

MICrO Protocol

Whitepaper

Decentralised Microcredit Infrastructure in USDC

Version 2.0 | 19 August 2026

Document status

- State tested at Sepolia Base; the founding pilot in Vietnam remains in pre-launch.
- The document preserves the technical structure of 25 chapters and replaces outdated economic, governance, liquidity, legal and operational assumptions.
- Font: Geist in all document.

Technical, economic and institutional whitepaper. It does not constitute legal, financial or investment advice.

Contents

1. Executive Summary
2. System Vision, Philosophy and Principles
3. The Global Microcredit Problem
4. MICrO Protocol Architecture Overview
5. Loan Life Cycle and Transaction Flow
6. Risk Management Framework
7. Liquidity and Capital Management
8. Credit Reputation and Score System
9. Sybil Anti-Fraud and Attack Protection System
10. Economic Model and Fixed Interest Structure
11. Tokenomics and MICrO Token Utility
12. Protocol Governance and Control
13. Smart Contract Security Architecture
14. Deployment Architecture and Network Strategy
15. Operational Model and Pilot Strategy in Vietnam
16. Compliance and Regulation Strategy
17. Legal and Operational Positioning
18. Audit Strategy and Security Certification
19. Disclosure and Risk Management
20. Evidence-Gated Roadmap
21. Technical Appendix
22. Economic Appendix
23. Documentation of Smart Contracts
24. Glossary
25. Conclusion

Chapter 1 — Executive Summary

Baseline v2.0 applicable to this chapter

- Fixed simple interest: 5% per month; variable guarantee manages risk and viability.
- Controlled start: 10–25 USDC, 30 days, 0% stake within envelope limited to 20% of the available block.
- active maximum: 100 USDC; 500 USDC is future ceiling subject to governance.
- Cohort 1: 25 participants in a planned programme up to 100; Vietnam remains in pre-launch.

1.1 — Objective of the Protocol

MICrO Protocol is a microcredit infrastructure in USDC that combines deterministic rules, on-chain reputation, variable stake, liquidity control and human governance. The objective is to test low-value credit with limited exposure and auditable evidence.

1.2 — Fixed price reference

All loans use fixed fixed simple interest of 5% per month. The rate does not increase with risk. The viability and economic protection are adjusted through stake, exposure, score, KYC, cooldown period, envelopes and anti-Sybil.

1.3 — Controlled start

The first loan is between 10 and 25 USDC, lasts 30 days and can operate with 0% stake (stake) only inside the envelope controlled unsecured. Within the capital activated for credit, maximum use remains limited to 80%; from this available block, only 20% can be used for first loans of 10 –25 USDC without collateral. This exception is limited by enhanced anti-Sybil controls, daily and weekly limits and review of correlated clusters.

1.4 — Progressive credit

Following loans usually last 90 days. The active maximum pilot is 100 USDC. Within the same 80% available block, up to 50% can be used for credit up to 100 USDC when the credit recipient has the capacity to deposit the required guarantee. The capacity between 101 and 500 USDC is future and depends on evidence, KYC, activated capital and governance.

1.5 — Guarantee, verification and status scale

Scale	Guarantee	Normal duration	cooldown period	Minimum verification	Status
10–25 USDC	0% only in unsecured envelope	30 days	7 days	enhanced anti-Sybil controls controls and pool review	Active in pilot
26–50 USDC	28%	90 days	5 days	Basic verification and guarantee capacity	Active in pilot
51–100 USDC	26%	90 days	3 days	Basic verification, score and guarantee capacity	Active in pilot
101–200 USDC	24%	90 days	To be defined by governance	KYC	Future, non-active
201–500 USDC	22% to 20%	90 days	To be defined by governance	KYC + selfie	Future, non-active

1.6 — Period of waiting and simultaneity

There is only one active loan per credit recipient. The cooldown period progresses from 7 days after 10–25, to 5 days after 26–50 and 3 days after 51–100. Above 100 USDC, any cooldown period can only be defined after pilot evidence and governance approval.

1.7 — Pilot design

The Vietnam Founding Pilot Programme remains in pre-launch. Cohort 1 includes 25 participants within a planned programme up to 100, with expansion only after review of evidence.

1.8 — Capital structure

The pilot's committed reserve can reach 112,500 USDC. The active credit limit is significantly lower and released by steps. The absolute ceiling of use is 80% of the capital activated and the reserve floor is 20%. Within 80% usable, the protocol separates operational sub-limits: 20% for first loans 10–25 USDC without collateral and up to 50% for loans up to 100 USDC with collateral deposited.

1.9 — Risk controls

Device, IP prefix, ASN, VPN/Tor, source of funds, request velocity and behavioural signals are combined into correlated wallet groupings. cooldown period, limits, revision and eligibility also operate at the level of the pool, not just the individual portfolio.

1.10 — Governance

The architecture defined is Safe 3-of-5 → Timelock → critical contracts. Bots observe, recommend and warn; privileged actions require human approval.

1.11 — Current State

Lending, repayments, reputation, multi-wallet flows, liquidity monitoring, governance, pause/unpause, V2 Monitor and synthetic scenarios were tested in Base Sepolia. This does not equal mainnet, completed external audit or data from human credit beneficiaries.

1.12 — Discipline of the roadmap

The roadmap is evidence-gated: testnet readiness, operational readiness, legal readiness, Cohort 1, cohort review, expansion up to 100, higher exposure and production.

1.13 — Pilot objective

The pilot intends to measure repayment, gross default, net credit loss, reserve integrity, fraud, false positives, transactions and progression of credit recipients. The protocol does not assume results before live observation.

1.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The MICrO Protocol is a decentralised microcredit infrastructure designed to provide low-value loans with strict risk control and systematic liquidity preservation. Unlike speculative financial systems or unstructured credit models, the protocol was designed from the beginning as a deterministic system, where each loan follows fixed and verifiable mathematical rules on-chain.

The protocol uses stablecoins (USDC) as a base settlement unit, ensuring monetary predictability and eliminating volatility associated with speculative assets. Each loan is supported by a progressive stake mechanism in which the credit recipient provides a fraction of the loan value as a partial guarantee. This mechanism reduces the net exposure of the system and establishes a direct economic incentive to meet obligations.

The operational model of the MICrO Protocol is based on three fundamental pillars

- 3 — Sustainable pool growth

Liquidity preservation is ensured by a rigid maximum use limit of the pool defined in:

This limit prevents all the capital from being committed simultaneously, ensuring that at least 20% of the capital

uidity is always available to absorb adverse events or unexpected delays.

- Operational Structure of Loans

The system uses a rigidly defined loan structure

- Eligibility based on previous history

This structure creates a progressive model where the initial risk is limited and access to higher values depends on the historical performance of the credit recipient.

The fundamental economic model of the protocol can be illustrated with typical examples

Net exposure represents the capital effectively exposed to the risk after the deduction of stake.

- lower values have proportionally higher protection
- higher values maintain operational efficiency
- net exposure remains controlled

The protocol was submitted to default simulations to assess its resilience under different operational conditions.

These results indicate that the system maintains positive sustainability up to approximately 15% of default, with marginal stability close to 20%.

This type of quantitative modelling is one of the main distinguishing elements of the MICrO Protocol for traditional credit systems.

- Security and Governance Structure

Protocol control is carried out through a governance model based on

This structure prevents unilateral changes and ensures that critical operational modifications follow a period of observation before execution.

In case of high risk, the protocol supports

That allows for temporarily suspending new credit issues while pool integrity is assessed.

The pilot phase was conceived as a controlled operational validation.

- reputational system behaviour

The strategic objective of the MICrO Protocol is not rapid growth, but rather

- sustainable and controlled growth

Over time, the accumulation of interest and retention of reserves allow the gradual increase in pool capacity, creating a positive cycle of sustainable growth.

Chapter 2 — System Vision, Philosophy and Principles

2.1 — Strategic Vision

The MICrO Protocol was designed with a strategic vision distinct from most blockchain-based financial projects. Instead of prioritising accelerated growth or maximising transactional volume, the system was designed to achieve structural stability and economic sustainability over time.

The main vision of the protocol is to create a decentralised microcredit infrastructure that is:

- expected
- auditable
- financially disciplined
- resilient to adverse events

Unlike traditional financial systems that rely heavily on manual analysis or subjective risk models, the MICrO uses programmed deterministic rules in smart contracts, reducing human dependencies and eliminating operational ambiguities.

In the long term, this approach allows the protocol to evolve to a structured global microcredit platform, maintaining a conservative risk model even under progressive growth of the user base.

2.2 — Central Financial Philosophy

The financial philosophy of the MICrO Protocol is based on three fundamental principles.

- 1 — Preservation of capital first
- 2 — Controlled risk exposure
- 3 — Predictable growth

Each of these principles was directly integrated into the technical architecture of the system.

- Preservation of capital first

The preservation of capital is treated as the system's top priority.

Unlike aggressive financial models using high leverage or total capital exposure, MICrO Protocol always maintains a mandatory liquidity reserve.

Structural parameter

- Maximum Pool Usage = 80%

That means

- only 80% of total liquidity can be used in loans
- at least 20% is always available

This reserve works as

- buffer against defaults
- protection against delays
- operational stabiliser

Without this mechanism, simultaneous adverse events could compromise pool integrity.

- Controlled risk exposure

Risk is not eliminated — it is controlled.

Each loan is issued on the basis of a calculated net exposure model.

Liquid exposure is defined as

- Net Exposure = Value loan

Guarantee value (stake)

For example

- loan = $100
- Stake = $26

Result

- Net Exposure = $74

This model creates a natural economic barrier against negligent or abusive behaviour by the credit recipient.

The higher the loan value, the greater the need for positive history and financial discipline.

- Predictable growth

System growth is not based on aggressive expansion, but on progressive accumulation.

The economic model assumes that

- interest paid by credit recipients gradually increases reserves

- Additional reserves increase future capacity
- growth occurs in controlled cycles

This cycle can be represented as

- Issuance loan
- Cumulative interest

Capacity increase

This mechanism creates a long-term sustainable model, avoiding continuous dependence on external financing.

2.3 — Determining credit model

One of the most important elements of the MICrO Protocol is its deterministic model.

In a deterministic system

- rules are fixed
- decisions are predictable
- behaviour is auditable

There are no arbitrary decisions.

Each loan application is automatically assessed on the basis of

- portfolio eligibility
- reputational score
- previous history
- stake available
- liquidity limits

If any parameter fails, the loan is automatically rejected.

This template eliminates

- favoritism
- subjectivity
- operational inconsistencies

And ensures uniform behaviour for all users.

2.4 — Progressive Model of the credit recipient

The system does not assume high initial confidence.

Trust is built progressively.

Structure

First loan

- low value
- short duration
- proportionally high stake

Following loans

- longer duration (90 days)
- potentially higher value
- proportionally reduced stake

This model creates an economic learning system where the credit recipient demonstrates responsible behaviour over time.

2.5 — System Conservation

The MICrO Protocol was deliberately designed as a conservative system.

That means

- rigid limits
- controlled growth
- calculated exposure

Conservative elements include

- mandatory duration of 90 days after first loan
- rejection of new portfolios
- Compulsory progressive stake
- maximum use limit of pool

These restrictions significantly reduce structural risk.

2.6 — Risk discipline philosophy

Risk discipline is integrated into the system from the lowest level of architecture.

There is no exclusive dependence on human behaviour.

The checks are

- mathematicians

- automated
- verifiable

The protection sequence follows a hierarchical structure

- 1 — User Stake
- 3 — Governing intervention
- 4 — Operational pause

This structure defines the call

- Hierarchical risk model

This model will be detailed in later chapters.

2.7 — Economic Discipline on Growth Times

A common error in emerging financial systems is to prioritize rapid growth.

MICRO Protocol follows the opposite path.

Growth only occurs when

- sufficient liquidity exists
- reserves are appropriate
- operational history is stable

If these conditions are not met

new loans are blocked.

This mechanism prevents uncontrolled growth.

2.8 — Objectives for system stability

The stability objectives of the protocol are defined quantitatively.

Critical indicators include

Target of the default rate

- < 15%

Critical threshold

- 20%

Failure threshold

- 30%

These limits have been defined on the basis of real economic simulations and represent clear operational borders.

