Aada Finance

Decentralized lending on Cardano

Aada Team

September 2022
Whitepaper v1.9.2

Abstract

While one might think that poverty results from rapacious financiers exploiting the poor, we believe it has much more to do with the lack of financial institutions, e.g., the absence of banks, not their presence. Only when borrowers have access to efficient loan networks can they escape the clutches of loan sharks, and only when savers can deposit their money in reliable banks can it be channeled from the idle to the industrious and from the rich to the poor.

Introduction

Lending as a service is not new. Lending originated during the XV century in Florence, Italy. The family of Medici, also known as the first bankers, opened their stool next to Cavalcanti palace in Florence. Shortly after starting, one of the Medici became the unofficial head of state of the Florentine republic. The riches accumulated by the family can only be outweighed by the wealth held by the current banking companies. Managing financial assets empowered the rich for centuries, from whom even the king of England had to get permission to go to war.

We at Aada believe we can reverse engineer the most profitable sector - banking. We seek to take the core function of first bankers and embed it into a code. In this regard, our ultimate goal is to leverage lending and borrowing and build it into a decentralized protocol owned by none and everyone.

Aada Finance V.1

Peer-to-Peer Lending And Borrowing on Cardano

The V1 dApp is an alpha version of Aada Finance's lending and borrowing protocol. The platform is built on the Cardano blockchain and enables users can lend and borrow Cardano-Native Assets (CNTs) in a peer-to-peer manner using the NFT bond strategy. The feature introduces a new way of Web3 lender-borrower interaction in the form of transferable and tradeable tokens representing the request and loan.

1. NFT bonds

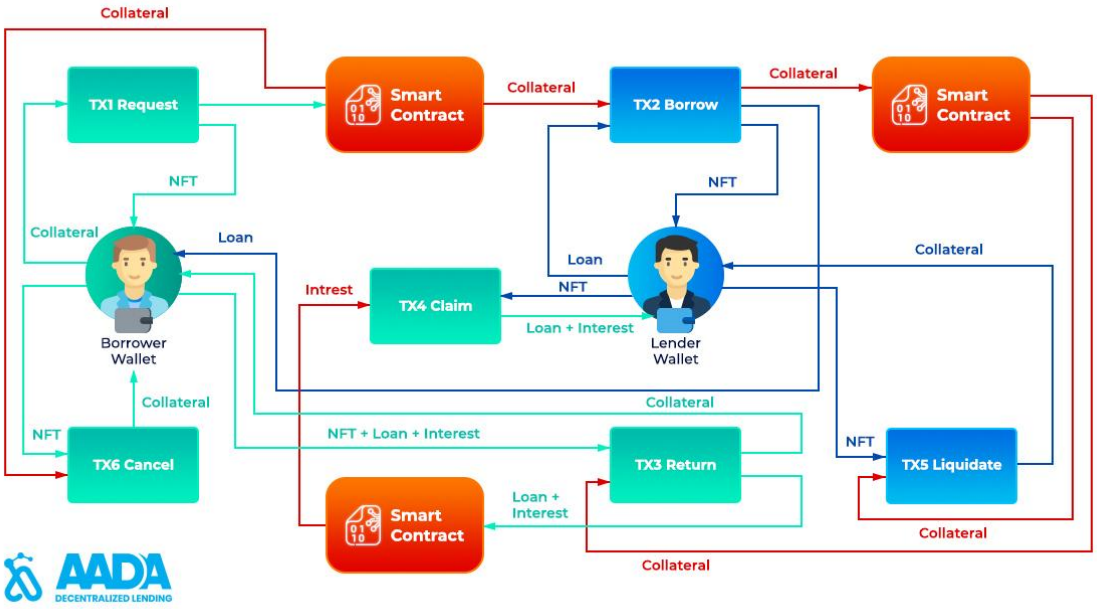
The protocol does not attribute loans to wallet addresses. Instead, it mints transferable, tradeable, and redeemable NFT bonds. This feature enables anyone holding a Lender NFT bond to claim a loan and interest. On the other hand, anyone with a Borrower NFT bond can redeem the deposited collateral.

