Templar Protocol Litepaper

@RoyalFool

Abstract

The Templar Protocol is a decentralized modular lending protocol that provides 0% interest stablecoin loans where access to liquidity vaults is gated by NFT. It will be built on the NEAR Protocol, a blockchain known for its scalability, reliability, and Chain Abstraction tools.

Key features of the Templar Protocol include the provision of interest-free stablecoin loans with configurable repayment duration, collateral ratio, borrowing limits, supported assets, origination fees, liquidation spread fees, NFT ownership requirements, liquidation parameters, insurance fund, and lending incentives. The protocol also introduces a novel yield mechanism derived from the spread on the liquidation as a substitute for charging interest. Importantly, the protocol will also utilize differential privacy based on the work of Tarun Chitra et al[1] and Chain Signatures[2] to unlock multichain functionality.

The system's functionality is composed of several operations: borrower operations, lending operations, a liquidation mechanism, and a recovery mode. These operations work together to maintain system solvency, align incentives, and ensure the stability of the protocol. To that end, each (Collateral FT, Stablecoin) liquidity vault will be deployed independently per NFT community.

Through these mechanisms, the Templar Protocol provides a platform for borrowing and lending within the NEAR ecosystem and broader multichain DeFi space.

Introduction

The world of finance has been transformed by cryptocurrencies, giving rise to Decentralized Finance (DeFi) - a new ecosystem of financial services that operates without traditional intermediaries. Within this landscape, innovations like smart contracts, stablecoins, and Non-Fungible Tokens (NFTs) have enabled increasingly sophisticated financial applications. The Templar Protocol, introduced in this paper, represents a novel approach in the DeFi space, combining these concepts to create a unique lending protocol. Built on the NEAR Protocol, known for its scalability and user-friendliness, the Templar Protocol aims to provide interest-free stablecoin loans, with access gated by NFT ownership. By introducing innovative features such as configurable loan parameters, a novel yield mechanism, differential privacy, and multichain functionality, the Templar Protocol seeks to become a foundational protocol for multichain, privacy, decentralized lending, eventually paving the way for Community Based Finance (Community-Fi) creating a more accessible and efficient financial system.

Key Features of Templar Protocol

- **Interest-free Stablecoin borrowing**: Templar Protocol offers 0% APR loans, allowing borrowers to unlock the value of their tokens without having to pay any interest or incur capital gains tax from selling. The only cost to the borrower is a one-time origination fee when the loan is taken out.
- **Multichain:** The protocol will use Chain Signatures from NEAR's Chain Abstraction stack that will enable users to use assets from other chains as collateral and stablecoin loans. This is especially useful for ecosystems that do not have native DeFi such as Bitcoin, Ripple, and Doge.
- **Privacy:** vaults may incorporate differential privacy. Only a specific subset of configurations may be compatible as public <-> private boundaries need to be clearly defined and formalized in order to ensure differential privacy guarantees.
- **Configurable Vaults:** Vaults are a specific (Collateral, Stablecoin) liquidity pool that can only be accessed by holders of a specific NFT collection. Lenders deposit stablecoins and receive CD tokens from the vault and borrowers deposit collateral and receive stablecoins from the vault. In addition to configuring privacy and multichain features on vault, communities may also specify the following parameters on a per vault bases:
    - **Repayment Duration**: The protocol does not enforce any specific repayment duration. The user can either keep the stablecoins they borrowed indefinitely while keeping the collateral deposited in the protocol with the potential for liquidation, or pay back the borrowed stablecoins. However, vaults may enforce specific repayment durations.
    - **Collateral Ratio**: May be either static or dynamically adjusted based on market liquidity conditions or asset volatility allowing borrowers to maximize their borrowing power while also ensuring there is enough buffer in low liquidity conditions so lenders recover their money.
    - **Borrowing Limits:** Maximum amount of stablecoins that can be borrowed against per account for a given collateral can be set for each vault or asset type to help manage risk and ensure protocol solvency. It may be adjusted based on total liquidity available in the vault.
    - **Supported Assets:** Supported Collateral and Loan assets. Each supported asset may have different risk parameters and collateral ratios. New assets can be added permissionlessly as long as liquidity is provided. To start, only stablecoins will be supported as loan assets, but that may change based on future governance decisions.
    - **Origination Fees:** One-time fees charged when a new loan is created. Can be a percentage of the borrowed amount or a flat fee. This is split between the Templar Protocol and the lenders of the vault. Templar must receive a minimum of 0.1% of the loan amount to cover operational costs. This may change based on future governance decisions.
    - **Liquidation Spread Fees:** Fees charged during the liquidation process that represents the difference between the original loan amount and the value of collateral upon liquidation. This acts as a yield mechanism for the protocol, replacing traditional interest. It may be distributed among various stakeholders (e.g., lenders, protocol, insurance fund, etc)
    - **NFT Ownership Requirements:** Specific NFTs required to access certain vaults or borrowing opportunities. Can be used to create exclusive lending pools for different communities or community subsets. May influence borrowing terms or limits based on the NFT's rarity or attributes or the number of NFTs held by an account. Enhances the utility and value proposition of NFTs within the DeFi ecosystem.
    - **Liquidation Parameters:** Parameters relevant to the process for liquidating loans below the Minimum Collateral Ratio (MCR). Such parameters include transfer of collateral to

