Author(s): David Krett (@dbkcan) Contributors: Henrique Barcelos (@hbarcelos) MIP6 Reference: https://forum.makerdao.com/t/mip6-huntingdon-valley-bank-loan-syndication-collateral-onboarding-application/14219/25

This assessment deviates from the standard smart contract technical assessment format because of the idiosyncratic nature of the RWA collateral type.

Risk Summary/Key Takeaways

- The technical smart contract risk is considered LOW

, as it will be using the standard MIP21 contracts with a manual liquidation oracle.

- Whilst technical risk is considered low the proposed solution requires manual/human monitoring of off-chain data, which will require that there are clear processes in place for monitoring the ongoing performance of the collateral based on the reporting required by the various Actors involved in running the RWA Master Participation Trust, as all liquidation activities will require a governance vote.

- Any technology or service required for the off-chain upkeeping of the deal will be the responsibility of the @Real

World Finance

(RWF) Core Unit. Below there is non-exhaustive list of the RWF responsibilities:

- Perform the off-chain monitoring of the deal to ensure the debt funded up to the debt ceiling is no greater than the funding provided under purchased participations and the balance of the participation funding account held by RWA Master Participation Trust (RWA MPTrust

).

- Provide or hire the infrastructure for storing the relevant documents off-chain.

- Perform the off-chain monitoring of the deal to ensure the debt funded up to the debt ceiling is no greater than the funding provided under purchased participations and the balance of the participation funding account held by RWA Master Participation Trust (RWA MPTrust

).

- Provide or hire the infrastructure for storing the relevant documents off-chain.

- As a result the technical assessment of these monitoring services is not in scope for this technical assessment.

- Should MakerDAO wish to scale up this solution beyond the contemplated debt ceiling of DAI 100 million, CES recommends that modifications to the MP21 contracts and/or protocol contracts be considered to bring more transparency on chain with respect to the status of the investment at any point in time.

General Information

Symbol:

RWA009

Token Name:

RWA-009

Ilk Registry Name:

RWA009-A: HVBank

Relevant MIP Information:

- MIP6: Huntingdon Valley Bank Loan Syndication Collateral Onboarding Application

- MIP21: Real World Assets – Off-Chain Asset Backed Lender

- RWF / LTS Huntingdon Valley Bank (“HVB”) - RWA Collateral Onboarding Risk Assessment

Total Supply:

1 WAD (1 * 10 ^ 18)

HV Bancorp Inc. website:

https://www.myhvb.com/

Github Repository:

GitHub - clio-finance/mip21-toolkit: MIP21 Toolkit: Equipment for Off-chain Asset Backed Lending in MakerDAO

Collateral Type Adapter:

The collateral will use the MIP21 authed join and exit functions.

Technical Information

Implements ERC20 Token Standard:

Yes

Compiler Version:

solidity:0.6.12

Decimals: 18

Overflow checks:

Mitigation against overflow race-condition:

No

Upgradeable contract patterns:

No

Access control or restriction lists:

No.

Non-standard features or behaviours:

No.

Key addresses:

- The auth governance address for RwaLiquidationOracle and RwaUrn contracts.
- The operator address that is permitted to operate on the RwaUrn contracts. This can be multiple addresses, however, each address must be approved by governance.

Additional notes:

- The RWAToken uses a custom implementation of SafeMath. While there is no mitigation against the allowance race-condition, the idiosyncratic nature of the contract does not make them a requirement.

Transaction Outline

- The ERC20 Token will act as a single token placeholder for up to 100 million USD or the agreed debt ceiling of real world loan participation certificates (Participations

) to be sold by HV Bancorp Inc. (HVBank

)

- This ERC20 Token will act as a placeholder for the collateral to be held by MakerDAO's trust - RWA MPTrust

. This real world collateral will be held by WSFS Bank - RWA MPTrust's

trustee. The collateral held at any point in time will consist of:

1. The trust's Participation Funding Account (PFA

) - which will be allowed to invest funds in US Government short term securities; and

1. The trust’s Authorized Investments Income Account (AIIA

) - which will collect all income earned from the investment of the PFA in short term government securities; and

1. The trust’s Participation Receipts Account (PRA

) - which will hold the monthly or regular remittances from HVBank

for both income/fee and debt repayments received from the loans underlying the Participations purchased by RWA MPTrust

; and

1. Participation certificates purchased by RWA MPTrust

from HVBank

.

