WHITEPAPER · VERSION 2.0 · JUNE 2026

The REMI Protocol

A confidential settlement layer for stablecoin payments • The xREMI utility & governance model • Issuer: REMI

ABSTRACT

A confidential settlement layer for stablecoin payments, and the xREMI utility and governance model

Public blockchains made value transfer fast and inexpensive, but they did so by making every transfer permanently visible. The REMI Protocol treats confidentiality as the property it is built to deliver rather than as a feature added later.

Issuer: REMI • Contact: hello@remi.ae • Version 2.0 · June 2026

ABSTRACT

When a stablecoin moves between two parties, the sender address, the receiver address, the amount, and the link between them are written to a ledger anyone can read forever. For payments and remittances this is not a minor inconvenience: it exposes balances, counterparties, and habits, and it makes regulated institutions reluctant to settle real customer flows. REMI begins as a regulated operating network that routes real money through licensed operators, and introduces a single native asset, **xREMI**, as the utility and governance token that powers the network once it has matured. This paper gives a formal account of the confidentiality model, distinguishes the two settlement routes, and presents the complete economic model of xREMI in mathematical form: its fee mechanics, staking and security model, fixed supply and emission schedule, and the structural demand created when every transaction fee is paid in xREMI.

01 Introduction

A remittance is a simple request. Someone wants to send value to someone else, often across a border, and wants the recipient to receive it quickly and at low cost. Public blockchains answered the speed and cost part of that request well: a stablecoin transfer settles in seconds and costs a fraction of a traditional wire. The part public chains did not answer is privacy. Every transfer is recorded on an open ledger, and that record does not expire. Anyone who learns which address belongs to a person can read that person's entire payment history, current balance, and the identities of everyone they transact with.

This is the gap the REMI Protocol exists to close. The protocol is designed so that a stablecoin payment can move between two parties without revealing to the public who sent it, who received it, or how much was sent, while still allowing the parties themselves and lawfully authorized reviewers to see the full record when they need to. We call the component that provides this the **confidentiality layer**.

REMI is built in a deliberate order. The operating network comes first. Licensed operators, the routing and compliance machinery that coordinates them, and real transaction volume are established before any token mechanics are switched on. The native asset, xREMI, is introduced afterward, once the network is carrying genuine activity.

> **xREMI earns its role by sitting on top of a network that already works, rather than being the reason the network is supposed to work.**

xREMI is a single token. Earlier versions of this design used two tokens: one to settle payments and one to capture value. That separation has been removed. There is now one native asset that serves three purposes once the token phase is live: it pays the fee on every transaction the network processes, it can be staked to help secure the network and to earn a share of those fees, and it carries the right to vote on the protocol's governance.

1.1 What this paper covers

Section 2 states the confidentiality problem precisely and gives an adversary model. Section 3 sets out the design principles. Section 4 describes the network-first architecture. Section 5 defines the confidentiality layer and its privacy properties. Section 6 specifies the two settlement routes and the role xREMI plays in each. Sections 7 through 12 develop the xREMI economic model

in full. Section 13 lays out the roadmap, Section 14 describes governance, Section 15 records the risks and limitations honestly, and Section 16 concludes. A notation table is provided in the appendix.

02 The Confidentiality Problem on Public Ledgers

2.1 Pseudonymity is not privacy

A public blockchain identifies participants by addresses rather than by legal names. This is often described as anonymity, but it is closer to a thin form of pseudonymity. An address is a stable identifier, and every payment it sends or receives is attached to it permanently. The moment any single address is linked to a real person, every past and future transaction of that address is exposed, together with the addresses on the other side of each transaction, which can then be deanonymized in turn. The ledger is a graph, and one labelled node tends to unravel its neighbourhood.

We can state this more carefully. Let the public ledger after a sequence of transactions be a labelled directed multigraph $G = (V, E)$, where each edge $e_k = (u_k \to v_k,\ a_k,\ t_k)$ records a transfer of amount a_k from address u_k to address v_k at time t_k. On a transparent chain, G is fully visible to every observer. An observer who holds a small deanonymizing map ϕ from a subset of addresses to real identities can propagate identity through the graph by following edges, clustering co-spending addresses, and matching amounts and timing against off-chain information.

> **CONSEQUENCE**
>
> The privacy of a participant is bounded not by their own caution but by the weakest link anywhere in their transaction neighbourhood.

2.2 Why transparency blocks regulated settlement

Regulated financial institutions operate under confidentiality obligations toward their customers. They cannot settle customer payments on a medium where account balances and counterparties are world-readable. At the same time they have reporting and audit obligations that an opaque medium would violate. A transparent public chain fails the first requirement; a fully opaque system fails the second.

What a regulated payment network needs is a medium that hides transaction detail from the public while preserving lawful access for the parties involved and for authorized supervisors. This combination of **confidentiality toward the public** together with **selective transparency toward authorized parties** is the requirement the protocol is engineered to satisfy.

REMARK 1 · SCOPE

This paper is deliberately scoped to confidentiality. It does not argue about fees, settlement times, or market size. Those are properties of the operating network and are addressed in REMI's network documentation. The question this paper answers is narrower and more fundamental: when value moves on a shared ledger, how does it move privately, and how is the asset that powers that movement designed.

03 Design Principles

The protocol rests on four commitments.

PRINCIPLE 1

Confidentiality by default

On the route where the protocol provides privacy, privacy is the normal state of a transaction, not an option a user must find and enable. The public sees an unreadable record; the parties and authorized reviewers see the truth.

PRINCIPLE 2

Selective transparency

Confidentiality toward the public is paired with disclosure toward those entitled to it. Authorized parties hold the means to read a transaction. No one else does.

PRINCIPLE 3

Network before token

The operating network is established and carries real volume before token mechanics are activated. Value accrues to the token because the network is used, not in advance of use.

PRINCIPLE 4

One asset, clearly bounded

A single native asset, xREMI, carries utility and governance. The paper states plainly what the asset does and does not claim to be, so its role is not confused with a settlement currency or an investment promise.

04 Network-First Architecture

The protocol is organized as four layers. Each layer produces something the layer above it depends on. xREMI sits at the top and becomes meaningful only after the layers below it are producing reliable activity.

04 xREMI Layer: utility & governance

Fees, staking and security, and governance. Activated after the network matures. It does not move money by itself.

