CIRCLE RESEARCH

Perimeter Protocol

Perimeter Protocol allows developers and builders to have access to an audited, open source protocol that they can freely use to build unique credit applications using USDC.

Authors
Rachel Mayer, Adrian Soghoian, Gordon Liao,
Jeremy Allaire, M2 Labs

September 2023

Contents

01

Abstract

This paper introduces a credit protocol for use on public blockchains.

It offers several important features, such as the ability to delegate loan management and monitoring, integration with permission standards, and the flexibility to accommodate different types of credit instruments. Unlike other on-chain alternatives, this protocol stands out for not relying on a protocol token and its adaptability to various scenarios. Alongside regulated payment stablecoins, this protocol marks an initial progress towards enabling market-based credit provision on public blockchains with full-reserve money.

02

Introduction

Over the past three decades, the internet has grown to provide more and more infrastructure for society and the economy. Built on open source software and openly defined and interoperable protocols, the internet has transformed information exchange, communications, media and commerce.

With the advent of new open source software and decentralized protocols for cryptographically secured records and data, the internet spawned crypto-currency and new public networks (aka. blockchains) for facilitating value exchange in a similar manner to protocols that support open, global, instant and nearly free information exchange and communications.

The growth in cryptocurrency and blockchain technology has also been inspired by ideas supporting the development of a new global economic and financial system built on sound money principles. These ideas emerged in reaction to the Great Financial Crisis of 2008, but are also rooted in ideas that developed in the 1930s in reaction to earlier financial crises.[1] Specifically, full reserve forms of banking and money ameliorate moral hazard that arises from deposit insurance and public guarantees for institutions that are too-big-to-fail.[2] These ideas have thus informed the development of stable-value crypto currencies tied to fiat currencies.

While one major area of focus has been the development of non-sovereign digital stores of value that are inherently full reserve (e.g. bitcoin), another approach has been to build on existing fiat government-debt backed money such as the US dollar and connect this form of government debt obligation to tokenized digital currency forms. This alternative approach, which builds on the strength of major geo-economic zones and government capacity to repay its debt, offers a practical path towards building a safer and more efficient global economic system built on sound money ideals.

Increasingly, both in practice and through regulatory policy, these new forms of digital dollars and digital cash offer a base layer for financial and economic activity that is inherently lower risk than current widely used and circulated forms of commercial bank electronic money. We define digital dollars and digital cash as a digital-token representation of fiat cash and government debt obligations with full backing.[3]

Today, the largest circulating form of such digital dollars and digital cash is USDC, which is backed 100% by highly liquid cash and cash-equivalent assets and is always redeemable 1:1 for US dollars.[4] Entities that use digital dollars and digital cash such as USDC understand that they are holding a fully-reserved, cash-equivalent digital currency instrument that can be transferred and exchanged at internet-speed and internet-scale, with very

high levels of security and privacy assurances. As a form of digital instrument, these forms of digital dollars and digital cash offer users near-instant global settlement finality, dramatically lowering counterparty risk in payments and settlements.

With increasing convergence among global financial regulators to license and supervise issuers of digital dollars and digital cash under prudential financial and regulatory supervision standards, we are approaching a time when households, businesses and financial institutions could adopt this form of digital currency on a mass scale.

Critics, however, have argued that full-reserve instruments such as digital dollars and digital cash and USDC could undermine the ability for banks to extend and intermediate credit that are needed for fueling real economic growth. These critical viewpoints are challenged by recent research that shows the adoption of digital cash can crowd-in deposits and thereby increase lending.[5]

One must revert to the 1930s for the origin of this debate. In the aftermath of Wall Street's collapse, which witnessed mass scale bank runs and hastened a global depression, economists and policy makers debated what form of money and banking rules would be necessary to avoid these persistent bank runs. One school of thought, the so-called Chicago Plan, led principally by a group of prominent economists from the Chicago School of Economics, argued that a safer financial system could be established if money and deposits were held on a full-reserve basis, entirely in government debt-obligations, and that this form of full-reserve banking should become the foundation of our payment system, which would reduce risk and provide greater stability. Separately, banks could lend money, but never on a fractional reserve basis.

