Native Bitcoin DeFi: Envisioning a New Bretton Woods System

New Bretton Woods Team

November 6, 2024

contact@nbwlabs.org
www.nbwlabs.org
Cambridge, MA

Table of Contents

Disclaimer

This whitepaper is provided solely for informational and research purposes, and we welcome constructive feedback to help us improve and update its content. Please note that this document is not a final, published version; the NBW team reserves the right to adjust the content of this document based on received input. This whitepaper does not constitute an offer to sell or a solicitation to buy any tokens, securities, or other financial instruments.

This document should not be interpreted as legal, financial, or investment advice and should not be used as a basis for making any legal, financial, or investment decisions.

免责声明

本白皮书仅供信息和研究参考之用，欢迎提出建设性反馈，帮助我们改进和更新内容。请注意，本文件并非最终发布版本；NBW团队保留根据收到的反馈调整本文件内容的权利。本白皮书不构成出售或购买任何代币、证券或其他金融工具的要约或邀请。本文件不应被解释为提供法律、财务或投资建议，也不应作为任何法律、财务或投资决策的依据。

Team

The New Bretton Woods (NBW) team is composed of Harvard students and alumni with diverse academic and industry backgrounds. In September 2024, the team secured a student membership at Harvard Innovation Labs (i-Labs) to advance their stablecoin project throughout the fall semester. This membership provides NBW access to i-Labs facilities and resources tailored to their project's stage of development. NBW operates independently of both Harvard University and Harvard Innovation Labs.

团队简介

新布雷顿森林（NBW）团队由拥有多样学术和行业背景的哈佛大学学生和校友组成。2024年9月，项目团队获得了哈佛大学创新实验室（i-Labs）的学生会员资格，以推进其稳定币项目在秋季学期的发展。此会员资格使NBW团队能够使用i-Labs的设施和资源，这些资源专为项目的发展阶段量身定制。NBW的运营独立于哈佛大学和哈佛创新实验室。

I. Introduction

In an era of unprecedented global financial challenges, the world faces a debt crisis of significant proportions, reminiscent of the economic turmoil that led to the establishment of the Bretton Woods system in 1944. Today's crisis, characterized by unsustainable national debts, expansionary monetary policies, and the erosion of traditional financial systems, poses a threat to individual wealth and economic stability worldwide. The global nature of this crisis, coupled with the interconnectedness of modern economies, calls for a new financial paradigm. Native Bitcoin DeFi, built on the BeL2 (Bitcoin-Elastos Layer 2) ecosystem, emerges as a potential solution, offering a "New Bretton Woods System" for the digital age.

1.1 The Global Debt Crisis and Historical Parallels

The current global financial landscape is fraught with challenges that echo historical patterns of economic decline:

1. Excessive Debt Accumulation: Nations worldwide have amassed debt at an alarming rate, with the United States alone carrying over approximately $36 trillion in national debt[1], and unfunded liabilities pushing the total to over $175 trillion.[2]

2. Monetary Expansion: Central banks, particularly the Federal Reserve, have engaged in quantitative easing and other accommodative monetary policies, significantly increasing the money supply in response to economic crises such as the COVID-19 pandemic. While these actions have supported economic activity, they also raise concerns about long-term inflationary pressures.

3. Currency Devaluation: The excessive printing of money has led to a significant erosion of purchasing power in many currencies, with the US dollar losing more than 25% of its value in recent years.

4. Shifting Global Dynamics: Economic power dynamics are evolving, with emerging markets gaining greater influence. Countries like China have taken steps to diversify their reserves, including adjusting their holdings of U.S. Treasury securities and exploring alternative reserve assets.

5. Market Distortions: The actions of central banks and governments have created artificial market conditions, leading to potential asset bubbles and increased economic fragility.
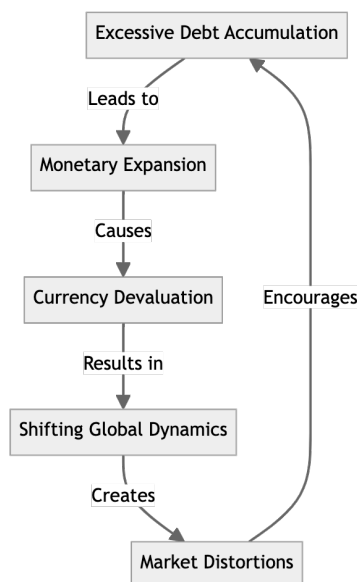
These challenges bear striking similarities to the economic conditions that led to the creation of the Bretton Woods system in 1944. At that time, the world was emerging from the devastation of World War

---

[1] U.S. Department of the Treasury, "America's finance guide: National debt," *U.S. Treasury Fiscal Data*, accessed November 13, 2024, link: https://fiscaldata.treasury.gov/americas-finance-guide/national-debt/

[2] U.S. Department of the Treasury, "Financial report of the United States government for fiscal year 2023 (Final)," *U.S. Government Publishing Office*, February 15, 2024, accessed September 2, 2024, link: https://fiscal.treasury.gov/files/reports-statements/financial-report/2023/02-15-2024-FR-(Final).pdf

II, and there was a pressing need for a new international monetary order to promote economic stability and growth.

1.2 The BeL2 Ecosystem: A Modern Parallel to Bretton Woods

The Bretton Woods system, established in 1944, was designed to create a stable international monetary system in the post-war era.[3] Its key features included:

1. Fixed exchange rates: Currencies were pegged to the US dollar, which was in turn pegged to gold.

2. The US dollar as the world's reserve currency: This gave the United States a central role in the global financial system.

3. The creation of international financial institutions: The International Monetary Fund (IMF) and the World Bank were established to promote global economic stability and development.

While the Bretton Woods System provided stability for nearly three decades, it ultimately collapsed in 1971 when the United States unilaterally terminated convertibility of the US dollar to gold.[4] This led to the current era of fiat currencies and floating exchange rates, which has been marked by increased financial instability and growing global debt.