- The trust’s Participation Funding Account (PFA

) - which will be allowed to invest funds in US Government short term securities; and

- The trust’s Authorized Investments Income Account (AIIA

) - which will collect all income earned from the investment of the PFA in short term government securities; and

- The trust’s Participation Receipts Account (PRA

) - which will hold the monthly or regular remittances from HVBank

for both income/fee and debt repayments received from the loans underlying the Participations purchased by RWA MPTrust

; and

- Participation certificates purchased by RWA MPTrust

from HVBank

.

At any point of time the sum of the funds 1) in the PFA and 2) funds outstanding on the participation certificates above will not exceed the debt ceiling established by MakerDAO (under the assumption that the principal portion of any funds from the Participation Receipt Account have been moved to the PFA).

- Participations

will be sold by HVBank

to the trust (RWA MPTrust

) established for the benefit of MakerDAO and will be held by WSFS

- as trustee for RWA MPTrust

. Participations will be purchased from HVBank

over a 12-18 month period and funded from the PFA

. The PFA

will be initially funded by minting 100 mm DAI upon governance approval and moving the converted US$ to the PFA

.

- On or before each purchase of a participation – the Calculation Agent - Ankura Trust Company LLC (Ankura

) - will complete any necessary due diligence and will deliver and upload to off-chain storage and to RWA MPTrust

verifying the proposed participation purchase meets the criteria detailed in the Master Participation Agreement

. Upon receipt of the certification report and the relevant executed participation certificate RWA MPTrust

will instruct WSFS

to pay HVBank

from the PFA

any amounts required to fund the purchased participation.

- As and when funds are received from the underlying loans of a Participation, HVBank

will send RWA MPTrust

's proportionate share of remittances to the WSFS

trustee account (PRA

). On a monthly basis, HVBank

will provide a report to Ankura

detailing the remittances made to the WSFS

trustee account, including a split of the amounts of principal and interest or fees comprising the aggregate amount.

- Any debt repayments for the underlying participations will be transferred to the PFA
- controlled by the Trustee

to either fund future participation purchases and/or to provide funding that may be required under existing participations held by the RWA MPTrust

.

- Any income/fees received under the Participations in the PRA

(net of servicing costs) will be sent on a monthly basis to the Surplus Buffer.

- Funds in the Trusts' investment income account (AIIA

) will be sent bi-annually to the Surplus Buffer. The funds in this account are generated from the short term investment of funds in the Trust's Participation Funding Account

. A result of the Trustee's standing instructions to invest "idle" cash on deposit in the accounts in "Authorized Investments

" (to be defined as "an exchange traded fund or money market fund composed of United States treasury securities with a term of three (3) months or less).

- Upon termination of the Master Participation Agreement the monies in the PFA
- invested in short term govt securities, less any amounts required to fund participations which have not yet expired - will be paid to the urn. In addition, any debt repayments received on an ongoing basis up to the maturity date of each individual participation - will continue to be received in the PRA

and on a monthly basis will be transferred to the urn, with any associated income/fee remittances from the underlying loans continuing to be paid on a monthly basis to the surplus buffer.

- As the loans underlying participation will have different terms (revolving loans, amortizing term loans) and rate basis (some fixed and some floating), the expected yield due to Maker is variable, making it difficult to set a constant stability fee. As such, the actual monthly variable net yield from participations will be paid directly to the surplus buffer. Monthly servicing reports, reporting income collected per participation and by principal and interest divisions, will determine whether the participations in RWA MPTrust

are in compliance with the terms contemplated in the Master Participation Agreement.

Sequence diagrams for the above transactions outline are detailed below.

Initial Funding/Purchases of Participations

[

1314×719 80 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/d/c/dcb41af350efd3025bbef0242bddb69fae486676.png)

Monthly Remittance of Payments and Reporting/Debt Repayments[

1401×733 105 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/9/4/944bcb7beff42fc25089391884ae92fc47166ea7.png)

Liquidation/Losses

- Events of default that occur within the facility will be reported by the Calculation Agent through the uploads of monthly data. Liquidation of the HVBank vault will need to be triggered manually by someone in MakerDAO proposing a governance vote to initiate liquidation (tell()

spell).

