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.

1 Introduction

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 and usher in the next financial paradigm.

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.

2 Pioneering the Be Layer2 from Bitcoin's Foundations

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:

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

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.

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.

3 Challenges with Bitcoin Layer 1

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.
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.
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.

4 Exploring Layer 2 Innovations

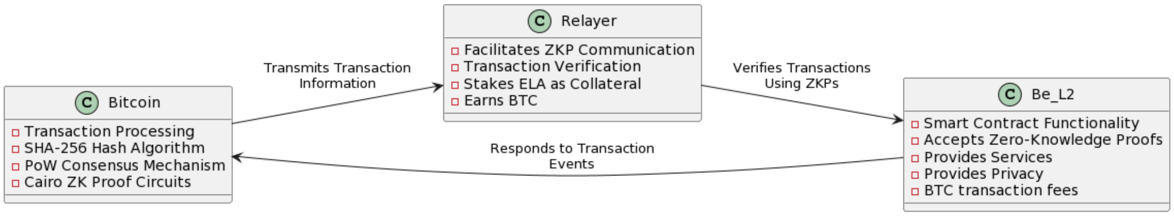
- **The Lightning Network.** The Lightning Network, as a second-layer solution, enhances Bitcoin's scalability by enabling quick, low-cost transactions without recording each one on the main blockchain. The Lightning Network operates on payment channels where users create a multi-signature wallet on 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.
- **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.
- **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.

- **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 Bitcoin-style security, fostering a secure and efficient digital transaction environment. Its challenge is in needing wide adoption by exchanges and institutions to be fully effective.
- **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.
- **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.
- **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.

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.

5 An Overview of BeL2 Technology

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.

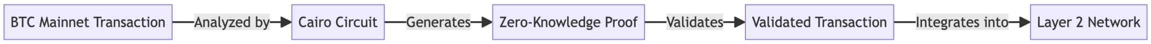


5.1 Integration of BTC Mainnet Transactions within Layer 2 Networks

Cario, 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. Cario, 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 Cario, which facilitates the generation of multifaceted proofs to:

1. Confirm the proper formatting of the transaction.
2. Validate the authenticity of the transaction's signature.
3. Confirm transaction inputs are greater than outputs, maintaining financial balance.
4. Verify that the referenced Unspent Transaction Outputs (UTXOs) originate from reliable sources.
5. Ascertain the functionality of the unlocking script within the transaction.

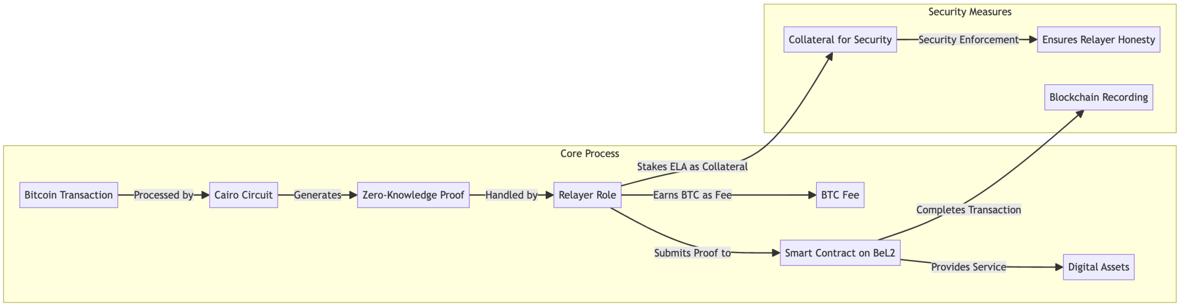
A BTC transaction proof comprises raw data and a zero-knowledge proof, verifying mainnet transactions. These transactions are validated and propagated based on the BTC network consensus. Each transaction on the BTC network can generate a zero-knowledge proof and retrieve its raw data. A complete transaction 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.



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

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 like BTC, ELA or USDC, thereby integrating a layer 2 SmartWeb solution.

In BeL2, users deposit digital assets like BTC, ELA or USDC into a smart contract to trade for Layer 1 Bitcoin. This framework also applies for lending or rights services. To minimize risks such as delays or non-transfers, especially in complex transactions, a Relayer is introduced. This Relayer, not a custodian but an executor, speeds up the transaction process. They are incentivized to ensure efficient and prompt transaction completions, addressing potential delays or inactivity from regular users.



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.

5.3 Enhanced Security through Transaction Management Gamification

- **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.

- **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.

- **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.

- **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.

- **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.

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

  1. If the Relayer initiates and proves a Bitcoin transfer, Bob receives the Bitcoin, completing the transaction with Alice's assets secured.
  2. Should the Relayer fail to broadcast the transaction, Bob can independently broadcast it, securing Alice's Bitcoin without any asset loss.
  3. If the Relayer acts improperly or not at all, Bob can provide proof and claim the Relayer's deposit, protecting her assets.

  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.

6 Incentivizing Blockchain Security through ELA Staking

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.

- **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.

- **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 multi-signature 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.

  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:

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

- **Rewards and penalties.** By being a relayer for transactions, you can get transaction fees (BTC). BTC rewards are derived from transaction fees. For instance using a BeL2 lending service as an example, 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:

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

  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.

- **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.

6.1 Interoperability and Financial Services Integration

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

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

This foundational trust enables the development of marketplace transactions and collateralized lending services on the Bitcoin mainnet. With Relayer services ensuring timely execution, market-responsive 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.

6.2 Power everything with BTC

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.

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.

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.

6.3 Leveraging Zero-Knowledge Proofs to Broaden Application Domains

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.

- **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.
- **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.
- **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 Elastos SmartWeb cloud and ecosystem partners, to support off-chain data into the fabric of Bitcoin transactions.

7 Project Roadmap: Strategizing the Path to Innovation

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.

- **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.

- **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.

- **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 digital asset (eg.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.

8 Exploring Staking Returns Across Platforms

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%.

8.1 Returns from Ethereum Layer 2 Projects

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.

- **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.

- **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.

- **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.

9 Conclusion

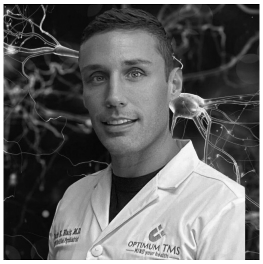
BeL2 adds a layer that integrates Bitcoin and Elastos SmartWeb technologies, targeting Bitcoin's limitations in speed, smart contracts, and privacy. This initiative fuses Bitcoin's security with advanced methodologies, like zero-knowledge proofs for private, secure transaction validation, and incorporates 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.

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 smart financial applications. This unlocks the considerable value currently dormant in Bitcoin holdings.

10 Executive Team

Sasha Mitchell
Head of Operations

Anders Alm
Head of Technical



Mark E. Blair
Head of Strategy

Jonathan Hargreaves
Head of Growth

- **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 SmartWeb 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.
- **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.
- **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.

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