The alternative view, which was widely pushed for by the large banks of the era, was to retain the fundamental role of risk taking and fractional reserve lending, but to establish a shared insurance pool for bank failures. This view ultimately won the day and led to the establishment of the Federal Deposit Insurance Corporation (FDIC). The introduction of FDIC insurance reduced the risk of bank runs but at the same time led to an increase in bank risk taking and leverage.[6] Discussions and debate on this has continued since, notably following the savings and loan crisis of the 1980s, and then again following the Great Recession.

More recently, the banking sector stress in 2023, including regional bank failures in the U.S. and the collapse of Credit Suisse in Europe, highlighted once again that explicit and implicit public support for financial intermediaries can lead to excessive risk-taking with distortive consequences. The Pyrrhic victory from containing the fall-out from the recent bout of banking issues only sowed the seed for greater expectations of future support.[7] Raising capital levels alone also does little to stem the misalignment of incentives associated with too-big-to-fail.

Proponents of full-reserve money have been advocating for market-disciplined credit creation that prevents excessive risk-taking subsidized by public sector guarantees. The push back from the other side is that bank-led credit provision is irreplaceable as the loan origination and subsequent loan monitoring processes are informational intensive, requiring private or "soft" information that only banks hold about their borrowers.

Which brings us full circle back to today, where open source technology, open public internet networks, and the invention of cryptographic forms of money and computing (e.g. blockchains) has spawned a new form of full-reserve cash equivalent money.

These technological advances greatly reduce the informational barriers and frictions that exist for market-based credit creation. The enforceability of financial contracts through immutable smart contract code coupled with the verifiability of on-chain data remedies the challenges of incomplete contracting. The reliance on "hard" information, made available at the discretion of users, instead of "soft" information also can curtail credit redlining that impinges the economic mobility of many.

If eventually trillions of dollars of value becomes digital dollars and digital cash, and effectively moves value from commercial bank liabilities into

government debt money, could this not undermine or limit credit creation?

Not only is the answer to this a resounding NO, but ultimately, we believe that digital dollars and digital cash combined with blockchain-native protocols can ultimately deliver a radically more efficient system of credit intermediation and delivery than the legacy fractional reserve banking system. Such a system, built on sound money principles, can open up capital flows and productive use of capital for households and businesses globally, and eventually deliver a safer and more inclusive global financial system.

Underlying this belief is an understanding that digital dollars and digital cash inherits from and integrates with a number of extraordinarily powerful attributes from innovations in blockchain that can unlock global scale credit delivery. These attributes of digital dollars and digital cash include:

- Radically lower cost of transmission, with digital asset settlement on mature public blockchains approaching fractions of a cent.
- Global-scale reach – effectively a form of money that can reach any internet-connected person, machine or entity, anywhere in the world.
- The speed of internet transmission, with existing blockchain networks enabling sub-section settlement finality.
- Programmable with tamper-resistant open source smart contracts, enabling highly flexible forms of financial contracts and economic arrangements that can execute and be enforced automatically.
- Transparency through public ledgers that are also privacy-preserving based on users' choice of data sharing.

Together, these attributes enable extraordinary reduction in information asymmetry and contracting frictions, far exceeding the capabilities of existing banking and lending practices. A combination of underlying safety and soundness with extremely capital efficient, high velocity money movement and programmable and enforceable financial contracts provides a foundation for building and delivering a system of credit intermediation that is far superior to the existing fractional reserve banking system of credit delivery.

Utility value from digital dollars and digital cash

Today, digital dollars and digital cash such as USDC is moving from an early adopter phase anchored in digital asset trading markets, into much more widespread use as a payment utility. Numerous companies, including major payments firms and financial institutions are beginning to use USDC as a core form of working capital and payments and settlement. Global demand for USDC has scaled dramatically over the past two years, with close to $26 billion in circulation, and over $12 trillion in transaction volume over the past 5 years.

As forms of digital dollars and digital cash such as USDC grow in usage for everyday payments and as more households and firms look to store value in this cash-like form of money, there is increasing demand from businesses to borrow and lend natively in digital currency. Increasingly, through blockchain-facilitated systems of borrowing and lending (both CeFi and DeFi), a new on-chain market for capital is being established.

Indeed, the next major phase of growth in digital currency and blockchains will likely be fueled by a fundamental shift from speculative value to utility value, driven by the power of using digital dollars and digital cash for payments, settlements and credit.

The next logical phase of growth for open source, on-chain protocols is the establishment of robust smart contracts and incentive designs that support the development of credit and debt capital markets. Such innovations can unlock real-world economic value for people and businesses everywhere, and are a critical next phase in building our shared vision for a more open, global, efficient and inclusive financial system.