An NFT bond walkthrough

2. How does V1 work?

Lending and borrowing on Aada works in a peer-to-peer manner. The user journey starts with a borrower who creates a loan request. This loan request locks the borrower's collateral[1] into a smart contract. It opens up the possibility of two scenarios:
a) The borrower can cancel the loan request and redeem the collateral.
b) The borrower finds a lender who supplies the loan.

[1] Collateral - is an asset deposited to a smart contract by a borrower. The collateral serves as an assurance of compensation in the event of borrower insolvency.



Aada V1 smart contract workflow

If the latter happens, the lender must send the loan amount to the borrower's wallet. Moving the collateral to a smart contract renders the borrower eligible to take it back only if the event of accurate repayment of the loan.

3. Are NFT bonds safe?

While they provide new use cases to the lending and borrowing concept, NFT bonds also enhance the protocol's safety. For instance, repaying a loan requires meeting either of the following conditions:

1. Burning the borrower NFT created at the time of the loan request
2. Repaying the loan and the interest

In other words, anyone holding the underlying bond can claim the collateral. As the NFT serves as proof of loan, its lack eliminates the possibility of unlocking the deposited assets.

NFTs are minted by using parameterized minting script and utilizing UTxO consumed at the time of the minting. This process allows a specific PolicyID pair to be created only once, leveraging the constantly changing UTxO reference.

4. Are NFT bonds superior?

The feature does not guarantee superiority. Nonetheless, it introduces a breakthrough approach to blockchain technology and DeFi. Some core NFT bond features include seamless on-top use of batchers and free debt movement within the State Machines.

Last but not least, the method aligns perfectly with Cardano's eUTxO fundamentals. It can easily be implemented within the Hydra scaling solution or continuous smart contract

versioning without any protocol issues. While it's yet to be tested in dynamic DeFi conditions, it fully embraces the principal concept of building on the Cardano blockchain.

5. Types of Liquidations

Liquidations are essential to lending and borrowing as they protect the lender from incurring dramatic losses. Aada ensures minimal lender risk by addressing two types of liquidation scenarios:

1. When the loan expires, and the borrower does not pay back the loan;
2. When the collateral value-to-loan drops significantly, which increases the risk of borrower insolvency;

5.1 Liquidations caused by loan expiration

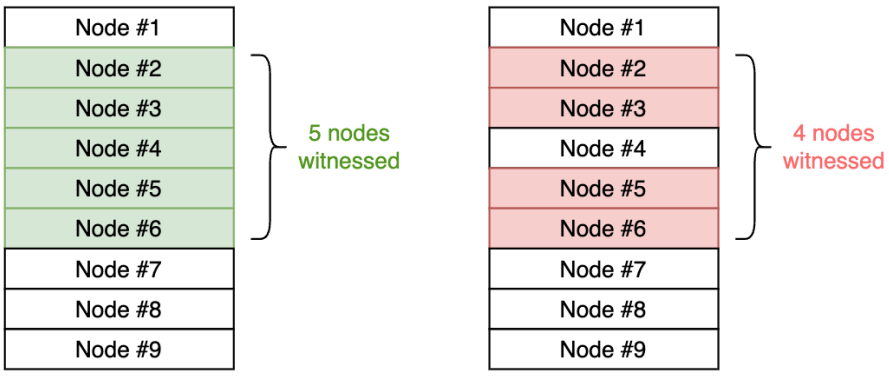
In the event of loan expiration - the lender is eligible to claim the whole collateral locked in the smart contract. The smart contract allows claiming the collateral only if the lender NFT bond is burned in the transaction.

5.2 Liquidations caused by price downfall (Oracle)

If the collateral value drops significantly, the lender becomes eligible to claim the borrower's collateral entirely or partially. Oracles are introduced to calculate the fraction of collateral required to compensate the lender and whether it can be liquidated off-chain.

The Liquidation Oracles constitute multiple distributed nodes. They are incentivized to operate fairly and continuously over time.

The borrower can choose any liquidation oracle they want at the time of loan request. However, the Aada client will support the multi-sig Aada Oracle. This oracle operates as a multi-sig minting policy where more than half of the oracle nodes must agree on executing a liquidation transaction.