lenders, full liquidation, or partial liquidation. May include Incentives for liquidators to maintain system health.
    - **Insurance Fund:** Pool of assets set aside to cover potential losses in the system. Can be funded through a portion of liquidation spread fees or other protocol revenues. Provides an additional layer of security for lenders. May be used to compensate users in case of smart contract vulnerabilities or extreme market events.
    - **Lending Incentives:** Rewards or benefits provided to users who supply stablecoin liquidity to the protocol includes a share of the liquidation spread fees and origination fees. May involve governance tokens or NFT community-specific rewards (ie FT tokens, additional NFTs, community status/privileges, etc). Designed to attract and retain lenders, ensuring sufficient liquidity in the system.
- **Scalability**: Our system design decisions, including building on top of NEAR protocol, are made with the goal of having 100M+ borrowers and lenders using our protocol. We believe NEAR can scale better than EVM chains[3] while providing a superior UX and access to other chains using NEAR's Chain Abstraction stack.
- **Security**: We aim to make the design and implementation of the protocol as simple as possible to minimize the attack surface for smart contract exploits. We also designed each vault to be independent to prevent cross asset contagion in the event of cascading liquidations and prevent attacks on a shared liquidity pool by manipulating oracles for low float coins, like what happened to Mango[4].
- **Growth and Early Adopter Incentives**: The protocol may offer incentives to early adopters and contributors to the system's growth.

Liquidation Spread Mechanism

The Templar Protocol introduces an innovative approach to generating yield by capturing liquidation spreads. In traditional lending protocols, interest is charged on loans to compensate lenders and cover operational costs. However, the Templar Protocol offers interest-free loans and instead relies on liquidation spreads as a revenue mechanism, in addition to origination fees. When a borrower's collateral value falls below the required Minimum Collateral Ratio (MCR) threshold, their position becomes eligible for liquidation. During this process, the collateral is sold at market price, which results in some slippage to due liquidity being taken. After the selling is complete, the amount of stablecoins acquired will be somewhere between the original loan amount, and the price at which the liquidation was originally triggered at, creating a spread. This spread is then captured by the protocol and distributed among various stakeholders. A portion may go to the liquidators as an incentive for maintaining system health, while another part could be allocated to the insurance fund to enhance protocol stability. The largest percentage of the spread is distributed to lenders as a form of yield, effectively replacing traditional interest payments. This mechanism allows the protocol to offer interest-free loans while still providing returns to lenders and maintaining system solvency. The size of the spread serving as yield is influenced by the liquidity for the amount of collateral asset being liquidated, the volatility of the collateral asset, the minimum collateral ratio, and the percentage of the spread distributed to lenders. The percentage of the spread given to lenders vs other parties may be dynamically adjusted based on market conditions, vault parameters, or protocol governance parameters, allowing for flexible risk management and yield optimization. The process is visualized in the following flow diagram. Note that all numbers are dollar values for ease of understanding, even if the asset type is NEAR, the collateral asset.

