STYN MULTI-SIG MODEL

Multi-Signature Governance

How SYTN Protects User Assets

Multisig-model v1.1 | SYTN | May 2026

DISCLAIMER PAGE

IMPORTANT NOTICE & LEGAL DISCLAIMER

Nature of this Document

This document has been prepared by SYTN Foundation for informational and technical purposes only. It describes the multi-signature governance architecture of the SYTN protocol as currently designed and implemented by the founding team. It does not constitute, and shall not be construed as, a prospectus, an offer to sell, or a solicitation of an offer to buy any securities, financial instruments, or investment products in any jurisdiction. It does not constitute financial, legal, tax, or investment advice of any kind. Readers seeking the complete investment disclaimer, token classification notice, restricted jurisdiction disclosure, and forward-looking statements notice are directed to the SYTN Protocol whitepaper, version 1.1, published May 2026 by SYTN Foundation.

No Representation on Completeness or Accuracy

While SYTN Foundation has taken reasonable care in preparing this document, no representation or warranty, express or implied, is made as to the accuracy, completeness, or fitness for any particular purpose of the information contained herein. The governance parameters, signer configurations, and architectural specifications described in this document are subject to change without notice at the discretion of SYTN Foundation and its DAO governance structure.

Technology and Protocol Risks

Participation in the SYTN protocol involves significant risks, including but not limited to smart contract vulnerabilities, oracle failures, collateral volatility, regulatory reclassification, liquidity constraints, and adverse market conditions. Prospective participants should carefully review the risk disclosures section of the SYTN Protocol whitepaper and conduct their own independent due diligence before making any decision to participate. SYTN Foundation accepts no liability for any loss or damage arising from reliance on this document or participation in the protocol.

Jurisdiction

This document is governed by the laws of Switzerland. Any disputes arising in connection with this document shall be subject to the exclusive jurisdiction of the competent courts of Switzerland, without prejudice to mandatory consumer protection provisions applicable in other jurisdictions.

INTELLECTUAL PROPERTY NOTICE

All content, methodologies, architectural designs, technical specifications, and governance innovations described in this document are the exclusive intellectual property of SYTN Foundation and its founding team, protected under applicable copyright, trade secret, and intellectual property law in Switzerland, Italy, the European Union, and other relevant jurisdictions.

The following constitute proprietary governance innovations of SYTN Foundation for which all rights are expressly reserved:

Multi-Signature governance architecture, the specific tripartite authority model separating operator, governor, and default admin roles within a single protocol governance system, including all associated permission hierarchies, constraint logic, and the principle that operational exposure is inversely proportional to authority level.

Institutional signer configuration framework, the criteria-based methodology for selecting and structuring independent multisig signers according to principles of institutional credibility, financial independence from protocol operations, and jurisdictional diversity, including the 3-of-5 threshold design and its associated mutual dependency logic.

DAO-to-multisig sequential validation framework, the governance architecture in which community voting via DAO precedes multisig execution as a democratic legitimacy verification layer, including all associated procedural integrity criteria and the constitutional distinction between substantive veto and procedural attestation.

Additional proprietary innovations of SYTN Foundation, including the price discovery engine, Decay-Adjusted VWAP mechanism, Decay-Adjusted TWAP fallback, universal asset wrapper, and compliance abstraction layer, are described and protected in the SYTN Protocol whitepaper and associated technical documentation. The publication of this document does not constitute a grant, waiver, or license of any intellectual property rights described above or in any other SYTN Foundation document.

Unauthorized reproduction, distribution, adaptation, or commercial use of any content or methodology described herein, in whole or in part, without prior written authorization from SYTN Foundation is strictly prohibited and may give rise to civil and criminal liability under applicable law. For licensing inquiries or institutional due diligence access: legal@sytnfinance.com

SYTN PROTOCOL

TABLE OF CONTENTS

0. The problem: who controls the keys?

In any system that holds assets on behalf of users, there is a fundamental question: who has the authority to move those assets, and what prevents that authority from being misused? In traditional finance, this is solved through layers of regulation, insurance, and institutional trust.