Left - liquidation is successful; right - liquidation can't happen

6. Aada V1 Liquidation Oracle - A Technical Breakdown

The current Aada protocol design puts a lot of trust on Oracle nodes predetermined at the request submission (a.k.a Loan request). It assumes that Oracles not only perform accurate price checks but will continue to do so as long as the loan is active. It turns out the latter is much harder to assure.

6.1 Decentralization as a scale

We must make concessions between non-coercion(decentralization) and centralization (dominance).

Decentralization is the scale, not the True or False.

Centralization or dominance helps to have control and order. In such an environment, progress is more manageable, and the future is predictable. However, establishing the free market concept in a centralized environment is impossible. In such cases, liberty is limited.

On the other hand, decentralization is the freedom we are all here for. A trustless environment enables the privilege of choice and independent qualities. Decentralization is an end game for crypto and an end game for society. Nothing less than that should ever be accepted.

6.2 The problem with the Aada Liquidation Oracle solution

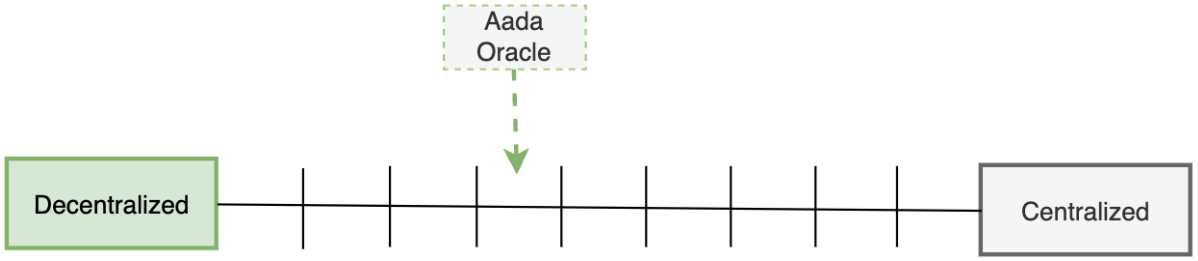
The main problem Aada has to solve is that the protocol needs to put its trust in an oracle.
First, we must trust that our nodes will always be fair and accurate. Secondly, the nodes will operate faithfully without disruptions for as long as Aada exists.

Compared to other networks where oracles are persistent and verified (i.e., Ethereum and Chainlink), Cardano does not yet have the oracle Aada could rely upon. Building an oracle and its incentive systems is as complex as building a Lending/Borrowing protocol.

6.3 The Cardano way

As Cardano started with the Byron era (centralization) and moved towards the Shelley era (decentralization) and one day will end up in the Voltaire era.
Similarly, Aada's Liquidation Oracle will start on the more centralized side of the scale and will move towards decentralization over time.

The one crucial factor is that the Oracle will be effectively decentralized, so there is no single point of failure nor one party that could purposely misbehave. One could see the approach as a 'Batcher' or a 'Scooper' when specific actions depend on the smaller group.

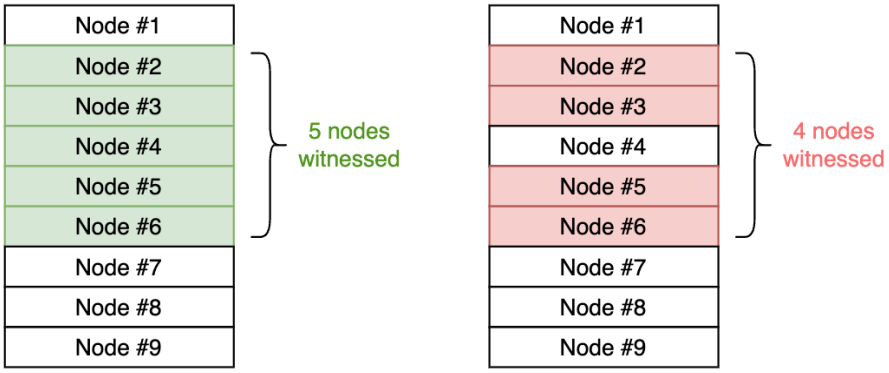


The Liquidation Oracle will be decentralized, so it's not controlled by one party.

6.4 The Aada Liquidation Oracle design

As mentioned previously, decentralization is a scale. It is not 1 or 0. Therefore, it's safe to assume that the Oracle design is closer to 1 (decentralized) than 0.