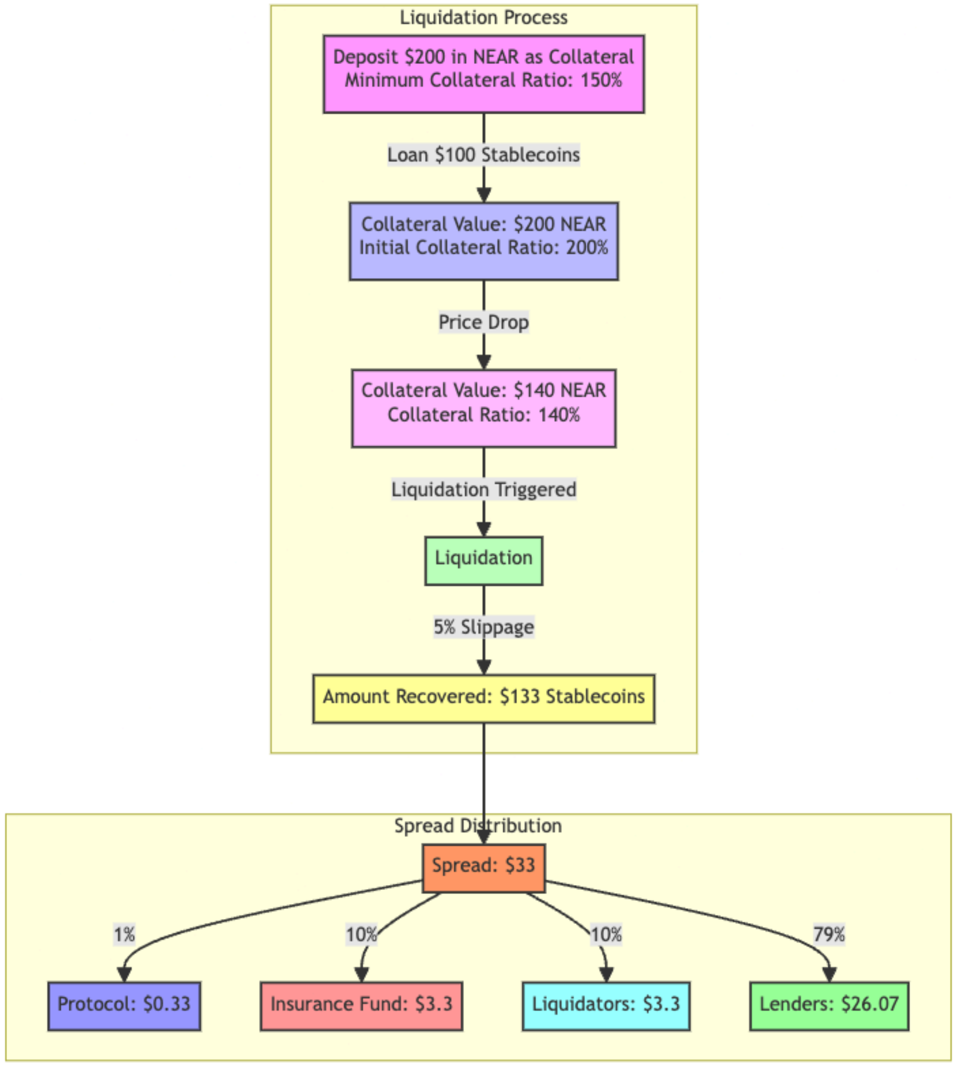

Figure 1

Contract System Functionality

- **Borrower Operations:** Borrowers interact with the protocol by connecting an account from their wallet. The NFTs held by the connected account dictate which vaults the borrower has access to. Once the user finds a suitable vault, they deposit a Fungible Token (BTC, ETH, NEAR, etc) as collateral and then borrow Stablecoins (USDT, USDC, FRAX, etc) against that collateral. A one time origination fee is charged to the borrower. The Initial Collateral Ratio must be greater than the Minimum Collateral Ratio (MCR) specified for the vault. In the future, the MCR may be lowered by staking Templar tokens.
- **Lending Operations:** Lenders interact with the protocol by connecting an account from their wallet. The NFTs held by the connected account dictate which vaults the lender has access to. Lenders deposit Stablecoins into a vault and receive certificate of deposit tokens which map to the specific vault and entitle them to a share of the fees and liquidation spread generated by the

vault or sell on the open market. In the future, Templar tokens would also be issued to lenders which may be staked to earn a share of the protocol fees or sold on the open market.

