**•连接 BTC 和传统银行业务。**使用 zkEmail 解决方案，Alice 可以通过转账 1000 美元从 Bob 那里购买比特币；银行转账电子邮件的零知识证明证实了交易，允许中继者在第二层网络上执行比特币转账。通过 zkEmail 技术，这一过程为银行转账电子邮件创建了无可辩驳的证据，确保了交易的合法性，并在 Elacity 等平台上实现了灵活的比特币交易，Elacity 是一个用于交易访问、分发和版税 NFT 权利的数字资产市场。

• **Future Prospects and Collaborations.** Looking ahead, there is potential to enrich the Bitcoin transaction ecosystem further by integrating additional off-chain services and data. Collaborative projects like CreDA

could harness the capabilities of many cloud services, including Alibaba Cloud, Tencent Cloud, and CELO, to support off-chain data into the fabric of Bitcoin transactions.

**•未来展望和合作。**展望未来，通过整合额外的链下服务和数据，有可能进一步丰富比特币交易生态系统。像 CreDA 这样的合作项目可以利用多个云服务的能力，包括阿里云、腾讯云和 CELO，将链下数据支持到比特币交易的结构中。

# 7 Project Roadmap: Strategizing the Path to Innovation

# 7 项目路线图：策略规划通向创新之路

The roadmap of our project delineates the strategic milestones necessary to fulfill our overarching vision. In the following sections, we outline the phases of our development, articulating the objectives and action plans that define each stage of progression.

我们项目的路线图描绘了实现我们总体愿景所需的战略里程碑。在以下各节中，我们概述了我们开发的各个阶段，明确了定义每个发展阶段的目标和行动计划。

**• Phase 1: Prototype Verification**

The initial phase is foundational, focusing on the establishment of circuits critical for verifying Bitcoin transaction proofs. These will be integrated and tested on the Elastos Smart Contract Chain (ESC), thereby enabling seamless interoperability between Bitcoin's foundational layer and Elastos's second layer. During this phase, a centralized team-controlled Relayer will facilitate transactions, serving as the initial step towards our end goal of complete network interoperability.

**•第 1 阶段：原型验证。**

初始阶段既是基础阶段，重点是建立对验证比特币交易证据至关重要的链路。这些将在 Elastos 智能合约链（ESC）上进行集成和测试，从而实现比特币基础层和 Elastos 第二层之间的无缝互操作性。在此阶段，一个由中心化的团队控制的中继节点将促进交易，作为我们实现完全网络互操作性最终目标的第一步。

**• Phase 2: Achieving Decentralization**

Our second phase is pivotal, marking the transition to a fully decentralized transaction ecosystem. We aim to implement a staking-based Relayer network, encompassing mechanisms for Relayer participation, incentivization, and punitive measures to safeguard network integrity and promote equitable contribution.

**•第二阶段：实现去中心化。**

我们的第二阶段至关重要，标志着向完全去中心化的交易生态系统的过渡。我们的目标是实施基于质押的中继网络，包括中继参与机制、激励机制和惩罚措施，以保护网络完整性并促进公平贡献。

**• Phase 3: Ecosystem Development** The third phase is about creating a simple ecosystem for exchanging Bitcoin (BTC), second-layer, and certain off-chain assets. It will enable using BTC as collateral for USDC loans on this network. The focus is also on making it easier for developers to build new applications using BeL2, aiming to boost innovation and the practical use of blockchain.

**• 第三阶段：生态系统发展。**

第三阶段是要创建一个简单的生态系统来交易比特币（BTC）、第二层及链外资产。这将使 BTC 被用作数字资产（例如 USDC）在该网络上的贷款的抵押物。重点还在于让开发人员更容易使用 BeL2 构建新的应用程序，旨在推动区块链的创新和实际应用。

# 8 Exploring Staking Returns Across Platforms

# 8 探索跨平台的质押收益

Participants staking Ethereum (ETH) to become validators can expect income derived from two principal sources: new ETH block rewards and transaction fees. The annual yield from these sources is dynamic, influenced by the total volume staked and network activity levels. Generally, as more ETH is staked, the individual rate of return diminishes. Market value fluctuations further impact this rate, which presently hovers around 5%.