Chapter 3 — The Global Problem of Microcredit

3.1 — Introduction to the overall credit gap

Access to credit is one of the fundamental pillars of individual and collective economic growth. However, a large part of the world population remains excluded from formal financial systems due to structural, regulatory or technological limitations.

International studies indicate that hundreds of millions of people in emerging economies do not have access to formal credit, even when they have real repayment capacity. This phenomenon is often referred to as:

- Global credit gap

This financial gap is mainly expressed in

- emerging economies
- regions with limited banking infrastructure
- populations with non-existent financial history
- informal workers

In these environments, traditional credit becomes inaccessible due to the absence of formal data or conventional financial guarantees.

3.2 — Dynamics of financial exclusion

Financial exclusion does not occur due to economic incapacity, but due to the absence of reliable validation mechanisms.

Traditional institutions depend on

- banking history
- tax records
- formal guarantees
- validated identification

Without these elements, access to credit is often refused, regardless of the actual ability to pay.

This phenomenon creates a negative cycle

- No credit
- No financial history

This cycle prevents large-scale economic mobility.

3.3 — Informal credit systems

In the absence of formal credit, communities often resort to informal funding systems.

These systems include

- personal loans
- Community credit
- local intermediaries
- informal loan sharks

Although functional in the short term, these systems present high structural risks.

Common characteristics

- extremely high interest rates
- lack of transparency
- no legal protection
- risk of financial abuse

In many cases, monthly rates above 10%–30% are common.

This type of structure creates prolonged financial dependence and reduces capital accumulation capacity.

3.4 — Microcredit developments and limitations

The modern concept of microcredit emerged as a direct response to financial exclusion, allowing small-scale loans for individuals without access to the traditional banking system.

Although effective in many contexts, the traditional microcredit model has significant limitations:

- dependence of intermediaries
- high administrative costs
- Extensive manual processes
- high operational risk

In addition, many traditional systems face difficulties in climbing without proportional increase in operational costs.

This factor limits the overall scope of these programmes.

3.5 — Structural challenges of microcredit systems

There are recurring structural challenges in conventional microcredit systems.

Main challenges

3.5.1 — Administrative burden

Manual loan management requires

- documentary validation
- manual analysis
- individual monitoring

These processes increase operational costs and reduce efficiency.

In small systems, these costs may represent a significant part of the total borrowed value.

3.5.2 — Risk concentration

Without automatic risk control mechanisms, systems can accumulate excessive exposure.

This results in

- increased defaults
- liquidity reduction
- operational collapse

Without strict limits, financial sustainability becomes uncertain.

3.5.3 — Limited scalability

Traditional systems rely heavily on human personnel.

As the number of users grows

- costs increase
- efficiency decreases

This behaviour limits global expansion.

3.6 — The role of digital infrastructure

Financial digitisation has opened up new possibilities to solve these challenges.

Blockchain technologies allow

- automatic execution
- reduction of intermediaries

- operational transparency

These characteristics make it possible to create autonomous financial systems with less dependence on centralised structures.

3.7 — Opportunity for decentralised microcredit

The convergence between blockchain and microcredit creates a significant structural opportunity.

decentralised systems can

- reducing operating costs
- automate validations
- increase transparency
- allow global scale

By eliminating unnecessary intermediaries, the total cost per loan can be significantly reduced.

This factor makes it possible to issue small-scale loans, something traditionally difficult in conventional banking systems.

3.8 — Decentralised credit risk challenges

Despite technological advantages, decentralised systems face their own challenges.

Main risks

Liquidity exhaustion

- Identity fragmentation

These risks require structural mitigation mechanisms.

The MICrO Protocol was designed specifically to meet these challenges.

3.9 — Size of market opportunity

The potential market for decentralised microcredit is significant.

Areas with greater need include

- Southeast Asia
- Sub-Saharan Africa
- Latin America
- Regions with high economic informality

In these markets, small loans can have significant economic impact.

Typical examples include

- inventory purchase
- Transport financing
- acquisition of tools
- cash flow management

Even low values can generate substantial economic impact.

3.10 — Why traditional systems do not solve this problem alone

Traditional systems face structural limitations that are difficult to overcome.

Main factors

- high fixed costs
- dependence on physical infrastructure
- complex regulation
- low technological adaptability

These limitations make it difficult to expand microcredit to populations with low financial volume.

Blockchain-based automated systems have clear advantages in this context.

Chapter 4 — Overview of Architecture of the MICrO Protocol

4.1 — Philosophy of architecture

The architecture of the MICrO Protocol was conceived as a modular and deterministic system, allowing a clear separation between operational responsibilities, risk control and liquidity management.

Unlike monolithic models, the protocol uses multiple specialized contracts that interact with each other through defined interfaces. This approach reduces the individual complexity of each module and allows independent component audits.

The fundamental principles of architecture include

Moderate

Auditability

Determinism

- Security by design

Each module only performs specific functions, avoiding unnecessary dependencies.

4.2 — Main intelligent contract modules

The protocol consists of several main contracts, each with well-defined responsibilities.

Main modules include

- 1 — LoanManager
- 3 — MicrocreditReputation
- 4 — Stablecoin Interface
- 5 — Governance layer
- 6 — Liquidity Pool Controller

This separation allows independent maintenance and controlled update through the governance mechanism.

4.3 — LoanManager contract

The LoanManager is the operational core of the protocol.

Main liabilities

- establishment of loans
- eligibility validation
- limit check
- cooldown period control
- Loan status record

This contract acts as the central point of entry for credit claims.

Main functional flow

Typical sequence

User request

- Eligibility verification
- Verification of liquidity reserve availability
- Security verification (stake)
- Creation loan

If any verification fails, the process is interrupted automatically.

- Eligibility logic

LoanManager checks

- if there is an active loan
- if cooldown period is over
- if minimum score is valid
- whether financial limits are respected

This mechanism prevents

- multiple simultaneous loans
- repeated applications
- systematic abuse

4.4 — MicrocreditLoan Contract

The MicrocreditLoan contract represents each individual loan.

Main functions

- calculation of interest
- management of the deadline

- repayment registration
- status update

Each loan maintains the following parameters

- credit recipient address
- loan value
- stake value
- interest rate
- due date
- repayment status

This contract allows full traceability of the life cycle of the loan.

- Interest calculation model

The formula used is deterministic

- Interest = loan Amount × Monthly Rate

Example

- loan = $100
- Rate = 5% / month

Result

- Interest = $15

This model simplifies validations and reduces unnecessary mathematical complexity.

4.5 — MicrocreditReputation Contract

The reputational system is responsible for managing financial history of users.

This contract records

- loans paid
- delays
- defaults
- frequency of use

The reputational score is automatically updated after each relevant financial event.

- Reputation Score Components

Main components

- 1 — Repayment History
- 4 — Time Consistency

These parameters allow classifying credit beneficiaries based on historical behaviour.

4.6 — Unified liquidity architecture

The protocol uses a unified liquidity pool instead of multiple independent pools.

All available funds are kept in a single operational pool, ensuring simplicity, efficiency and centralised risk control.

4.6.1 — General structure

The liquidity of the protocol is organised as

Unified liquidity reserve

This pool contains

- capital available for loans
- implicit reserves
- operating buffer

There are no physically separated pools in the contract.

4.6.2 — Pool usage limit

To ensure stability, the use of the pool is limited.

- Maximum Pool Usage = 80%
- At least 20% liquidity always reserved

This limit protects protocol against

- liquidity exhaustion
- peaks of demand
- default events

4.6.3 — Implicit Reserve

Although there is a single pool, the system maintains an implicit reserve by limiting its use.

This reserve is not kept in a separate pool.

It is guaranteed through the maximum use policy.

4.7 — Integration of stable currency

The protocol uses stablecoins as a base unit.

At the current stage

USDC (testnet)

Reasons for this choice

- monetary stability
- High liquidity
- broad compatibility
- financial predictability

All loans are issued in this unit.

4.8 — Governance layer

The governance of the protocol is implemented through

Multisig

Timelock

- Emergency controls

This model prevents immediate changes to critical parameters.

- Governance flow

Typical sequence

- Creation of the proposal

Timelock delay

- Multisig approval

This flow reduces the risk of malicious changes.

4.9 — Emergency control mechanisms

The protocol includes an emergency pause system.

Available functions

- pause()

- unpause()

During paused state

- new loans are blocked
- repayments remain allowed

This mechanism protects system integrity.

4.10 — System interaction flow

Full flow

- credit recipient Request
- Validation by LoanManager
- Reputation check
- Verification of reserve capacity
- Creation loan
- Transfer of funds
- repayment monitoring

This flow represents the normal operating behaviour of the system.

Chapter 5 — Loan Life Cycle and Transaction Flow

Baseline v2.0 applicable to this chapter

- An active loan per credit recipient.
- Progressive cooldown period: 7 / 5 / 3 days for 10–25 / 26–50 / 51–100 USDC.
- Loans after bootstrap: standard duration of 90 days.

5.1 — Application for eligibility

The credit recipient shall connect a portfolio and provide only the data necessary for the relevant step and risk signals. The system checks active loan, cooldown period, score, KYC, device/network, source of funds, grouping, request velocity and envelope capacity.

5.2 — Start-up journey

For an eligible credit recipient without a history, the loan is 10–25 USDC for 30 days. The guarantee is 0% only when there is capacity in the unsecured bootstrap sub-limit, which cannot exceed 20% of the available block of 80% of the capital activated.

5.3 — Normal journey

After a valid repayment and cooldown period, the credit recipient may apply for 26–100 USDC for 90 days, limited by the scale of score, the applicable verification and the ability to deposit collateral. Guaranteed credit up to 100 USDC can use up to 50% of the available block of 80%.

5.4 — Score scale

Score 0–20: up to 25 USDC. 21–40: 50. 41–60: 70. 61–80: 90. 81–100: 100.

5.5 — Calculation of the security (stake)

The system calculates a guarantee from 28% to 26–50 USDC and 26% to 51–100. Future tiers use 24% for 101–200 USDC, 22% for 201–300 USDC, 21% for 301–400 USDC and 20% for 401–500 USDC. The 101–200 range requires KYC; 201–500 requires KYC + selfie.

5.6 — Price disclosure

Before confirmation are presented main, duration, stake and total repayment with fixed fixed simple interest of 5% per month.

5.7 — Authorisation and disbursement

The contract validates limits, permission, balances, projected usage and pause state. Disbursement is recorded on-chain and updates exposure and monitoring.

5.8 — Asset loan controls

Only a loan may be active per credit recipient. New requests, correlated attempts and portfolio, device or fund origin bypasses are blocked or revised.

5.9 — Repayment

The credit recipient pays principal and interest. The guarantee is released in accordance with applicable rules, the unified pool receives the funds and the reputation is updated.

5.10 — Reminder cycle

The system communicates 7 days, 3 days and 24 hours before maturity; in due date; and after +1, +3 and +7 days. The classification of default occurs at +30 days, subject to authorised execution.

5.11 — cooldown period

The cooldown period is 7 days after 10-25, 5 days after 26-50 and 3 days after 51–100. History does not delete cluster or risk-triggered KYC controls.

5.12 — default

Failure to comply changes reputation, registers gross default, applies stake effects when existing and calculates net credit loss separately. Bots do not mark default with autonomous financial authority.

5.13 — Future capacity

Any loan above 100 USDC requires landmark evidence, governance, KYC and capital; contract documentation does not imply activation.

5.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The life cycle of a loan in the MICrO Protocol was conceived as a deterministic, fully traceable and auditable process. Each phase of the cycle is defined by explicit conditions that ensure financial integrity and operational predictability.

The full cycle of a loan includes the following steps:

Each of these steps performs specific validations that prevent abusive behaviour and preserve pool stability.

The process starts when a user requests a loan through the function

Before execution, the system validates multiple parameters.

- necessary stake must be available

If any condition fails, the transaction is automatically reversed.

The stake represents a partial loan guarantee.

The stake value is calculated based on a progressive table.

This model protects the pool from excessive losses.

After validation and stake confirmed, the contract creates the loan.

This data is stored permanently on-chain.

The deadline is calculated automatically

This differentiation reduces initial risk.

