BiFi

Multichain DeFi Ecosystem

White Paper
Version 1.0

December 2020

https://BiFi.finance
https://theBifrost.io

Abstract

BiFi (abbreviation of Bifrost Finance) is the decentralized finance platform built on Bifrost, the universal multichain middleware. BiFi aims to create a multichain DeFi ecosystem for cryptocurrencies with financial products and services that interoperate across multiple blockchains with scalable efficiency.

This document describes the first steps to begin forming such an ecosystem—the decentralized lending and staking protocols.

Contents

1. Introduction

Finance is the flow of money. Over the course of history, financial systems have evolved to efficiently allocate assets. However, these systems have also become increasingly centralized, capital concentrated and power consolidated. The advent of blockchain technology and Bitcoin opened a new way for assets to flow without a central authority, and the introduction of smart contracts and Ethereum expanded the possibility of transacting without intermediaries.

Yet for most of their existence, cryptocurrencies could only be sent or received. Other financial methods like trading, loans, and derivatives needed a centralized finance (CeFi) platform like an exchange to be the trusted custodian. In recent years, decentralized finance (DeFi) has emerged as a system that tokenizes assets and automates the flow of assets with smart contracts—allowing cryptocurrencies to be traded, borrowed, leveraged, and hedged, according to decentralized protocols and without any intermediaries. DeFi can realize the potential of cryptocurrencies.

As its potential becomes clearer, so do its limitations. Operational risks from price volatility and security vulnerabilities continue to be amended with new innovations. Yet the fundamental limitations of blockchains and DeFi stem from the lack of interoperability and scalability.

The lack of *interoperability* means that blockchains cannot work with one another. Without it, each blockchain is confined to its own isolated capital market, unable to transact with other markets. Unable to interoperate, countless blockchains are competing for the hegemony to become the single dominant blockchain.

Even if a single blockchain achieves dominance, it will face the problem of *scalability*. By the nature of blockchains, the amount of information that one network can process is limited. To become a mature financial system, however, DeFi must also manage personal information, credit ratings, and other financial records on blockchains, which is too much for any one blockchain to manage. With several governments and institutions poised to operate their own networks, the fragmentation of assets and information across multiple blockchains seems inevitable.

Hence, it is imperative to enable *Multichain DeFi* to realize the true vision of cryptocurrency, wherein multiple blockchains can seamlessly interoperate, increasing connectivity, efficiency, and accessibility. If Bitcoin introduced the concept of digital assets and Ethereum introduced the possibility of trustless contracts, BiFi is an attempt to create a decentralized financial infrastructure that connects all the markets and creates new opportunities.

The foundation of finance is lending and trading. Lending imbues money with time value, and trading powers its efficient allocation. Both are quintessential to the flow of money. This paper outlines the first steps to lay the groundwork for the finance of the future.