在不同平台质押以太坊（ETH）成为验证者的参与者可以期待来自两个主要来源的收入：新的 ETH 区块奖励和交易费用。这些来源的年度收益是动态的，受总质押量和网络活动水平的影响。一般而言，随着更多的 ETH 被质押，个人回报率将减少。市值的波动进一步影响了这一比率，目前这一比率徘徊在 5%左右。

## 8.1 Returns from Ethereum Layer 2 Projects

## 8.1 以太坊第二层项目的收益

Layer 2 protocols on Ethereum are engineered to bolster the network's scalability by enabling quicker transaction processing at reduced costs. Revenue for participants in these solutions primarily stems from transaction fees, supplemented occasionally by additional incentives specific to certain projects. Currently, transaction fees on Layer 2 are not redistributed to nodes or the main network.

以太坊 Layer 2 协议旨在通过实现更快的交易处理和降低成本来增强网络的可扩展性。这些解决方案参与者的收入主要来自交易费，有时还会获得特定项目的额外激励。目前，Layer 2 上的交易费用并未重新分配给节点或主网络。

• **Arbitrum.** In 2022, Arbitrum amassed $22 million in sequencer revenue and $6 million in profits. Optimism, in contrast, garnered $18 million in sequencer revenue with profits of $4 million. The first quarter of 2023 saw Arbitrum outperform Optimism by $4 million in revenue and $3 million in profits. In March 2023 alone, Arbitrum sequencers realized profits exceeding $2.5 million. As of April 13, 2023, Arbitrum's Total Value Locked (TVL) stood at an impressive $2.27 billion.

**•Arbitrum**。2022 年，Arbitrum 的排序器收入达到了 2200 万美元，利润为 600 万美元。相比之下，Optimism 的排序器收入为 1800 万美元，利润为 400 万美元。2023 年第一季度，Arbitrum 的收入和利润超过 Optimism ，分别为 400 万美元和 300 万美元。仅在 2023 年 3 月，Arbitrum 排序器就实现了超过 250 万美元的利润。截至 2023 年 4 月 13 日，Arbitrum 的锁定总价值（TVL）达到惊人的 22.7 亿美元。

• **Polygon.** The third quarter of 2023 for Polygon saw a TVL of around $900 million, with an average of 364K daily active addresses and about 2.3 million daily on-chain transactions. The total on-chain profit for this quarter reached $5.1 million.

•**Polygon**。2023 年第三季度，Polygon 的 TVL 约为 9 亿美元，平均每日活跃地址为 36.4 万，每日链上约 230 万笔交易。本季度的链上利润总额达到 510 万美元。

• **Optimism.** Optimism operates as a Layer 2 scaling solution for Ethereum, employing Rollup technology to enhance transaction capacity and reduce costs. Its TVL for the third quarter of 2023 was $750 million, with 96K daily active addresses, around 478.3K daily on-chain transactions, and a total on-chain profit for the quarter of $2.8 million. The cumulative on-chain profit on the Optimism mainnet currently stands at $15 million, equivalent to 8,600 ETH.

•**Optimism**。Optimism 是以太坊的第二层扩展解决方案，采用 Rollup 技术来增强交易能力并降低成本。2023 年第三季度，其 TVL 为 7.5 亿美元，每日活跃地址为 9.6 万个，每日链上约 47.83 万笔交易，本季度链上利润总额为 280 万美元。Optimism 主网的累计链上利润目前为 1500 万美元，相当于 8600 ETH。

# 9 Conclusion

# 9 总结

BeL2 adds a layer that integrates Bitcoin and Elastos SmartWeb technologies, targeting Bitcoin's limitations in speed, smart contracts, and privacy. This initiative fuses Bitcoin's security with advanced methodologies, like zero-knowledge proofs for private, secure transaction validation, and incorporates the Ethereum Virtual Machine. It enhances Bitcoin's smart contract capabilities and extends its utility in decentralized finance and NFT markets. The approach includes multi-signature processes and a Relayer deposit staking mechanism for network security. BeL2's strategy is to enhance Bitcoin's capabilities with smart contracts powered by BTC without altering its core principles, innovatively using existing infrastructures to address specific challenges.

BeL2 引入了一个集成比特币和 Elastos SmartWeb 技术层，旨在解决比特币在速度、智能合约和隐私方面的限制。这一举措将比特币的安全性与先进方法相融合，例如使用零知识证明进行私密、安全的交易验证，并引入了以太坊虚拟机（EVM）。它不仅增强了比特币的智能合约能力，还扩展了其在去中心化金融和 NFT 市场中的实用性。该方法包括多重签名过程和用于网络安全的中继存款博弈机制。BeL2 的战略是在不改变其核心原则的情况下，通过由 BTC 作为 gas 驱动的智能合约来增强比特币的能力，巧妙地利用现有的基础设施来应对特定挑战。

In summary, BeL2 marks a significant advancement in Bitcoin's evolution, upholding its foundational principles while boosting functionality. The integration of advanced technologies aims to leverage Bitcoin's vast market capital, enabling more efficient and diverse financial applications. This unlocks the considerable value currently dormant in Bitcoin holdings.