POWERS ↑

03 Network Operators

Licensed exchanges, payout endpoints, and off-ramp partners that execute the parts of a transaction touching regulated rails. They provide regulated execution and liquidity.

02 Remi Core: control plane

Quote creation, compliance orchestration, routing, settlement tracking, metering, and reconciliation. It turns a request into a coordinated movement of value and produces the auditable record.

01 Network Participants

Applications and platforms that originate payments and remittances and bring real demand to the network. They originate the transactions.

FIG. 1 The four layers of the protocol. Activity flows from participants through the control plane to operators; the xREMI layer powers fees, staking, and governance once the network below it is producing measurable, auditable volume.

05 The Confidentiality Layer

5.1 What it protects, and where it lives

The confidentiality layer is an on-chain component, introduced in the protocol's second phase once the operating network is established. Its job is to let a stablecoin transfer take place on a shared ledger without disclosing its sensitive content to the public, while letting authorized parties read that content in full. We describe the layer abstractly and do not tie it to any particular ledger or cryptographic construction. What matters here is the set of properties it provides.

DEFINITION 1 · CONFIDENTIAL TRANSFER

A confidential transfer is a transaction whose public on-chain representation is a record r from which an observer without authorization cannot recover the sender identity, the recipient identity, or the transferred amount, and cannot link r to other transfers of the same parties beyond a fixed anonymity set.

DEFINITION 2 · ANONYMITY SET

For a confidential transfer r, the anonymity set $A(r)$ is the set of candidate transfers among which r is indistinguishable to an unauthorized observer. The privacy afforded by the layer is increasing in $|A(r)|$.

We model an unauthorized observer as a probabilistic adversary $\mathcal{A}$ who sees the full public ledger and any off-chain side information available to the public. Attempting to identify the true sender of a confidential transfer r from its anonymity set, the best the adversary can do without authorization is guess within the set:

$$\Pr[\mathcal{A} \text{ links } r \text{ to its true sender}] \;\leq\; \frac{1}{|A(r)|} + \varepsilon \tag{1}$$

where ε is a negligible quantity capturing any leakage from the encoding and from timing or amount side channels. A well-constructed layer keeps ε negligible and $|A(r)|$ large, driving the linking probability toward chance. On a transparent chain the corresponding probability is 1, because the sender is written in clear.

PROPERTY 1 · PUBLIC CONFIDENTIALITY

For any confidential transfer, the sender, recipient, and amount are hidden from every unauthorized observer, and the linking probability obeys the bound in equation (1).

5.2 Selective transparency

Confidentiality toward the public is only half of the requirement. The other half is that the right parties can still read the transaction. We model this with a disclosure relation.

DEFINITION 3 · AUTHORIZED READER

Let $\Pi(r)$ be the set of parties authorized to read confidential transfer r: the sender, the recipient, REMI as protocol operator, and any reviewer mandated by law. Each authorized party $\pi \in \Pi(r)$ holds a credential k_π such that $\mathrm{Open}(r, k_\pi)$ returns the full plaintext content of r. For any party $\pi' \notin \Pi(r)$, no efficient procedure recovers that content.

PROPERTY 2 · SELECTIVE TRANSPARENCY

A confidential transfer is readable in full by every party in $\Pi(r)$ and by no party outside it. The public record reveals nothing beyond what Property 1 permits.

Together the two properties give the combination regulated settlement requires. The public is shut out; the participants and the lawful supervisors are let in. There is no third state in which the data is simply lost.

5.3 xREMI as the fuel of confidential settlement

Processing a confidential transfer on chain consumes xREMI. The token is the gas that powers the confidentiality layer: a transaction that asks the layer to hide its content pays for that work in xREMI. This is the first and most direct utility of the token, and it ties the token's usage to the exact activity the protocol is built to provide.

> **The more confidential settlement the network performs, the more xREMI is consumed to perform it.**

06 Settlement Routes and Protocol Operations

The protocol supports two settlement routes. They differ by whether the recipient's jurisdiction recognizes digital assets. The confidentiality layer applies to one of them; xREMI powers both.

6.1 Route A: stablecoin to stablecoin between recognized jurisdictions

In Route A the sender is in a jurisdiction with a mature legal framework for stablecoins, and the recipient is in a jurisdiction that also recognizes them. The sender sends a stablecoin and the recipient receives a stablecoin. The entire transaction lives on chain end to end, exactly the situation in which public exposure would otherwise be total. This is where the confidentiality layer does its work.

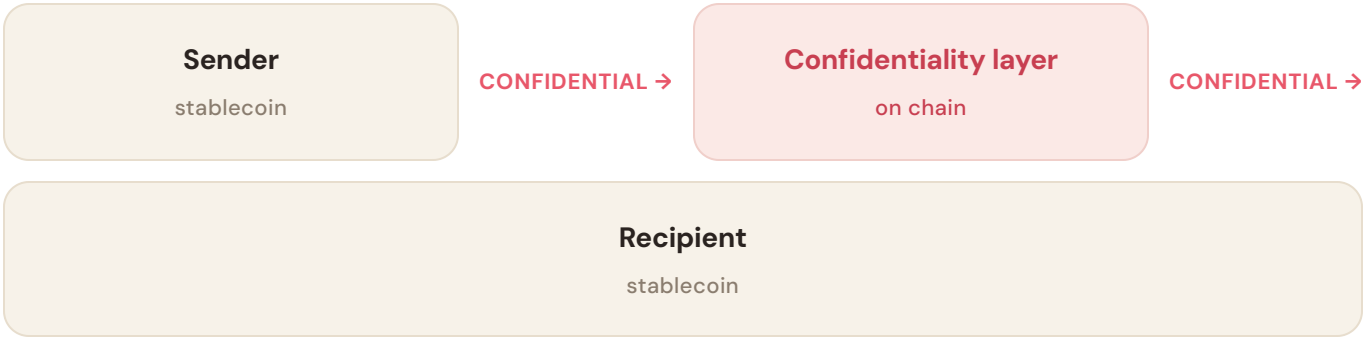

FIG. 2 Route A. A stablecoin moves from sender to recipient through the on-chain confidentiality layer. The public record is unreadable. The fee is paid in xREMI and is never taken out of the amount being sent. Route A is the highest-value use of the protocol: confidentiality is both most needed and fully available.