Perimeter Protocol

Perimeter protocol is a new standard for credit creation on the internet. The Perimeter protocol is an open source set of smart contracts to enable the seamless exchange of stablecoin capital on secure, open and permissionless networks.

Perimeter brings credit to organizations using standards for underwriting and permissioning in one protocol. It is adaptable and flexible enough to accommodate a wide range of credit use cases; from invoice factoring for small and medium sized businesses (SMBs), to institutional crypto credit for trading opportunities, global payroll advances or instant settlement capabilities for fiat to USDC. The incorporation of “real world” productive assets with an entity’s on-chain activity on Perimeter can accommodate a variety of businesses wherever they are in their adoption cycle of blockchain technology. All types of businesses and capital providers, large and small, can communicate through Perimeter.

The protocol provides flexibility to Pool Admins, who underwrite risk and operate pools, to adjust fee and pool parameters, while also bringing predictability and transparency to Lenders. With zero protocol fees and no native token, the Perimeter protocol is primed for builders and developers to build on a shared public infrastructure to enhance existing markets such as:

- Venture debt, with auditable on-chain covenants and non-restrictive account requirements
- Trade finance solution for multinational companies
- Revenue based financing for companies with on-chain records of activities
- Stablecoin instant settlement for reducing the friction latency inherent in fiat payment systems
- Syndicated loan markets for different industries
- Emerging markets fintech capital for both consumer and SMB borrowers

Perimeter protocol is intended to serve as a trusted public good utility infrastructure. An audited, set of smart contracts that developers and teams can rely on and utilize to safely fork and build new credit applications. The automation and flexibility of a deployed credit smart contract infrastructure creates greater capital efficiency and allows borrowers, lenders and underwriters to build on top of shared capital markets infrastructure, using the safety and soundness principles of open source development brought to credit.

Perimeter protocol also is built to expand on protocol composability. Perimeter leverages Verite protocol for access control, participant eligibility, as well as in future versions bringing underwriting attestations for borrowers on chain. Leveraging decentralized identity with privacy first principles, Perimeter Protocol notably improves upon existing credit institutions where troves of data are stored and at risk of being compromised. Perimeter is designed such that it can be easily extended to other identity standards as the ecosystem grows. These sets of verifiable credentials, coupled with on-chain payment and default history, can open up real time credit rating assessments of borrowers and pool performance, something not possible in the existing credit markets today.

Perimeter protocol will never be deployed by Circle to a mainnet environment, instead we encourage developers to contribute to the shared GitHub repo, create their own forks, deployments to Ethereum ecosystems as well as front-ends or API-driven access points to the protocol to help build the long tail capital markets use cases Perimeter can accelerate.

04 Protocol Participants

Borrowers

Businesses and organizations can leverage Perimeter to access stablecoin native capital financing to support their business. Borrowers can take out different types of loans depending on their business needs. Depending on the terms, borrowers may be required to post collateral. They may pledge different assets, whether tokenized Real World Assets or native digital assets.

Pool admins

Pool Admins are specialized entities that underwrite credit risk and manage liquidity in the Perimeter protocol. They may be experts in credit risk management or specialize in certain industries, such as emerging markets, supply chain finance, crypto capital markets, e-commerce merchants, etc.

Pool Admins' main responsibilities are to:

- Source qualified borrowers and lenders into their capital pools
- Perform due diligence necessary to underwrite borrowers
- Evaluate borrowers' requests for capital, negotiate terms of loan details, collateral, capital needs and finalize any legal agreements
- Monitor liquidity and withdrawal requests of the pools
- Collect and verify any required continued reporting requirements from borrowers
- Liquidate, collect and pursue remedies against borrowers in the event of a default

Pool Admins earn fees for the above responsibilities, see the Fees section below.

Lenders

Lenders provide liquidity into pools by depositing digital dollars and digital cash, starting with USDC and EURC. Lenders deposit funds into different pools to earn interest from them, according to a lender's risk appetite and due diligence performed based on publicly available pool information, on-chain data such as borrower repayment history, underwriting assessments and performance, and a Pool Admin's reputation.