- loan Duration and Start Access Policy

The default maturity of loans in the MICrO Protocol is 90 days.

There is a controlled exception for the first access to the system, called Bootstrap loan.

- does not require initial user stake

the corresponding stake can be temporarily supported by the protocol as an initial inclusion mechanism

This exception exists to allow new users to access the system without the need for initial capital, reducing the entry barrier and promoting financial inclusion.

- applies only to the first eligible loan
- values are intentionally low to limit risk exposure

After issue, the loan goes into active state.

- the contract monitors the remaining time

No manual change is required.

repayment occurs through function

If the deadline expires without payment, the loan will be defaulted.

After repayment or default, the reputational score is updated.

The score influences future eligibility.

a mandatory cooldown period is applied.

This mechanism reduces abusive cycles.

The verification takes place before the creation of the loan.

There are no undefined intermediate states.

This simplifies audit and analysis.

Each relevant action generates on-chain events.

This mechanism allows for complete traceability.

The integrity of the cycle is guaranteed by

This model reduces operational risk.

Chapter 6 — Risk Management Framework

Baseline v2.0 applicable to this chapter

- Risk is controlled by stake, exposure, reputation, KYC, cooldown, liquidity and anti-Sybil — not variable interest.

6.1 — Risk philosophy

The protocol preserves capital before pursuing growth. The risk is contained by independent layers and verifiable limits.

6.2 — Exposure risk

punctuation and tier limit main. The active credit limit limits aggregate exposure. The 80% hard cutting prevents compromising all activated liquidity.

6.3 — Economic alignment

Variable stake creates partial loss alignment and absorption. Bootstrap 0% is a limited specific operational exception, not open-ended unsecured lending.

6.4 — Price limit

Interest remains fixed at 5% simple per month. Additional risk reduces exposure, increases verification or blocks eligibility; does not increase the price of the credit recipient.

6.5 — Liquidity States

Normal below 70%; WATCH from 70%; pause-readiness from 75%; hard harvest from 80%; spare floor from 20%.

6.6 — default thresholds

Warning noncompliance is 15% and critical is 25%, calculated on a exposure-weighted principal basis. Net credit loss is analysed after recoveries and stake effects.

6.7 — Identity risk and Sybil

Wallet, device, network, ASN, VPN/Tor, source of funds, speed and behaviour are evaluated individually and by cluster.

6.8 — Concentration risk

Limits per beneficiary of credit, tier, cohort, cluster, origin of funds, day and week prevent invisible concentration.

6.9 — Operational risk

Runbooks, alert routing, backups, health monitoring and separation of responsibilities reduce human and technological failure.

6.10 — Risk of governance

Safe 3-of-5 and Timelock remove single-owner control. Signer costody and recovery continue production requirements.

6.11 — Risk of smart contracts

Invariants, rate limits, single active loan, pause, access control, testnet regression and external audit protect the lifecycle.

6.12 — Legal and data risk

KYC/AML, privacy, consumer terms, slow analysis and token posture are gateways prior to production.

6.13 — Limit of human decision

Automation observes and recommends. Pause, unpause, authorised default, upgrades, capital activation and critical changes remain approved by human intervention.

6.14 — Calibration

Thresholds are monitored during the pilot and may restrict exposure. The 5% rate is not used as a calibration mechanism.

6.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The MICrO Protocol is designed with a risk management model integrated directly into the system architecture. Instead of relying exclusively on human supervision, control mechanisms are implemented in smart contracts and mathematical deterministic rules.

The approach used follows a central principle

Risk must be constrained before capital is exposed.

In other words, no loan is issued without multiple protection mechanisms being applied in advance.

The system does not eliminate risk — but controls its distribution and impact.

The protocol uses a multilayer protection model.

Each layer absorbs part of the risk before the next layer is affected.

Each level acts as a progressive barrier to losses.

The stake represents the first line of defense against losses.

- mandatory before the issue of the loan

This mechanism reduces net pool exposure.

Interest paid by credit recipients accumulate value over time.

This margin creates a natural operating reserve.

Without accumulated interest, the pool would be vulnerable to successive small losses.

This reserve acts as a financial buffer.

If risk indicators exceed defined limits, governance may intervene.

These actions are executed through timelock.

new loans can be suspended.

This mechanism prevents the risk from getting worse.

The economic model of the protocol was tested with multiple scenarios of default.

Simulations indicate consistent structural results.

These values represent typical system behaviour under simulated conditions.

This model allows for early response.

One of the most dangerous risks in financial systems is excessive use of liquidity.

To avoid this scenario, the protocol defines

Even under stress, minimal liquidity is preserved.

Insufficient liquidity can cause systemic failure.

The protocol protects liquidity through

These mechanisms ensure operational stability.

Each credit recipient is assessed individually.

These rules reduce individual exposure.

This mechanism reduces systemic load.

Protocol monitors critical indicators.

preventive measures can be applied.

Net exposure represents real capital at risk.

This model allows predicting potential impact of defaults.

Sybil attacks represent a significant risk.

The protocol reduces this risk through

new wallets do not receive immediate access to high values.

The preservation of capital is the primary objective.

Without these measures, the system would be vulnerable.

In addition to financial risk, there are operational risks.

The governance model reduces these risks.

Chapter 7 — Liquidity and Capital Management

7.1 — Capital architecture

The MICrO Protocol strictly distinguishes the committed capital from the activated capital. The pilot's committed reserve may reach 112,500 USDC but is not a fully exposed pool. Only a substantially lower active credit limit is released by stages after approval of governance and verification of operational conditions.

7.2 — Unified credit reserve

The protocol uses a single operating lending pool. There are no liquidity reserve, Emergency Pool or separate accounting divisions of interest. The protection is the result of use limits applied to the activated capital and unactivated capacity kept out of exposure.

7.3 — Use limit and reserve floor

Maximum use is 80% of the active credit limit. Consequently, at least 20% of the capital activated remains available as a reserve floor. This floor is a restriction of use, not a second pool.

7.4 — Operational States

Normal: use less than 70%. WATCH: 70% or more. Pause-readiness: 75% or more use. Hard mowing: 80%. New disbursements are blocked when they can breach the ceiling.

7.5 — Limits per segment

During the initial phase, unsecured start-up is limited to 20% of the available block of 80% of the capital activated. The credit supported by guarantee up to 100 USDC is limited to 50% of that same block available. The remaining capacity supports safety, delays, concentration and phased expansion.

7.6 — Capital activation

Each increase in the envelope requires evidence of repayments, absence of adverse concentration, integrity of the reserve floor, revision of risk clusters and execution Safe 3-of-5 via Timelock.

7.7 — Interest treatment

The interest paid returns to the unified pool. There is no fixed 80/20 split between pools. Accounting separates principal, interest, recovered or secured stake and net losses without fragmenting operational custody.

7.8 — Pressure and pause logic

WATCH initiates enhanced review. Pause-readiness prepares human action. Reaching or designing 80% prevents further exposure. Bots watch and warn, but do not run pause or unpause autonomously.

7.9 — Integrity of reservation

The central metric is the joint integrity of the committed reserve, activated capital and 20% floor. The protocol reports use, concentration, maturity, delays, gross default and net credit loss.

7.10 — Conclusion of design

Architecture favours preservation of liquidity before growth. The committed reserve supports capacity; the active envelope defines real risk; hard cutting limits exposure.

7.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The protocol uses a unified pool-based liquidity model with user control.

- Liquidity Model = Unified Pool with Usage Control

These structures can be introduced into future versions, but are not part of the current implementation.

This model maintains operational stability.

Interest paid by users is accumulated in the unified pool.

This model belongs to future versions.

The system protects liquidity through

In future versions, the protocol may introduce

- Current Implementation = Single Unified Pool

Liquidity Pool represents the capital available for lending.

This pool is the main source of operational liquidity.

Liquidity Pool funds are used exclusively for

- maintenance of operational availability

Any misuse of this capital would undermine the stability of the system.

This reserve is progressively accumulated through

Without this reservation, successive defaults could compromise the system.

This model creates progressive growth of the reserve over time.

This pool is used only in critical situations.

This reserve is not used in normal operations.

One of the most important mechanisms of the protocol is the maximum use limit of the pool.

This limit prevents excessive exposure.

Even under high load, minimum liquidity remains available.

The total capital of the system is divided into multiple functions.

This structure creates financial redundancy.

Interest paid by credit recipients shall be reinvested automatically.

This mechanism creates organic pool growth.

This cycle creates sustainable growth.

In stress scenarios, the system applies conservative measures.

- temporary suspension of new loans

When default occurs, losses are progressively absorbed.

- 2 — Cumulative interest makes up for losses

This structure reduces direct impact on Liquidity Pool.

Liquidity growth occurs through

It doesn't depend on exponential growth.

The system monitors critical indicators.

These indicators allow continuous assessment of financial health.

Multiple scenarios were modeled.

These scenarios help set safe operating limits.

Long-term sustainability depends on

Without these elements, the system would become unstable.

MICrO Protocol is designed to prevent uncontrolled growth.

Chapter 8 — Credit Reputation and Score System

Baseline v2.0 applicable to this chapter

- Ladder live: score 0–20 → 25; 21–40 → 50; 41–60 → 70; 61–80 → 90; 81–100 → 100 USDC.

8.1 — Objective

The reputation transforms observed behaviour into progressive eligibility, without assuming identity or solvency from a single sign.

8.2 — Score interval

The operational score ranges from 0 to 100 and is updated with repayments, punctuality, defaults, inconsistencies, revisions and authorised signals.

8.3 — Active scale

0–20: maximum 25 USDC. 21–40: 50. 41–60: 70. 61–80: 90. 81–100: 100. There are no gaps between bands.

8.4 — Pilot limit

No score authorises more than 100 USDC during active pilot. The ceiling of 500 is a future capacity controlled by governance.

8.5 — Eligibility for startup

Credit recipients without history may enter the bootstrap 10–25 provided they comply with wallet, device/network rules, fund origin, cluster, envelope and applicable verification.

8.6 — Positive evidence

Early or punctual repayment, device consistency, absence of adverse correlation and repeated history can support progression.

8.7 — Negative evidence

Late payment, default, circular melting, multiple correlated wallets, abnormal speed or inconsistency KYC reduce score, impose review or block.

8.8 — Interaction with KYC

punctuation does not replace KYC. Basic KYC applies to 51–100 and may be required before by risk.

8.9 — Interaction with cooldown period

high score does not eliminate cooldown period: 7/5/3 days as the tier completed, besides cluster-level cooldown period.

8.10 — Explanation

Decisions record reasons, rules, version and evidence to allow for audit, human review and false positive measurement.

8.11 — Limitation of calibration

Weights and thresholds require live calibration. Synthetic results and Base Sepolia demonstrate functioning, not predictive quality in production.

8.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The reputational system of the MICrO Protocol is the core of individual risk management. Unlike traditional models that depend on formal banking history, the protocol builds reputation directly based on on on-chain financial behaviour.

This model allows users without formal financial history to build credibility progressively, using only verifiable interactions within the protocol.

The reputational system serves three main objectives

- 3 — Allow for progressive credit growth

Each user action contributes to a verifiable financial history.

The reputational score is calculated based on verifiable events rather than subjective evaluations.

Each financial event generates a change in score.

This model ensures consistency between users.

The reputational score is represented by a numerical value.

This system allows automatic throshold-based decisions.

New users start with base score.

This value represents absence of history.

After first successful repayment

This mechanism creates natural progression.

The score increases when the user demonstrates consistent behaviour.

This model rewards financial discipline.

This mechanism penalises irresponsible behaviour.

This model creates controlled progression.

The reputational history remains permanently stored.

This prevents manipulation of the system.

Each user maintains complete history.

The system monitors behaviour over multiple loans.

These data allow longitudinal analysis.

Sybil attacks are one of the main risks in decentralised systems.

The reputational system reduces this risk through

New wallets cannot obtain high values immediately.

This mechanism reduces incentive for massive portfolio creation.

Limits are defined based on the score.

Users with a negative history can regain reputation.

- Successful subsequent repayments

This mechanism allows gradual recovery.

The system allows us to identify suspicious patterns.

These signs can be used for intervention.

All reputational data is stored on-chain.

This model eliminates manual manipulation.