6.2 Route B: stablecoin in, local currency out

In Route B the sender's jurisdiction recognizes stablecoins but the recipient's does not. Because the recipient cannot lawfully receive a digital asset, the transaction cannot remain on chain to the end. It proceeds in three steps:

01 The stablecoin travels on chain to a regulated crypto partner located in the recipient's country.

02 That partner performs the off-ramp, converting the stablecoin into local currency. This off-ramp transaction is fuelled by xREMI.

03 The partner then transfers the local-currency amount from its own account to the recipient's bank account through a normal domestic bank transfer.

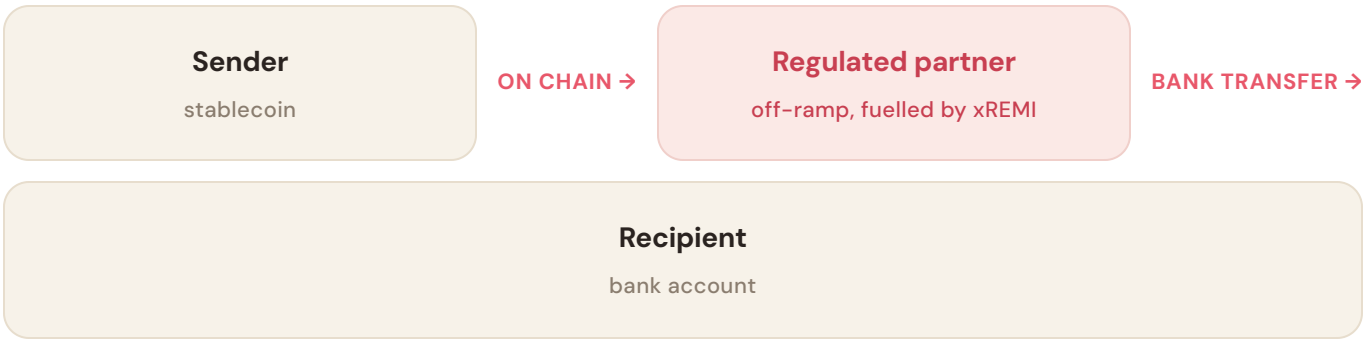

FIG. 3 Route B. The stablecoin reaches a regulated partner in the recipient's country, which off-ramps it to local currency and pays the recipient by bank transfer. The digital asset never reaches the recipient. The confidentiality layer is not invoked, because the on-chain leg here is transport to a partner for conversion rather than a confidential transfer between two end users. What carries over from Route A is the role of the token: xREMI fuels the off-ramp leg.

6.3 The fee is paid separately, in xREMI

In both routes the transaction fee is paid in xREMI and is never deducted from the amount being sent. The send amount arrives whole. The cost of the transaction is paid alongside it, in xREMI, from the sender's wallet. This matters for two reasons: the recipient receives exactly what the sender intended, with nothing shaved off in transit, and the fee becomes a clean, separable quantity denominated in the network's own asset.

> **REMARK 2**
>
> A sender who originates in fiat still pays the network fee in xREMI. Section 11 explains how ordinary users who do not hold or follow digital assets are supplied with xREMI so this is possible, and why that supply is funded by a specific part of the token allocation.

07 The xREMI Token

xREMI is the single native asset of the protocol. It is a utility and governance token. It is **not** a stablecoin, it is **not** pegged to any currency, and it does **not** represent a claim on a reserve. Its market price floats, written as P throughout. The token has three utilities.

UTILITY 1

Fees

Every transaction pays its fee in xREMI. On Route A the token fuels confidential settlement; on Route B it fuels the off-ramp. Developed in Section 8.

UTILITY 2

Staking & security

Holders can lock xREMI to help secure the network and earn a share of the fees the network collects. Developed in Section 9.

UTILITY 3

Governance

xREMI carries the right to vote on the protocol's parameters and direction. Developed in Section 14.

REMARK 3 · WHAT XREMI DOES NOT CLAIM TO BE

- Not required for the network's first phase of regulated operation.
- Not the settlement asset; payments settle in stablecoins or local currency.
- Not a promise of yield or return.
- Not a substitute for licensing, compliance, custody, or the responsibilities of operators.

The token's value is meant to follow real, measured network usage, not to stand in for it.

08 Fee Mechanics and Token Economics

8.1 The fee is dynamic and is paid in xREMI

The protocol does not fix the transaction fee at any particular figure. The fee is a variable the network participant originating a transaction sets according to its own business model. We write the fee of a single transaction in account terms as F_{tx}, expressed in a unit of account such as a major currency. The fee is paid in xREMI, so it must be converted from the unit of account into a quantity of tokens at the token's market price P at the time of the transaction.

DEFINITION 4 · FEE QUANTITY IN XREMI

For a transaction with fee F_{tx} and token price P, the quantity of xREMI paid as the fee is $q = F_{\text{tx}}/P$.

$$q = \frac{F_{\text{tx}}}{P} \tag{2}$$

Equation (2) is the hinge of the whole economic model. The network sources F_{tx}/P tokens from the holder for every transaction. Because the fee is denominated in a unit of account but settled in xREMI, every transaction creates a demand for the token proportional to the value of activity and inversely proportional to the token's price.

8.2 Fee distribution

The xREMI collected from each fee is split by a fixed rule. Half goes to the stakers who secure the network. A further forty-five percent goes to the REMI Foundation treasury, which funds operations, development, compliance, and ecosystem growth. The final five percent is burned, removing it from supply permanently.

$$R_{\text{stk}} = 0.50\,q, \qquad T_{\text{found}} = 0.45\,q, \qquad B = 0.05\,q \tag{3}$$

with $R_{\text{stk}} + T_{\text{found}} + B = q$ by construction.

FIG. 5 The fee distribution rule (“feeonomics”). Each fee paid in xREMI is divided into a stakers' share, a treasury share, and a burn, in the fixed proportions of equation (3).