The Native Bitcoin DeFi and NBW system emerges as a potential "New Bretton Woods System" for the digital age, drawing inspiration from the original while addressing its limitations:
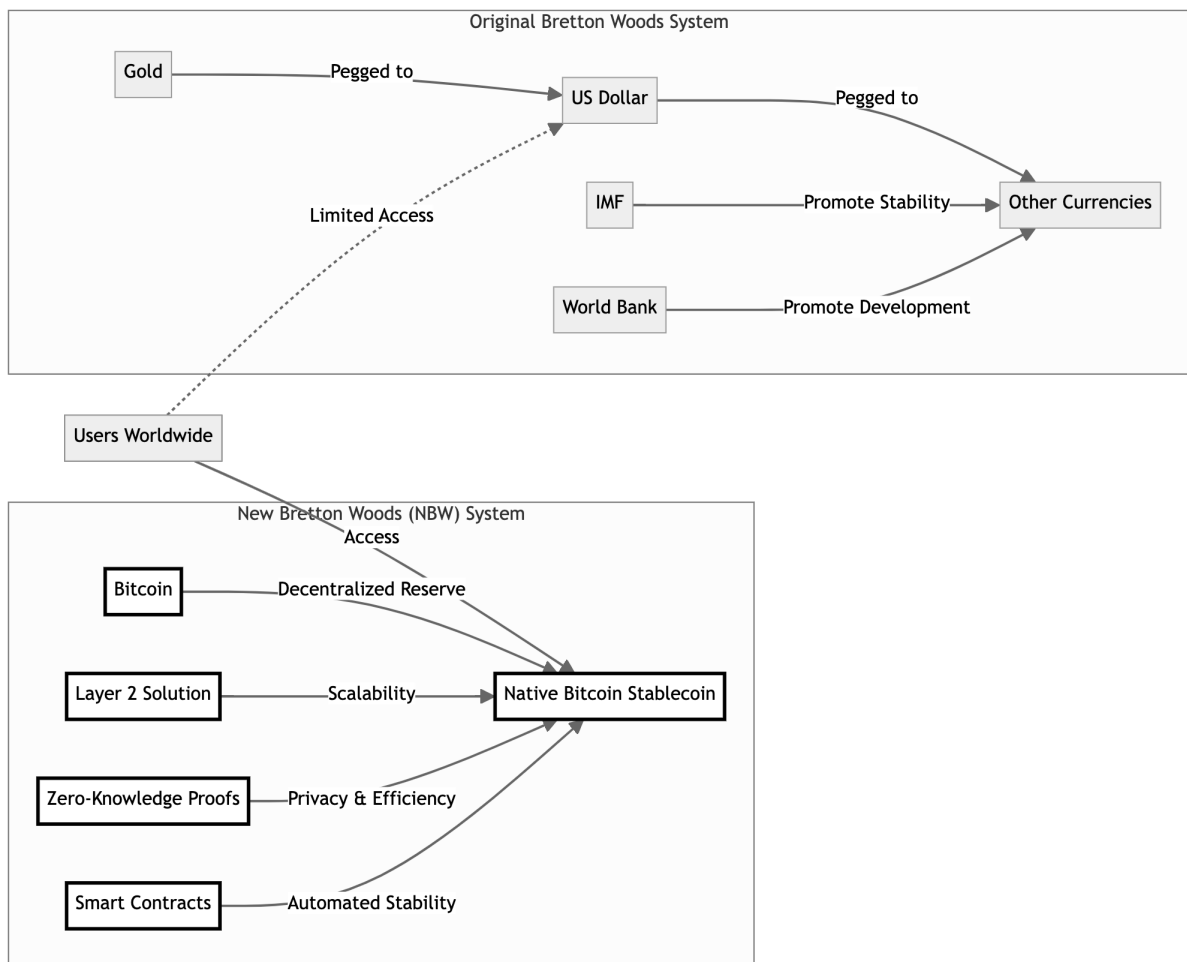
1. Decentralized Reserve Asset: Bitcoin serves as the underlying asset, providing a digital store of value with a fixed supply, replacing the role of gold in the original system.

---

[3]Robert L. Hetzel, "Launch of the Bretton Woods System," *Federal Reserve History*, November 22, 2013, accessed Sep 1, 2024, link: https://www.federalreservehistory.org/essays/bretton-woods-launched

[4]Ibid.

2. Stable Value Anchor: Native Bitcoin Stablecoin offers a stable medium of exchange without relying on a single nation's currency, addressing the "Triffin Dilemma" that plagued the original Bretton Woods system.

3. Global Accessibility: Unlike the original system, which was primarily accessible to nations, the NBW system is open to individuals and organizations worldwide.

4. Automated Stability Mechanisms: Smart contracts and zero-knowledge proofs replace the need for central bank interventions, providing more transparent and predictable monetary policy.

5. Flexibility and Innovation: The Layer 2 solution allows for continuous improvement and adaptation to changing economic conditions.

1.3 Native Bitcoin DeFi: Empowering Individual Financial Sovereignty
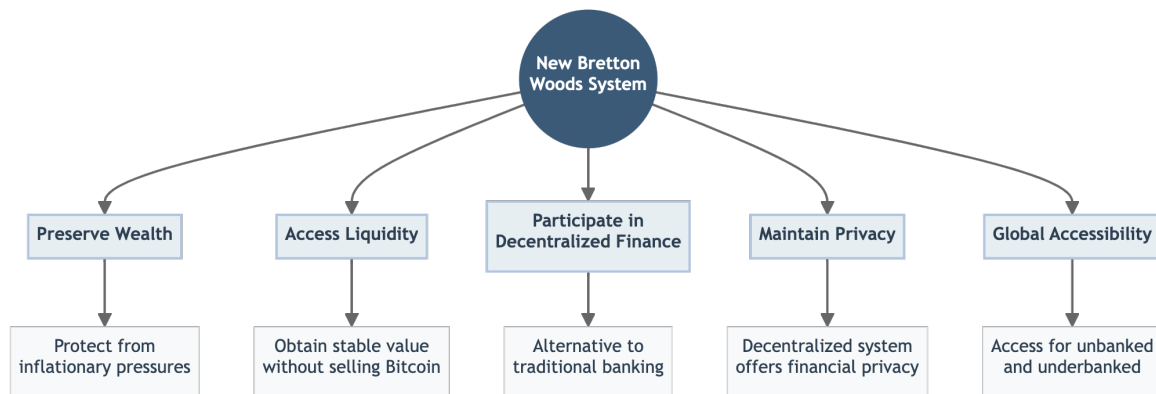
The Native Bitcoin DeFi and New Bretton Woods (NBW) system is designed as a comprehensive and decentralized platform to support a diverse ecosystem of financial products and services, rather than a single stablecoin product. The NBW system is an innovative zero-knowledge proof and clearing layer built on the Bitcoin blockchain, designed to create a stable cryptocurrency (Native Bitcoin Stablecoin) while leveraging Bitcoin's security and scarcity.

Key features of the NBW system include:

1. Cross-Chain Functionality: BeL2 enables interaction between Bitcoin and EVM-compatible chains.

2. Zero-Knowledge Proofs: Allow for the verification of Bitcoin transactions on other chains without compromising security or privacy.

3. Arbitrator Network: A decentralized network that facilitates cross-chain operations and dispute resolution.

By allowing users to generate a stablecoin using Bitcoin as collateral, Native Bitcoin DeFi provides a powerful tool for individuals to:

1. Preserve Wealth: Use Bitcoin as a reserve asset to protect against inflationary pressures.

2. Access Liquidity: Generate stablecoins using Bitcoin as collateral without selling the underlying asset.

3. Participate in Decentralized Finance: Access a range of DeFi services built on the NBW system.

4. Maintain Financial Privacy: Leverage zero-knowledge proofs for enhanced transaction privacy.

5. Global Accessibility: Access DeFi services regardless of geographic location or traditional banking status.

1.4 A Platform for Innovation

The NBW system is designed as a platform to support a diverse ecosystem of DeFi products and services:

1. DeFi Products: The system allows for the creation of various DeFi products, each with its own specific features and use cases.

2. Decentralized Governance: The arbitrator network enables community-driven decision-making and protocol upgrades.

3. Flexible Fee Structures: The system supports customizable fee structures for different products and services.

4. Interoperability: By bridging Bitcoin with EVM-compatible chains, the system enables interaction with existing DeFi ecosystems.

As we explore the technical foundations, economic model, and potential impacts of the Native Bitcoin DeFi and NBW system in the following sections, we will demonstrate how this platform can serve as a "New Bretton Woods" for the digital age. By providing stability, accessibility, and innovation, it offers a decentralized solution to navigate the challenges posed by global financial instability, contributing to a more resilient and equitable financial ecosystem.