Chapter 9 — Sybil Anti-Fraud and Attack Protection System

9.1 — Objective and state

The anti-Sybil system has been prepared for the pilot, but its actual effectiveness remains subject to calibration with live data. No isolated signals authorize credit; decisions combine deterministic rules, correlation analysis and human review.

9.2 — Identity and wallet signs

Signs include wallet age, on-chain history, creation cadence, address reuse, transaction patterns, and wallets relationships.

9.3 — Device and network controls

Device fingerprint, IP prefix, ASN, approximate geolocation, VPN, Tor, proxies and networks considered suspicious are evaluated. These signals are treated proportionally and with data minimization.

9.4 — Correlation of origin of funds

The system identifies wallets funded by the same origin, coordinated funding sequences, fan-out and fan-in, common repetitive and intermediate values.

9.5 — Grouping of correlated portfolios

Correlated Wallets, Devices, Networks and Funding Sources form operational clusters. The risk is measured at both individual and cluster levels.

9.6 — Grouping checks

Cluster-level cooldown period, speed limits, exposure limits, mandatory revision for high risk and blocking simultaneous or sequential attempts to circumvent individual limits apply.

9.7 — Start-up limits

The unsecured segment operates within daily and weekly envelopes, limited to 20% of the available block of 80% of the capital activated. Reaching an envelope suspends new authorizations without affecting repayments.

9.8 — Progressive verification

The protocol may require lightweight verification or scale KYC before monetary threshold when there are signs of fraud, strong correlations or behavioural inconsistencies.

9.9 — Speed and behaviour

Repeated requests, device changes, merging immediately prior to request, circular reimbursement, time patterns and coordinated behaviour are monitored.

9.10 — Human Review and Governance

High-risk cases enter into manual review. Bots can observe, classify, recommend and warn; privileged decisions remain subject to authorised operators and governance.

9.11 — False positives and review

The pilot measures false positives, climbing time, review rate and outcomes. A revaluation mechanism prevents statistical correlation from being automatically treated as evidence of fraud.

9.12 — Privacy and conservation

The data shall be limited to what is necessary for security, subject to defined retention, access control and jurisdiction-specific legal review.

9.13 — Calibration declaration

The controls were tested with synthetic data and multi-wallet scenarios. There are no effective results based on human credit beneficiaries of the Vietnam pilot.

9.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

decentralised systems face specific risks related to fragmented digital identity. Unlike traditional financial institutions, where each client has a verifiable formal identity, decentralised protocols operate with cryptographic addresses that can be created without restrictions.

This behaviour creates the risk known as

In this type of attack, a single user controls multiple portfolios and tries to obtain multiple loans simultaneously, increasing system exposure.

MICrO Protocol is designed to mitigate this risk through multiple layers of protection.

A typical Sybil attack follows a predictable pattern

- 2 — Request for multiple loans
- 3 — Initial repayment for creating a reputation
- 4 — Simultaneous request for higher values

This behaviour can cause significant losses if not mitigated.

The protocol assumes that this behaviour will occur and implement preventive mechanisms.

The anti-fraud system follows a multi-layer architecture.

Each layer reduces the probability of successful attack.

Each layer reduces incremental exposure.

New users cannot immediately access high values.

gradual access to higher values.

This model reduces initial impact of attacks.

The mandatory cooldown period is one of the main defenses against abuse.

- reputation cannot be handled quickly

This mechanism slows down coordinated attacks.

Reputation growth is deliberately slow.

This behaviour reduces incentive for artificial manipulation.

This model prevents rapid gains in trust.

The system analyzes behaviour patterns to identify suspicious activities.

- multiple recently created portfolios
- repeated requests in short intervals

These patterns indicate potential fraud.

Very recent portfolios present a higher risk.

The system can apply age-based restrictions of the portfolio.

This mechanism reduces initial risk.

The system allows identifying groups of portfolios with similar behaviour.

- multiple portfolios with similar funding

These signals indicate potential fraudulent cluster.

The protocol was tested using a multi-wallet simulation model.

This model allowed us to observe real behaviour under simulated conditions.

Results demonstrated operational stability under multiple scenarios.

Certain behaviors trigger automatic responses.

These events reduce future eligibility.

In cases of high risk, the system may require additional stake.

- portfolio associated with suspicious cluster

This mechanism reduces net risk.

If critical standards are identified

These actions are executed via multisig.

This model limits financial impact.

The purpose of the system is not only to detect fraud — but to make it economically impossible.

If the cost of fraud is greater than the potential gain

fraud becomes economically irrational.

Chapter 10 — Economic Model and Fixed Interest Structure

10.1 — Fixed price for the credit recipient

The economic baseline uses fixed fixed simple interest of 5% per month. The rate does not vary with score, tier or risk and is not an ordinary operating parameter of governance.

10.2 — Formula

Interest = Main × 0,05 × Months. Total repayment = Main + Interest. There is no capitalisation within the loan or additional fee by loan during the pilot.

10.3 — Examples

A bootstrap of 10 USDC for 30 days pays 10.50 USDC; 25 USDC pays 26.25 USDC. A loan of 50 USDC for 90 days pays 57.50 USDC; 100 USDC pays 115 USDC.

10.4 — Risk adjustment

The risk is not covered by variable interest. It is controlled by variable stake, exposure limit, reputation, KYC, cooldown period, liquidity envelopes, concentration and anti-Sybil.

10.5 — Guarantee scale

10–25 USDC: 0% only in unsecured controlled envelope. 26–50: 28%. 51–100: 26%. 101–200: 24%. 201–300: 22%. 301–400: 21%. 401–500: 20%.

10.6 — Active and future intervals

The active maximum pilot is 100 USDC. The ranges between 101 and 500 USDC document future governance-controlled capacity; they do not represent current availability. Level 101–200 requires KYC. Levels 201–500 require KYC + selfie.

10.7 — Exposure accounting

Gross exposure is the main disbursed. Net exposure considers stake effectively available for loss absorption. Gross default and net credit loss after recoveries or stake effects are reported separately.

10.8 — default methodology

Default rate is calculated on a principal expose-weighted basis. Target values and thresholds are monitoring hypotheses, not guarantees. Up to 15% is a healthy operating range; about 20% is marginal; approximately 30% is structurally unsustainable.

10.9 — Economic viability

A universal break-even rate is not presented because viability depends on the mix of tiers, duration, stake, recoveries, operational costs and pace of capital reuse. The old estimate of 9.54% is not protocol baseline.

10.10 — Treatment of the liquidity reserve

Main, interest and recoveries return to the unified operational pool. There is no 80/20 fixed distribution for a separate liquidity reserve.

10.11 — Transparency

The credit recipient shall know in advance the principal, duration, stake and total repayment. Price predictability is a central property of the model.

10.12 — Pilot validation

The pilot measures reimbursement, default, net loss, use, reserve integrity and stake effects. Any expansion is conditioned by evidence.

10.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The economic model of the MICrO Protocol was developed with a focus on long-term financial sustainability, avoiding dependence on artificial growth or continuous influx of external capital.

Unlike systems based on inflationary incentives or constant subsidies, the MICrO Protocol uses an economic model based on:

This model allows liquidity to gradually increase over time while maintaining controlled exposure.

The main objective of the economic model is to ensure

- Net positive reserve growth with controlled default rates

That is, positive net growth while defaults remain within acceptable limits.

The basic interest rate used in the system is

This value was selected based on multiple economic simulations and risk analyses.

The goal was to find a balance between

- Interest = loan Amount × Interest Rate

This model simplifies mathematical validation and audit.

Net exposure represents the real capital at risk after application of the stake.

This model significantly reduces potential losses in the event of default.

The profitability of the pool depends on three main factors

These three factors determine net growth.

These factors increase pool capacity over time.

The impact of default was analysed through extensive simulations.

These values demonstrate economic behaviour under different conditions.

These limits define clear operational boundaries.

The minimum interest rate required for sustainability under different scenarios has been calculated.

This figure shows that the 5% rate depends on effective control of defaults.

the system depends more on risk discipline than high interest.

Economic growth occurs through repeated cycles.

This cycle creates progressive expansion.

This mechanism partially compensates for losses.

This mechanism reduces financial impact.

These limits guide operational decisions.

Interest paid shall be distributed among multiple functions.

This model strengthens financial stability.

The model was tested under multiple scenarios.

Results showed predictable behaviour.

The capital efficiency is measured by the ability to generate return without increasing excessive risk.

These mechanisms reduce financial waste.

The sustainability of the protocol depends on

Without these elements, the system would become unstable.

The MICrO Protocol is designed to operate within predictable financial limits.

Chapter 11 — Tokenomics and MICrO Token Utility

11.1 — Supply and allocation

The maximum reference supply is 10,000,000,000 MICrO. The current formulation provides for: Lending Pool Support 40%; Reserve & Stability 15%; Team 15%; Ecosystem 10%; Strategic Partners 10%; Community 5%; Governance Reserve 5%.

11.2 — Credit denominated in USDC

Protocol loans remain denominated and settled in USDC. The Lending Pool Support allocation does not mean that credit recipients receive loans in MICrO.

11.3 — Support function

The Tokens reserved for Lending Pool Support are intended for future mechanisms of economic support, incentives, capitalization or conversion subject to final design, governance and legal analysis.

11.4 — Limits on utility

The token does not replace underwriting, KYC, liquidity controls or governance execution. Any utility must be introduced progressively and without compromising the predictability of the credit in USDC.

11.5 — Governance

Governance rights, if activated, do not eliminate Safe 3-of-5 or Timelock for critical actions. On-chain execution remains limited by security architecture.

11.6 — Vesting and disclosure

Vesting, unlocks and custody, market-making and fundraising require own documentation and legal review before any public offer or TGE.

11.7 — Terminology of capital planning

Fundraising values or capital scenarios are planning assumptions, not closed rounds, executed commitments or valuation guarantees.

11.8 — System separation

token economics and lending economics are analysed separately. The sustainability of the pilot shall be demonstrated by repayments, losses, costs and capital in USDC.

11.9 — Evidence gate

Any expansion of the utility of the token depends on audit, legal stance, operational governance and evidence of credit operation.

11.10 — Mint policy

The maximum and total supply is 10,000,000,000 MICrO. The 10 billion tokens are created entirely at genesis mint. After this operation, there is no future, ordinary or emergency mint. The creation function shall be removed, irrevocably deactivated or technically unable to exceed the supply created in the genesis.

11.11 — Circulation and unlocks

Genesis mint does not equal integral circulation. The quantity in TGE circulating supply will be low and defined before launch. The remaining tokens remain in treasury, vesting contracts and locked allocations, according to schedules, cliffs, milestones and published conditions.

11.12 — Vesting and treasury

Team vesting includes a long cliff. The strategic vesting is set before the corresponding round. The treasury remains blocked and governed through Safe 3-of-5 and Timelock, with no possibility of unilateral unlocking.

11.13 — Burn and buyback policy

Burn may be allowed, but it's never automatic. Any relevant burn requires published policy, public proposal, approval of Safe 3-of-5 and execution through Timelock. The permissible origin is limited to tokens acquired through buyback or tokens of the expressly authorised treasury. Tokens belonging to users cannot be burned by protocol.

11.14 — Burn limits

Each burn complies with a limit previously published or approved in a specific governance proposal. Burn does not alter the ban on future mint and does not create authorisation to reissue the destroyed tokens.

11.15 — Buyback and use of revenue

Buyback is optional, non-automatic and can only use distributable economic surplus. The revenue priority is: solvency, reserve floor, expected losses, operating costs and credit capacity; only then can they be considered buyback, burn or other mechanisms associated with the token.

11.16 — Emergency powers

Emergency powers cannot create tokens, unlock vesting, unilaterally move the treasury, execute burn without authorisation or bypass Timelock. Any material change in governance remains subject to mandatory delay.

11.17 — Solvency principle

No issuance, release, repurchase, burning, distribution or use of tokens may compromise the solvency, minimum reserve, operational liquidity or credit capacity of the MICrO Protocol.