8.3 Aggregate fee flow

Consider a settlement period with N transactions. Let transaction i carry a fee $F_{\text{tx}}^{(i)}$ in the unit of account and let $\bar{P}$ be the representative token price over the period. The total quantity of xREMI collected as fees is

$$Q = \sum_{i=1}^{N} \frac{F_{\text{tx}}^{(i)}}{\bar{P}} = \frac{1}{\bar{P}} \sum_{i=1}^{N} F_{\text{tx}}^{(i)} = \frac{N\,\overline{F}_{\text{tx}}}{\bar{P}} \tag{4}$$

where $\overline{F}_{\text{tx}}$ is the mean fee per transaction. The period's flows to stakers, treasury, and burn are then $0.50\,Q$, $0.45\,Q$, and $0.05\,Q$ respectively. The quantity of tokens cycling through the fee mechanism rises with the number of transactions and the average fee, and falls with the token price. This is the quantitative content of the claim that token usage tracks network usage.

09 Staking and Network Security

9.1 Why holders stake

Staking is the act of locking xREMI in the protocol to support the network. It does two things at once. It strengthens security, because the value committed to honest participation grows with the amount staked; and it earns the staker a share of the fees the network collects, because half of every fee is distributed to stakers. The two effects reinforce each other: a holder who expects fee income has a reason to stake rather than sell, and a larger staked base makes the network more secure, which supports the activity that generates the fees.

9.2 Individual rewards

Rewards from the stakers' share are distributed in proportion to stake. Let an individual stake s_i out of a total staked supply $S_{\text{stk}} = \sum_j s_j$. From a single transaction fee, the individual receives

$$R_i \;=\; R_{\text{stk}} \cdot \frac{s_i}{S_{\text{stk}}} \;=\; 0.50\, q \cdot \frac{s_i}{S_{\text{stk}}} \tag{5}$$

Over a settlement period with aggregate fee quantity Q from equation (4), the individual's reward is

$$R_i^{\text{period}} \;=\; 0.50\, Q \cdot \frac{s_i}{S_{\text{stk}}} \tag{6}$$

9.3 Yield and its dependence on participation

Let $\sigma = S_{\text{stk}}/C$ be the fraction of circulating supply C that is staked, and let Q_{yr} be the annual quantity of xREMI paid to the stakers' pool, equal to 0.50 times the annual fee quantity. The token-denominated annual yield on a unit of stake is

$$y \;=\; \frac{Q_{\text{yr}}}{S_{\text{stk}}} \;=\; \frac{Q_{\text{yr}}}{\sigma\, C} \tag{7}$$

For a given pool of fees, yield falls as more of the supply is staked, because the same rewards are shared among more stake. This is not a flaw; it is the mechanism that finds an equilibrium level of participation. Yield is high when few stake, which attracts more staking, which lowers yield, until the marginal holder is indifferent between staking and not.

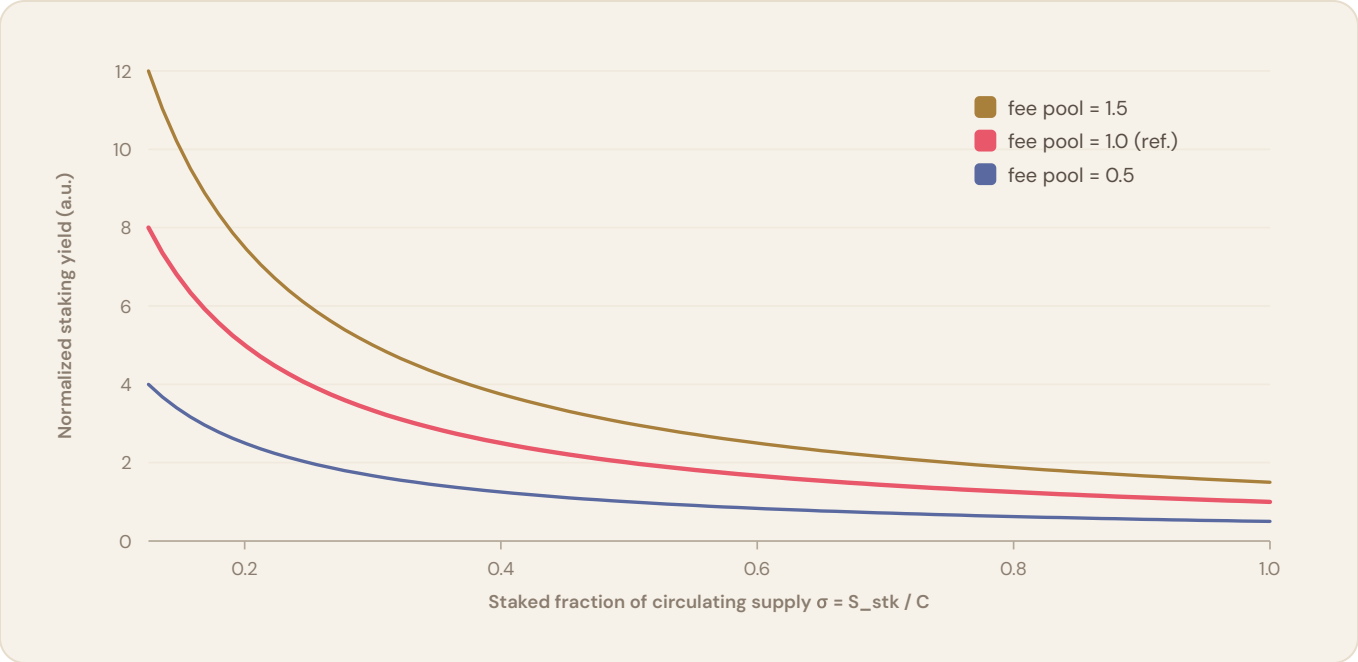

FIG. 6 Staking yield as a function of the staked fraction σ, for three sizes of the annual stakers' fee pool. Yield is decreasing in participation, producing a self-correcting equilibrium rather than a runaway.

9.4 Security as a function of staked value

Let the market value of staked xREMI be $\Sigma = P \cdot S_{\text{stk}}$. We adopt a simple security assumption standard for stake-secured systems.

ASSUMPTION 1 · COST OF ATTACK

The economic cost of mounting an attack that requires controlling a fraction θ of stake is at least $\theta\,\Sigma$, since an attacker must acquire and commit that much staked value and places it at risk.

PROPOSITION 1

The economic security of the network is non-decreasing in both the staked supply S_{stk} and the token price P, and the staking reward mechanism increases S_{stk} by paying half of all fees to stakers.