II. Technical Approach

The New Bretton Woods (NBW) system is built on a sophisticated technical foundation that combines innovative blockchain technologies to create a secure, efficient, and flexible platform for decentralized finance. This section details the key components and their interactions within the system.
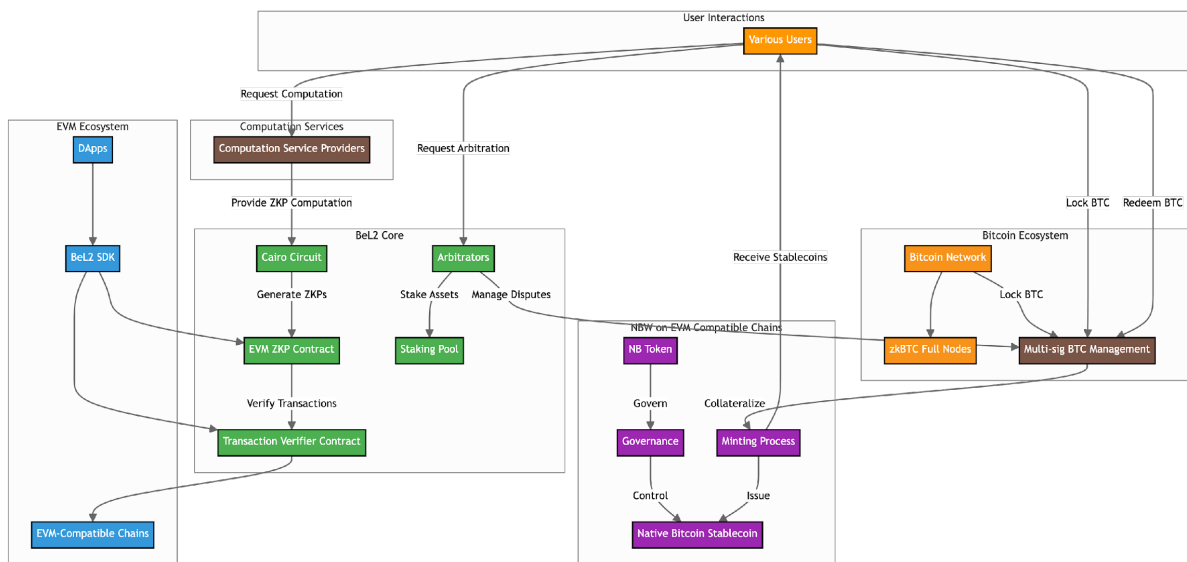
2.1 BeL2 (Bitcoin-Elastos Layer 2)

BeL2 serves as the foundational layer of the NBW system, enabling interaction between Bitcoin and other blockchain networks, particularly EVM-compatible chains.

2.1.1 Core Components

1. zkBTC Full Nodes: Specialized nodes that monitor the Bitcoin network and generate zero-knowledge proofs (ZKPs) of Bitcoin transactions. These nodes can run on ordinary hardware, including mobile devices, enhancing the network's decentralization.

2. Cairo Circuit: A computational circuit built using the Cairo programming language, designed for efficient generation and verification of ZKPs of Bitcoin transactions. The Cairo Circuit is essential for creating proofs that can be verified on other chains, ensuring privacy-preserving and scalable transaction verification.

3. Arbitrator Network: A decentralized network of Arbitrator Nodes responsible for relaying data and proofs between the Bitcoin network and EVM-compatible chains. Arbitrator Nodes manage cross-chain interactions, facilitate dispute resolution, and play a crucial role in maintaining the

integrity and decentralization of the system. They earn fees for their services and stake $ELA as collateral to ensure honest behavior.[5]

4. EVM ZKP Contract: A smart contract deployed on EVM-compatible chains that interacts with the zero-knowledge proofs generated by zkBTC Full Nodes. The EVM ZKP Contract verifies these proofs, enabling the integration of Bitcoin's value and security into the EVM ecosystem.

5. Transaction Verifier Contract: A smart contract on EVM-compatible chains that receives and processes requests to verify Bitcoin transactions, maintaining a list of verified transactions. This contract allows other smart contracts to interact with verified Bitcoin transactions without needing to understand the complexities of the Bitcoin network.

While the zkBTC Full Nodes and Cairo Circuit form the decentralized computational backbone, the Arbitrator Network, comprised of Arbitrator Nodes, is responsible for coordinating cross-chain transactions and dispute resolution. Anyone may stake to become Arbitrator Nodes as the system matures and proves its stability.

The BeL2 infrastructure operates independently from the NBW system but allows for interaction. The Arbitrator Network within the NBW system interacts with the BeL2 infrastructure to access verified Bitcoin transaction data and proofs, enabling the management of the Native Bitcoin Stablecoin.

2.1.2 Zero-Knowledge Proofs

BeL2 utilizes advanced zero-knowledge proofs to verify Bitcoin transactions on other chains without compromising security or privacy. This allows for:

- Efficient verification of Bitcoin transactions on EVM-compatible chains without requiring full Bitcoin node capabilities.

- Enhanced privacy by proving the validity of transactions without revealing transaction details.

- Scalability improvements by reducing the amount of data that needs to be processed on-chain.

2.1.3 Cross-Chain Interoperability

BeL2 enables interoperability between Bitcoin and EVM-compatible chains:

- Bitcoin transactions can be verified and utilized in smart contracts on EVM-compatible chains.

- Allows for the creation of Bitcoin-backed assets on other chains without moving BTC off the main Bitcoin network.

- Supports cross-chain asset swaps and other complex DeFi operations.

2.2 Native Bitcoin Stablecoin

Native Bitcoin Stablecoin is a core component of the NBW system, allowing users to create stable assets backed by Bitcoin without moving BTC off the main network.

2.2.1 Collateralization Process

1. Users lock their BTC on the Bitcoin main network using a special script.

2. zkBTC Full Nodes generate a zero-knowledge proof of this transaction.

3. The proof is relayed to EVM-compatible chains through the Arbitrator Network.

4. The EVM ZKP Contract verifies the proof.

5. Once verified, users can mint Native Bitcoin Stablecoin on the EVM-compatible chain.

---

[5]Elastos (ELA) has been chosen as the staking token for the NBW platform for three primary reasons. First, because it is merged mined with Bitcoin, Elastos inherits Bitcoin's robust security, providing a solid foundation for NBW's blockchain network. Second, the NBW platform is built on Bel2 infrastructure, which initially launches on the Elastos Smart Chain; therefore, ELA is a natural choice for staking. Finally, adopting ELA as the staking token demonstrates NBW's commitment to supporting the Elastos community, acknowledging their contribution of resources that enabled the advancement of NBW's technology.

2.2.2 Stability Mechanisms

- Overcollateralization: Native Bitcoin Stablecoins are backed by more Bitcoin than their face value to account for price volatility.

- Dynamic Collateral Ratios: The system adjusts collateral requirements based on market conditions and risk parameters.

- Liquidation Process: If the collateral value falls below a certain threshold, the system initiates a liquidation process to maintain overall stability.