- Write-Offs for participations will be recognized off-chain, and the amount of maximum participation funding adjusted and reported accordingly in the monthly report to be completed by Ankura

the verification agent. Any on-chain write-offs will be recognized after the final participation repayments have been made to the RwaUrn. We understand that in the event there is debt to be written off, after all debt repayments have been received, RWA Foundation

will be responsible for taking the necessary governance approvals to cull() any written-off debt that remains outstanding after final repayments have been received.

Emergency Shutdown

- In the event of Emergency Shutdown we understand that RWA Foundation

(the trust sponsor and entity responsible for executing MKR tokens holders governance decisions) will be responsible for ensuring that the RWAJar and RWAUrn contract addresses are updated with Genesis

, such that payment can continue to be received for any successor deployments or DAI token holders repayments.

Architecture

MIP21 Contracts

For onboarding the HVBank

Collateral we will be using the MIP21 standard contracts which disables automatic liquidation of the vault and ensures that the borrower is prevented from minting more DAI than the Debt Ceiling (line). Any liquidation of the vault would require that Maker Governance trigger a liquidation.

For the proposed HVBank

implementation, we will be using the following MIP21 contracts:

- RwaToken
- RwaUrn
- RwaLiquidationOracle
- RwaJar - a new smart contract that will allow any fees earned on the participation to be remitted directly to the Surplus Buffer on a monthly basis.

With the following MIP21 proscribed spell used for the initial deployment of the collateral and to facilitate manual liquidation of the collateral in the event of a default:

- RWA Onboarding Spell

The spell will lock the ERC20 token into the RWAUrn. As this token is solely acting as a placeholder for the actual Participation certificates – physically held by the Trust – and automatic liquidation has been disabled, the on-chain value that will be reported will be the debt ceiling of $100mm. The actual value of the collateral can only be determined based on the uploaded participation certificates and on-going reports from the Calculation Agent detailing the balances in the Trust's various accounts and the funding that has been provided at any point in time for the Participations held and maintained by the RWA MPTrust

.

Some modifications will be required to the standard MIP21 implementation. Specifically, to accommodate the preference to structure this transaction with the Stability Fee set to 0 with monthly remittances of interest and fees to be paid monthly directly to the Surplus Buffer - these modifications are facilitated through the RwaJar contract.

MIP21 Modifications Required to Facilitate the Transaction

Based on the transaction outline and term sheet provided by @Real

World Finance, modifications will be made to the MIP21 standard technical arrangements to accommodate the fact that on a monthly basis – and until the expiration of the Master Participation Agreement – the payments detailed below will be paid to the Surplus Buffer:

1. The portion of monthly remittances from HVBank

paid to the PRA

, representing income from the underlying loan participations (net of waterfall expenses); and

1. Any investment income earned in the trust's investment account (AIIA

) which will be sent to the Surplus Buffer bi-annually…

It should be noted that until expiration of the Master Participation Agreement, on a monthly basis, the monthly remittances received in the PRA

, representing debt repayments for the loans underlying the Participations will be swept to the Trusts' funding account (PFA

), to fund existing and new participations.

After expiration of the Master Participation Agreement, as existing Participations may not have yet expired and income and debt repayments will continue to be received until the expiry of the individual participations, any amount representing permanent debt repayments (as determined by the Calculation Agent) will be paid on a monthly basis to the urn.

To accommodate this, we have created a simple generic permissionless RwaJar contract containing a function void()

that allows the Trust on a monthly basis to repay income/fee remittances (DAI sent to this contract) directly to the surplus buffer. This module uses similar logic that MakerDAO Core Units are currently using to repay DAI to the Surplus Buffer. Given that this code is already widely used we do not believe that a contract audit will be necessary. This contract was reviewed by @Protocol

Engineering Core Unit to ensure that no incremental technical risk is incurred by the Maker Protocol who have approved this contract and are aligned with our assessment that no audit is required.

Summarized below is a summary of the MIP21 contracts which will be utilized.