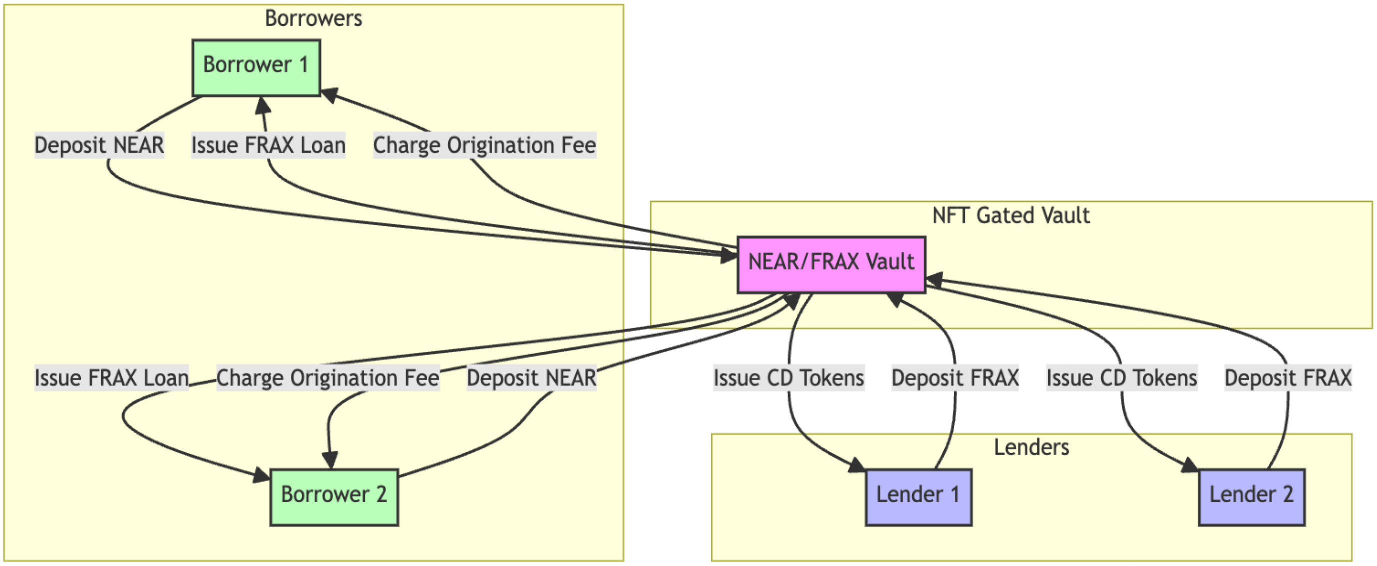

Figure 2

- **Borrowing Redemption Mechanism:** At any time, the protocol allows borrowers to repay their borrowed Stablecoins to the vault. The borrower may also withdraw their collateral provided the new collateral ratio of the loan is greater than the minimum collateral ratio + ε, If the loan is fully repaid, then the borrower may withdraw all their collateral.
- **Lending Redemption Mechanism:** At any time, the protocol allows lenders to withdraw their loaned stablecoin from the vault by depositing their CD tokens. When the CD tokens are redeemed, any accrued share of origination fees or liquidation spread yield will also be available for withdrawal. If the vault is in recovery mode and there are no available stablecoins to withdraw, the lender will be added to a queue and the stablecoins will be sent to them automatically when the protocol gets more stablecoins either from more repayments or from liquidated collateral.