11.18 — Token decision matrix

Theme	Formal decision
Maximum supply	10,000,000,000 MICrO
Genesis mint	10,000,000,000 MICrO
Future minting	None after genesis
TGE circulating supply	Low and set before launch
Unlocks	Published schedule and milestones
Team vesting	Long cliff
Strategic vesting	Set before round
treasury	Blocked and governed
Burn	Allowed only according to published policy
Buyback	Optional and limited to distributable surplus
Origin of burn	Tokens bought back or authorised treasury tokens
Burn limit	Defined by governance
Revenue allocation	Reserve and credit capacity first; token afterwards
Emergency powers	Explicitly limited
Governance changes	Mandatory Timelock

11.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

MICrO Token is the protocol's complementary economic element designed to support future governance, operational incentives and ecosystem stability.

Unlike purely speculative tokens, MICrO Token is designed with specific utility functions directly related to the operation of the microcredit system.

The token is not used as the main currency of loans, a function performed by stablecoins as USDC, but as an instrument of operational support and economic incentive.

This model reduces financial volatility and improves operational predictability.

The total supply of MICrO Token is defined as

- Total Supply = 10,000,000,000 MICrO

This value has been selected to allow distribution flexibility and long-term growth support.

The total supply is fixed and non-inflationary.

There are no automatic additional creation mechanisms after the initial launch.

The initial distribution was designed to balance operational sustainability and strategic incentives.

This distribution supports multiple functions.

The largest portion of supply is dedicated to liquidity support.

This allocation allows for controlled expansion.

This allocation creates an additional strategic reserve.

This reserve works as an economic buffer.

Team allocation follows structured vesting rules.

This model reduces risk of early sale.

Part of the tokens are reserved for ecosystem development.

This fund allows for sustainable growth.

A small portion is intended for Community incentives.

This mechanism facilitates initial adoption.

MICrO Token will allow future governance.

This functionality will be activated after system maturity.

The token can be used for staking.

Staking creates economic alignment between users and protocol.

The search for the token will be influenced by

Real utility sustains economic value.

There are no inflationary mechanisms.

This model reduces inflationary pressure.

This model creates sustainable utility.

Chapter 12 — Governance and Control of the Protocol

12.1 — Defined governance path

The architecture defined is Safe 3-of-5 → Timelock → critical contracts. No individual EOA satisfies the normal governance process.

12.2 — Safe 3-of-5

Five independent signers form the set of authorizations; three approvals are required. Final custody should be hardware-backed, with operational separation and replacement procedures.

12.3 — Timelock

Safe-approved critical actions are executed through Timelock, creating observable delay for review, alerts and incident response.

12.4 — Critical actions

They include upgrades, change of limits, capital activation, pause/unpause, role management, treasury movements and enabling future tiers.

12.5 — Fixed interest limit

The fixed simple interest of 5% per month constitutes a fixed baseline. They are not presented as ordinary risk pricing variable or governance calibration.

12.6 — Human approval

Bots do not independently execute privileged actions. They observe, simulate, recommend and warn; human operators initiate and approve actions according to runbooks.

12.7 — Emergency controls

Pause protects new disbursements and risk functions without preventing, where technically possible, repayments and orderly recovery. Unpause requires documented evaluation.

12.8 — Operations of signatories

Production deployment remains conditioned to signer set confirmation, costy, registry, backups, incident reporting and recovery tests.

12.9 — Audit trail

Proposals, approvals, execution, on-chain events and operational evidence are registered for audit.

12.10 — Parameter classes

Parameters are classified as fixed, bounded or reserved for the future phase. Bunded changes respect predefined limits; future capabilities require milestone evidence and complete governance execution.

12.11 — Limitations of governance

The architecture was tested at Base Sepolia. This is not equivalent to production, completed external audit or legal validation.

12.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The governance of the MICrO Protocol is designed on the basis of operational security, transparency and distributed control principles. Unlike centralised systems where critical decisions are made by a single entity, the protocol uses a structured governance model based on multiple authorised participants.

The main objective of the governance system is to ensure that no critical change can be executed unilaterally, significantly reducing the risk of human error, abuse or impairment of individual keys.

The central philosophy can be summarized as

- Controlled governance with mandatory delay

In other words, all critical changes follow a mandatory cooldown period before execution.

The governance structure consists of three main elements:

- 1 — Multisignature Wallet

Each component has specific and independent functions.

This structure prevents direct changes without multiple approval.

The system uses a multisignature portfolio as a decisional core.

- at least 3 signatures are required
- no individual person controls the system

This configuration balances security and operationality.

Without enough quorum, no action occurs.

The protocol uses a Timelock mechanism to ensure that all critical changes are executed with deliberate delay.

- preventive intervention in the event of malicious error or behaviour

Critical protocol contracts are controlled by Timelock.

This means that no change can occur without going through Timelock.

The minimum delay applied to all critical actions is

The 48-hour value was defined based on operational safety principles.

Without this delay, critical changes could be implemented without the possibility of intervention.

All changes follow a mandatory sequential flow

This model prevents immediate execution of critical actions.

The following actions require Timelock

None of these actions can be executed instantly.

In development and testing environments, Timelock can be temporarily reduced.

- Production Deployment = Always 48 hours

This ensures consistency with the safety model described in this document.

This flow ensures predictability.

Each change follows a defined cycle.

This model ensures operational consistency.

The protocol includes an emergency pause mechanism.

This function allows to block new credit issues.

This behaviour preserves liquidity.

After solving the problem, the system can be reactivated.

This process follows the approval of governance.

This mechanism allows for safe recovery.

Certain parameters can be adjusted via governance.

Each change follows the full flow of governance.

- multiple signatories are used

All changes are recorded on-chain.

Initially, the system uses multisig-based governance.

Token-based governance can be introduced.

This transition will occur only after operational maturity.

Chapter 13 — Smart Contract Security Architecture

Baseline v2.0 applicable to this chapter

- Safe 3-of-5 → Timelock → critical contracts; no single EOA in the normal process.
- Base Sepolia has been tested; production and external audit continue gated.

13.1 — Safety objectives

The architecture protects funds, accounting, loan states, role and governance, assuming human failure, abuse, Sybil correlation and adverse conditions.

13.2 — Access control

Roles use least privilege. Critical actions belong to Safe 3-of-5 → Timelock; no single EOA normally controls the system.

13.3 — Invariants of the loan

A credit recipient has at most an active loan. Main, stake, maturity, repayment and status obey explicit transitions and auditable events.

13.4 — Level validation

Contracts and services validate the maximum live of 100 USDC, score ladder, stake 28%/26% in live tiers and future stage status for 101–500.

13.5 — Validation of the cooldown period

The cooldown period is calculated by the finished tier: 7 days for 10-25, 5 for 26-50 and 3 for 51–100. Group-level cooldown period is applied outside the contract when necessary.

13.6 — Interest invariant

The calculation uses 5% simple per month and defined duration. Normal governance does not use the rate as variable risk mechanism.

13.7 — Liquidity invariant

Disbursement is rejected if it increases use above 80% of the active envelope. The 20% reserve floor belongs to the unified pool.

13.8 — Arithmetic and token safety

Solidity 0.8.x, checks-effects-interactions, safe token handling, verified decimals and rounding tests protect accounting.

13.9 — Implementation of default

Failure classification occurs after defined lifecycle and requires authorised operator or governed mechanism. Bots have no independent financial authority.

13.10 — Concept of pause

Pause blocks new risk and preserves, where possible, repayments and recovery. Unpause requires review and governed execution.

13.11 — Timelock controls

Upgrades, roles, capital activation, pause/unpause and future capacity clearance pass through Timelock after 3-of-5 approval.

13.12 — Monitoring

Loan, repayment, default, stake, use, pause and governance events feed V2 Monitor and alerts.

13.13 — Evidence of testing

Base Sepolia covered multi-wallet flows, repayments, reputation, governance, pause/unpause, pool monitoring and stress/synthetic scenarios.

13.14 — External guarantee

Testnet testing does not replace independent audit, formal review, signer operations or production validation.

13.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

Security is one of the fundamental pillars of the MICrO Protocol. Since the early development phase, the system has been designed with a focus on preventive protection, integrating safety mechanisms directly into the logic of smart contracts.

Unlike systems that rely exclusively on external audits after development, the MICrO Protocol adopts a model of:

In this model, risks are considered during initial design and mitigated before final implementation.

The main objective of the security architecture is to ensure

The development of contracts follows a strict set of principles.

Each critical function includes explicit checks.

If a condition is not met

This behaviour prevents inconsistent states.

All operations follow predictable rules.

To reduce attacks based on rapid repetition of orders, a rate limiting mechanism has been implemented.

a new request may only occur after the defined interval.

Before creating a new loan, the system checks active status.

This mechanism reduces abusive behaviour.

Mathematical operations are overflow protected.

This model avoids unexpected results.

Critical functions have access restrictions.

These functions are accessible only via governance.

Critical changes are not executed immediately.

follow a process with mandatory delay.

This delay allows external validation before execution.

The system includes an emergency pause function.

block new operations in case of risk.

Each loan application is subject to multiple checks.

The protocol defines a controlled mechanism to declare default (default), ensuring that execution is supervised and cannot be abused.

After the MC-02 security remediation, the markUnfulfillment() function ceased to be allowed and began to require explicit authorisation.

A loan is considered in default when

Where these conditions are verified, the loan becomes eligible for marking as default.

The execution of the markUnfulfillment() function requires authorised operators.

The function is neither automatic nor allowless.

Only approved entities may implement this action.

These operators are defined through the governance system and can be updated via Timelock.

The authorised model was adopted to avoid

Without this control, any user could force undue default.

After valid execution of markFailure()

- The protocol absorbs controlled exposure

All changes to authorised operators follow

No operator can be added or removed without going through the governance process.

All critical operations generate events.

These events allow continuous monitoring.

The protocol was tested under multiple scenarios.

These tests validated functional integrity.

Simulations with high volumes were performed.

This kind of test validates robustness.

The protocol was prepared for external audit.

The goal is to ensure complete transparency.

Chapter 14 — Network Strategy and Deployment Architecture

14.1 — Current network status

The relevant contracts and flows were tested in Base Sepolia. The current state is tested on testing network, not mainnet or production.

14.2 — Tested capacities

Lending, repayment, reputation, multi-wallet flow, liquidity monitoring, governance, pause/unpause, Monitor V2, stress testing and synthetic fraud scenarios were executed.

14.3 — Stablecoin

The test environment uses USDC testnet representation. The pilot and any production depend on the selection and verification of the correct USDC contract on the chosen network.

14.4 — Contract deployment

Deployments must be reproduceable, verified, versioned and associated with approved address registry. Roles and ownership follow Safe 3-of-5 → Timelock.

14.5 — Pilot implementation environment

The pilot uses consolidated runtime with separate responsibilities for risk, fraud, chain, health, alerts, backup and repayment. Hosting provider is not fixed as protocol baseline.

14.6 — Separation of environments

Development, Base Sepolia, staging/pilot and eventual production use separate secret, PRCs, wallets, databases and alert channels.

14.7 — Observability

Monitoring covers contract events, balances, usage, repayments, overdue states, cluster signals, health, lateency, backups and governance execution.

14.8 — Implementation milestones

Production requires audit, legal readiness, signer costady, runbooks, recovery tests, verified addresses, monitoring and formal governance approach.

14.9 — Update and reversal

Changes follow review, testing, Safe approach and Timelock. Pause and recovery are tested before activating new capital.

14.10 — Scalability journey

Postpilot, workers can be separated gradually. Public scale can use independent services, queues/events, redundancy and failover, only when justified by evidence.

14.11 — Discipline of allegations

“Tested” describes Base Sepolia; “prepared” describes pre-launch operations; “live” will only be used after real credit recipients and activated capital.

14.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The deployment strategy of the MICrO Protocol is designed to allow progressive validation of the system before entering a productive environment.

Instead of launching directly into the mainnet environment, the protocol follows an incremental model based on:

This model significantly reduces operational risk during the initial stages.

The approach allows testing real behaviour under controlled conditions before exposure to real capital.

MICrO Protocol is currently implemented in the network

This network was selected for offering

This choice allows testing real operations without exposure to financial risk.

This configuration ensures compatibility with standard tools.

Protocol contracts are implemented in a modular manner.

Each contract is deployed separately.

This allows controlled updates.

The system uses standardized tools.

These tools ensure operational consistency.

In addition to contracts, the protocol uses auxiliary components.