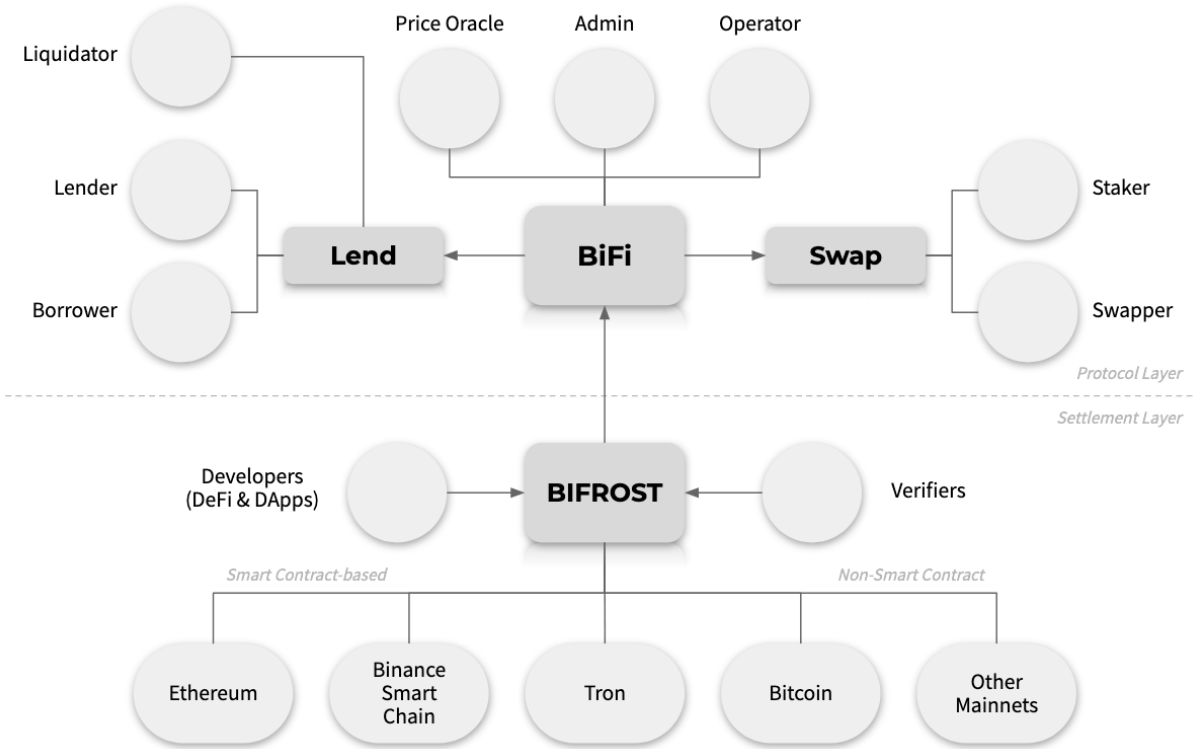
2. Overview

BiFi is a multichain DeFi project built on Bifrost, the Universal Multichain Middleware. Bifrost is not another blockchain, nor is it an exclusive ecosystem. Rather, it can be thought of as a universal language for blockchains to communicate with each other. Bifrost offers a full development suite that includes integrated development environments, operational tools, and security modules.[1]

In its first iteration, BiFi establishes two decentralized protocols, as outlined in this document. The lending protocol implements depositing and borrowing, and the staking protocol implements liquidity pools, which will serve as the foundation for the upcoming decentralized exchange (DEX). To attract liquidity and ensure stability, BiFi distributes governance tokens as incentives to the initial users, who eventually become the stakeholders and administrators of the protocol.

In its initial stage, BiFi offers lending and staking protocols on the Ethereum blockchain. In later stages, it will connect these protocols to other blockchains that fully support smart contracts, such as Binance Smart Chain, Tron, Polkadot, and Cosmos, and ultimately blockchains that do not, like Bitcoin. To support multichain interactions, BiFi also provides its own proprietary multichain wallet that supports multichain DeFi services on BiFi as well as essential P2P payments functions.

Ultimately, Bifrost's multichain technology used to develop BiFi will become commercially available to other multichain DeFi projects, to form a full financial ecosystem for all blockchains.



[1] Bifrost White Paper: https://thebifrost.io/static/Bifrost_WP_Eng.pdf

3. Lending Protocol

The lending protocol implements money markets for lending and borrowing, with pools of assets and floating interest rates algorithmically determined by the supply and demand for the asset.

Compared to peer-to-peer lending, this pool-based approach allows improved liquidity, provides transparent interest rates, reduces speculative risks, and streamlines the lending process without the need for a counterparty.

It will ultimately allow users to deposit assets of one blockchain and borrow assets of another, without the risk of entrusting funds to centralized intermediaries.

Interest rates are determined algorithmically based on the supply and demand for the asset. If the amount of deposits in the market increases, the interest rates decrease, making borrowing more advantageous. If the amount of borrows increase, the interest rates increase, making depositing more advantageous.

Furthermore, the interest calculation is designed to be compounding, and as transactions increase in the market, it increasingly approaches 'per-block compounding'.