In order to lend into a pool, lender's must first meet the access control criteria set by the Pool Admin in their pool. Once a lender is allowed access, a lender must complete two transactions, approving a transaction that allows the pool contract to spend funds on behalf of the lender, and a second transaction that allows the deposit of tokens into the protocol and minting the appropriate Pool Tokens, an ERC-20 token that represents a Lender's share in the pool that are then transferred to the lender's wallet address. Pool Tokens are not transferable in this version of Perimeter.

Lenders can request to withdraw and exchange their Pool Tokens back for the initial asset deposited in the pool, plus accrued interest. Details on how lenders can withdraw their capital are provided in the Lender Withdrawal section below.

05

Pools

Pools give Lenders the benefit of diversified borrower exposure, differentiated maturity and credit risk exposures. Pools are built on top of the ERC-4626 open standard, making protocol integrations easier and less error-prone.

A pool's lending APY varies with the loan terms each borrower has in the pool, interest payments, and defaults occurrence. Each Pool Admin will have their own methodology for calculating their Pool's expected return, Perimeter will only supply necessary inputs for different implied yield methods.

Pools are highly configurable, and can consist of potentially many loans and many borrowers. Pools can also be single borrower pools, which might also have the same borrower and Pool Admin as a configuration. Pools also have an end date, whereby no new loans can be created or new capital accepted.

Loans in a pool can be fixed term loans with a set maturity (set in days), or open term loans in which a borrower can pay down a portion or all of the loan at their discretion. Open term loans have a call back option from the Pool Admin.

Interest accrual methodology

Interest on a loan in a given pool is paid on a set schedule, set by the terms of the loan. Those interest accruals and re-payments lead to an increase of the Pool Token exchange rate in a pool and are the main mechanisms for interest to accrue to the Lenders. The principal is repaid at the time of maturity for each loan or at borrower's preference for open term loans.

Interest accrues to pool specific Pool Tokens. The protocol expects interest payments to be made according to a loan's payment schedule, starting from the timestamp a Borrower draws down funds from the loan into their wallet. Daily interest is calculated on a 30/360 basis across the protocol. When Pool Token holders withdraw, they will receive the pro rata share (see Pool Token mechanics below) of the total of the principal amount of liquidity supplied plus accrued interest (paid in kind), minus any defaults and pool fees. Borrower's interest owed is calculated only on the principal borrowed (i.e. interest amount is not compounded) but earnings are automatically reinvested into the pool reserve unless a lender's request to withdraw.

Pool token mechanics

Lenders deposit liquidity into a pool to receive pool-specific tokens according to the ERC-4626 standard interface. Lenders receive ERC-20 tokens that are non transferable. Token supply is governed by an exchange rate to and from the underlying pool asset type. This exchange rate is dynamic and based on deposit and withdrawal activity, interest payments, active loans and defaults.

The exchange rate is based on a definition of the pool's Net Asset Value (NAV). In Perimeter, this is defined as:

outstandingLoanPrincipals + liquidityReserve + interestAccrued

Definitions:

- **outstandingLoanPrincipals:** total sum of active loan principals that have yet to paid back to the pool, as well as defaulted loan principals
- **liquidityReserve:** undeployed capital sitting in the pool, not attached to any loan
- **interestAccrued:** sum of all interest payments, including the current period (not yet paid), prorated by the current block's timestamp relative to the payment date. This serves to reward lenders who enter earlier in a given period (assuming there are active loans).

The exchange rate to convert pool tokens to and from a pool asset type is:

NAV / Pool Token Supply

This exchange rate is the key calculation used in deposit and withdrawal flows. On withdrawal, pool tokens are burned; on deposit, pool tokens are minted.

Withdrawal mechanisms

Pools have two parameters set by a Pool Admin to adjust the lender withdrawal experience of their pool: a Liquidity Gate and a Request Period. In Perimeter, the lender withdrawal mechanics are designed to optimize for greater predictability and pool stability, at the expense of lenders not being able to withdraw as much as their capital in a given period.

Pool Admins have the flexibility to set a Request Period (in days) and a Liquidity Gate (in percentage) configuration to accept withdrawals from lenders. Lenders request a withdrawal in a given period to be able to withdraw that amount in any of the following periods at any time, paying a withdrawal request fee for the optionality to do so. These requests are "batched" against a fixed portion of the pool liquidity for equitable distribution, which lenders claim at any point in the following periods. The portion of the pool's liquidity earmarked for withdrawals in a given period is protected by the smart contract against the Pool Admin deploying liquidity for new loans, ensuring it's available for the lenders. Withdrawal requests if not claimed during the window carry over until the next period. Withdrawal requests can also be canceled at any time for a cancellation fee.