Security scales with $\Sigma = P\, S_{\mathrm{stk}}$, increasing in each factor. Equation (6) shows staking earns a positive share of fees whenever network activity is positive, which raises the return to staking relative to holding idle and therefore raises the equilibrium S_{stk}. Hence the reward mechanism raises Σ and with it the cost of attack.

10 Supply, Emission, and Vesting

10.1 Fixed supply

The total supply of xREMI is fixed at

$$S_0 = 1{,}000{,}000{,}000 \ \text{xREMI} \tag{8}$$

No mechanism mints new tokens beyond this cap. The burn in equation (3) only reduces supply, so total supply is non-increasing over time. After cumulative fee throughput Q_{cum} tokens have been paid as fees, the total supply is

$$S(Q_{\text{cum}}) = S_0 - \beta\, Q_{\text{cum}}, \qquad \beta = 0.05 \tag{9}$$

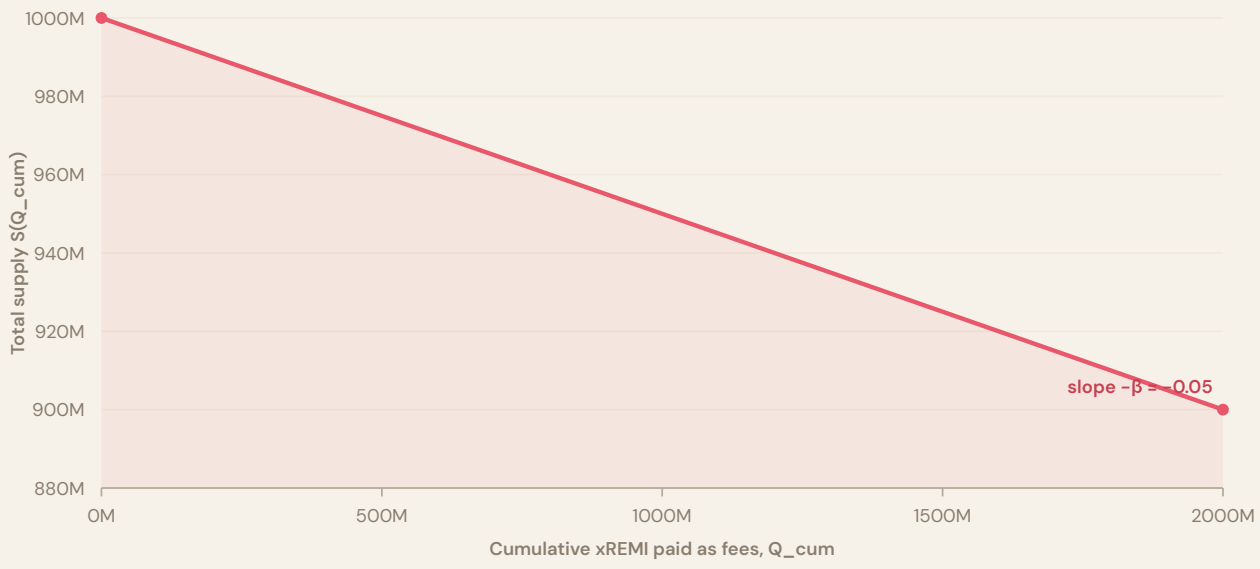

FIG. 7 The deflationary supply path implied by the burn. Total supply declines linearly in cumulative fee throughput at the rate $\beta = 0.05$. The relationship is purely mechanical and makes no assumption about market size.

10.2 Allocation

The fixed supply is allocated across four categories at the token generation event.

TABLE 1 **Initial allocation of the fixed xREMI supply**

CATEGORY	SHARE	AMOUNT	VESTING
Ecosystem & Community	40%	400,000,000	Programmatic release over 84 months
Investors	20%	200,000,000	12-month cliff, then 36-month linear
Team & Core Contributors	20%	200,000,000	12-month cliff, then 36-month linear
The REMI Foundation	20%	200,000,000	6-month cliff, then 48-month linear
Total	**100%**	**1,000,000,000**	**n/a**

10.3 Vesting in closed form

Each category releases its allocation over time according to a cliff and a linear schedule. For a category k with allocation A_k, cliff length c_k, and linear duration d_k, the vested amount at month t is

$$V_k(t) = \begin{cases} 0, & t < c_k, \\ A_k \dfrac{t - c_k}{d_k}, & c_k \le t < c_k + d_k, \\ A_k, & t \ge c_k + d_k. \end{cases} \tag{10}$$

Nothing is released during the cliff; afterward the allocation is released linearly until fully vested at month $c_k + d_k$. The Ecosystem & Community category has no cliff and releases linearly across the full 84 months. The total vested supply and the circulating supply are

$$V(t) = \sum_k V_k(t), \qquad C(t) = V(t) - \beta\, Q_{\text{cum}}(t) \tag{11}$$

The long schedules (up to seven years for the ecosystem allocation and four years for team and investors) are chosen so that supply enters the market gradually and in step with the network's growth rather than all at once.