2.2.3 Redemption Process

Users can redeem their Native Bitcoin Stablecoins for the underlying BTC:

1. User initiates a redemption request.

2. The system burns the equivalent amount of Stablecoins.

3. A zero-knowledge proof of this burning is generated and verified.

4. The corresponding amount of BTC is unlocked on the main Bitcoin network.

2.2.4 Price Stability

The system includes mechanisms to maintain the Stablecoin's peg:

- Arbitrage opportunities encourage users to mint or redeem Stablecoins to keep the price close to $1.

- The system may include stability fees or other incentives to manage supply and demand.

2.2.5 Friction Mechanisms

The system implements different levels of friction (fees) for redemption:

- Low or no friction for original Bitcoin depositors redeeming their own Bitcoin.

- Higher friction for third-party stablecoin holders to discourage speculative behavior and protect system stability.

2.3 Arbitrator Network

The Arbitrator Network is a crucial component that facilitates cross-chain operations and ensures the security and stability of the system.

2.3.1 Arbitrator Nodes

- Decentralized nodes responsible for relaying data and proofs between different blockchain networks.

- Manage redemptions and dispute resolution.

- Stake BTC or ELA (Elastos tokens) as collateral to ensure honest behavior.

- Validators who stake BTC or ELA receive proportional rewards from the network's fee generation.

2.3.2 Consensus Mechanism

- The network uses a consensus algorithm to agree on the state of cross-chain operations.

- Ensures agreement on which Bitcoin transactions have been verified on EVM chains.

2.3.3 Dispute Resolution

- In case of discrepancies or conflicts, the Arbitrator Network provides a mechanism for resolving disputes.

- Helps maintain the integrity of cross-chain operations.

2.4 BeL2 SDK

The BeL2 SDK provides developers with tools to build applications leveraging the NBW system's architecture.

2.4.1 Key Features

- APIs for interacting with BeL2-specific smart contracts.
- Libraries for verifying zero-knowledge proofs of Bitcoin transactions.
- Tools for constructing and signing Bitcoin transactions for use in the NBW system.
- Event listeners for monitoring both Bitcoin and EVM-compatible chain events.

2.4.2 Developer Experience

- Abstracts complex cross-chain interactions, allowing developers to focus on application logic.
- Supports multiple programming languages for broader accessibility.
- Includes comprehensive documentation and example applications.

2.5 Security Considerations

2.5.1 Multi-layered Security Approach

- Leverages Bitcoin's robust Proof-of-Work consensus.
- Uses zero-knowledge proofs for enhanced privacy and efficiency.
- Implements the Arbitrator Network for additional oversight and dispute resolution.

2.5.2 Smart Contract Security

- All smart contracts undergo rigorous auditing to minimize vulnerabilities.
- Implements upgradeable contract patterns for future improvements without compromising security.

2.5.3 Economic Security

- The overcollateralization of Native Bitcoin Stablecoin provides a buffer against market volatility.
- The staking requirements for Arbitrator Nodes create economic incentives for honest behavior.

2.6 Scalability and Future Developments

2.6.1 Layer 2 Scaling Solutions

- The system is designed to be compatible with future Layer 2 scaling solutions on both Bitcoin and EVM-compatible chains.
- Potential integration with other technologies and platforms.

2.6.2 Cross-Chain Expansion

- While initially focused on Bitcoin and EVM-compatible chains, the system is designed to potentially incorporate other blockchain networks in the future.

2.6.3 Continuous Improvement

- The governance mechanism allows for ongoing upgrades and improvements to the protocol.
- Research into advanced cryptographic techniques, such as recursive zero-knowledge proofs, for further efficiency gains.

This technical approach creates a robust foundation for the New Bretton Woods system, enabling a wide range of decentralized finance applications while maintaining the security and decentralization principles of Bitcoin. By bridging Bitcoin with the programmability of smart contract platforms, it opens up new possibilities for creating a more stable, accessible, and innovative global financial system.

III. Price Stability Mechanisms

The stability of Native Bitcoin Stablecoin is crucial to the success of the New Bretton Woods (NBW) system. Given the global prominence of US dollar and the need to enhance liquidity for users, we allow the NBW stablecoin to be pegged 1:1 to the U.S. dollar. The NBW platform maintains its peg by leveraging overcollateralization, dynamic parameters, and arbitrage incentives. This section outlines the key mechanisms used to ensure price stability across various stablecoin products that can be created on the platform.

3.1 Overcollateralization

The foundation of Native Bitcoin Stablecoin's stability is the overcollateralization model.

3.1.1 Collateral Ratio

- The system requires users to deposit more Bitcoin value than the stablecoins they mint.
- Typical collateral ratios range from 120% to 200%, depending on market conditions.

3.1.2 Dynamic Collateral Requirements

- Collateral requirements adjust based on market volatility and overall system risk.
- During periods of high volatility, the required collateral ratio increases automatically.

3.1.3 Liquidation Thresholds

- If the value of the collateral drops below a certain threshold (e.g., 120% of the minted stablecoins), the position becomes eligible for liquidation.
- This ensures the system always maintains sufficient collateral to back all issued stablecoins.

3.2 Redemption Mechanism

Proper management of redemption and liquidation processes is essential for maintaining the stability of the stablecoin and protecting the interests of both Bitcoin depositors and stablecoin holders.

3.2.1 Redemption Mechanism

- Voluntary Redemption: Users can redeem their stablecoins for the underlying Bitcoin collateral at any time, subject to the system's rules.
- Tiered Redemption Friction:
  - Low or No Friction: Original Bitcoin depositors can redeem their own Bitcoin with minimal fees or penalties.
  - Higher Friction for Third Parties: Third-party stablecoin holders may face higher fees or restrictions when redeeming for Bitcoin to discourage speculative behavior and protect system stability.

3.2.2 Liquidation Process

- Triggered Liquidation: If a user's collateral-to-debt ratio falls below the required liquidation threshold due to a drop in Bitcoin's price or an increase in the user's debt, their position becomes eligible for liquidation.
- Liquidation Priority:

- The system prioritizes liquidating the most undercollateralized positions first to minimize systemic risk.

- Liquidation Mechanism:
  - The system implements a gradual redemption process, starting with higher-leveraged positions first.
  - This approach aims to minimize market impact and protect users' positions.

3.3 Arbitrage Incentives

Arbitrage plays a key role in maintaining the stablecoin's peg by incentivizing market participants to correct price deviations.

3.3.1 Minting Arbitrage

- When the stablecoin price rises above $1, users are incentivized to mint new stablecoins (by depositing Bitcoin as collateral) and sell them on the market for a profit.

- This increases the supply of stablecoins in the market, pushing the price back toward the peg.

3.3.2 Redemption Arbitrage

- When the stablecoin price falls below $1, users are incentivized to buy stablecoins on the market at a discount and redeem them for the underlying Bitcoin at par value.

- This reduces the supply of stablecoins in the market, pushing the price back toward the peg.

3.4 Decentralized Oracles

Accurate price information is crucial for the stability mechanisms to function properly.

3.4.1 Multi-source Oracles

- The system uses decentralized oracles that aggregate price data from multiple trusted sources.

- This approach reduces the risk of incorrect pricing due to manipulation or data errors from a single source.

3.4.2 Oracle Redundancy

- Multiple independent oracle networks provide price feeds to the system.

- Redundancy enhances reliability and ensures continuous operation even if one oracle network fails.

3.5 Customizable Parameters

The NBW platform allows for customization of stability parameters, including collateral ratios, redemption thresholds, and interest rate models.