To make it work in motion, the Aada Liquidation oracle will be built out of 9 nodes. These nodes will be responsible for witnessing correct liquidation transactions. If enough nodes witness the transactions - the lender will be able to liquidate the loan. The consensus is that five nodes out of nine have to witness the transaction for liquidation to happen.



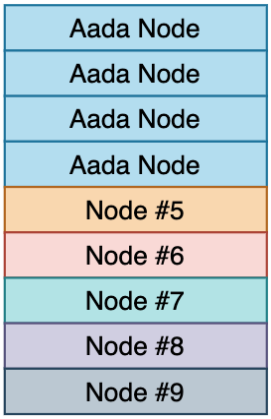
Successful liquidation *Failed liquidation.*

6.5 The Nodes

The perfect decentralization would consist of nine distributed nodes. In reality, this is possible only when these nodes have their operations in place, and an assurance of continuity is present.

Well-distributed Liquidation Oracle Nodes

To mitigate the risks of continuity disruption, the Aada Liquidation Oracle plans to start with four controlled nodes, reducing the number over time.



Current Liquidation Oracle Design

Four nodes are enough to mitigate the risk of discontinuation while still not being able to act on their own. In short, Aada won't be able to liquidate any loans without another node's approval.

The risk the protocol takes to assure proper implementation of the concept vastly outweighs its temporary dominance. In the event of an external attack on the users' funds - Aada is the one that will suffer the most. At the same time, all other nodes are safe from such risk. Ultimately, a loss Aada could suffer will never exceed the gain it can make from an improper liquidation.

7. The AADA token

7.1 Voting

The AADA token's primary aim is to empower the community to take the principal role in decision-making. All token holders are eligible for a say in the improvement proposals in the on-chain governance.

7.2 Liquidity farming

Liquidity farming is a must-have incentive that aims to ensure minimum price fluctuation for the AADA token. The goal can be achieved through double-reward incentives where users can farm AADA tokens by providing liquidity on major Cardano DEXs. By increasing the token's liquidity, the protocol will safely utilize AADA as **Collateral** on the V.1 dApp. Meanwhile, trading AADA will be more efficient and secure minimum slippage rates.

7.3 Staking

The **Staking** feature was one of Aada Finance's incentives for the protocol's long-term supporters. It allowed users to earn AADA using the native dApp.
The protocol opened two staking pools - one with a 6-month and a 12-month lock period. They gave users a high APR of 12% and 20%, respectively.

Users who staked and locked their AADA in the staking pools can view their positions by visiting the **STAKING** tab in the top right corner. Each staking position can be viewed only by the address holding the proof-of-stake NFT.

8. Governance

The Aada Finance on-chain governance allows improving the protocol with unique features and upgrades with the approval of AADA token holders. By empowering project supporters to participate in decision-making, Aada Finance fulfills its concept of becoming a community-driven lending protocol.

8.1 Decision making

Engaging the community through on-chain governance optimizes the protocol's ability to adapt to changing market conditions. Moreover, it makes core upgrades transparent and easier to implement. However, it must first go through an off-chain discussion on the **Aada Governance Forum**. The entire process of proposing and implementing protocol improvements involves three primary steps:

1. Bootstrapping an **Improvement Discussion**
2. Submitting a formal **Improvement Proposal**
3. On-chain voting

Implementing each **Improvement Proposal** takes place after the voting ends. A proposal is approved only if it receives 51% or more **Yes** votes. All votes that pass successfully face implementation shortly after their conclusion.

8.2 Governance voting

Voting on each proposal relies entirely on the protocol supporters and is executed via app.aada.finance. AADA token holders receive governance power proportional to the sum of their AADA balance.

1 AADA = 1 Voting Power

Governance voting can include multiple proposals, allowing users to have a say in several proposals within one transaction. The voting lasts 1 epoch (5 days) and costs ~0.20 ADA (network transaction fee).

The **Voting Power** estimation includes staking bonds and liquidity farming tokens. However, determining the exact AADA balance in liquidity pools might result in slight miscalculations due to price fluctuations.

Example: Voting power 100 = 20 AADA + 20 staked AADA + 60 AADA in a DEX liquidity pool.