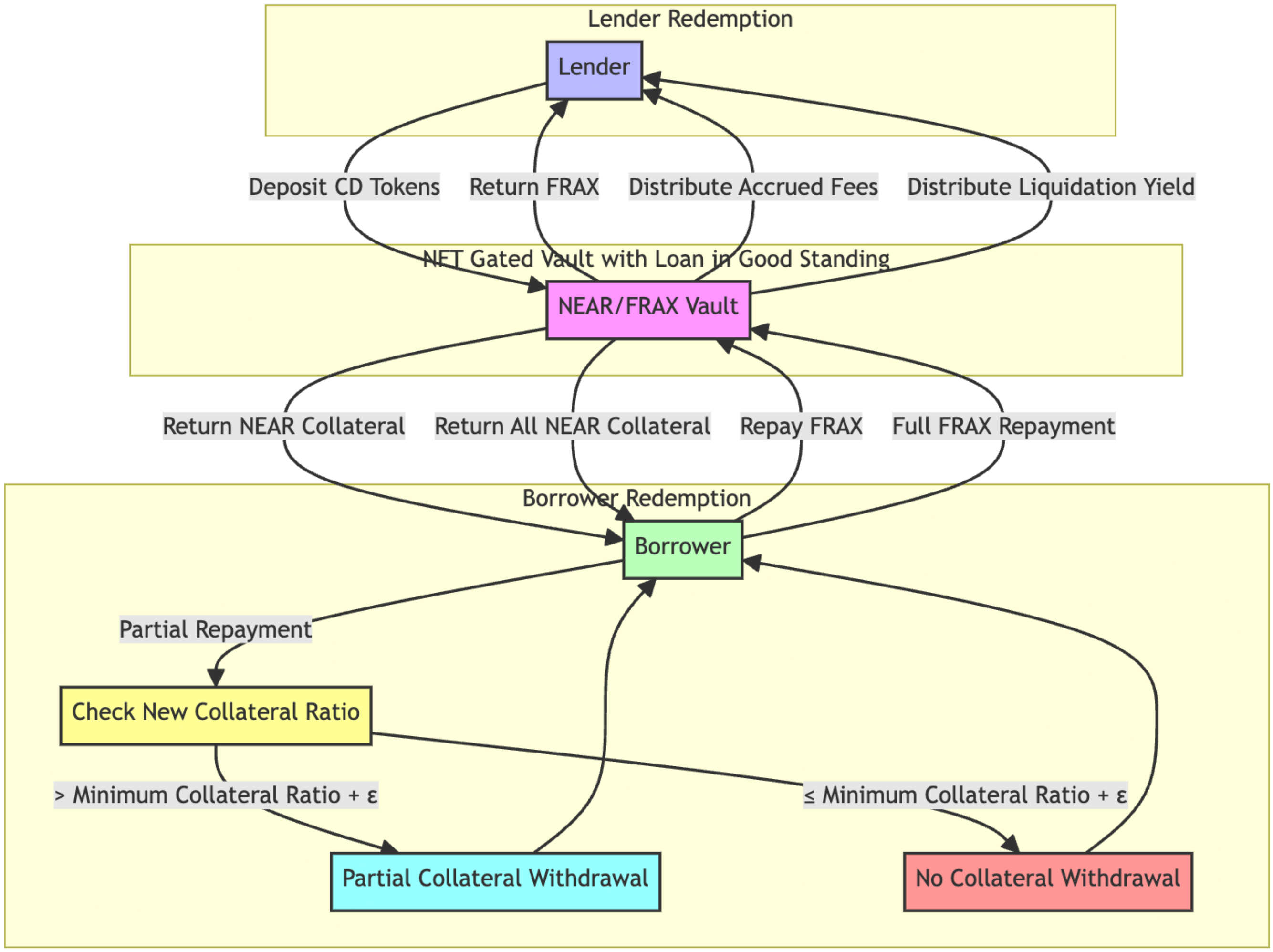

Figure 3

Position Liquidation Mechanism: The liquidation bot iterates through all open loans in the vault, and for all loans where the current collateral ratio ≤ MCR, it liquidates the collateral. The liquidation can take several forms depending on the parameterization of the vault:

1. Transfer of the collateral asset to lenders who may choose to hold or liquidate
2. Bot liquidates the collateral in full into stablecoins
3. Bot partially liquidate the collateral into stablecoins until the collateral ratio for the loan is above some parameterized threshold

The collateral liquidation will take place on Defuse, an upcoming novel Decentralized Exchange which has access to deep multichain liquidity. After the liquidation back into stablecoins takes place and slippage is accounted for, any stablecoins in excess of the original borrowed amount will be split between the protocol, liquidators, insurance fund, and the lenders, with the bulk of the spread going to the lenders. In the future, Templar tokens may be granted upon liquidation to all borrowers, lenders, and liquidators involved.

- **Liquidation Bot:** Off Chain service that tracks open loans in a vault and calls the liquidate function on the vault contract on any loans that are below the MCR. The liquidation bot's account is then awarded a share of the liquidation spread. Lenders, Market Makers, or a subsidiary of the foundation could run the liquidation bots.
- **Insurance Fund:** The Insurance Fund takes a share of the liquidation spread. Its purpose is to provide a backstop in the event that the stablecoin value from liquidating collateral is less than the original stablecoin value borrowed. This should only be needed when there are low liquidity conditions, which is most likely to happen during extreme selloffs.