3.1. Deposit

When users deposit their assets to the lending protocol, it is aggregated into a pool from which other users may borrow. Deposited assets accrue interest according to the deposit interest rate for that asset set by the supply and demand in the market. Unlike peer-to-peer lending, this pool-based approach allows users to withdraw their funds at any time.

Like money market accounts in traditional banking, deposits allow users to earn interest on their idle assets with minimal risk.

3.2. Borrow

Once users deposit their asset, they can use their deposit as collateral to borrow another asset. Borrowed assets accrue interest according to the borrowing interest rates for the assets set by the supply and demand in the market for each asset. Unlike peer-to-peer lending, this collateralized approach allows users to borrow funds without specifying terms like maturity dates.

The maximum amount of borrowing users can do with their deposit is determined by the ***collateral ratio***. For example, if a user deposits an asset worth 1,000 USD and with 80% collateral ratio, he or she can borrow up to 800 USD. Users cannot borrow more or withdraw deposits if that would bring the value of collateral exceed this ratio. To borrow more, they may deposit more or repay the loans to lower the ratio.

Collateral ratio is set differently for each money market, and the maximum borrowable amount, or ***borrow limit*** is determined by the total deposits that can be used as collateral. For example, if a user deposited 1,000 USDT (1,000 USD) and 1,000 DAI (1,000 USD), with collateral ratio of each set to 70% and 80% respectively, their borrow limit is 1,500 USD (700 and 800 USD, respectively) and the effective net collateral ratio is 75%.

The collateralized borrowing enables more financial flexibility for individuals and strategies for traders. For example, an individual who wishes to hold ETH but needs USDT in the short term can borrow USDT and keep ETH as a collateral. Traders can take a long position on ETH by depositing ETH, borrowing DAI against it, and purchasing more ETH with it. They can also take a short position by depositing DAI, borrowing ETH, selling at an exchange, and buying ETH at a lower price to repay the loan.

3.3. Liquidation

Loan-to-Value ratio (LTV) is the ratio of the values of deposited assets over borrowed assets, representing the status of the collateral loan of a user. The LTV of a user may increase based on several factors:

- Decrease in price of the asset deposited as collateral
- Increase in price of the asset borrowed
- When the value of deposit amount with interest becomes smaller than the value of borrowed amount with interest

A financial service must execute a liquidation process before the LTV exceeds 1 (100%) in order to preserve assets. A decentralized financial service cannot execute liquidation by itself. Therefore, it must create an economic system that incentivizes the liquidators to quickly repay the outstanding loan and protect the protocol.

The level of LTV when the collateralized assets become subject to liquidation is the ***Liquidation Threshold***. When a user's LTV is above the liquidation threshold, a liquidator may pay for the outstanding loan in return for the collateral. BiFi sets the liquidation threshold above the collateral ratio and below 1 (100%), so that the difference between 1 and the liquidation threshold becomes the maximum profit for the liquidator (***Liquidation Incentive***).

For example, assume that the collateral ratio for the deposited asset was 80% and that the liquidation threshold is 90%. If a user has deposited assets worth 100 and borrowed other assets worth 80, his or her LTV ratio is 80%, since $LTV = borrows/deposits = 80/100 = 80\%$. If the value of collateral decreases or the value of borrows increase due to price changes, the LTV could reach 92%. Since the LTV exceeds the liquidation threshold, the deposited asset becomes subject to liquidation. A liquidator can pay for the outstanding loan on behalf of the user (expected cost of repayment of

92) and claim the collateral (expected gain of 100), profiting 8 or about 8.7%. This potential profit incentivizes liquidators to make the repayment before LTV exceeds 1 and protocol suffers losses.

3.4. Interest Rates

Interest rates for deposited and borrowed assets are determined algorithmically by the supply and demand for each asset. ***Utilization*** (U) captures such relationships of supply and demand, defined as the ratio of total amount of borrowed assets (B_t) and deposited assets (D_t).

$$U = \frac{B_t}{D_t}$$

The annual borrowing interest rate (R^B_{year}) incorporates the utilization (U), the ***minimum interest rate*** for borrowers (R_{min}), and the ***sensitivity*** to the rate change to utilization (S).