9. NFT Bond Marketplace

We see NFT Bonds as tradable decentralized securities. In the mature market, one could use an NFT Bond to hedge against or enhance their long/short positions. Therefore, we

commit to enabling users to swap their NFT bonds with other market participants. To achieve this, we will provide an open-source tool and API to query NFT bond details from the Cardano Node and validate it.

However, as an MVP, we will enable NFT marketplaces to consume data and allow users to trade NFTs. We will decide when to build an in-house NFT marketplace based on usage and user behavior.

10. Other features

10.1 Health factor

The **Health Factor** is the numeric representation of the safety of the supplied assets against the borrowed assets and their underlying value. The higher the value, the safer the state of the funds are against a liquidation scenario. If the health factor reaches the liquidation threshold, liquidation is triggered.

$$Health\ factor\ = \frac{Collateral/(Loan + Interest)}{Liquidation\ Threshold}$$

The **Health factor** is the **Collateral** divided by the sum of the **Loan** and **Interest**, all divided by the **Liquidation Threshold**.

10.2 Liquidate and swap

The **Liquidate and swap** function allows users to swap collateral for the initial token used as a loan. If liquidation is possible, the user can initiate the **Liquidate** function from the **Dashboard** tab and choose the **Liquidate and swap** option.

The protocol will allow the lender to select the DEX to perform the collateral swap without leaving the Aada Finance dApp.

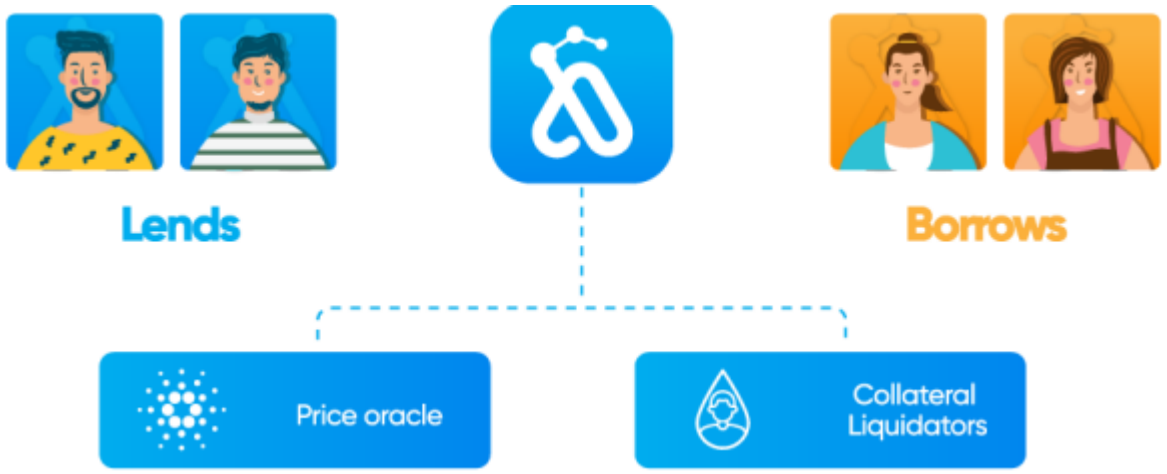
10.3 Multi-asset borrowing

Multi-asset borrowing is a feature that enables users to utilize their funds creatively and openly. In other words, the **Loan**, **Collateral,** and **Interest** assets can be different. In the event of liquidation, the lender can use the **Liquidate and swap** feature to homogenize the collateral with the lent asset.