3.5.1 Governance-Controlled Parameters

- The governance system enables $ELA holders to propose and vote on changes to system-wide parameters or specific product parameters.

- This flexibility allows the system to adapt to changing market conditions and community preferences.

3.6 Fee Structure

The fee structure is designed to support the network while providing incentives for long-term participation.

3.6.1 Transaction Fees

- A fee of 0.05% (5 basis points) is charged on transactions involving the minting and redemption of stablecoins.

- These fees support network operations and cover costs associated with Zero-Knowledge proof calculations.

3.6.2 Fee Payment Options

- Fees can be paid in either stablecoins or ELA.

- Users paying fees with ELA may receive a discount.

- Gas fees for minting operations can be paid using ELA (Elastos token), providing additional flexibility for users within the BeL2 ecosystem.

3.7 Continuous Monitoring and Adjustment

The stability of the system is continuously monitored and adjusted.

3.7.1 Real-time Analytics

- Advanced analytics tools monitor the health of the system in real-time.

- Key metrics include collateral ratios, minting and redemption volumes, price deviations, and liquidation events.

3.7.2 Governance-led Improvements

The DAO can propose and implement improvements to the stability mechanisms based on data-driven insights.

Emergency Measures:

- In extreme market conditions, the DAO can vote to implement additional stability measures, such as adjusting collateral requirements or temporarily pausing redemptions.

Stability Reserve:

- A portion of system fees is allocated to a stability reserve fund.

- The reserve can be used to defend the peg or cover system losses in emergency situations.

By combining these diverse stability mechanisms, the NBW system aims to create a robust and flexible platform for Bitcoin-backed stablecoins that can maintain their peg even in highly volatile market conditions. The multi-layered approach provides redundancy and adaptability, allowing the system to respond effectively to a wide range of market scenarios while leveraging the security and value proposition of Bitcoin as the underlying collateral.

IV. User Experiences in the New Bretton Woods System

The New Bretton Woods (NBW) system is designed to cater to a diverse range of users, each with their own needs and objectives. This section outlines how different actors will interact with and benefit from the platform.

4.1. Bitcoin Holders

Bitcoin holders are a primary target audience for the NBW system, as it allows them to utilize their BTC holdings without selling.

Experience:

- Collateralization: Users can lock their Bitcoin as collateral to mint Native Bitcoin Stablecoins.

- Yield Generation: Opportunity to earn yield on Bitcoin holdings through various DeFi strategies.

- Liquidity Access: Ability to access liquidity without selling Bitcoin, preserving long-term opportunity.

- Risk Management: Tools to monitor collateral ratios and manage liquidation risks.

User Journey:

1. Connect Wallet: Connect their Bitcoin wallet to the NBW platform.

2. Lock Bitcoin: Lock Bitcoin into the protocol as collateral.

3. Mint Stablecoins: Mint Native Bitcoin Stablecoins based on the value of their collateral.

4. Utilize Stablecoins: Use stablecoins in DeFi applications, trading, or as a hedge against volatility.

5. Monitor Position: Keep track of their collateralization ratio and adjust as needed.

6. Repay and Reclaim: Repay the stablecoins and unlock their Bitcoin collateral when desired.

4.2. Stablecoin Users

These users seek a stable store of value and medium of exchange within the crypto ecosystem.

Experience:

- Stability: Access to a Bitcoin-backed stablecoin pegged to the US dollar.

- DeFi Integration: Allow for the use of stablecoins across various DeFi protocols.

- Low Fees: Benefit from efficient Layer 2 operations for reduced transaction costs.

- Redemption Options: Ability to redeem stablecoins for underlying Bitcoin or fiat currencies when desired.

User Journey:

1. Acquire Stablecoins: Obtain Native Bitcoin Stablecoins through exchanges or by purchasing from other users.

2. Engage in DeFi: Use stablecoins in DeFi platforms for various financial activities.

3. Earn Yield: Participate in yield farming or provide liquidity to earn returns.

4. Redeem Assets: Redeem stablecoins for Bitcoin or fiat currency as required.

4.3 Developers

Developers are crucial for expanding the NBW ecosystem and creating new applications.

Experience:

- Comprehensive SDK: Access to robust tools and libraries for building applications on the NBW platform.

- Documentation: Extensive resources and tutorials for project integration.

- Testnet Environment: Ability to test applications in a risk-free sandbox.

- Support and Grants: Opportunities to receive funding and support for innovative projects.

User Journey:

1. Access Resources: Explore the NBW developer documentation and SDK.

2. Build and Test: Develop applications and test them on the NBW testnet.

3. Community Engagement: Participate in hackathons and developer forums.

4. Deployment: Launch applications on the NBW compatible chains.

5. Feedback Loop: Gather user feedback and iterate on application development.

4.4. Institutional Users

Institutions looking to enter the DeFi space will find robust and compliant options within the NBW ecosystem.

Experience:

- Scalability: Support for high-volume transactions and large-scale operations.

- Risk Management: Advanced tools for portfolio and risk management.

- Compliance: Integration with KYC/AML protocols and regulatory reporting features.

- Custody and Security: Access to institutional-grade custody solutions and security measures.

User Journey:

1. Onboarding: Complete institutional onboarding, including compliance checks.

2. Integration: Connect NBW platform capabilities with existing systems.

3. Deploy Capital: Allocate funds to various NBW products and strategies.

4. Manage Portfolio: Utilize analytics and management tools for oversight.

5. Compliance Reporting: Generate necessary documentation for regulatory compliance.

4.5. Cross-Chain Users

Users looking to operate across multiple blockchain networks will find the NBW system particularly beneficial.

Experience:

- Interoperability: Easily transfer assets between Bitcoin and EVM-compatible chains.

- Unified Management: Manage assets and activities across multiple chains through a single interface.

- Expanded Opportunities: Access a broader range of DeFi applications and liquidity pools.

- Efficiency: Benefit from optimized routing and reduced transaction costs.

User Journey:

1. Connect Multi-chain Wallets: Link wallets from different blockchain networks.

2. Asset Transfers: Conduct cross-chain asset transfers or swaps effectively.

3. Engage in DeFi Activities: Participate in cross-chain DeFi opportunities.

4. Monitor Assets: Keep track of holdings and positions across networks.

5. Optimize Strategies: Leverage cross-chain data to facilitate exchange of information and value.

By catering to these diverse user groups, the NBW system aims to create a comprehensive and inclusive ecosystem that serves the needs of both retail and institutional participants. The platform's design focuses on providing intuitive interfaces, robust tools, and clear information to ensure a smooth and rewarding experience for all users, regardless of their level of expertise or specific objectives within the DeFi space.

V. Governance and Economic Model

The New Bretton Woods (NBW) system operates without its own native token. The network security and governance are maintained by the Arbitrator Network through a voting mechanism to prevent fraudulent transactions and zkProcessors generating and verifying zero-knowledge proofs.

5.1 Arbitrator Network

Arbitrators act as the foundational nodes of NBW.

5.1.1 Eligibility

To become an eligible arbitrator, one must either:

1. stake a specified amount of BTC or ELA

2. restake the BPOS NFT from Elastos mainnet

5.1.2 Benefits

1. Participation in NBW governance and decision-making

2. Revenue sharing from NBW system commissions

3. Potential future airdrops from the NBW community

5.2 ZK Processors:

5.2.1 Mechanism

1. Zero-knowledge proofs for NBW transactions require zkProcessors for computation

2. zkProcessors compete to generate proofs for NBW transactions

5.2.2 Incentives

Successful processors receive compensation through:

1. Transaction fees

2. Potential future airdrops from the NBW community (Note: The NBW Team has no plans to create a native or governance token for the project).