In a blockchain-based system like SYTN, we solve it through a mechanism called multi-signature governance, a set of rules, enforced by code, that ensures no single person or entity can unilaterally control the protocol's operations.

The simplest way to understand this: imagine a bank vault that requires three different keys,

held by three different people, to open. No single keyholder can access the vault alone. Even if one key is stolen, the vault remains secure. SYTN's governance works on the same principle, but enforced automatically by smart contracts rather than by physical locks.

1. Three roles, three levels of authority

SYTN separates authority into three distinct roles, each with different powers and different safeguards. This separation is the core security design: the role that operates most frequently has the least power, and the role with the most power is the hardest to use.

Role	What it does	What it cannot do	Safeguard
Operator	Handles routine daily operations: relaying messages between chains, posting confirmations, updating records.	Cannot change rules, cannot upgrade the system, cannot move user assets outside of normal verified processes.	Limited permissions enforced by the smart contract itself, even if this key is compromised, no assets are at risk.
Governor	Makes system changes: software upgrades, fee adjustments, adding support for new asset types.	Cannot act immediately, every change is announced publicly 48 hours before it takes effect.	48-hour time delay: if a malicious change is proposed, the community and team have two full days to review it and cancel it before it executes.
Default Admin	Emergency authority: can pause the system in a crisis, can assign or revoke roles, can override governance parameters.	Cannot act alone, requires agreement from multiple independent parties.	Multi-signature requirement: 3 out of 5 designated signers must approve any action (see below).

1.1 The operator

The operator is the role that runs most frequently. It is a software-controlled account (often called a “hot wallet”) that the backend system uses to perform routine tasks: confirming that a deposit has been received, relaying withdrawal instructions to vault contracts on other blockchains, and updating the records that prove all wrapped assets are fully backed. Crucially, the operator is designed with minimal authority. It can only do what the smart contracts explicitly allow it to do. It cannot change fees, it cannot upgrade contracts, it cannot transfer user assets to unauthorised addresses. If the operator’s private key were compromised by an attacker, the attacker could not steal funds, because the Operator simply does not have the permissions to do so. This is an intentional design choice: the most exposed component has the least power.

1.2 The governor

When the protocol needs to evolve, for example, to support a new type of tokenized asset, to adjust fee structures, or to deploy an improved version of a smart contract, these changes are proposed through the governor.

The governor is implemented as the Protocol Timelock, a timelock mechanism that enforces mandatory public review windows before any change takes effect.. The Timelock works as follows: when a change is proposed, it is recorded publicly on the blockchain but does not take effect for at least 48 hours. During this waiting period, anyone can inspect the proposed change.

If the change is legitimate, it executes automatically after the delay. If it is malicious or erroneous, the default admin (the multisig) can cancel it before it takes effect.

This mechanism prevents a class of attacks where a compromised governance key attempts to silently alter the system. Because every change is visible on-chain before it executes, there are no surprise modifications. The 48-hour window is specifically chosen to provide sufficient time for review even across time zones and weekends.

1.3 The default admin

The default admin is the highest-authority role in the system, reserved for emergency actions and fundamental governance decisions. It is controlled by an industry-standard multi-signature wallet.

Page 2A multi-signature wallet requires a minimum number of designated signers to approve any transaction before it can execute. SYTN's default admin is configured as a 3-of-5 multisig: there are five designated signers, and any three of them must independently approve an action for it to proceed.
This means:
No single person can take emergency action alone, regardless of their role in the organisation.
Even if two signers are compromised, collude, or become unavailable, the system remains secure and operable.
The loss of any two keys does not lock the protocol, because the remaining three can still reach the threshold.

2. Who holds the keys?

The identity and independence of the multisig signers is as important as the mechanism itself.