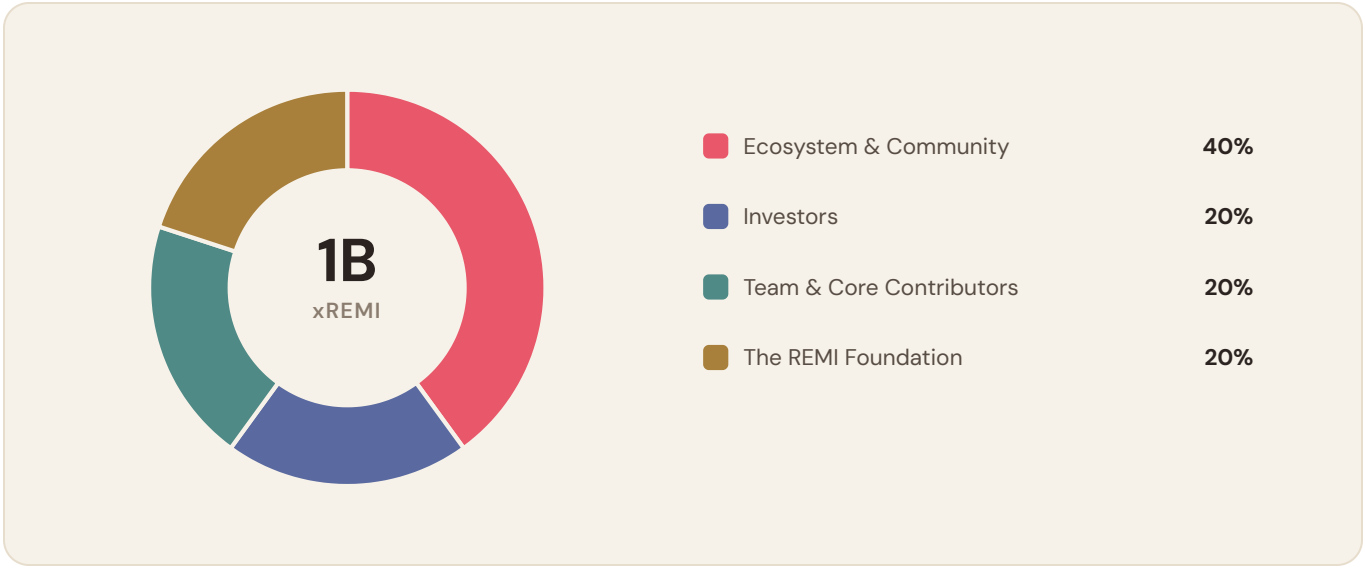

FIG. 8 Initial token allocation by category. The Ecosystem & Community share is the single largest category: it funds bringing ordinary users into a token-paid fee model (Section 11.2).

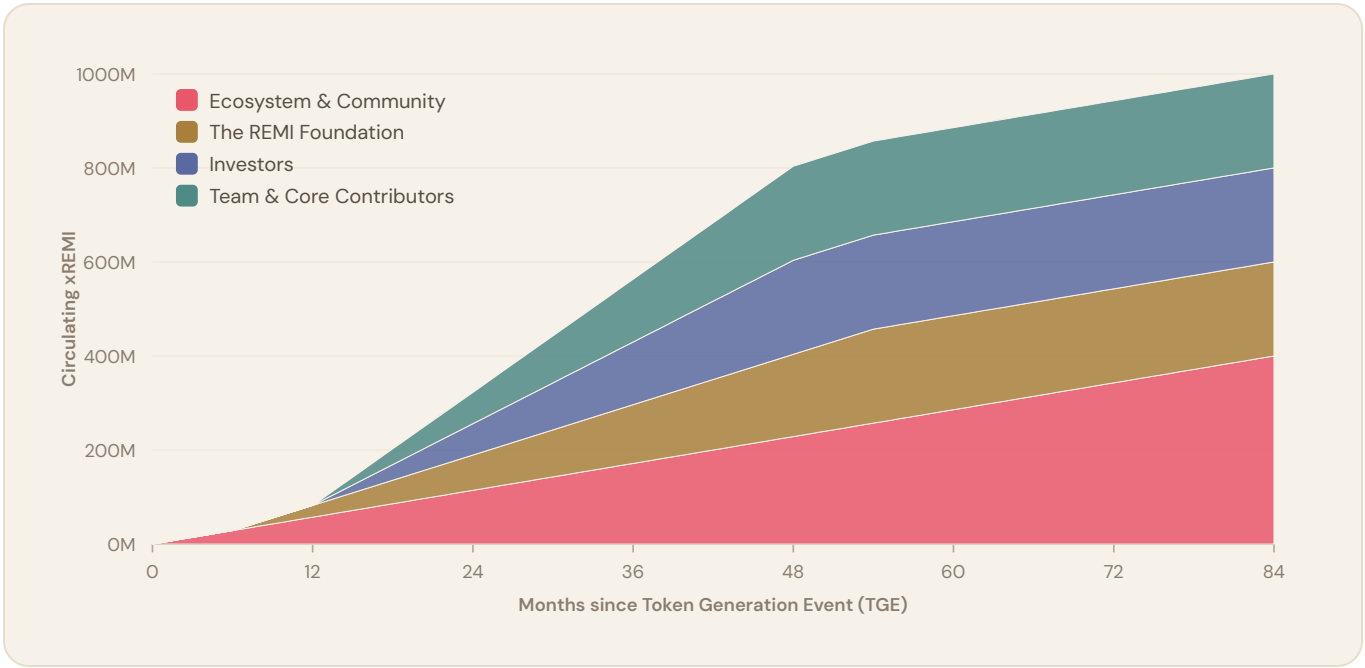

FIG. 9 Cumulative emission of xREMI by allocation category over the 84 months following the token generation event (equation 10). The upper envelope is total vested supply, approaching the fixed cap of one billion tokens.

FIG. 10 Per-category vesting trajectories, with each category's cliff marked (dotted). After its cliff, each category vests linearly to completion; Ecosystem & Community has no cliff and releases across the full 84 months.

11 Demand Formation and Market Adoption

11.1 Structural demand from fees

The defining feature of the model is that every transaction fee on the network is paid in xREMI, whatever the origin of the transaction. A stablecoin payment pays its fee in xREMI; a fiat-originated remittance pays its fee in xREMI as well. Because the fee is denominated in a unit of account but settled in the token, each transaction forces a quantity of tokens to be sourced from the market. From equation (4), the quantity demanded for fees in a period is

$$D = \frac{N \overline{F}_{\text{tx}}}{P} \tag{12}$$

This is demand that comes from *using* the network, not from speculation about its future. It rises with the number of transactions and with the average fee. Holding network activity fixed, it rises as the price falls, a stabilizing force on price.