RwaToken

Source code

An implementation of the ERC20 token standard, with the balanceOf(address) of the deployer of the contract being set to 1 WAD at deployment. There are 18 decimals of precision.

There are three state changing functions, that are all available to the token holder, and are specific to the ERC20 token standard:

There are three state changing functions, that are all available to the token holder, and are specific to the ERC20 token standard:

- transfer(address dst, uint wad) external returns (bool)

;

- transferFrom(address src, address dst, uint wad) public returns (bool)

;

- approve(address usr, uint wad) external returns (bool)

;

RwaUrn2

Source code

The RwaUrn is unique to each MIP21 collateral type. Aside from the core DSS wards, can, rely(address)

, deny(address)

, hope(address)

, and nope(address)

functions, there are five functions:

- file(bytes32, address)
- lock(uint256)
- free(uint256)
- draw(uint256)
- wipe(uint256)
- exit(uint256)

The file

function can only be called by governance (via the auth

modifier)

The rest of the functions can only be called by those who have been given the operator

permission (hoped

or noped

) on the RWAUrn contract. And any Dai drawn by the RwaUrn2 can only be sent to the outputConduit address defined by governance when deploying the contract.

RwaLiquidationOracle

Source code

The RwaLiquidationOracle contract consists of six state-changing functions (besides the usual DSS rely(address)

, deny(address)

), all protected by the auth

modifier and can only be called by governance:

- file(bytes32, address)
- init(bytes32 ilk, bytes32 val,address doc,uint48 tau)
- bump(bytes32 ilk,uint256 val)
- tell(bytes32)
- cure(bytes32)
- cull(bytes32)

There is one externally accessible view function called good(bytes32)

that anyone can use to check the liquidation status of the position. This function does not change contract state.

This is not a typical Maker oracle. It will only report on the liquidation status of RwaUrn2

, and can only be acted upon by governance. To state it plainly, this oracle is not vulnerable to flash loan attacks or any manipulation aside from a governance attack.

file

can be called by governance to change the vow address (used in cull

).

init

is the initialization function. It takes 4 parameters:

- ilk

: name of the vault, in this case, RWA009.

- val

: estimated value of the collateral token.

- doc

: link to legal documents representing the underlying legal scheme.

- tau

: minimum delay between the soft-liquidation and the hard-liquidation/write-off. It should be noted that for this transaction tau will be set to 0 so no soft liquidation will be possible.

bump

can be called by governance to increase the estimated value of the collateral.

tell

can be called by governance to start a soft-liquidation.

cure

can be called by governance after a soft-liquidation has been triggered to stop it.

cull

can be called by governance to start a hard-liquidation/write-off. This will mark all the remaining debt of the vault as bad debt and impact the Surplus Buffer (vow

).

RwaJar

Source Code

The RwaJar contract is a permissionless contract which contains the following functions:

1. a function void()

which will transfer any DAI balance contained in the contract to the current vow address, obtained directly from the DSS on-chain change-log (chainlog).

1. A function toss(uint256 wad)

which will pull the specified amount of DAI from the sender’s wallet to the current vow address, obtained directly from the chainlog. This function requires that the RWAJar contract has been previously approved by the msg.sender to transfer the specified amount of DAI.

1. The relevant DaiJoin and DAI addresses that this contract references are immutable after the deployment – so there is no risk that the RWAJar will send DAI to a fraudulent account address or that it will mistakenly take any other token as if it was DAI.

As indicated above, this contract has not been audited but duplicates logic contained in a commonly used smart contract by MakerDAO, used for returning unused Core Unit budgets to the Surplus Buffer. This contract has full test coverage and has been approved and reviewed by @Protocol

Engineering who is in agreement that an audit of this contract is not required.

Overview of technical setup and actors

The following diagrams detail the proposed high level technical setup in terms of the different flows that will occur for funding of the participations and the remittance of regular monthly debt, interest, and fee payments for the underlying loans (Maker smart contracts in Orange, and the involved actors in gray).