The Liquidity Gate creates a limit on the percent of the liquidity reserve that can be withdrawn by lenders in aggregate. This ensures that a proportion of Lender capital can be withdrawn on a given withdrawal date, and can also reduce runs from the pool. The Liquidity Gate does not encourage withdrawal requests and does not give additional benefits or preference to the withdrawal requester based on timing or size of the withdrawal request. While lenders should not be deprived of their access to liquidity, Pool Admins should smooth withdrawal pressure over a longer period of time to ensure that the liquidity risk premium is not subsidized by long-term investors. The expected outcome is that over a defined time period, lenders request to withdraw and can get all their balance out over a known number of periods. These lender requests are visible to all on the protocol.

For example, a Pool Admin can configure a pool to be a monthly Request Period at 10% Liquidity Gate, or quarterly Request Period at 25% Liquidity Gate. For every pool, lenders will be able to request and stagger their withdrawals in advance over a known period of time to withdraw and redeem Pool Token back to principal token.

In the case where there is excess liquidity in the pool and the Pool Admin wants to wind down operations, the Pool Admin can close the pool which will automatically set the Liquidity Gate to 100%, this would allow all lenders to redeem their pro rata share of Pool Token without any fees or gates.

Access Control & Permissioning

The Perimeter protocol, pools, and loans are governed by customizable, robust access and permission controls designed for security and customizability while preserving privacy of the participants.

Perimeter manages core protocol permissions using a series of roles with specific responsibilities. The protocol Admin can designate addresses for each role, e.g. Deployer, Operator, and Pauser. None of these roles have access to move funds within the protocol.

Permission to create and manage a pool, is checked by calling a PoolAdminAccessControl contract that implements a standard is Allowed() check to gate PoolAdmins. The Operator can change this contract address to new implementations to continue to expand on the set of supported identity solutions and credentials. Perimeter includes a default contract that starts with restricting access to addresses to Pool Admins starting with valid KYB credentials leveraging the Verite standard for open source and decentralized identity.

Lender and Borrower access is determined on a Pool by Pool basis by the Pool Admin. Perimeter includes a default contract in which Lender eligibility can be configured using Verite credentials or via an AllowList managed by the Pool Admin. One such example of this would be a Pool Admin requiring all lenders to be Accredited Investors in the United States, or only allowing non US persons as Lenders via Verite credential schemas.

07

First Loss Capital & Default

First loss captial

First loss capital is a safety measure that offers more protection to lenders in the event of a Default. Each pool has a required first loss reserve of 10,000 USDC amount, which is initially funded by the Pool Admin and gates receiving deposits from lenders. Any additional first loss capital can be in the currency of the loans denominated in the pool. In this version of the protocol, only the Pool Admin can deposit first loss capital and is not open to third parties.

A percentage of borrower interest, by default set at 5%, is also deposited into the first loss reserve vault as a means of protection. Protocol implementation of First Loss Capital can be changed to fit use case and developer needs.

All first loss capital can be claimed back by the Pool Admin once a pool has been closed and all defaults and liquidation proceedings have ended.

Default

Borrowers and Pool Admins will likely sign legal agreements outside of the knowledge of the protocol that encode all material information on the protocol itself. Defaulting on a loan on Perimeter is defined as:

- A missed payment, whether interest payment or principal payment.
- A missed replenishing of the collateral, following the breach of the liquidation threshold. The same grace period applies.

There are other events that could trigger a default, unknown to the protocol, depending on the borrower profile and use of proceeds. Those events are defined more clearly in any of the legal agreements, but over time they can be monitored on-chain. For example, a typical default event might be if the Borrower's on-chain credit score falls below a certain level, or if their aggregate amount in a certain wallet falls below a certain level.