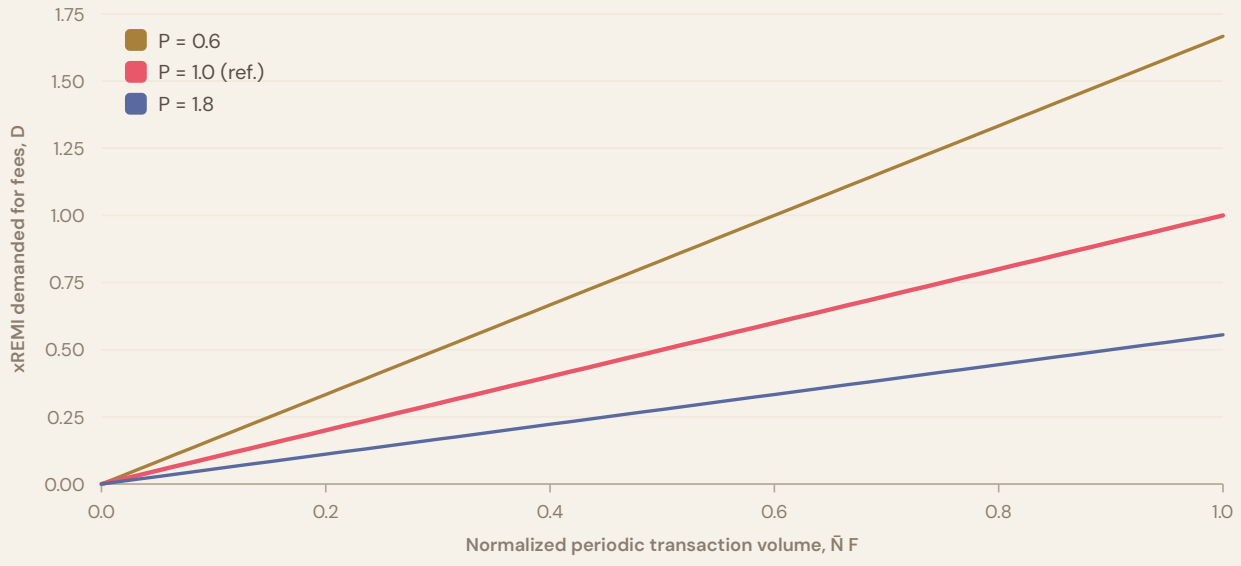

FIG. 11 Structural demand for xREMI from fee settlement (equation 12). Demand grows with transaction volume and is larger at lower token prices, holding volume fixed. Axes are normalized to keep the model market-agnostic.

11.2 Bringing non-crypto users into an xREMI fee model

Equation (12) sets up a practical problem. Most people who send remittances do not hold xREMI and do not follow digital assets at all. Yet the model asks every transaction to pay its fee in xREMI, including an ordinary fiat-to-fiat remittance. The bridge between these two facts is the **Ecosystem & Community** allocation.

Forty percent of the total supply, four hundred million tokens, is dedicated to the community for exactly this purpose. It funds the activities that put xREMI into the hands of ordinary users and that teach the market how the token is used. Users can be supplied with xREMI to pay their fees, and they can earn more xREMI by transacting on the network. As they transact, they accumulate the token, they learn its role, and the demand in equation (12) grows from a widening base of real users rather than from a narrow base of crypto holders.

> REMARK 4
>
> This is why the community allocation is the single largest category in Table 1. It is not a marketing line; it is the mechanism that makes a token-paid fee compatible with users who do not start out holding the token.

12 The Protocol Flywheel

The pieces developed above form a single feedback loop. We describe it as a dynamical system to make the feedback explicit, while being clear that it is a model of incentives and not a guarantee of outcomes. Let V denote network transaction volume, P the token price, and σ the staked fraction. Qualitatively,

$$V\uparrow \Rightarrow\ Q\uparrow \Rightarrow\ R_{\text{stk}}\uparrow \Rightarrow\ \sigma\uparrow \Rightarrow\ \text{security}\uparrow \Rightarrow\ V\uparrow \tag{13}$$

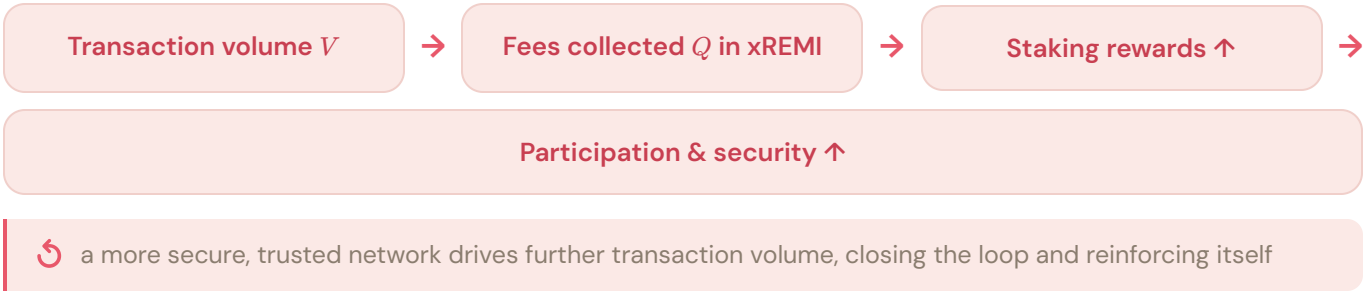

FIG. 12 The protocol flywheel. Usage generates fees, fees reward staking, staking deepens participation and security, and a more secure and trusted network supports further usage. A parallel loop runs through demand (equation 12) and burn (equation 9), which support the token's value.

REMARK 5

The loop turns in both directions. If usage falls, fee income falls, staking yield falls, and the supporting forces weaken. The model does not assume the loop only spins one way. The claim is narrower and defensible: the incentives are aligned so that real usage, when it occurs, is rewarded and reinforced.

13 Roadmap: From Regulated Network to Governed Protocol

The protocol is delivered in three phases. The ordering is the point: each phase establishes something the next one relies on.

PHASE 1

Regulated execution

The operating network is launched and validated with real participants, real operators, and regulated movement of money. This phase does not depend on the token. Its purpose is to prove the network works and produce genuine, measurable activity.

PHASE 2

Confidential & digital-asset layer

The confidentiality layer is built on chain, and xREMI is introduced as the asset that fuels transactions. Confidential stablecoin settlement and the off-ramp routes of Section 6 come into operation, and the fee, staking, and demand mechanics begin to apply.

PHASE 3

Governance & value capture

xREMI becomes the governing asset once the network has sufficient volume, operational evidence, compliance maturity, and stakeholder participation for governance to be meaningful. Decisions pass to the holders of staked xREMI.

FIG. 13 The staged path: a working regulated network comes first, the confidential on-chain layer and the token come second, and governance comes last, once the network can support it.

14 Governance

Governance is a Phase 3 function. Staked xREMI carries voting rights over the parameters this paper has deliberately left as variables: the fee level is set by participants, the burn and distribution shares are protocol parameters, and the schedule of future development is open. The matters that fall to governance include:

- adjustments to the fee and distribution parameters;
- the admission of new operators and settlement assets;
- the allocation of treasury funds toward ecosystem growth;
- the protocol's upgrade path.