These components allow interaction with the system.

This approach simplifies initial operation.

Loans use stablecoins as a base unit.

This transition maintains full compatibility.

These requirements ensure financial predictability.

Before migration to production, a pilot phase will be carried out.

This pilot allows practical validation.

This process reduces production risk.

After full validation, the protocol will be migrated to the productive environment.

The choice will depend on costs and stability.

Modular architecture allows future expansion to multiple networks.

This approach allows for global growth.

Gas costs were considered during design.

These measures reduce transaction costs.

These values make the system accessible.

The system includes monitoring mechanisms.

These data allow continuous supervision.

multiple validations are performed.

Deployment roadmap follows a clear sequence.

This model allows for controlled growth.

Chapter 15 — Operational Model and Pilot Strategy in Vietnam

15.1 — Pilot State

The Vietnam Founding Pilot Programme is in pre-launch. There are still no data from human credit beneficiaries, live repayment results or signed institutional partnership that can be presented as completed.

15.2 — Structure of the programme

The programme is planned for up to 100 participants. Cohort 1 includes 25 participants; subsequent cohorts are only activated after review of evidence.

15.3 — Bootstrap

The first loan is between 10 and 25 USDC, lasting 30 days and 0% stake exclusively within the unsecured controlled envelope. This segment can use up to 20% of the available block of 80% of the activated capital.

15.4 — Normal pilot loans

Subsequent loans have a standard duration of 90 days, depend on history and score, and respect active maximum of 100 USDC. Credit up to 100 USDC with the required stake can use up to 50% of the available block of 80%. The capacity up to 500 USDC is future and governance-controlled.

15.5 — Progress of the cooldown period

After 10–25 USDC: 7 days. After 26–50: 5 days. After 51–100: 3 days. A single active loan per credit recipient is maintained. Future tiers are subject to governance, evidence and enhanced verification.

15.6 — Active limit

The pilot's committed reserve can reach 112,500 USDC; Cohort 1's active credit limit is significantly lower and released in stages.

15.7 — Operational period

The first operational observation period is 90 days, without confusing the 30-day bootstrap duration with the overall evaluation period.

15.8 — Indicator families

Financial: repayment, default, net loss, interest, utilisation and reserve integrity. Risk: Clusters, fraud, funding-source correlations, false positives and progression time. Operational: decision time, reviews, governance actions, uptime and incidents. credit recipient: bootstrap completion, progression, repeat eligibility, rejection and experience.

15.9 — repayment cycle

Reminders: 7 days, 3 days and 24 hours before; due date; overdue +1 and +3; risk scaling +7; default classification +30, subject to contract rules and authorised review.

15.10 — behavioural classes

A: Pays early. B: after first reminder. C: after a 24-hour reminder. D: due date. And: bark. F: default. These classes feed analysis and reputation without granting financial authority to the bot.

15.11 — Implementation model

In the pilot, responsibilities are separated in a consolidated runtime: bot risk, bot fraud, bot chain, bot health, bot alerts, bot backup and bot repayment. Independent workers and independent services belong to later stages.

15.12 — Expansion Gate

Expansion requires KPI review, booking integrity, cluster control, operational availability and Safe/Timelock authorisation.

15.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The MICrO Protocol is designed to be implemented progressively, Bootstrap with a controlled pilot phase before expansion to a complete operating environment.

This model reduces initial risks and allows validating actual user behaviour before introducing larger financial volumes.

The operational approach is based on

Each phase of the system is validated before the transition to the following.

The pilot phase aims to validate the operational stability of the system under real conditions.

This set of validations allows operators to adjust parameters before expansion.

The economic model of the protocol was validated through multiple structured simulations to evaluate the behaviour of the system in different operational scenarios.

These simulations are designed to reproduce realistic conditions of use, including:

The objective of these simulations was to validate

- recovery capacity after adverse events

The simulations were performed with multiple user profiles, representing different patterns of financial behaviour.

Each group was used to test

- efficiency of financial protections

The main objectives of the simulations were:

- Evaluate the tolerance thresholds for default

These tests have validated that the economic model remains sustainable within the defined limits.

The simulation results showed that the system

- Supports progressive credit recipient growth
- Protects capital under stress conditions

During the pilot, loans will have limited values.

This model reduces initial exposure.

After the first successful repayment, you can access new loans.

This model allows for gradual growth.

During the pilot, the frequency of loans will be limited.

These rules reduce systemic risk.

Monitoring of default is one of the main indicators.

This model allows for early response.

During the pilot, the data will be analysed weekly.

This monitoring allows for continuous adjustments.

During the pilot phase, governance will play an active role.

This model allows operational control.

If critical indicators are reached

Performance will be assessed based on specific metrics.

These indicators determine future reactions.

The pilot phase will be considered successful when

After pilot validation, the system can gradually expand.

Chapter 16 — Compliance and Regulation Strategy

16.1 — Proportional KYC tiers

10–25 USDC: no KYC by default, with enhanced anti-Sybil and possible lightweight verification. 26–50: score-gated, no KYC by default unless triggered by risk. 51–100: basic KYC.

16.2 — Future tiers

101–200 USDC requires KYC and only exists as future expansion. 201–500 requires KYC + selfie and remains subject to governance, activated capital and legal review.

16.3 — Risk-triggered escalation

KYC may be required before the threshold when device, network, funding-source, behaviour or cluster signals justify.

16.4 — Combating money laundering and sanctions

Prior to the live pilot, proportional screening, monitoring and recordkeeping, review and alert response procedures shall be in place, adjusted to the applicable jurisdiction.

16.5 — Data protection

Collection, retention, access and transfer of personal data depend on minimization, legal basis, security, transparency and local review.

16.6 — Controlled pilot position

The pilot is not described as an unrestricted public offer. Availability is limited, cohort-based and subject to eligibility rules.

16.7 — Absence of legal conclusion

The whitepaper describes architecture and operational intent; it does not determine licensing, token classification, tax treatment or local permissions.

16.8 — Pre-production mark

production requires specific legal advice, defined entity and contracts, approved KYC/AML policies and consumer protection processes.

16.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The MICrO Protocol is designed with awareness of regulatory requirements associated with digital financial services. Although using decentralised technology, the system has been structured to allow progressive integration with legal and operational requirements in different jurisdictions.

Unlike completely anonymous and unregulated systems, the MICrO Protocol provides for mechanisms that allow the implementation of identification, monitoring and control processes when necessary.

The main objective of the compliance strategy is

- Allowing a law-abiding operation without compromising protocol integrity

That is, allow legal compliance without compromising technical functionality.

The philosophy of compliance is based on three fundamental principles.

This model allows adapting the system to different regulatory environments without requiring profound structural changes.

The system allows gradual activation of legal requirements.

The protocol is designed to operate in multiple jurisdictions.

This flexibility allows for international expansion.

The system provides integration with identity verification services.

This level reduces initial barriers.

The protocol provides for integration with money laundering prevention mechanisms.

This model reduces regulatory risk.

Transactions can be analysed to identify suspicious behaviour.

These signals may activate additional restrictions.

The system is designed with consideration for European data protection rules.

GDPR (General Data Protection Regulation)

This model protects data from users.

This model reduces risk of regulatory conflict.

Depending on the jurisdiction, specific licences may be required.

These decisions will be taken on legal basis.

As the protocol uses stablecoins, it is necessary to consider

Regulated Stablecoins are preferred.

As the system grows, new requirements can be integrated.

This model allows for progressive evolution.

- ? institutional structure already consolidated

We now enter an even more critical chapter for investors and real operation.

Chapter 17 — Legal and Operational Positioning

17.1 — Neutral reference for jurisdiction

The protocol does not assume Portugal, a company by Portuguese quotas or the designation “MICrO Protocol, Lda.” as a definitive legal structure.

17.2 — Selection of the entity

The entity, jurisdiction, corporate governance and contractual relations will be defined before production, based on pilot, target market, costy, fundraising, token design and expert advice.

17.3 — Pre-launch in Vietnam

Vietnam is the site planned for the founding pilot, but institutional outreach does not equal signed partnership, regulatory authorisation or start of operation.

17.4 — Analysis of credit activity

Credit licensing, intermediation, price limits, disclosure, collection, consumer protection and treatment of non-compliances in the applicable jurisdiction shall be assessed.

17.5 — Digital assets

Token issue, utility, fundraising, costy and distribution require separate analysis. No passages constitute an offer of securities or a promise of return.

17.6 — Contractual framework

credit recipient terms must describe principal, fixed simple interest of 5% per month, duration, stake, repayment, late/incompliance treatment, privacy, complaints and applicable law.

17.7 — Operational responsibility

Responsibilities between entity, signers, operators, KYC suppliers, local partners and technology providers should be formalised.

17.8 — Evidence and allegations

Public clays distinguish tested, prepared, planned and live. Results from Base Sepolia or simulation are not presented as production data.

17.9 — Legal basis

No mainnet/public launch occurs before the completion of the relevant legal and regulatory workstream.

Chapter 18 — Audit Strategy and Security Certification

18.1 — State currently tested

The system has been tested in Base Sepolia for slowing, repayment, reputation, multi-wallet flow, pool monitoring, governance, pause/unpause, Monitor V2 and synthetic scenarios of stress and fraud.

18.2 — Limitation of scope

Testnet evidence does not equal mainnet, production, completed external audit or data from human credit beneficiaries.

18.3 — Governance tests

The Safe 3-of-5 → Timelock → critical contracts must be tested end-to-end, including proposals, delays, execution, failure, cancellation and emergency response.

18.4 — Guarantee of contracts

Audit covers access control, accounting, stake, lifecycle loan, default, pause, upgrades, oracle or dependence assumptions and liquidity invariants.

18.5 — Operational security

Includes signer costady, wallets hardware, secrets, CI/CD, backups, alert routing, incident communications and disaster recovery.

18.6 — External auditing framework

Independent audit is a requirement prior to public material production. The document does not state that this audit has already taken place.

18.7 — Continuous guarantee

Security reviews, monitoring, dependence updates, bug bounty and regression testing continue after lunch.

18.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

Security is one of the fundamental pillars of the MICrO Protocol. Since the system manages financial assets and performs automated operations through smart contracts, it is essential to ensure that all components are independently and continuously checked.

The MICrO Protocol adopts an approach based on

This model reduces technical and operational risks before the introduction of real capital.

The design of the system was developed based on structural safety principles.

These principles have been incorporated since initial development.

Protocol security is based on a multi-layer architecture.

This model reduces dependence on a single failure point.

All major contracts will be subject to independent audits before launch in production environment.

The MICrO Protocol intends to work with recognised independent entities.

Prior to the external audit, a rigorous internal process will be carried out.

This very strengthens this chapter.

Even after formal audits, the system will continue to be tested regularly.

If vulnerabilities are identified

a structured process will be activated.

This cycle ensures effective resolution.

The protocol may implement a public bug bounty programme.

This model increases collective security.

Critical changes to the protocol will be controlled by structured governance.

The system includes rapid response mechanisms.

In addition to contracts, the infrastructure will be protected.

This model reduces operational risk.

Data integrity will be protected through

This model protects future audit.

recommendations will be implemented.

The ultimate objective is to obtain recognised safety certification.

This step increases institutional confidence.

Chapter 19 — Disclosure and Risk Management

Baseline v2.0 applicable to this chapter

- Gross default is exposure-weighted principal; net credit loss deducts recoveries/stake effects.
- Default warning: 15%; critical: 25%.

19.1 — No guarantee

Microcredit involves risk of default, fraud, loss, technical failure, operational error and regulatory change. The architecture reduces risk; it does not eliminate it.

19.2 — Credit risk

Gross default is measured by main exposure-weighted. Warning: 15%. Critical: 25%. Approach at 30% indicates structural loss and requires expansion suspension.

19.3 — Risk of loss

Net credit loss considers recoveries and stake effects. Stake does not guarantee full recovery, especially in bootstrap without stake.

19.4 — Liquidity risk

The active envelope, 80% ceiling, 20% floor and staged activation limit illiquidity. The committed reserve is not all exposed.

19.5 — Sybil risk and fraud

Device, network, funding and cluster controls may fail or generate false positives. The pilot measures effectiveness and supports review.