SYTN’s five signers are deliberately chosen to represent different interests and to prevent any single group from having a majority:

Signer	Role	Why This Party	Keys Held	Can They Form Majority Alone?
1 & 2	Founding team members	Operational knowledge, ability to respond quickly in emergencies.	2 of 5	No (need 3)
3	Legal and compliance advisor	Ensures regulatory obligations are met before emergency action proceeds.	1 of 5	No
4	Independent blockchain security institution	Technically credible third-party entity with no financial interest in SYTN's operations; acts as a check on the founding team.	1 of 5	No
5	Regulated neutral institutional body	External regulated entity with no economic exposure to the protocol; provides institutional-grade independence from both the team and signer 4.	1 of 5	No

The precise identities of signers 3, 4, and 5 are institutional placeholders at this stage. Final nominations will be announced following the presale phase, concurrent with the publication of the first governance transparency report. This sequencing is deliberate: selecting signers after the protocol's early maturation phase allows SYTN to verify the independence of each counterparty over time, rather than formalising commitments prematurely.

All signers are required to rotate their keys on a quarterly basis. Key rotation is itself a multisig-approved action, creating a verifiable and unbroken chain of custody that is publicly auditable on-chain.

2.1 Key rotation

The requirement that all signers rotate their keys on a quarterly basis is not a formality. It is one of the most operationally consequential elements of the multi-sig framework, and it deserves a precise explanation of how it works and why it matters.

Key rotation is the process by which each signer replaces their active cryptographic key with a newly generated one, invalidating the previous key entirely.

The purpose is to neutralise a specific class of long-term vulnerability: an attacker who compromises a key silently, without the signer's knowledge, and waits for an opportune moment to act. By limiting the

operational lifetime of any given key to ninety days, SYTN ensures that the window of exploitation for a compromised key is finite and bounded, even in scenarios where the compromise goes undetected.

The mechanics of the rotation process are governed by the same 3-of-5 threshold that applies to all other multisig actions. A rotation cannot be performed unilaterally by the signer whose key is being replaced: it must be proposed on-chain and approved by at least two additional signers before it takes effect. This means the rotation record itself is a public blockchain transaction, carrying a timestamp, the identifier of the outgoing key, and the identifier of the incoming key.

The result is what the document describes as an unbroken chain of verifiable custody: a complete, tamper-proof history of every key that has ever held signing authority over the protocol's default admin role, auditable by anyone at any time.

The question of what happens *between* rotations, specifically, what occurs if a key is compromised in the interval between two rotation cycles, is addressed by the structural constraints discussed in the adversarial scenarios section above. Because a compromised key alone cannot reach the 3-of-5 threshold, and because every action it participates in is publicly visible on-chain, a compromised key cannot act silently. The risk window between rotations is bounded both temporally, by the ninety-day cycle, and operationally, by the requirement for multi-party consensus on every action and the full on-chain transparency of that consensus.

3. What the multi-signature can and cannot do

The multisig has broad emergency authority, but it operates within boundaries set by the smart contracts themselves: It can:

Pause the protocol in an emergency (e.g., if a vulnerability is discovered), preventing all trading and withdrawals until the issue is resolved.

Cancel a pending governor action if it is determined to be malicious or erroneous during the 48-hour review window.

Revoke or reassign the operator role if the operator's key is compromised.
Add or remove multisig signers (subject to the 3-of-5 threshold).

It cannot:

Directly access, move, or redirect user assets held in vault contracts. Vault releases require verified burn proofs, which the multisig cannot fabricate.
Bypass the compliance attestation system. Even with full multisig authority, trades still require valid compliance attestations from both counterparties.
Make changes silently. Every multisig action is a blockchain transaction, publicly visible and permanently recorded.

3.1 Adversal scenarios

A governance model is only as credible as its ability to withstand stress. The 3-of-5 configuration is not an arbitrary choice: it represents a deliberate balance between operational resilience and security against coordinated failure. Understanding what the system can and cannot survive under adversarial conditions is essential for any reader conducting serious due diligence on the protocol.