> **Tying the vote to staked tokens links governance power to the holders who have committed capital to the network's security, aligning the people who decide with the people who bear the consequences of the decision.**

15 Risk Factors and Limitations

We state the principal risks plainly.

Regulatory risk

The legal treatment of stablecoins and other digital assets differs across jurisdictions and continues to change. Route A depends on both the sender's and the recipient's jurisdictions recognizing stablecoins, and the set of jurisdictions where this holds is not fixed. The protocol's reach grows or shrinks with that legal landscape.

Adoption risk

The demand model in Section 11 depends on real usage. If the network does not attract genuine transaction volume, the fee, staking, and demand mechanics have little to act on. The community allocation funds adoption work, but it does not guarantee adoption.

Price risk

xREMI is not a stablecoin. Its price floats and can fall. The yield in equation (7) and the security in Proposition 1 both depend on the token's value, so a sustained fall in price weakens both.

Confidentiality assumptions

The privacy properties in Section 5 are stated as security goals. Their realization depends on the construction of the on-chain layer and on keeping the leakage term ε in equation (1) negligible. Side channels in timing or amounts can erode privacy if not handled with care.

Model risk

The flywheel of Section 12 describes aligned incentives. It is not a promise of a particular price path or return, and it can run in reverse if usage declines.

16 Conclusion

Public ledgers solved the cost and speed of moving value and left privacy unsolved. For payments and remittances that omission is decisive, because the people and institutions who would use these rails cannot accept that every transfer is permanently public. The REMI Protocol is organized around closing that gap. It starts as a regulated operating network that moves real money through licensed operators, and it adds an on-chain confidentiality layer that lets stablecoin payments settle privately between recognized jurisdictions while remaining readable to the parties and to lawful supervisors. A single asset, xREMI, powers that layer, secures the network through staking, and governs the protocol once it has matured.

The economics follow from one design choice: every transaction fee is paid in xREMI and is never taken out of the amount being sent. That choice turns network usage into token demand, funds the stakers who secure the network, and burns a small share of every fee. The supply is fixed, its release is gradual, and the largest allocation is dedicated to bringing ordinary users into a token-paid fee model they did not start out understanding.

> **The network proves itself first, the token follows the proof, and governance follows the network. That sequence is what distinguishes a payments protocol that happens to use a token from a token in search of a use.**

A Notation

TABLE 2 **Notation used throughout the paper**

SYMBOL	MEANING
F_{tx}	Transaction fee in the unit of account (dynamic, set by the participant)
P	Market price of xREMI in the unit of account
q	Quantity of xREMI paid as the fee of a single transaction, $q = F_{\text{tx}}/P$
N	Number of transactions in a settlement period
$\overline{F}_{\text{tx}}$	Mean transaction fee in the unit of account over a period
Q	Total xREMI collected as fees in a period
R_{stk}	xREMI distributed to stakers, $0.50\,q$ per fee
T_{found}	xREMI to the Foundation treasury, $0.45\,q$ per fee
B	xREMI burned, $0.05\,q$ per fee
β	Burn fraction of each fee, $\beta = 0.05$
s_i	Stake of an individual staker
S_{stk}	Total staked xREMI
R_i	Reward to an individual staker
σ	Staked fraction of circulating supply, $\sigma = S_{\text{stk}}/C$
y	Token-denominated annual staking yield
Σ	Market value of staked xREMI, $\Sigma = P\,S_{\text{stk}}$

S_0	Fixed total supply, 1,000,000,000 xREMI
Q_{cum}	Cumulative xREMI paid as fees to date
$S(\cdot)$	Total supply as a function of cumulative fees
$V_k(t)$	Vested amount of category k at month t
$V(t)$	Total vested supply at month t
$C(t)$	Circulating supply at month t
D	Structural demand for xREMI from fees in a period
$A(r)$	Anonymity set of a confidential transfer r
$\Pi(r)$	Set of parties authorized to read transfer r
ε	Negligible privacy leakage term

Equations in plain language

Every numbered equation in this paper, stated once in ordinary words for readers who would rather skip the notation.

(1) **Privacy bound.** Even seeing the whole public ledger, an outsider's chance of guessing who sent a confidential transfer is no better than picking at random from the crowd it is hidden among.

(2) **Fee in tokens.** The fee for one transaction, in xREMI, is the fee in ordinary money divided by the token's price, so it is an amount of tokens, not a fixed sticker price.

(3) **Fee split.** Every fee is divided the same way: half goes to stakers, 45% to the Foundation treasury, and 5% is burned (destroyed forever).

(4) **Total fees in a period.** Add up all the fees over a stretch of time: it equals the number of transactions times the average fee, divided by the token's price.

(5) **Your cut of one fee.** A staker earns a slice of each fee equal to their share of all staked tokens: stake more, earn more.

(6) **Your cut over a period.** The same idea across many transactions: your total reward scales with your share of everything that is staked.

(7) **Staking yield.** Yield is the yearly reward pool divided by how much is staked, so the more people stake, the smaller each share becomes, which keeps participation in balance.

(8) **Hard cap.** There will only ever be one billion xREMI. No mechanism creates more.

(9) **Shrinking supply.** Because 5% of every fee is burned, the total number of tokens can only fall over time, never rise.

(10) **Unlock schedule.** Each group's tokens unlock on a timetable: nothing during the initial “cliff” wait, then released steadily until fully delivered.

(11) **What is actually in circulation.** Add up every group's unlocked tokens for the total released, then subtract whatever has been burned to get the amount truly circulating.

(12) **Demand from real use.** The need to buy tokens just to pay fees equals transaction volume times the average fee, divided by price: demand created by usage, not by speculation.

(13) **The flywheel.** More usage leads to more fees, which means bigger staking rewards, which draws more staking and security, which builds trust, which in turn brings still more usage.

01 This whitepaper is for informational purposes only and does not constitute an offer to sell or a solicitation to buy any token, security, or financial instrument. xREMI is intended as a utility and governance token within the REMI Protocol and is not intended to be a security. Readers should consult their own professional advisors before making any financial decision. Forward-looking statements are subject to risk and uncertainty, and actual results may differ. See Section 15 for a discussion of risks.