All zkProcessor implementations are welcome to participate through the incentive mechanisms. Performance-optimized processors can achieve up to 10x better speed and energy efficiency.

5.3 Transaction Fee

5.3.1 Fee Structure:

1. NBW charges a 0.05% fee on all Native Bitcoin DeFi transactions

2. Special discount available when paying fees with $ELA

5.3.2 Fee Governance:

1. Arbitrators vote on the allocation and use of collected fees

2. Other allocation methods may be proposed and voted on

5.4 Long-term Vision

Our governance model is designed with sustainability and long-term growth in mind. By aligning incentives among users, developers, and contributors, we aim to create a robust, decentralized ecosystem that can adapt and thrive in the evolving DeFi landscape.

5.5 Transparency Commitment

We believe this balanced approach to our governance will foster trust, encourage participation, and support the long-term success of the New Bretton Woods system. Our goal is to create a fair, transparent, and sustainable economic model that benefits all participants in our ecosystem.

VI. Products and Applications

The New Bretton Woods (NBW) ecosystem is designed to offer a comprehensive suite of decentralized financial products and services. This section outlines the core offerings and potential future developments within the platform, demonstrating how NBW leverages Bitcoin's security and the flexibility of DeFi to create innovative financial solutions.

6.1 Core Products

6.1.1 Native Bitcoin Stablecoin

The flagship product of the NBW system is the Native Bitcoin stablecoin, which allows Bitcoin holders to access stable value without selling their BTC.

Key Features:

- Bitcoin-Collateralized: Backed by Bitcoin held on the main network.
- Stability Mechanisms: Maintains a 1:1 peg with the USD through overcollateralization and other stability measures.
- Liquidity Access: Enables Bitcoin holders to obtain liquidity without relinquishing ownership of their BTC.
- DeFi Integration: Usable across various DeFi applications on EVM-compatible chains.

Use Cases:

- Trading pairs in decentralized exchanges.
- Collateral for other DeFi products.
- Medium of exchange for everyday transactions.
- Store of value during market volatility.

6.1.2 Lending and Borrowing Platform

A decentralized platform that allows users to lend their Native Bitcoin stablecoins or borrow against their Bitcoin collateral.

Features:

- Variable and fixed interest rate options.
- Overcollateralized loans to ensure system stability.
- Liquidation mechanisms to protect lenders.
- Integration with other DeFi protocols for yield optimization.

Use Cases:

- Earning interest on stablecoin holdings.
- Accessing liquidity without selling Bitcoin.
- Leveraging Bitcoin holdings for future opportunities.

6.1.3 Decentralized Exchange (DEX)

A decentralized exchange built on the NBW system, facilitating trades between Native Bitcoin stablecoins, Bitcoin, and other cryptocurrencies.

Features:

- Automated Market Maker (AMM) model for liquidity provision.
- Cross-chain swaps leveraging the BeL2 infrastructure.
- Low fees due to efficient Layer 2 operations.

Use Cases:

- Trading between different assets in the NBW ecosystem.
- Providing liquidity to earn trading fees and rewards.
- Arbitrage opportunities between different platforms.

6.2 Advanced DeFi Products

6.2.1 Synthetic Assets

Leveraging the stability of the Native Bitcoin stablecoin, the NBW system can support the creation of synthetic assets representing real-world assets or cryptocurrencies.

Potential Synthetic Assets:

- Stock indices (e.g., S&P 500, NASDAQ).
- Commodities (e.g., gold, oil).
- Fiat currencies.
- Cryptocurrencies not natively supported on the platform.

Use Cases:

- Gaining exposure to traditional financial assets within the crypto ecosystem.
- Creating diversified assets portfolios.
- Hedging against market volatility.

6.2.2 Options and Derivatives

A platform for creating and trading options and other derivatives based on Bitcoin and other supported assets.

Features:

- American and European style options.
- Cash-settled futures contracts.
- Perpetual swaps with funding rates.

Use Cases:

- Hedging Bitcoin positions.
- Speculating on future price movements.
- Generating yield through options writing.

6.2.3 Yield Farming and Liquidity Mining

Incentive programs to encourage liquidity provision and participation in the NBW ecosystem.

Features:

- Staking rewards for providing liquidity to various pools.
- Bonus rewards for long-term liquidity provision.
- Gamified yield farming experiences to increase engagement.

Use Cases:

- Earning additional returns on idle assets.
- Bootstrapping liquidity for new products and trading pairs.

6.3 Governance and DAO Tools

6.3.1 Decentralized Autonomous Organization (DAO) Platform

A suite of tools for creating and managing DAOs within the NBW ecosystem.

Features:

- Customizable governance models.
- Proposal creation and voting mechanisms.
- Treasury management tools.
- Integration with other NBW products for DAO operations.

Use Cases:

- Creating investment DAOs.
- Managing protocol development and upgrades.
- Coordinating community-driven initiatives.

6.3.2 Governance Dashboard

A comprehensive dashboard forarbitrators to participate in the governance of the NBW ecosystem.

Features:

- Real-time voting and proposal tracking.
- Delegation mechanisms for voting power.
- Analytics on governance participation and outcomes.
- Educational resources on protocol parameters and their impacts.

Use Cases:

- Participating in protocol upgrades and parameter adjustments.
- Allocating ecosystem resources to different initiatives.
- Shaping the long-term direction of the NBW system.

6.4 Cross-Chain Bridge and Interoperability Tools

6.4.1 Cross-Chain Asset Bridge

Leveraging the BeL2 infrastructure to create a secure and efficient bridge between Bitcoin and EVM-compatible chains.

Features:

- Trustless bridging of Bitcoin to EVM chains.

- Support for multiple EVM-compatible chains.
- Real-time monitoring of cross-chain transactions.
- Integration with hardware wallets for enhanced security.

Use Cases:

- Moving assets between different blockchain ecosystems.
- Accessing DeFi opportunities on various chains.
- Arbitrage between different blockchain markets.

6.4.2 Interoperability SDK

A software development kit that allows developers to easily integrate NBW products and Bitcoin functionality into their existing DeFi applications.

Features:

- Libraries for interacting with the BeL2 protocol.
- Tools for verifying zero-knowledge proofs.
- Templates for common cross-chain operations.
- Extensive documentation and developer support.

Use Cases:

- Integrating Bitcoin collateralization into existing lending platforms.
- Adding Native Bitcoin Stablecoin support to wallets and exchanges.
- Developing new cross-chain DeFi applications.

6.5 Real-World Asset (RWA) Integration

6.5.1 Tokenized Real-World Assets

A framework for bringing real-world assets onto the NBW platform, backed by the stability of the Native Bitcoin Stablecoin.

Potential Tokenized Assets:

- Real estate.
- Invoices and accounts receivable.
- Intellectual property rights.
- Commodities and precious metals.

Features:

- Legal and regulatory compliance tools.
- Fractionalization of high-value assets.
- Automated dividend and interest distributions.
- Secondary market for trading tokenized assets.