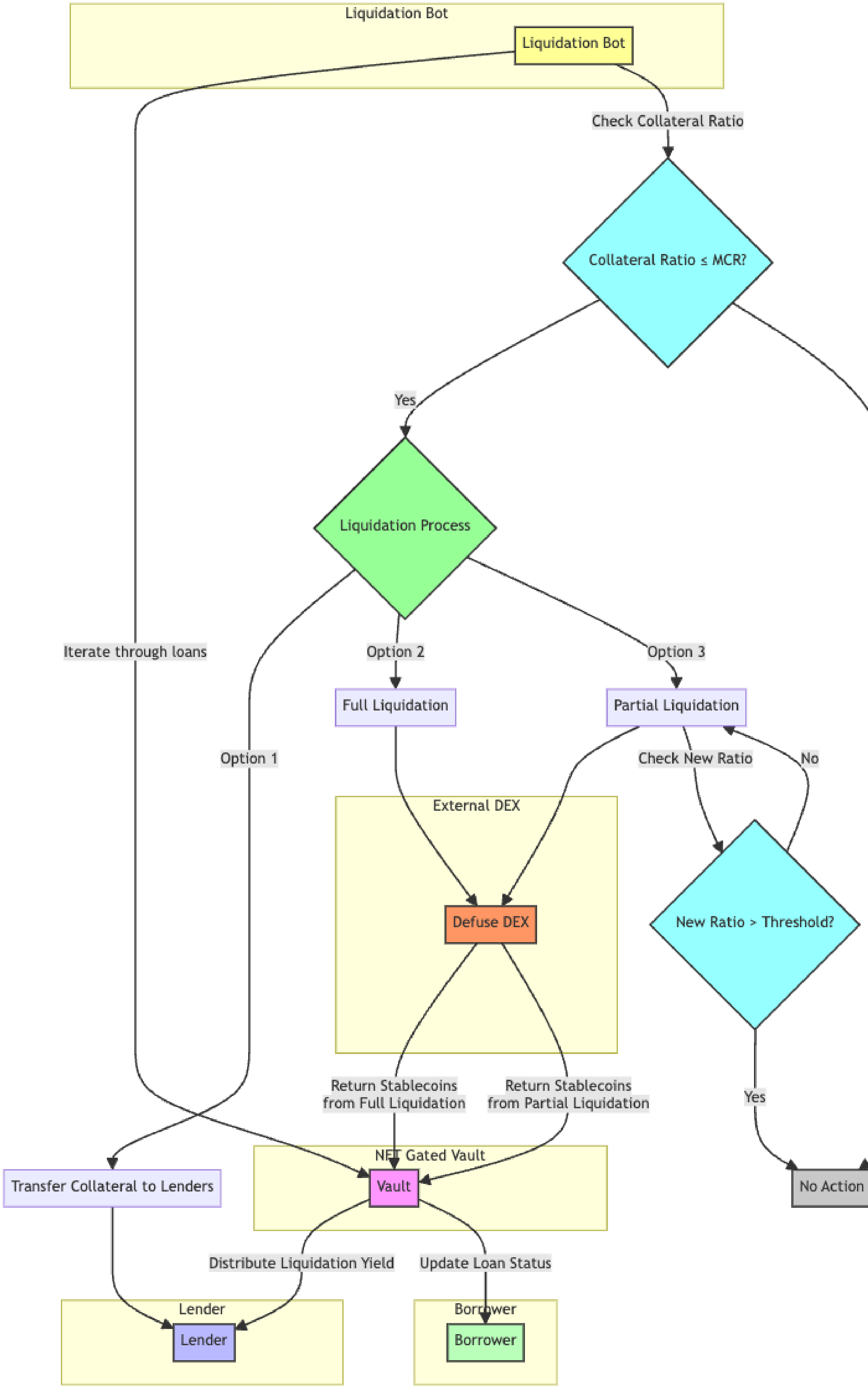
Liquidation Bot
Liquidation Bot
Check Collateral Ratio
Collateral Ratio ≤ MCR?
Yes
Liquidation Process
No
Iterate through loans
Option 1
Option 2
Option 3
Full Liquidation
Partial Liquidation
Check New Ratio
No
External DEX
Defuse DEX
New Ratio > Threshold?
Return Stablecoins
from Full Liquidation
Return Stablecoins
from Partial Liquidation
Yes
NFT Gated Vault
Transfer Collateral to Lenders
Vault
No Action
Distribute Liquidation Yield
Update Loan Status
Lender
Lender
Borrower
Borrower