Aada Finance V.2

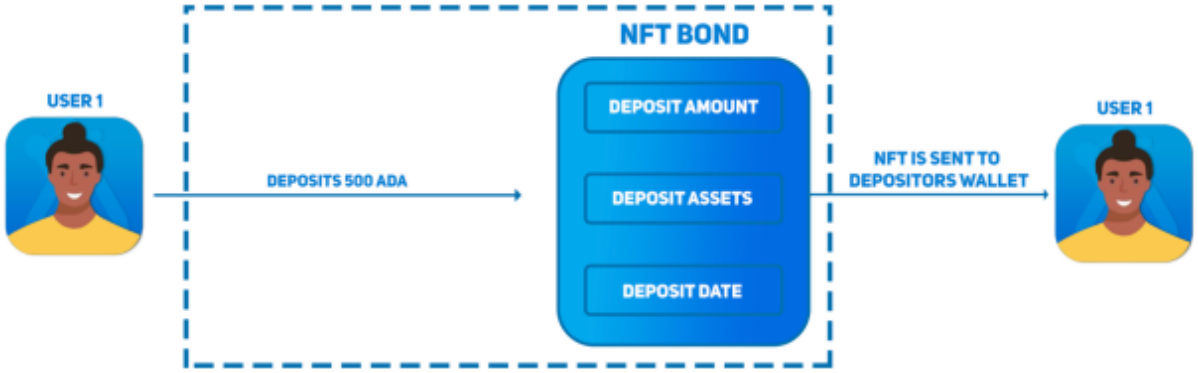
Pooled Lending And Borrowing Using NFT Bonds

The Aada Finance V.2 protocol will introduce more complex mechanics that allow pooled lending and borrowing using the NFT bond strategy. Users will be able to take and supply loans without loan maturity while maintaining their ability to transfer, redeem and trade their bonds at any time. The following element aims to enhance the DeFi possibilities on Cardano.

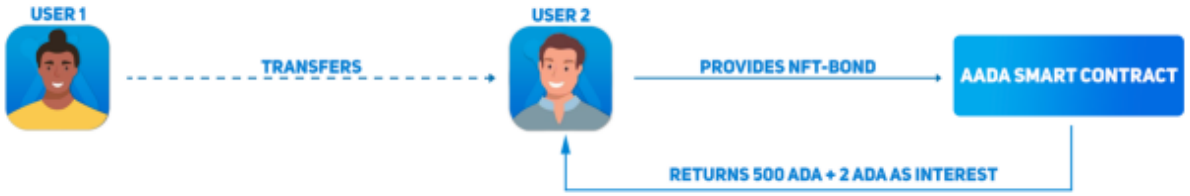


1. NFT bonds and pooled lending and borrowing

When a lender deposits assets into the Aada protocol, the latter mints a new NFT bond as a representation of the deposit.



Anyone holding the NFT bond has the right to redeem the deposit. This means a deposit can be transferred.



Same way for borrowers. The initial borrower (who also deposits collateral) creates an NFT bond representing the loan and the deposit.

This means anyone bearing the NFT can redeem the initial deposit by:
1) Repaying the loan
2) Providing the NFT bond as a right to claim the deposit

In other words, Aada is an intermediary between the **Lender** and the **Borrower** by minting NFT bonds with each interaction. **Lenders**, also known as depositors, pool their assets into the smart-contract controlled pool. These assets can be borrowed at any time by a borrower. On the other hand, **Borrowers** have to pay an interest rate automatically calculated through asset utilization.

A low utilization rate means the underlying asset is left unused, resulting in lower interest rates for depositors and borrowers. However, when a specific asset is in demand and the utilization rate is high - interest rates will grow. Such events can result in fewer assets borrowed (due to higher prices) while attracting more depositors seeking high returns on their deposits.

2. Stability and utilization rate

2.1 Utilization rate

Utilization rate is an essential factor in calculating interest rate. It also drives liquidity up or down depending on the amount of assets available to borrow.

The **Utilization rate** is calculated as follows:

$$U = TotalBorrows \,/\, TotalLiquidity$$

U monitors which share of the reserve's total capital is borrowed at time t. As **U** gets closer to 100%, the capital becomes scarcer until no more liquidity is available.

When U = 100%, this situation can be problematic because depositors will face a lack of withdrawable funds.

Still, high utilization results in high returns for depositors. Therefore, maximizing utilization while protecting liquidity is essential for proper utilization. The interest rate model is calibrated around an optimal utilization rate $Uoptimal$ per reserve that reflects market conditions. $Uoptimal$ can be determined by looking into the historical **Utilization rate**.

Historical data will help to determine the market conditions and calculate the most optimal rate for the borrowers.

2.2 Borrow interest rate

Aada's **Interest rate** aim is to manage liquidity risk and optimize the **Utilization rate**. The borrow interest rates come from the **Utilization Rate** (**U**). **U** is an indicator of the availability of capital in the pool. The **Interest rate** is used to manage liquidity risk through user incentives:

- When capital is available: low-interest rates encourage more loans from borrowers;
- When capital is scarce: high-interest rates encourage repayments of loans and more deposits from lenders.