19.6 — Risk of smart contracts

Bugs, upgrades, token behaviour, PRC dependencies and access-control errors can affect funds. External audit continues production requirement.

19.7 — Risk of governance

Signers may lose access, coludate or respond slowly. Threshold, Timelock, hardware and runbooks mitigate these risks.

19.8 — Operational risk

Hosting, databases, bots, alerts, backups and operators may fail. Separate responsibilities, observability and recovery tests are required.

19.9 — Regulatory risk

Lending, KYC/AML, privacy, consumer protection and token rules vary by jurisdiction. The pilot does not eliminate local obligations.

19.10 — Market risk and stable currency

USDC Depeg, Chain Congestion, Fees and Infrastructure Outages may interrupt the service or change exposure.

19.11 — Risk of pilot evidence

Sepolia base and simulations do not predict human behaviour. Live results may require reduced exposure or redesign.

19.12 — Residual risk

Even after mitigation there is residual risk. Expansion decisions must document acceptance, owner, threshold and stop condition.

19.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The MICrO Protocol involves automated financial operations and as such is subject to multiple types of risk. The transparent identification and dissemination of these risks is an essential element in the credibility of the system.

This chapter describes the main identified risks and strategies adopted to mitigate them.

Transparency on risks does not eliminate risk, but allows it to be managed effectively.

Smart contracts are programmes run automatically and, despite rigorous audits, may contain vulnerabilities.

These measures significantly reduce the likelihood of critical failures.

The economic model of the protocol depends on multiple factors.

- adverse behaviour of users

This risk is especially relevant in microcredit systems.

These mechanisms help protect the pool.

- ? sustainability up to about 15–20% default

Insufficient liquidity may prevent new loans or repayments.

- maximum use limit of pool

The behaviour of users may vary significantly.

This risk is typical in credit systems.

Governance involves human control and can introduce risks.

Legal changes can affect operations.

This model allows for future flexibility.

The protocol depends on stablecoins and external infrastructure.

- ?? Network base — low and stable cost

Technical infrastructure may fail.

Private key management is critical.

Human operations can make mistakes.

This model reduces operational failures.

Fast growth can bring instability.

This model protects institutional image.

Even with all measures implemented

This recognition is essential for any financial system.

Users should understand that

This principle ensures transparency.

Chapter 20 — Evidence-Gated Roadmap

20.1 — Principle of the roadmap

The roadmap is controlled by evidence, not promotional dates. Each phase requires input criteria, metrics, review and documented decision.

20.2 — Mark A: preparation of the testing network

Requires functional contracts in Sepolia Base, repayments, reputation, multi-wallet testing, governance, pause/unpause, monitoring, stress tests and critical issues solved.

20.3 — Marco B: operational preparation

Requires Safe 3-of-5, Timelock, signer costy, runbooks, alerts, backups, lifecycle repayment, KYC providers and incident response.

20.4 — Marco C: legal preparation

Requires appropriate entity and contracts, slowing review, AML/KYC, data protection, consumer terms and token/fundraising posture.

20.5 — Marco D: Cohort 1 launch

Activates 25 participants, bootstrap 10–25 USDC, active reduced envelope, daily/weekly limits and enhanced monitoring.

20.6 — Marco E: review of the cohort

Evaluate repayment, default, net loss, use, reserve integrity, clusters, false positives, operations, incidentals and credit recipient outcomes.

20.7 — Marco F: expansion up to 100

Additional cohorts are activated only when approved thresholds are satisfied and there are no open critical risks.

20.8 — Marco G: upper exposure

Any capacity above 100 USDC requires evidence of pilot, audit, capital, KYC, governance and legal review. The 500 USDC ceiling is future capacity, not promise.

20.9 — Marco H: production

Mainnet or public scale requires independent audit, operational resilience, observability, mature governance and formal decision.

20.10 — Break conditions

Hard use, critical default, reserve loss, cluster attack, governance failure, security incident or legal disability suspend progression.

20.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The development of the MICrO Protocol follows a structured approach based on progressive phases. Each phase includes technical objectives, operational validations and verifiable milestones.

- prepare the system for real use

Unlike many projects that present vague schedules, the MICrO Protocol bases roadmap on real technical milestones.

This phase included the conceptual design of the system and the definition of fundamental principles.

- definition of the microcredit model

This phase established the structural basis of the protocol.

During this phase the main contracts of the system were developed.

This phase represents the technical foundation of the protocol.

At this stage, the system was deployed in a testnet.

This phase confirmed technical feasibility.

- (And this directly reflects what you have already done.)

This phase focused on the validation of system behaviour under extreme conditions.

- multiple loan simulations
- economic sustainability analysis

This result is extremely relevant for investors.

Few projects reach this level.

The governance model has been implemented at this stage.

This is a critical milestone of maturity.

This will be the first phase with real users.

After the pilot, external audit will be carried out.

This step prepares the system for real capital.

After auditing, initial liquidity will be introduced.

Initiate actual controlled operations.

At this stage the MICrO Token will be created.

The final phase involves global expansion.

Each phase will be validated with specific criteria.

The transition between phases only occurs after validation.

The roadmap is aligned with the central view

- expand access to credit globally

Each phase brings the system closer to that goal.

Chapter 21 — Technical Appendix

Baseline v2.0 applicable to this chapter

- Active values limited to 100 USDC; 101–500 parameters are future capacity documentation with progressive KYC.

21.1 — Component model

LoanManager coordinates eligibility and lifecycle; loan contracts register terms and states; reputation maintains evidence; governance contracts control critical functions; monitoring observes events.

21.2 — Loan States

Requested → Approved → Active → Repaid or Overdue → Unfulfilled under explicit conditions. Invalid transitions are rejected.

21.3 — Start-up parameters

Main 10–25 USDC; 30-day duration; 0% stake only within the unsecured controlled envelope; 7-day later cooldown period. The sub-limit of first unsecured loans shall not exceed 20% of the available block of 80% of the activated capital.

21.4 — Active normal parameters

26–50 USDC: 28% stake and 5 days cooldown period. 51–100 USDC: 26% stake and 3 days cooldown period. Standard duration: 90 days. Guaranteed credit up to 100 USDC can use up to 50% of the 80% available block, subject to scoring, verification and stake capacity.

21.5 — Future parameters

101–200: 24% and KYC. 201–300: 22%, KYC + selfie. 301–400: 21%, KYC + selfie. 401–500: 20%, KYC + selfie. They remain disabled until approval by governance and sufficient evidence.

21.6 — Calculation of interest

interest = main × 5% × months. There is no componding on loan or risk-based rate variation.

21.7 — Verification of use

projected use must remain ≤80% of the active credit limit. The pool keeps at least 20% unused.

21.8 — Eligibility checks

Single active loan, band score, cooldown period, KYC, pause state, envelope capacity and risk decision are checked before disbursement.

21.9 — Off-chain risk data

Device/IP/ASN/VPN, funding-source, cluster and speed controls are processed with audit trail and privacy controls; results authorize, review or block requests.

21.10 — repayment events

repayment updates state loan, pool accounting, stake disposition and reputation. Main, interest and recovery are distinct accounting fields.

21.11 — Treatment of default

After +30 days and applicable checks, authorised operator executes the classification. Gross default and net credit loss are issued for reporting.

21.12 — Governance interface

Safe 3-of-5 approves; Timelock delays and executes; critical contracts receive the action. Bots do not call privileged functions autonomously.

21.13 — Semantics of pause

Pause prevents further risk. Repayment and recovery functions must remain available whenever implementation permits.

21.14 — Monitoring scheme

Events include request, application, disbursement, repayment, overdue, default, stake, usage, pause and governance.

21.15 — Evidence of implementation

Base Sepolia was used for technical validation. Production addresses, signer registry, audit and legal readiness remain pending.

21.16 — Version control

Parameters, ABI, address, risk rules and monitoring schema must have synchronized version and changelog.

21.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The MICrO Protocol is based on a modular architecture composed of multiple interconnected smart contracts. This architecture is designed to allow clear functional separation, facilitating audit, maintenance and future evolution.

The main architecture includes the following modules

Each module has specific responsibilities and defined interfaces.

The main system consists of contracts that operate in a coordinated manner.

This separation reduces internal complexity.

The technical loan cycle follows a defined sequence.

Each step is validated by on-chain logic.

Each loan has defined states.

This model allows complete traceability.

After reimbursement, a cooldown period is applied.

The system requires stake proportional to the value of the loan.

This mechanism protects the pool against losses.

This model is already implemented in the contract.

Liquidity is managed through a central pool.

This parameter protects financial stability.

The interest calculation follows a defined model.

This model was tested in simulations.

Non-compliances are automatically processed.

This system influences eligibility.

System control is carried out through structured governance.

This model reduces operational risks.

The system supports emergency pause.

This mechanism has already been tested by you.

The system uses external stablecoins.

The frontend communicates with contracts through blockchain APIs.

This model allows user interaction.

Users interact via wallets.

Critical parameters are controlled by governance.

This model ensures institutional control.

Updates may be required over time.

This model allows for safe evolution.

The system supports continuous monitoring.

Chapter 22 — Economic Appendix

Baseline v2.0 applicable to this chapter

- Scenarios vary stake, exposure, default, recoveries and costs. Interest remains fixed at 5% simple/month.

22.1 — Fixed interest convention

All examples use 5% simple interest per month: I = P × 0.05 × m. Variable rates as a risk mechanism are not tested.

22.2 — Start-up examples

10 USDC for one month: 0.50 interest and 10.50 repayment. 25 USDC: 1.25 interest and 26,25 repayment.

22.3 — Normal examples

50 USDC for three months: 7,50 interest and 57,50 repayment. 70: 10.50 and 80.50. 90: 13,50 and 103,50. 100: 15 and 115.

22.4 — Examples of guarantee (stake)

50 USDC at 28% requires 14 USDC of stake. 70 to 26% requires 18.20. 100 to 26% requires 26. Bootstrap 10–25 uses 0% only in the controlled envelope.

22.5 — Future scale

101–200: 24%; 201–300: 22%; 301-400: 21%; 401-500: 20%. These calculations don't activate the tiers.

22.6 — Exposure definitions

Gross exposure is primarily disbursed. Gross default is primarily in default on an exposed-weighted basis. Net credit loss subtracts recognised recoveries and stake effects.

22.7 — Portfolio scenarios

The scenarios vary mix of tiers, repayment, default, recoveries, stake, costs, use and reuse of capital. The rate of credit recipient shall remain fixed.

22.8 — Interpretation of thresholds

Up to 15% of default is a healthy monitoring zone; 15–25% requires increasing containment; 25% is critical; approximately 30% indicates structural unsustainability.

22.9 — Liquidity model

The committed reserve up to 112,500 USDC supports capacity, while only a smaller active envelope assumes risk. Maximum use: 80%; spare floor: 20%.

22.10 — Breakdown between start-up and collateralised credit

Within the available block of 80% of the capital activated, unsecured startup can use up to 20%. Initial credit with guarantee up to 100 USDC can use up to 50%. The remaining capacity preserves operational reserve, cohort flexibility and phased expansion.

22.11 — Accounting of the unified reserve

Main, interest, recoveries and stake effects are accounted for separately, but belong to the unified pool architecture. There is no fixed split of revenue between pools.

22.12 — Statement on the balance point

There is no universal break-even interest rate of 9.54%. The break-even depends on losses, recoveries, capital, duration, mix, use and operational costs.

22.13 — Pilot indicators

Repayment rate, exposure-weighted default, net credit loss, interest collected, use, reserve integrity and cost per loan sustain the economic assessment.

22.14 — Limitations

The simulations are hypotheses. Only live data from Cohort 1 allow calibrating behaviour, loss distribution and viability.

22.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The economic model of the MICrO Protocol was developed based on extensive simulations that seek to assess the sustainability of the pool over time.

Unlike simplified theoretical models, this system has been validated through

The objective of this chapter is to demonstrate that the economic model is functional and resilient within defined parameters.

The basic economic parameters of the system have been defined to ensure initial stability.

These parameters define the economic behaviour of the system.

The simulations were structured to replicate users' realistic behaviour.

This model allows the observation of systemic behaviour.

Multiple scenarios with different default rates were simulated.

- ? sustainability up to approximately 15–20%

The sustainability model depends on the relationship between

When this condition is maintained, the system remains sustainable.