Use Cases:

- Owning real-world assets using cryptocurrency.
- Accessing liquidity for illiquid assets.
- Creating diversified assets portfolios spanning both crypto and traditional assets.

6.5.2 RWA-Backed Lending

A specialized lending platform that allows holders of tokenized real-world assets to use them as collateral for loans in Native Bitcoin stablecoins.

Features:

- Valuation oracles for real-world assets.
- Customizable loan terms based on asset type and risk profile.
- Integration with legal frameworks for collateral claims.
- Secondary market for loan participations.

Use Cases:

- Accessing liquidity without selling valuable real-world assets.
- Leveraging real-world asset holdings for crypto assets.
- Creating new yield opportunities for stablecoin holders.

6.6 Advanced Trading Tools

6.6.1 Algorithmic Trading Platform

A platform that enables users to create, backtest, and deploy trading algorithms using the Native Bitcoin Stablecoin and other assets in the NBW ecosystem.

Features:

- Visual programming interface for creating trading strategies.
- Historical data access for backtesting.
- Real-time data feeds and execution engines.
- Risk management and performance analytics tools.

Use Cases:

- Developing and deploying automated trading strategies.
- Market making and liquidity provision.
- Arbitrage between different products in the NBW ecosystem.

6.6.2 Social Trading and Copy Trading

A social platform that allows users to share trading strategies and follow successful traders.

Features:

- Performance tracking and leaderboards.
- Customizable risk management for copy trading.
- Revenue sharing between strategy creators and followers.
- Integration with NBW's core trading products.

Use Cases:

- Novice traders learning from experienced participants.
- Strategy creators monetizing their trading skills.
- Diversifying trading approaches without extensive knowledge.

6.7 Education and Onboarding

6.7.1 Interactive Learning Platform

An educational platform designed to onboard new users to the NBW ecosystem and DeFi concepts.

Features:

- Gamified learning experiences.
- Simulated assets exchange environments.
- Tutorials on using various NBW products.
-

Use Cases:

- Onboarding new users to the NBW ecosystem.
- Educating users about DeFi concepts and risks.
- Encouraging responsible participation in the platform.

6.7.2 Developer Hub

A comprehensive resource center for developers looking to build on the NBW platform.

Features:

- Detailed API documentation.
- Sample code and project templates.
- Regular hackathons and coding challenges.
- Grants program for promising projects.

Use Cases:

- Accelerating development of new applications on NBW.
- Fostering innovation within the ecosystem.
- Building a strong developer community around the platform.

The products and applications outlined in this section represent the core offerings and potential future developments within the NBW ecosystem. By providing a comprehensive suite of DeFi tools and services, all anchored by the stability and security of Bitcoin, the NBW system aims to create a new paradigm for decentralized finance. As the ecosystem grows and evolves, we anticipate the emergence of even more innovative applications that leverage the unique capabilities of the BeL2 infrastructure and the Native Bitcoin Stablecoin.

VII. Roadmap

The development and deployment of the New Bretton Woods (NBW) system is an ambitious project that will unfold over several phases. This roadmap outlines our key milestones and objectives for the coming years, with a focus on building a robust, secure, and widely adopted decentralized finance ecosystem anchored by Bitcoin.

Phase 1: Foundation and Prototype (Q1-Q3 2024)

Research and Development

- Finalize Technical Architecture: Established the technical blueprints for BeL2 and the Native Bitcoin Stablecoin.
- Develop Cairo Circuit: Created and tested the Cairo Circuit for generating and verifying BTC transaction proofs.

- Implement Core Zero-Knowledge Proof System: Built the foundational ZKP mechanisms essential for cross-chain verification.

Prototype Development

- Built EVM ZKP Contract Prototype: Developed a prototype of the EVM ZKP Contract for efficient verification of BTC transactions.
- Developed zkBTC Full Nodes: Created a basic version of the zkBTC Full Nodes to monitor the Bitcoin network.
- Proof-of-Concept for Stablecoin Issuance: Demonstrated the issuance and redemption process of the Native Bitcoin Stablecoin.

Community and Partnerships

- Established Key Partnerships: Collaborated with blockchain projects and research institutions.
- Initiated Community Outreach: Began educating potential users and developers about the NBW system.

Phase 2: Testnet Launch and Core Infrastructure (Q4 2024 - Q1 2025)

Whitepaper

- Publish Whitepaper and Documentation: Release comprehensive whitepaper and technical documents to the public.

Testnet Deployment

- Launch BeL2 Testnet: Deploy the testnet with basic functionality for public testing.
- Deploy Test Nodes: Release test versions of zkBTC Full Nodes and Arbitrator Nodes.
- Introduce Test Stablecoin: Implement a test version of the Native Bitcoin Stablecoin on the testnet.

Core Infrastructure Development

- Develop Arbitrator Network: Build and test the decentralized Arbitrator Network.
- Enhance zkBTC Full Nodes: Improve the functionality and performance of the full nodes.
- Optimize Smart Contracts: Finalize and optimize the EVM ZKP Contract and Transaction Verifier Contract.

Developer Tools

- Release BeL2 SDK Alpha: Provide an initial SDK for developers to build on the platform.
- Provide Documentation: Offer tutorials and guides to assist developers.

Security and Audits

- Conduct Security Audits: Perform thorough audits of all core components.
- Implement Security Enhancements: Address any vulnerabilities identified during audits.

Phase 3: Mainnet Launch and Basic Products (Q2-Q3 2025)

Mainnet Deployment

- Launch BeL2 Mainnet: Deploy the fully functional mainnet.
- Deploy Production Nodes: Release production-ready zkBTC Full Nodes and establish the Arbitrator Network.
- Launch Native Bitcoin Stablecoin: Introduce the stablecoin on the mainnet.

Core Product Release

- Release Lending and Borrowing Platform: Offer basic lending and borrowing services.
- Launch Decentralized Exchange (DEX): Provide a platform for trading assets within the NBW ecosystem.

Governance Implementation

- Implement Governance Features: Enable basic governance functionalities for smart contracts.

Ecosystem Growth

- Initiate Developer Grants Program: Encourage development through funding.
- Host Hackathons: Promote innovation and community engagement.

Phase 4: Advanced Features and Scaling (Q4 2025 - Q2 2026)

Advanced Product Development

- Implement Synthetic Assets: Introduce synthetic asset support.
- Develop Options and Derivatives: Offer advanced trading instruments.
- Enhance Yield Farming Programs: Expand liquidity mining and yield opportunities.

Cross-Chain Expansion

- Develop Cross-Chain Asset Bridge: Enable interoperability with multiple EVM-compatible chains.
- Implement Interoperability Tools: Provide tools for cross-chain operations.

Scaling Solutions

- Research Layer 2 Scaling: Explore and implement solutions for increased throughput.
- Optimize ZKP Processes: Improve the efficiency of zero-knowledge proof generation and verification.

Enhanced Governance

- Launch Full DAO Platform: Establish a comprehensive governance system.
- Implement Advanced Voting Mechanisms: Introduce sophisticated proposal and voting processes.

Phase 5: Real-World Asset Integration/ECOSYSTEM (Q3 2026 - Q4 2026)

RWA Integration

- Develop Tokenization Framework: Create standards for tokenizing real-world assets.
- Launch RWA-Backed Lending Platform: Offer lending services backed by real-world assets.
- Establish Institutional Partnerships: Collaborate with traditional finance institutions for asset onboarding.