Interest rate model

Liquidity risk appears when utilization is high. It becomes more problematic as U nears 100%. To tailor the model to this constraint, the interest rate curve is split into two parts around an **Optimal Utilization rate** ($Uoptimal$). Before $Uoptimal$, the curve is slight, followed by a sharp increase.

The interest rate Rt follows the model:

$$if\ U < U_{optimal}: \qquad R_t = R_0 + \frac{U_t}{U_{optimal}} R_{slope1}$$

$$if\ U \geq U_{optimal}: \qquad R_t = R_0 + R_{slope1} + \frac{U_t - U_{optimal}}{1 - U_{optimal}} R_{slope2}$$

2.3 Deposit APY

The borrow interest rates paid are distributed as yield for NFT bondholders who have deposited in the protocol, excluding a share of yields sent to the ecosystem reserve defined by the reserve factor. This interest rate is paid on the capital lent out and then shared among all the liquidity providers. The **Deposit APY** (Dt) is:

$$D_t = U_t(SB_tS_t + VB_tV_t)(1 - R_t)$$

- U_t, the utilisation ratio
- SB_t, the share of stable borrows
- S_t, the average stable rate
- VB_t, the share of variable borrows
- V_t, the variable rate
- R_t, the reserve factor

3. Governance

3.1 Voting rights

To vote, you need to hold AADA in your wallet or stake AADA tokens in the Aada Safety Module. Additionally, we do want to provide higher vote weight to users who are providing liquidity on DEX pools. This would put Adaa's future into the hands of people who care about the protocol's success.

3.2 Voting threshold

The threshold is dynamic and can change depending on the quorum plus the difference in votes for and against a proposal. If there are only a few votes against a proposal, the threshold will not change.

However, if the number of votes against the proposal is significant, the threshold can be raised so that there must be more votes in favor of the proposal. This is done to ensure that a proposal receives widespread approval before implementation.

For example:
If the quorum is 30%, the differential is 25%, and 3% of the total votes are against the Proposal, the threshold would remain at 30% (because 25+3 = 28 < 30).

If the quorum is 30%, the differential is 25%, and 6% of the total votes are against the Proposal, then the threshold would be raised to 31% (because 25+6=31), so more "yes" votes would be required for the Proposal to pass.

3.3 Aada Improvement proposal (AIP)

AIP is an acronym for Aada Improvement Proposal, just as BIP stands for Bitcoin Investment Proposal. The AIPs set out the technical standards (protocol specifications, contract standards, client APIs, etc.) for the Aada protocol.

4. The AADA token

4.1 Staking

Staking incentives

Stakers within the **Safety Module** receive **Safety Incentives**. The initial SI rewards are [750 AADA/day + collected platform fees] to be split between the stakers. The **Safety Incentive**'s allocation quarterly date should be voted on before the end of the 3 months (90 days) distribution schedule.

In the case of a late or no vote on a new SI allocation plan, the current allocation will continue until a vote or until the Aada Reserve is empty.

4.2 Risk of staking

In the case of a shortfall event, the Safety Module uses up to 30% of the assets locked to cover the deficit.

Shortfall event

The primary role of the **Safety Module** is to protect the protocol against unexpected loss of funds stemming from:

- **Smart contract risk:** On the smart contract layer, there is a risk of a bug, a design flaw, or a potential attack.
- **Liquidation risk:** The risk of an asset failing that is being used as collateral on AADA; the risk of liquidators failing to capture liquidation opportunities promptly; or the risk of the principal asset being repaid having low market liquidity.
- **Oracle failure risk:** Risk of the Oracle system failing to properly update prices in the event of a severe market downturn and network congestion; risk of the Oracle system failing to properly submit prices, resulting in improper liquidations.

In a shortfall event, the **Safety Module** will use up to 35% of the capital delegated as a pledge. Recovery issuance occurs if the seized SM assets don't cover the total debt. The drawn SM amount and the issued AADA go toward covering the deficit.

The 35% rate and all related variables are subject to reduction, increase, and alteration via an AIP.