Without stake, the system becomes extremely vulnerable.

Pool growth was modeled in progressive phases.

Stress tests were performed to assess load stability.

The impact of defaults was modelled with multiple scenarios.

- High defaults compromise liquidity

Variations in critical parameters were tested.

- Major defaults reduce stability

The balance point represents the minimum economic limit.

This result helps in future management.

Prolonged scenarios were evaluated.

During the initial pilot, it is expected

This will be the first real economic test.

Economic limits have been set.

This model allows for early reaction.

An operational reserve is recommended.

This mechanism increases resilience.

This model supports sustainable growth.

- dependent on operational discipline

Chapter 23 — Documentation of Smart Contracts

Baseline v2.0 applicable to this chapter

- Critical governance: Safe 3-of-5 → Timelock. Privileged actions are human-approved.

23.1 — Scope of documentation

This chapter describes interfaces and invariants of baseline v2.0. The versioned source code and ABI remain the implementing authority.

23.2 — Responsibilities of LoanManager

Validate eligibility proof, single active loan, cap score, cooldown period, stake, duration, pause and projected use before disbursement.

23.3 — Loan registration

Minimum fields: credit recipient, main, interest bass, duration, due date, stake, state, timestamps and version identifier.

23.4 — Interface of reputation

Registers repayments, timing class, late/incompliance evidence and punctuation updates. It doesn't authorize values above live cutting.

23.5 — Liquidity interface

Displays active envelope, main outstanding, available liquidity, utilisation and cutting. Do not model liquidity reserve or Separate Emergency Pool.

23.6 — Interest parameter

Baseline is 5% simple per month. Change score or risk class does not change the rate.

23.7 — Range parameters

Assets: 10–25 USDC with 0% only in the unsecured controlled envelope; 26–50 USDC with 28%; 51–100 USDC with 26%. Futures: 101–200 USDC with 24% and KYC; 201–300 USDC with

22% and KYC + selfie; 301–400 USDC with 21% and KYC + selfie; 401–500 USDC with 20% and KYC + selfie.

23.8 — Parameters of the cooldown period

7, 5 and 3 days for completed active echelons. Future tiers only receive their own waiting periods after governance, review of evidence and explicit updating of parameters.

23.9 — Issuance and supply of MICrOToken

The contract creates exactly 10,000,000,000 MICrO in genesis mint. After initial creation, no address, scroll, multisig, Timelock or emergency power can execute new mint. Maximum supply cannot be increased by upgrade or change of governance.

23.10 — MICrOToken Burn

The burn, when allowed by implementation, only processes specifically authorised tokens or treasury tokens. Any relevant operation requires published policy, 3-of-5 Safe approval and Timelock. Burnt Tokens cannot be recreated.

23.11 — Locks and clothing

Non-rolling tokens remain in contracts or governed accounts with verifiable calendars, cliffs and milestones. treasury cannot unlock or transfer tokens through emergency powers.

23.12 — Governance contracts

Safe requires 3 of 5 signatures. Timelock receives approved operations and executes after delay. Critical contracts recognize only configured roles.

23.13 — Privileged functions

They include capital activation, parameter bonds, role, pause/unpause, upgrades and future-tier support. All require approved by human governance intervention.

23.14 — Catalogue of events

LoanRequested, LoanCreated, Repaid, Overdue, Unfulfilled, StakeHandled, EnvelopeChanged, Paused, Unpaused and Executed Governance support audit trail.

23.15 — Conditions of error

Rejections include active loan, cooldown period, score, KYC/risk decision, stake, balance, allowance, use, pause and disabled tier.

23.16 — Implementation references

Base Sepolia is the tested environment. Registry and address must be published by version; production references are not inferred from this document.

23.17 — Audit requirements

Invariant valid audit, access control, accounting, token integration, upgrade path, pause semantics and event completeness.

23.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

MICrO Protocol uses a structured set of interconnected smart contracts that perform all critical system operations.

This chapter documents the main functions, interfaces and operational parameters of the main contracts.

This documentation does not replace the source code, but provides a structured and understandable view of its functionality.

Main contracts of the MICrO Protocol include

Each contract has specific functions and defined responsibilities.

The LoanManager contract is responsible for the overall coordination of loans.

This contract acts as the central point of the operational flow.

Main function responsible for Bootstrap a loan application.

This function represents the main input point of the user.

Function responsible for approving the loan.

This function ensures operational integrity.

Function responsible for obtaining the current status of a loan.

The MicrocreditLoan contract carries out direct financial operations.

This contract implements the central financial logic.

Function responsible for the actual creation of the loan.

Function responsible for payment of the loan.

This function closes the loan cycle.

- ? repay does not allow new active loan

Function responsible for marking a default.

The MicrocreditReputation contract maintains the reputational score.

This contract influences future decisions.

Function responsible for updating reputation.

This mechanism encourages positive behaviour.

Function responsible for getting current score.

This mechanism controls eligibility.

The MICrOToken contract manages the native token.

This token supports future incentives.

Function responsible for transferring tokens.

The governance of the system is carried out through dedicated contracts.

This model guarantees collective control.

Timelock applies delay to critical changes.

This mechanism protects stability.

The system depends on critical parameters.

These parameters determine economic behaviour.

Events are automatically recorded.

This model supports traceability.

Access control is based on permissions.

Contracts interact through internal calls.

This model maintains modular structure.

Updates follow controlled process.

This template prevents unexpected changes.

Contracts are implemented on specific networks.

Chapter 24 — Glossary

Baseline v2.0 applicable to this chapter

- Reserve floor means minimum capacity not used in the unified pool, not a separate liquidity reserve.

24.1 — Active credit limit

Part of the capital effectively activated for letting. It is materially lower than the pilot's committed reserve.

24.2 — committed pilot reserve

A committed capital capacity for the programme, up to 112,500 USDC; does not mean immediate exposure.

24.3 — spare floor

Minimum 20% of the active envelope that remains unused within the unified pool. It's not a separate pool.

24.4 — maximum use

Maximum limit of 80% of the active envelope that may be compromised.

24.5 — Bootstrap

First loan of 10–25 USDC for 30 days, potentially unsecured only in the controlled envelope. The unsecured sub-limit does not exceed 20% of the available block of 80% of the activated capital.

24.6 — Active pilot limit

Maximum of 100 USDC available during live pilot.

24.7 — Future limit on governance

Documented capacity up to 500 USDC, unavailable until landmark evidence and governance.

24.8 — Stake

Value placed by the credit recipient for economic alignment and partial loss absorption. It varies by tier.

24.9 — Simple monthly interest

Interest calculated without capitalisation: principal × 5% × number of months.

24.10 — cooldown period

Period after repayment before new eligibility: 7/5/3 days in live tiers.

24.11 — Grouping

Set of wallets or requests correlated with device, network, source of funds or behaviour.

24.12 — Basic KYC

Verification applicable to tier 51–100 and previous risk triggers.

24.13 — Safe 3-of-5

Multisig in which three out of five signers approve an action.

24.14 — Timelock

Contract that delays the execution of approved critical actions.

24.15 — Gross default

Main default calculated on an exposure-weighted basis.

24.16 — Net loss of credit

Loss after recognised recoveries and stake effects.

24.17 — Evidence gate

Set of criteria that must be met before expansion.

24.18 — Tested at Sepolia Base

Function demonstrated on testnet; does not equal mainnet or production.

24.19 — pre-launch

State in which operations and controls are prepared, but human credit beneficiaries have not yet started the pilot.

24.20 — Automation approved by human intervention

Model in which bots observe and recommend, but privileged actions require human approval.

Chapter 25 — Final Conclusion

Baseline v2.0 applicable to this chapter

- The unsecured exception applies only to startup 10–25 USDC within the controlled envelope.

25.1 — Integrated Thesis

MICrO Protocol proposes USDC credit with deterministic rules, progressive reputation, variable stake, limited liquidity and auditable governance.

25.2 — Predictable price for the credit recipient

The price is fixed: 5% simple interest per month. The risk is managed by exposure, stake, score, KYC, cooldown period, envelopes and anti-Sybil.

25.3 — Controlled inclusion

Bootstrap 10–25 USDC allows 0% stake only within a controlled envelope, limited to 20% of the available block of 80% of the activated capital. It does not represent open credit without guarantee or general disposal of economic alignment.

25.4 — Limited pilot

The active maximum is 100 USDC. Cohort 1 has 25 participants in a programme planned up to 100. Vietnam remains in pre-launch until there are credit beneficiaries and real operations.

25.5 — Conservative capital

The committed reserve up to 112,500 USDC is conceptually separated from the active credit limit. The protocol preserves 20% of activated capital and never exceeds 80% of use.

25.6 — Layer defense

Wallet, device, network, source of funds, behaviour and clusters support individual and correlated limits, with human review for high risk.

25.7 — Governance under human control

Safe 3-of-5 and Timelock protect critical contracts. Automation does not receive autonomous financial authority.

25.8 — Evidence already obtained

Base Sepolia has demonstrated slowing, reimbursement, reputation, governance, monitoring and controls. This evidence is technical, not proof of living social or economic viability.

25.9 — Evidence still required

The pilot shall demonstrate reimbursement, losses, reserve integrity, anti-Sybil effectiveness, operational quality and outcomes of credit recipients. External audit and legal workstreams continue production gates.

25.10 — Final declaration

The value of MICrO will depend on the ability to convert conservative architecture into real evidence. Expansion, higher tiers, token utility and production only advance when the corresponding gates are satisfied.

25.90 — Additional technical development

The following notes preserve the useful analytical reasoning of the original extensive version, already framed by reference v2.0 presented in the previous sections.

The MICrO Protocol was conceived as a decentralised financial infrastructure focused on accessible, sustainable and technologically robust microcredit.

Throughout this document, the technical, economic and operational foundations supporting the system were presented, demonstrating that the protocol was developed based on structured principles and progressive validation.

The aim of MICrO is not only to introduce a new technology tool, but to create a functional system that can be used in real scenarios, with direct impact on access to credit.

The MICrO Protocol combines multiple technical and economic components to form an integrated system.

- modular architecture based on smart contracts
- Stake system as economic protection
- governance based on multisig and timelock

These elements are designed to work together, forming a coherent and auditable system.

Throughout the development phases, the system was validated in a testnet environment, demonstrating real functionality in loan and repayment operations.

This level of validation represents an important milestone in the development of the protocol.

One of the core principles of the MICrO Protocol is explicit risk recognition.

Unlike models that assume optimal user behaviour, MICrO has been designed to:

The system incorporates multiple mitigation mechanisms, including

This model allows stability even in adverse scenarios.

Economic sustainability is one of the fundamental pillars of the Protocol.

Simulations have shown that

- the system remains sustainable with moderate defaults
- losses are absorbed through stake
- progressive growth increases stability

The results observed indicate that the protocol has predictable behaviour within defined operational limits.

This predictability is essential for real financial operation.

The governance of the MICrO Protocol is designed to ensure collective control and operational security.

This system reduces human risk and protects protocol integrity.

Governance plays a central role in maintaining operational stability.

Security remains a continuous commitment throughout the protocol life cycle.

The MICrO Protocol adopts an approach based on

This approach allows identifying and correcting vulnerabilities before they can cause significant impact.

Security is not treated as an isolated event, but as a continuous process.

The launch of the protocol will follow a controlled approach.

This approach allows validating real behaviour before expansion.

The pilot is an essential step for operational maturity.

The long-term vision of the MICrO Protocol is to expand access to credit in a sustainable and inclusive way.

- integrating new reputational mechanisms

Growth will be progressive and controlled.

This model allows for sustainable expansion.

The MICrO Protocol is designed based on recognised software engineering, financial security and operational governance practices.

These elements position the protocol for continuous evolution and adaptation to real operating environments.

MICrO Protocol represents a structured approach to decentralised microcredit, combining blockchain technology with traditional financial principles.

Progressive development, combined with robust mechanisms of security and governance, allows us to create a system that can evolve from experimental environment to real operation.

Careful implementation, combined with continuous monitoring and progressive validation, is the basis for building a sustainable and reliable system.

The future of the MICrO Protocol will be defined by its ability to adapt, resilience and commitment to security and transparency.