NOTE: STEP 1 OF THE TECHNICAL IMPLEMENTATION HAS BEEN UPDATED PLEASE SEE IN THE THREAD BELOW → ADDENDUM TO INITIAL RISK ASSESSMENT - CHANGE IN DRAW DOWN IMPLEMENTATION - these modifications will not change any of the contracts used in the implementation solely the execution of the spell - such that no draw from the urn will be greater than 25MM DAI

1. ## Post Governance Approval/Post Spell

[

1600×1132 203 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/d/d/dd2caa54aff19da340f6e19282747f3b60550ebe.jpeg)

Immediately after approval by executive vote of the spell the RwaToken will be deployed using the RwaToken factory contract and 1 RwaToken will be minted and transferred to the MCD_PAUSE_PROXY and act as a placeholder representing the participation certificates and trust's investment account balances, which at any point in time are being held by RWA MPTrust

.

The spell will be cast with the following parameters:

- Debt Ceiling: 100_MILLION_DAI
- Stability Fee: ZERO
- Liquidation Ratio: 100
- MCD_PAUSE_PROXY (Maker Governance) will be permissioned as the operator of the RWAUrn to facilitate the draw of DAI at the time the spell is cast

The code for the spell will then transfer the RWAToken (RWA009) and will draw (mint) $100 million Dai to the RWA Foundation account at Genesis

. RWA Foundation

will provide instructions to Genesis

to convert the DAI to USD and send to the trusts' escrowed Participation Funding Account

(Steps 1 and 2 in the above schematic).

2. Ongoing Purchase of Participations From the Participation Funding Account

Purchase of participations will occur completely off-chain during the term of the Master Participation Agreement as described in the @Real

World Finance risk assessment. In summary, participation purchases will occur as follows:

1. HVBank will relay information about participation purchases being offered to RWA MPTrust

to the RWA MPTrust

's Calculation Agent (Ankura

);

1. Ankura

will complete due diligence on the offered participation(s) on behalf of the Trust and upon confirming that it meets the requirements of the Trust will provide certification that the participation meets the purchase requirements. The certification will be uploaded to off chain storage and will be delivered to the RWA MPTrust

’s trustee WSFS

who will provide the necessary funding required under the participation purchase to HVBank

who will deliver the executed participation certificate to WSFS

to hold as security/collateral for the participation purchase.

1. Excess funds within the Participation Funding Account

will be invested by WSFS

in short term securities, as permitted under the Master Participation Agreement

. Net income from these investments will be paid to the trust’s Authorized Investment Income Account

, for monthly distribution to MakerDAO’s surplus buffer on a monthly basis (along with other income from participations as described in the next section below).

1. On a monthly basis, until the expiration of the Master Participation Agreement

any principal repayments received by the RWA MPTrust

will be sent to the Participation Funding Account

(and not be used to reduce the balance in the RWAUrn) to fund future participations that may be offered by HVBank

.

3. Monthly Remittances

[

1600×1098 300 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/3/b/3b8258c395bf420046d6183a82237b0a3e6c3bd9.jpeg)

The key transaction steps are detailed below:

1. HVBank

on a regular ongoing basis, as and when received sends principal and income received on RWA MPTrust

participations to the trust’s Participation Receipt Account

;

1. HVBank

sends a monthly remittance report to Ankura

(Calculation Agent);

1. Genesis

the crypto broker sends the monthly exchange report to Ankura

;

1. WSFS
2. the trustee sends a monthly Authorized Investment Income Account

report to Ankura

;

1. Ankura

completes a detailed consolidated monthly report of RWA MPTrust

’s net income after all servicing activities aggregating 1) Investment and Participation Income and 2) Participation funding repayments, and uploads to MakerDAO off-chain storage for ongoing monitoring by @Real

World Finance;

1. WSFS
2. sends the net amount of the monthly remittance to Genesis, for conversion from USD to DAI - detailing which amounts are paid to the RWAUrn and which to the RWAJar contracts;
3. Genesis

sends the DAI equivalent of the monthly investment and participation income component of the remittances to the RWAJar contract;

1. Genesis

sends the DAI equivalent of participation funding requirements to the RWAUrn contract for reducing the debt in the RWAUrn contract;

1. @CES

’s automated keeper

- which will run as a job in Makers’ keeper network (this job is under development and will be reviewed by @Protocol

Engineering

before deployment) calls void() on a monthly basis to send any DAI in the RWAJar contract directly to the Surplus Buffer;

1. @CES

automated keeper

- which will run in the same job as 9 above, calls wipe() on a monthly basis to repay any DAI in the RWAUrn contract and reduce the DAI debt outstanding.