Advanced Trading Tools

- Release Algorithmic Trading Platform: Provide tools for automated trading strategies.
- Implement Social Trading Features: Enable copy trading and community engagement.

Ecosystem Expansion

- Foster Third-Party Development: Encourage external projects to build on NBW.
- Solidify NBW's Market Position: Establish the platform as a leading DeFi ecosystem.

Regulatory Compliance

- Engage with Regulators: Work to ensure compliance in key jurisdictions.
- Implement KYC/AML Features: Introduce necessary compliance measures for RWA integration.

Phase 6: Global Adoption and Future Innovation (2027 and beyond)

Global Expansion

- Establish Regional Hubs: Set up localized support and community growth centers.
- Form International Partnerships: Collaborate with global financial institutions.

Innovation Pipeline

- Pursue Emerging Technologies: Research advancements like quantum-resistant cryptography.
- Regular Protocol Upgrades: Implement improvements based on governance decisions.

Education and Onboarding

- Launch Comprehensive Educational Platform: Provide resources for users and developers.
- Enhance User Experience: Develop user-friendly interfaces to facilitate mainstream adoption.

Long-Term Vision Realization

- Advance Toward a New Financial Standard: Aim to make NBW a cornerstone of global finance.
- Adapt and Evolve: Continuously refine the system based on technological and market developments.

Throughout all phases, we will maintain a strong focus on security, decentralization, and community engagement. Regular updates and adjustments to this roadmap will be made based on technological developments, market conditions, and community feedback.

Our ultimate goal is to create a robust, decentralized financial system that leverages the security of Bitcoin while providing the flexibility and innovation of modern DeFi platforms. By following this roadmap, we aim to progressively build and scale the New Bretton Woods system, establishing it as a cornerstone of the future global financial landscape.

VIII. Conclusion

As we stand at the precipice of a new era in global finance, the New Bretton Woods (NBW) system emerges as a pioneering solution to the challenges that have long plagued our economic structures. By bridging the security and scarcity of Bitcoin with the innovation and flexibility of decentralized finance, NBW offers a robust framework for a more stable, transparent, and inclusive financial future.

Addressing Global Financial Challenges

The NBW system directly addresses the shortcomings of the current global financial system:

1. Debt Crisis Mitigation: By providing a stable, Bitcoin-backed currency, NBW offers an alternative to the debt-driven fiat system, potentially reducing the risk of sovereign debt crises.

2. Inflation Protection: The fixed supply of Bitcoin, coupled with the stability mechanisms of the Native Bitcoin Stablecoin, provides a hedge against inflationary pressures.

3. Financial Inclusion: The decentralized nature of NBW opens up advanced decentralized financial services to anyone with an internet connection, regardless of their geographic location or traditional banking status.

4. Transparency and Trust: Leveraging blockchain technology and zero-knowledge proofs, NBW ensures unprecedented levels of transparency while maintaining privacy, fostering trustlessness in financial transactions.

Technological Innovation

At its core, NBW represents a leap forward in financial technology:

1. Cross-Chain Interoperability: The BeL2 infrastructure enables effective communication between Bitcoin and EVM-compatible chains, unlocking new possibilities for decentralized applications.

2. Zero-Knowledge Proofs: By implementing advanced cryptographic techniques, NBW ensures the security and privacy of transactions while enabling efficient verification across different blockchain networks.

3. Scalability Solutions: The system's design incorporates Layer 2 scaling solutions, preparing for widespread adoption without compromising on decentralization or security.

Economic Model for the Future

The NBW system introduces a new economic paradigm:

1. Bitcoin as Digital Gold: By utilizing Bitcoin as the underlying asset for a stablecoin, NBW redefines the concept of sound money for the digital age.

2. Decentralized Governance: Thearbitrator network and its governance model ensure that the system can evolve and adapt based on the collective wisdom of its community.

Comprehensive Financial Ecosystem

NBW is not just a single product, but a comprehensive DeFi ecosystem:

1. Diverse Product Offerings: From lending and borrowing to synthetic assets and real-world asset integration, NBW provides a wide array of tools and services.

2. Developer-Friendly Platform: With its SDK and developer resources, NBW encourages innovation and the creation of new financial applications.

3. Education and Onboarding: By prioritizing user education and easy onboarding, NBW paves the way for widespread adoption of decentralized finance.

Global Impact and Future Outlook

As we look to the future, the potential impact of the NBW system is profound:

1. Reshaping Global Finance: By providing a decentralized alternative to traditional monetary systems, NBW has the potential to reshape the global economic landscape.

2. Empowering Individuals: NBW puts financial sovereignty back in the hands of individuals, allowing them to truly own and control their assets.

3. Driving Innovation: The open and programmable nature of NBW will likely spur a new wave of financial innovation, leading to products and services we have yet to imagine.

4. Promoting Stability: By offering a more stable and transparent decentralized financial system, NBW could contribute to greater economic stability on a global scale.

Challenges and Responsibility

While the potential of NBW is immense, we acknowledge the challenges ahead:

1. Regulatory Landscape: Navigating the complex and evolving regulatory environment will be crucial for the widespread adoption of NBW.

2. Security Imperative: As a DeFi system handling significant value, maintaining the highest standards of security will be an ongoing priority.

3. Scalability and User Experience: Ensuring that the system can handle widespread adoption while maintaining a user-friendly experience will be key to success.

4. Community Governance: The effectiveness of the decentralized governance model will be critical in guiding the future development of the system.

Collective Impact

The New Bretton Woods system represents more than just a technological innovation; it is a vision for a fairer, more stable, and more accessible global financial system. As we embark on this journey, we invite developers, economists, policymakers, and individuals from all walks of life to join us in building this new financial paradigm.

By leveraging the security of Bitcoin, the innovation of decentralized finance, and the power of community governance, NBW has the potential to usher in a new era of economic prosperity and financial inclusion. As we move forward, we remain committed to our core principles of security, decentralization, and user empowerment, working tirelessly to realize the full potential of this groundbreaking system.

The road ahead is challenging, but the potential rewards are immense. Together, we have the opportunity to reshape the global financial landscape, creating a system that works for everyone, not just a privileged few. The New Bretton Woods system is not just a project; it's a movement towards a more equitable and sustainable financial future. We invite you to be part of this historic transformation.

References

[1] U.S. Department of the Treasury, "America's finance guide: National debt," *U.S. Treasury Fiscal Data*, accessed November 13, 2024.

[2] U.S. Department of the Treasury, "Financial report of the United States government for fiscal year 2023 (Final)," *U.S. Government Publishing Office*, February 15, 2024, accessed September 2, 2024.

[3] Robert L. Hetzel, "Launch of the Bretton Woods System," *Federal Reserve History*, November 22, 2013, accessed September 1, 2024.

[4] Ibid.

[5] Elastos (ELA) has been chosen as the staking token for the NBW platform for three primary reasons. First, because it is merged mined with Bitcoin, Elastos inherits Bitcoin's robust security, providing a solid foundation for NBW's blockchain network. Second, the NBW platform is built on Bel2 infrastructure, which initially launches on the Elastos Smart Chain; therefore, ELA is a natural choice for staking. Finally, adopting ELA as the staking token demonstrates NBW's commitment to supporting the Elastos community, acknowledging their contribution of resources that enabled the advancement of NBW's technology.