- Once a Pool Admin triggers a default by changing the loan state, it will start a series of events as follows:
- Lenders who are Pool Token holders immediately following the event of default loan change on chain are now the affected lenders

- Lenders are affected through a “worst case recovery” method, and thus the relative share of each Pool Token holder’s position with respect to the defaulting loan size and accrued interest is reduced to reflect a zero recovery amount on the loan. This is implemented through an updated Pool NAV, where the outstanding loan principal contribution is reduced to reflect the defaulted loan, which decreases the value of each Pool Token through the exchange rate.
- Protocol automatically distributes the appropriate loan amount proceeds from the First Loss reserves back into the Pool. The distributed amount from the first loss reserve back into the pool is the principal of the loan amount, or the total available first loss capital (whichever is less).
- Pool Admin starts any collateral liquidation proceedings if applicable to the loan, as outlined above. If there is any further difference in the total defaulted amount and what was recovered from Collateral and First Loss pool, the Pool Admin can pursue further remedies against the borrower off chain.
- Pool Admin, at any time during the above process, can distribute a portion or all of the recovered amount segregated in loan to affected lenders by sending on chain payment to the Lender addresses.

There can be multiple defaults happening in the pool simultaneously across different borrowers, in which case the above process happens in parallel across multiple loans and borrowers.

To summarize, lenders have the following waterfall structure as means of protection within a pool:

1. First Loss
2. Collateral (if any pledged against certain loans)
3. Pursuit of other remedies off-chain

08 Fees

Within the protocol, fees are meant to align incentives between the stakeholders. These fees ensure that many entities will build on Perimeter to enable a suite of products for their own use cases. The fees are purely set for incentive alignment and efficiency of pools between Pool Admin, Borrower and Lender. There are no Protocol fees in this version of Perimeter.

There are four types of fees:

- Pool fees
- First loss fees
- Withdrawal fees
- Late fees

Pool fees

Pool fees are determined by the Pool Admin on a pool by pool basis. Pool fees can be charged in multiple ways, a Pool Admin can enable any combination of the below:

1. Origination fee: Charged as originated fees on funded loans on a per annual basis. Pool fees are paid to Pool Admins on the loans payment schedule. The fees are charged from the borrower in addition to the interest payment fees.

Servicing fee: Charged as a percentage of loan interest, deducted from loan borrower interest payment.

2. Fixed fee: Charged as a fixed fee on a predefined frequency, deducted from the liquidity reserve. If the liquidity reserve does have insufficient liquidity, the remaining fee balance attempts to charge on the next day. Pool Admins can only withdraw the full amount each period.

Withdrawal fees

Withdrawal request fee

Withdrawal request fees ensure the deposit and withdrawal pressure on the liquidity reserve of the pool is protected from run risk and liquidity arbitrage opportunities. Withdrawal request fees are set by the Pool Admin in their pool

and are charged as a fixed percentage of a requested withdrawal amount (in pool tokens). The fees are deducted from the Lender's balance when a Lender requests a withdrawal amount for the next Request Period. The fees accrue to the liquidity reserve pool to ease withdrawal pressure on future withdrawals. At a pool's end date, withdrawal request fees are automatically set to zero.

Withdrawal cancelation fee
Withdrawal cancellation fees are optional fees set by the Pool Admin that are applied to a withdrawal cancellation request. This fee prevents a Lender from submitting malicious withdrawal requests and always canceling their outstanding request after claiming the withdrawal. At a pool's end date, withdrawal cancellation fees are automatically set to zero.

First loss fees

First loss fees are set by protocol governance, initially set at 5%, and are charged as a percent of borrower interest diverted to the first loss pool contract on a loans payment schedule. At a pool's end date, after all defaults have been resolved, the Pool Admin can claim any undistributed first loss fees back.

Late fees

Late fees are set by the Pool Admin at a loan level, and are charged to the borrower as a percent of the payment amount on interest in addition to the payment interest. Late fees accrue to the First Loss Reserve pool when made. A Pool Admin can claim the total of the First Loss Pool amount, which will be the initial contribution minimum, first loss fee and any late fees accrued at end of pool term once defaults have been resolved.

Lenders thus receive a full blended interest of all active loans in a given pool, minus any pool, first loss and withdrawal fees.

Fee examples

As an example, assume a Pool Admin chooses just the originated loan fee as their fee election at 1% and sets a 0.50% withdrawal fee. Assume there is only one loan in the pool for 10M USDC for 60 days at 10%.