Contract Risk Summary

NB: The reader should note that his assessment is solely with respect to the smart contract transactions

and interfaces required to affect the on-chain state changes

required under the proposed architecture and excludes any technical functionality related to the technical infrastructure required for monitoring and uploading data to MakerDAO off-chain

storage and ongoing monitoring. We understand that @Real

World Finance

will be developing any technical infrastructure required for integrating any off chain transaction flows needed for the proposed transaction with @Data

Insights Core Unit

.

Risk Analysis Conclusion: Low technical risk

The RWA code implementation resides within a sandbox-like environment, and any operation not related to locking, freeing, drawing, wiping, or voiding in the RwaUrn and RWAJar contracts must be voted on by governance. The code itself is lightweight. This implementation uses simplified Oracle and Urn contracts to achieve the functionality required for this specific instance of RWA. Furthermore, MIP21 contracts have been live in production for over a year, and are thus deemed low risk to reuse for this implementation.

The only addition required to the MIP21 suite of contracts is the addition of the new RWAJar contract – which as indicated is to allow the payment of monthly investment and income received from the participations directly to the surplus buffer as the stability fee will be set to 0.

As indicated above this contract provides 2 simple permissionless functions void()

and toss(uint256 wad)

which will route the payment of DAI directly to the Surplus Buffer to the spell designated vow address. The void()

function sends all DAI owned by this Smart contract whereas the toss(uint256 wad)

function sends a specified amount of DAI from the msg.sender’s wallet, provided the RWAJar contract has been pre-approved to send the DAI. This new contract has been reviewed and approved for use by Protocol Engineering without an audit due to its simple semantics and permissionless operation.

Supporting Materials

Sūrya’s Description Report

Files Description Table

File Name	SHA-1 Hash
mip21-toolkit/src/oracles/RwaLiquidationOracle.sol	88c2b4fac899d39af0198c1fb4776171e4249c19
mip21-toolkit/src/tokens/RwaToken.sol	8d75732d93e0ad82a7bf3e0faf34550082291775
mip21-toolkit/src/urns/RwaUrn2.sol	ce511f510a5d456cf686a9f64a5b46a064043c31
mip21-toolkit/src/jars/RwaJar.sol	b14b29aaf896c14832511c17966104888f7bfbf5

Contracts Description Table

Contract

Type

Bases

└

Function Name

Visibility

Mutability

Modifiers

RwaUrn2

Implementation

└

Constructor

Public

NO!

└

rely

External

auth

∟

deny

External

auth

∟

hope

External

auth

∟

nope

External

auth

∟

file

External

auth

∟

lock

External

operator

∟

free

External

operator

∟

draw

External

operator

∟

wipe

External

NO!

∟

quit

External

NO!

∟

add

Internal

∟

sub

Internal

∟

mul

Internal

∟

divup

Internal

∟

rad

Internal

RwaToken

Implementation

∟

add

Internal

∟

sub

Internal

∟

Constructor

Public

NO❗

∟

transfer

External

NO❗

∟

transferFrom

Public

NO❗

∟

approve

External

NO❗

RwaLiquidationOracle

Implementation

∟

rely

External

auth

∟

deny

External

auth

∟

add

Internal

∟

mul

Internal

∟

Constructor

Public

NO❗

∟

file

External

auth

∟

init

External

auth

∟

bump

External

auth

∟

tell

External

auth

∟

cure

External

auth

∟

cull

External

auth

∟

good

External

NO❗

RwaJar

Implementation

∟

Public

NO❗

∟

void

External

NO❗

∟

toss

External

NO❗

Legend

symbol

meaning

function can modify state

function is payable

Contract Inheritance Graph

There are no inherited contracts in the MIP21 contracts (excluding tests). See below.

[

1600×96 22.2 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/0/0/000835ae6dd86e50ea7935cd9797d8df63929bd3.png)

Contract Call Graph

[

683×1600 205 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/c/9/c92cecbac70d116c0c9b805d02a21c4ed90413bb.jpeg)