总之，BeL2 标志着比特币演进的重要进展，保持其基础原则的同时提升功能。先进技术的集成旨在充分利用比特币庞大的市场资本，实现更高效、和多样性的智能金融应用，释放目前在比特币持有中潜在的巨大价值。

# 10 Executive Team

# 10 执行团队

**Sasha Mitchell**
Head of Operations
运营负责人

**Anders Alm**
Head of Technical
技术负责人

**Mark E. Blair**
Head of Strategy
战略负责人

**Jonathan Hargreaves**
Head of Growth
市场负责人

• **Elacity**. Founded by CEO Sasha Mitchell, Elacity will lead BeL2 operations. Elacity's team has developed the Access Economy Protocol (AEP), a platform enhancing digital rights management. Under the technical leadership of CTO Anders Alm, Elacity offers a marketplace for digital assets, ensuring strong IP protection and enabling creators to earn directly and immediately from their work. Collaborating with Mark E. Blair, a Cyber Republic Member and a longstanding supporter of Bitcoin and Elastos, Elacity will lead the oversight, development, and engagement of the BeL2 project. This includes managing execution, community feedback, and providing leadership, while maintaining core communication with the project sponsors at the Elastos Foundation.

•**Elacity**。Elacity 由首席执行官 Sasha Mitchell 创立，他将领导 BeL2 的运营。Elacity 的团队开发了 Access Economy Protocol（AEP），这是一个增强数字版权管理的平台。在首席技术官 Anders Alm 的技术领导下，Elacity 提供了一个数字资产市场，确保了强大的知识产权保护，并使创作者能够直接从他们的工作中获利。Elacity 将与 CR 成员、比特币和 Elastos 的长期支持者 Mark E.Blair 合作，领导 BeL2 项目的监督、开发和参与，包括执行管理、社区反馈，并与 Elastos 基金会的项目赞助商保持核心沟通。

• **Elavation**. Led by Jon Hargreaves's, Elavation is a growth team focused on executing Business Development, Marketing, and Ecosystem Alignment tasks for Elastos' BeL2 project. Their goal is to position Elastos as a Web3 leader through the SmartWeb's Bitcoin Layer 2 innovation. They aim to foster partnerships, enhance marketing efforts, and streamline Elastos' ecosystem, focusing on rapid deployment and global branding to maximize Elastos' impact in the blockchain and Web3 space. Elavation is set to drive innovation and growth within Elastos in 2024.

• **Elavation**。由 Jon Hargreaves 领导，Elavation 是一个专注于执行业务发展、营销和生态系统协调的增长团队，为 Elastos 的 BeL2 项目提供支持。他们的目标是通过 SmartWeb 的比特币第二层创新，将 Elastos 定位为 Web3 的领导者。他们旨在促进合作伙伴关系，加强营销工作，并简化 Elastos 的生态系统，注重快速部署和全球品牌推广，以最大程度地发挥 Elastos 在区块链和 Web3 领域的影响力。Elvation 计划在 2024 年推动 Elastos 的创新和增长。

• **Elastos Foundation**. The Elastos Foundation is dedicated to developing the Elastos SmartWeb, a blockchain-driven Internet, fostering a secure, decentralized online ecosystem where users control their data and digital rights. Instrumental in the initial development of BeL2, the foundation will sponsor BeL2 and offer crucial support and guidance, encouraging a safer, user-focused Internet evolution.

•**Elastos 基金会**。Elastos 基金会致力于发展 Elastos SmartWeb，这是一个区块链驱动的互联网，促进一个安全、去中心化的在线生态系统，使用户能够掌控其数据和数字权利。该基金会在 BeL2 的初期开发中发挥了关键作用，将赞助 BeL2 并提供关键的支持和指导，鼓励一个更安全、以用户为中心的互联网发展。

Finally, we would like to thank members Luca S, Rivers Kong, Greg, and many other Elastos community members and ecosystem teams for their help in writing this BeL2 White Paper.

最后，我们要感谢 Luca S、Rivers Kong、Greg 以及其他 Elastos 社区成员和生态系统团队，在撰写本 BeL2 白皮书时为我们提供的帮助。