To protect liquidity, BiFi sets optimal utilization level ($U_{optimal}$) and different sensitivity rates for situations above or below such optimal utilization level (S_1, S_2). S_2 is greater than S_1, to accurately reflect the cost of capital as the liquidity decreases.

$$R^B_{year} = \begin{cases} if\ U < U_{optimal},\ R_{min} + U \cdot S_1 \\ if\ U > U_{optimal},\ R_{min} + U_{optimal} \cdot S_1 + (U - U_{optimal}) \cdot S_2 \end{cases}$$

The annual depositing interest rate incorporates the borrowing interest rate, utilization, and ***spread*** (σ), which creates a spread between R^B_{year} and R^D_{year} that becomes allocated as an insurance for the market and as an earned income for the protocol.

$$R^D_{year} = R^B_{year} \cdot U \cdot \sigma$$

BiFi divides R^D_{year} and R^D_{year} by the number of blocks per year to calculate per-block interest rates.

$$R^D_{block} = \frac{R^D_{year}}{blocks\ per\ year}$$

$$R^B_{block} = \frac{R^B_{year}}{blocks\ per\ year}$$

4. Staking Protocol

The staking protocol establishes liquidity pools, with pools of staked earning rewards proportionately distributed to the liquidity providers, or ***stakers***. The rewards are described in more detail in *5. Protocol Incentives.*

The staked liquidity will be the foundation for a decentralized exchange (DEX) that enables automated trading of different cryptocurrencies, or ***swaps***. Swappers will pay fees for this decentralized trading, and stakers will proportionately share the fees generated.

Unlike centralized exchanges (CEX), DEX does not have a bid-ask spread and thus does not require market makers. It enables users to directly swap assets without a need for an intermediary, eliminating the risks associated with centralized exchanges such as fraud, hacking, and wash trading.

The assets approved to be staked and to be rewarded with incentives are determined initially by BiFi and later by the governance committee.

5. Protocol Incentives

Any protocol is vulnerable to volatility in its initial stages, particularly when the liquidity is low. To increase liquidity and establish stability, BiFi rewards the participants who contribute to the growth and maintenance of the market with ***incentives*** in the form of tokens called BiFi tokens.

Participants can use these incentives in several ways:

- Sell for a financial profit
- Pay fees for multichain DeFi products and services
- Vote for governance proposals (See *7. Governance*)

This section defines the contributions recognized by BiFi and the distribution of the incentives.

5.1. Contribution

5.1.1. Lenders & Borrowers

BiFi recognizes the use of the lending protocol as a contribution that grows the ecosystem, thus rewards users with incentives proportionate to their individual deposits and borrow amounts.

5.1.2. Stakers

BiFi recognizes the use of the staking protocol as a contribution that grows the ecosystem, thus rewards users with incentives proportionate to their individual staked amount.

5.1.3. Operators

The implementation of BiFi is designed to provide an increasingly accurate interest rates and reward allocation for each market as the number of actions increase. In order to optimize the transaction fee for users, we extract the computation process and allow others, i.e., ***operators*** to execute this process, to receive the incentives in return.

Initially, BiFi serves as the operator of the protocol and later it will open this process to any users wishing to assist in operating the protocol.

5.2. Distribution

In every block, the incentives accrue proportionately to each user and decrement linearly. Initially, BiFi sets the total amount of incentives and the speed of decrement. Later, the governance committee may vote to change these parameters.

For the lending protocol, the amount of incentive allocated to each market is proportionate to the total liquidity in each market. For the staking protocol, the amount of incentive allocated to each asset is determined by the governance committee.

For both, incentive accrues every block, and can be claimed at any time.

6. Protocol Design

6.1. Market Handlers & Market Managers

Market Handlers manage the depositing and borrowing services for each market (deposit, borrow, withdraw, repay), and store the deposit and borrow amounts of all users of that market.