5. Other features

5.1 Price oracles

Price oracles will help to calculate the **Health Factor,** which might trigger liquidation. Prices will be queried from Chainlink, Charli3, and/or other Oracles. However, a Liquidation Oracle might also come in use. The following will be built and maintained by the Aada team.

5.2 Liquidation oracle

NFT bonds are liquidated off-chain when the loan **Health Factor** reaches 1. Since Aada can’t alter the value of the bonds, it uses the Oracle system to identify if the loan and its deposit have been liquidated.

5.3 NFT bonds

For liquidity providers, the Aada protocol provides an NFT bond strategy. Upon deposit, the depositor receives an NFT bond with details of the deposit. After a successful deposit, the NFT bond is minted and sent to the depositor's wallet. This NFT is transferable as any other NFT meaning that anyone who holds the NFT can claim the initial Deposit. The bond has the right to claim only the deposit created at the time of NFT minting.

In the case of the loan, an NFT bond is minted. However, the user can only retrieve its deposit if the loan is returned. The NFT bond concept creates a secure market method of

presenting a deposit's value. Anyone providing the NFT can retrieve the initial deposit from the Lender or the Borrower. However, the borrower's NFT bond requires returning a pledge.

The concept of interest rate redirection is also naturally implemented in the Aada protocol. The accumulated interest sum can be checked off-chain using the platform. The value gained over time by the borrowers' interest rate payments is, in fact, distinct from the principal value. The interest stream is the continual flow of accrued interest over time.

To implement the NFT bond strategy, Aada introduces the following concepts:

1. **Deposit balance** - The value that is deposited to the liquidity pool;
2. **NFT bond** - This NFT is the right to claim a deposit. Whoever owns the NFT can claim an initial deposit;
3. **Interest rate oracle** - The Oracle allows finding accumulated interest over time;
4. **Liquidation oracle** - In the event of liquidation, the NFT becomes inactive and can't be used to redeem the deposit.

Limitations of the tokenization model

Compared to the aToken approach, the NFT bond model described here has numerous advantages, but it also has some disadvantages, including the following:

- Accumulated interest can only be found using off-chain code;
- After an event of liquidation, the user still holds the NFT even if redeeming the initial deposit is impossible.

5.4 Liquidations

Liquidation is a process that occurs when the loan **Health Factor** goes below 1. It will trigger whenever the collateral value cannot cover the loan/debt value. This might happen when the collateral decreases its value or the borrowed debt increases in value.
The **Collateral** vs. **Loan value** ratio is shown in the **Health Factor**. In a liquidation, up to 50% of the borrower's debt is repaid. That value + liquidation fee is taken from the available collateral.

5.5 Health Factor

For each Loan (NFT bond), these risks parameters enable the calculation of the **Health Factor**:

$$H_f = \frac{\sum Collateral_i \; in \;\; ADA \times Liquidation \, Threshold_i}{Total \; Borrows \; in \;\; ADA}$$

When the **Health Factor** is less than 1 (more assets borrowed than deposited), the loan may be liquidated to maintain solvency, as described in the diagram below:

Risk Parameters Safeguard Solvency

6. Is there any risk?

No platform is entirely risk-free. The smart contract risk (the possibility of a flaw in the Haskell code) and the liquidation risk are two dangers that must be considered at all times. To reduce the risk to the greatest extent possible, the Aada team will conduct a thorough external audit before deploying the V.2 code on mainnet. In addition, there will be a bug bounty program that will be active at all times.

7. Tokenomics

Supply

29,500,000	Distributed	Percentages	Initial release	Cliff (months)	Price	Vesting (months)
Strategic Partners	2,000,000	6.78%		4		12
Private Round	5,500,000	18.64%	25.00%	1	$0.20 - $0.30	9
Public Round	1,250,000	4.24%	100.00%	0	$0.35 - $0.45	1
Core Team	3,000,000	10.17%		6		24
Public distribution	4,000,000	13.56%		4		9
Marketing and referral	1,500,000	5.08%		0		9
Advisors	1,000,000	3.39%		3		9
Staking and governance	10,250,000	34.75%		6		18
Token liquidity	1,000,000	3.39%	100.0%	0		1
	29,500,000	100%				

You can find more information about the protocol in the Gitbook Documentation.