Figure 4

- **Recovery Mode:** The protocol recovery mode activates for a vault when there are no stablecoins available for borrowers to take out a loan or stablecoins available for lenders to withdraw. Lenders wishing to withdraw while the protocol is in recovery mode are added to a queue. When it is their turn, the stablecoin will be sent to them automatically when the protocol gets more stablecoins either from more deposits from other lenders, repayments from borrowers, or liquidated collateral from liquidation bots. During Recovery Mode, new loan creation is disabled. Recovery Mode is deactivated when there are stablecoins available to lend and the recovery mode lending withdrawal queue is empty.

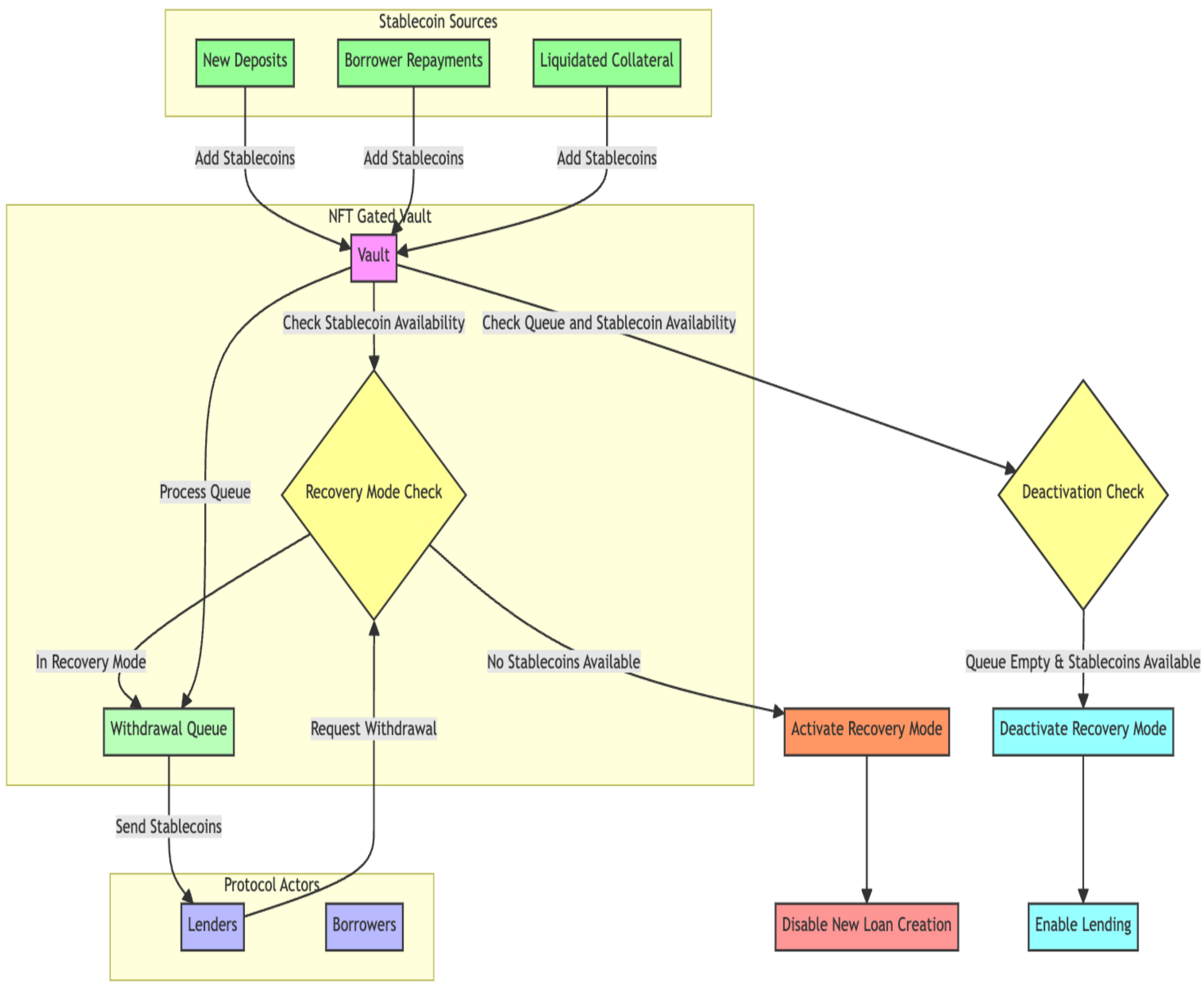

Figure 5

Multichain Functionality

The Templar Protocol leverages NEAR's innovative chain signatures to extend its capabilities across multiple blockchains, significantly enhancing its interoperability and reach. This integration is crucial for creating a seamless, cross-chain lending and borrowing ecosystem. Here's how the Templar Protocol incorporates chain signatures:

Understanding Chain Signatures

NEAR's chain signatures leverage Multi-Party Computation (MPC) and a distributed network of node operators to create joint signatures from arbitrary payloads, allowing NEAR users to control external blockchain accounts. They also unlock the ability of NEAR smart contracts to sign transactions and the ability to exchange keys that contain balances on foreign chains directly as an alternative to using those keys to sign a transaction on the foreign chain to exchange assets.

Implementation in Templar Protocol

Multichain Collateral

Borrowers can use assets from different blockchains as collateral once they deposit those assets into an account where the keys are controlled via MPC. Chain signatures derive the accounts from the keys and a service, potentially an oracle, fetches the balance of the assets held by the account.

Multichain Lending Vaults

The protocol can create lending pools that accept stablecoins and collateral from various blockchains.

Chain signatures derive the accounts from the keys and a multichain balance oracle provides the value of stablecoins and FTs deposited into the MPC account to the Templar Protocol contract.

Cross-Chain NFT Validation

NFTs from different blockchains can be used for access control.

Chain Signatures derive the accounts from the keys and verify NFT ownership using a multichain balance oracle which provides NFT ownership information to the MPC account to the Templar Protocol contract.

Interchain Liquidation Process

Chain Signatures open up more possibilities, and access to broader multichain liquidity, in how collateral liquidations occur. Liquidation bots could:

a) Create a transaction to liquidate on the native chain or using a multichain dex such as Defuse
b) Transfer the keys on NEAR to a Key Exchange for liquidation
c) Transfer the keys directly to a vault subaccount for holding liquidated assets if lenders for a given vault want to hold the collateral assets they acquired at a discount during liquidation.

Benefits of Multichain Functionality

Increased Liquidity

Access to assets and users from multiple blockchains expands the Total Addressable Market of the protocol. It also unlocks liquidity opportunities for large ecosystems that don't have access to native DeFi such as BTC, XRP, and DOGE. In liquidation scenarios, having access to multichain liquidity ensures better execution prices, and thus better spreads and more yield for lenders while allowing potentially lower MCRs for lenders.

Broader Accessibility

Users can participate regardless of their preferred blockchain ecosystem.

Enhanced Risk Distribution

Diversification across multiple chains reduces systemic risks associated with any single blockchain.

Improved Capital Efficiency

Users can utilize their cross-chain assets without needing to bridge them manually.

Conclusion

The Templar Protocol introduces a novel approach to decentralized finance (DeFi) lending and borrowing. Its core innovation lies in providing interest-free stablecoin loans, with access controlled by NFT ownership. This unique model creates a mutually beneficial ecosystem for both borrowers and lenders. The protocol distinguishes itself through several key features:

1. Configurable loan parameters, allowing for flexibility in collateral ratios, borrowing limits, liquidation thresholds, and more.
2. NFT-based access control, enabling community-specific lending pools and incentives.
3. A novel yield mechanism derived from liquidation spreads, replacing traditional interest-based yields.
4. Integration with the NEAR Protocol, leveraging its scalability, user-friendliness, and multichain capabilities like Chain Signatures.
5. Implementation of differential privacy for enhanced security and user protection.

These features collectively position the Templar Protocol as a modular and innovative solution in the DeFi space, addressing key challenges of existing lending platforms while introducing innovative mechanisms for risk management and yield generation. By combining these elements, the Templar Protocol aims to create a more accessible, efficient, and secure decentralized lending ecosystem.

Disclaimer

The information provided in this litepaper pertaining to Templar is for general informational purposes only and is not a formal offer to sell or a solicitation of an offer to buy any securities, options, futures, or other derivatives related to securities in any jurisdiction. Nothing contained herein constitutes investment, legal, tax or other advice nor is it to be relied on in making an investment or other decision.

No regulatory authority has examined or approved of any of the information set out in this litepaper.