Market Manager intermediates all the handlers, calculating the information for the lending protocol across all markets. It also receives price information from the price oracle, and handles the liquidation process.

6.2. Compounding Interest Rate

BiFi implements ***per-block compounding interest***. Since the method of compounding is the same for deposits and borrows, both R_{bl}^{D} and R_{bl}^{B} can be expressed as R.

For per-block compounding interest, the amount with interest (A_{i_n}) for the principal (P_i) starting at block i and ending at block j is calculated as follows:

$$A_{i_n} = P_{i_1} \times \prod_{i=i_1+1}^{i_n} (1 + R_i)$$

However, this requires R_i to be stored at every block, making it inefficient in terms of storage.

To improve this, BiFi stores the current cumulative product of interest rates as ***Exchange Interest Rate*** (R^X). From block i to block j, R^X multiplies $(1 + R)$ to the existing value of R^X, then saves that value in R^X.

$$R^X_{i,j} = \prod_{i}^{j}(1 + R_i)$$

R^X is updated every time there is an action in a block. If there is no action in several blocks, it means D_t and B_t have remained the same, and since those variables determine R, it also means R^X is the same. When there is an action, R^X can be updated by multiplying $(1 + R)$ by the number of blocks there has been no action.

$$R^X_{i,j} = (1 + R_i)^{j-i}$$

If no action occurs for an extended period of time, this overdue update can have high computational cost. In order to preserve the computational efficiency regardless of the period without any actions, BiFi opts for $(1 + 3R)$, instead of $(1 + R)^n$. The functions $y = (1 + R)^n$ and $y = 1 + Rn$ are approximately the same when the value of R is small.

6.3. Incentive Manager

The incentives distributed to depositors, borrowers, and stakers adjust according to the total liquidity in all of the markets supported by the protocol.

Incentives are managed by the ***Incentive Handler***, which interacts with market handlers and the market manager to allocate and distribute the incentives.

6.4. Price Oracle

To ensure the stability and security of the protocols, BiFi has an abstracted oracle that can integrate to external price feed oracles, such as Chainlink's Price Feed Oracle.

7. Governance

In the beginning, the BiFi will have centralized control of the protocols by the ***administrator***, such as setting the parameters for interest rates and liquidation.

As the protocol matures with more users and more liquidity, BiFi will transition to the decentralized autonomous organization (DAO) controlled by the ***stakeholders***, namely the holders of BiFi tokens, who have contributed to the protocols by providing liquidity and using the services.

The administrator and stakeholders control the rights such as the following:

- Electing new administrators
- Setting parameters for the interest rate and liquidation for each currency
- Updating the model implementations
- Approving, suspending, or resuming currencies for protocols
- Allocating, minting, or burning incentives
- Withdrawing the earned income of the protocols

8. Multichain

Powering the multichain DeFi can be seen in two vectors: expansion of services and enhancement of capability. BiFi will expand its services by supporting more assets with stable liquidity and market demand. At the same time, it will enhance the capability of blockchains by overcoming the limits of a single blockchain like Ethereum, such as its high gas fees and low transaction throughput.

BiFi leverages Bifrost to enable the multichain capability and ensure its security. Bifrost, the underlying multichain middleware of BiFi, integrates functional modules to high-capacity blockchains, enabling interoperability and increasing efficiency.[2]

To create not only a scalable, but also a secure multichain platform, Bifrost implements multiple layers of solutions, offering proprietary message relay and monitoring systems, while incorporating verification processes and third-party interoperability solutions.

This reliable interoperability across multiple blockchains—multichain—is a necessary evolution for the blockchain industry. It will connect all the capital markets, enable cheaper and faster transactions, and allow more innovative financial opportunities for all blockchains, nations, and people, without a central authority. Multichain will turn the promise of blockchains into reality.

[2] Bifrost Technology Demo: https://www.youtube.com/watch?v=Bs2AtG81TVI