- The pool fee would be 10,000,000 USDC * 1% * (60/365) = 16,438 USDC, paid in two installments of 30 days, in addition to borrower interest payments.
- The borrower's monthly interest payment is 82,191.78 USDC (164,383.56/2).
- The total monthly payment for the borrower is thus 8,219 + 82,191.78 USDC = 90,410.78.
- The first loss fees would be 10,000,000 USDC * 10% * (60/365) * 5% = 8,219 USDC. This portion of 82,191.78 goes to the first loss reserve pool.
- A lender requests to withdraw 1,000,000 USDC on day 15, lender will pay 1,000,000 * 0.50% = 5,000 USDC and will be eligible to withdraw 1,000,000 at the next Request Period pending reserve liquidity.

Protocol Parameters & Roles

The Protocol Roles and Parameters are structured to give Pool Admins the utmost flexibility in their operations and prioritizes protocol security and programmatic governance. Moreover, the roles also have limited intervention in protocol particularly on the use of funds within pools, and are limited to extreme safety measures in the event of a major attack.

Global roles

Admin
Assigns and delegates roles

Deployer
Upgrades any upgradable contracts

Operator
Sets the Global Parameter variables

Pauser role
Pauses creations of new pools, withdrawals and loan fundings. This is a security countermeasure. In the event of an emergency, a pausable contract can be paused, to halt the execution of its functions that respect its paused status.

Global parameters

A number of Global Parameters exist and can be set by a Protocol Operator, these include:

- Supported loan and pool asset types
- Permissioning policies for Pool Admins when instantiating pool
- Protocol-wide fees (if any)

Pool parameters

These parameters are set by the Pool Admin when first deploying the pool contract and cannot be mutated post deployment:

Loan asset: what loan asset is the pool denominated in that lenders can deposit and withdraw, only **one** currency from the Global Loan Asset list.

These variables can be changed during the lifecycle of a pool:

Liquidity gate: a percentage that defines how much of the liquidity reserve pool can be withdrawn from every Request Period.

Request period: how often, in days, can lenders request to withdraw from liquidity reserve subject to the Liquidity Gate percentage.

Pool capacity: total liquidity size of a pool. Once this value is reached, the pool cannot be lent into.

Pool fees: as described above, any combination of the following:

- Origination fees
- Servicing fees
- Fixed fees

End date: The end date which lender's can withdraw all remaining principal and accrued interest. The period can be decreased by the Pool Admin, but not increased.

Lender access control list: specifies which set of lender Verite credentials or whitelisted addresses a Pool Admin allows to access the pool

Loan parameters

These parameters are set by the Pool Admin when finalizing loan details with a borrower within a pool, the loan contract cannot be mutated post borrower drawdown:

Loan type: fixed or open term.

Principal: amount to be borrowed

Duration: in days, loan maturity

Payment period: how often interest payments are to be made, in days

Collateral: if collateral is required on the loan, and if so what asset type

Late fees: charged to the borrower as a percent of the payment amount on interest in addition to the payment interest

Appendix

[1] See, for instance, Fisher, Irving. 100% money. Adelphi Publication, New York, 1935.

[2] Pennacchi, George. “Narrow banking.” Annu. Rev. Financ. Econ. 4, no. 1 (2012): 141-159.

[3] In the ideal case, the token’s reserve assets should consist entirely of central bank balances and short-term government securities.

[4] The vast majority of the USDC reserve is invested in the Circle Reserve Fund (USDXX), an SEC-regulated money market fund managed by BlackRock. Daily independent third-party reporting on the fund is publicly available. Circle also maintains the stated goal of eventually holding all reserves as a form of direct obligation of the Federal government, as balances held at the Federal Reserve in combination with short-duration Treasury securities.

[5] See, for instance, a) Chiu, J., Davoodalhosseini, S.M., Jiang, J. and Zhu, Y., 2023. Bank market power and central bank digital currency: Theory and quantitative assessment. Journal of Political Economy, 131(5), pp.1213-1248; b) Whited, T.M., Wu, Y. and Xiao, K., 2022. Will Central Bank Digital Currency Disintermediate Banks?. Available at SSRN 4112644.; c) Sarkisyan, S., 2023. Instant Payment Systems and Competition for Deposits. Jacobs Levy Equity Management Center for Quantitative Financial Research Paper.

[6] Berger, Allen N., Richard J. Herring, and Giorgio P. Szegö. “The role of capital in financial institutions.” Journal of Banking & Finance 19, no. 3-4 (1995): 393-430.

[7] For instance, the Bank Term Funding Program effectively introduces government rescue for banks that have taken on excessive interest rate market risk.

circle.com/circle-research