The most commonly raised concern is the collusion scenario: what happens if three signers coordinate to abuse their authority? The structural answer lies not in the multi-sig mechanism alone, but in the combination of the multi-sig with the constraints imposed by the smart contracts themselves.

Even a fully colluding majority cannot redirect user assets held in vault contracts, because vault releases require verified burn proofs that no signer, individually or collectively, can fabricate. They cannot bypass the compliance abstraction layer (CAL), which operates as an independent on-chain enforcement layer regardless of governance authority.

What a colluding majority *can* do is limited to the actions listed in section 3: pausing the protocol, cancelling a pending governor action, or reassigning the operator role. Each of these actions is a publicly visible blockchain transaction, permanently recorded and immediately auditable by any observer.

The transparency of on-chain execution means that collusion is not silent: it leaves an immutable record that the community, external auditors, and regulators can inspect in real time.

The second scenario, key loss or permanent unavailability, is structurally more subtle. If two signers become permanently unavailable through death, incapacity, or irreversible key loss, the effective pool shrinks from five to three, at which point the 3-of-5 threshold becomes functionally unanimous among the remaining parties. This is not a catastrophic failure mode, but it is a material change in the trust model, transforming a distributed consensus requirement into a de facto requirement for full agreement among the survivors.

The protocol's response to this scenario is the quarterly key rotation mechanism, which is designed precisely to prevent silent degradation of the signer set: each rotation is itself a multisig-approved action, meaning the composition and availability of the signer group must be actively confirmed every ninety days. A signer who fails to participate in a rotation cycle triggers a documented gap in the chain of verifiable custody, creating a transparent signal that the governance structure requires remediation before the gap compounds.

The third scenario concerns the founding team acting adversarially as a block. Signers 1 and 2 together hold two of the five keys. To reach the threshold of three, they require at least one external signer, the legal and compliance advisor, or one of the two independent institutional signers, to agree.

This mutual dependency is structural and cannot be overridden by any unilateral decision of the founding team. Because the independent signers hold no financial interest in SYTN's operations, they have no economic incentive to approve an action that serves the team's interests at the expense of the protocol's users. Their independence is not merely a procedural declaration: it is the load-bearing element of the entire trust architecture.

4. Progressive decentralization

The 3-of-5 multisig is the starting configuration, chosen because it provides strong security guarantees while remaining operationally practical in the early stages of the protocol’s life. As SYTN matures and the token-holder community grows, the governance structure is designed to evolve:

Increase the signer count. The multisig can be expanded from 3-of-5 to 5-of-9, 7-of-12, or any other threshold that maintains a strong supermajority requirement. More signers means more distributed trust.

Include governance delegates. As the veSYTN governance system matures, elected token-holder delegates can be added as multisig signers, giving the community direct representation in emergency governance.

Reduce team representation. Over time, the founding team's share of multisig keys decreases as external and community signers are added, ensuring that governance transitions from a founder-led model to a community-governed model.

4.1 The relationship between the DAO and multi-sign

A natural question arises from reading this document: if the multisig holds the highest emergency authority, and the DAO holds authority over governance decisions, how do the two structures interact? The answer is that they do not operate as parallel and independent channels. They operate sequentially, with distinct and complementary roles that reinforce rather than duplicate each other.

The process works as follows. Any proposed change to the protocol, whether a fee adjustment, the introduction of a new sAsset, or a modification to collateralisation parameters, originates as a public proposal on the protocol's DAO governance platform, the native Solana governance framework. During the voting window, which runs between three and seven days depending on the category of the decision, every staked SYTN holder may cast their vote. A proposal advances only if it reaches the dynamic quorum threshold defined for that category.

Once a vote closes with a favourable outcome, the proposal does not execute automatically. It transitions to the multisig layer, where at least three of the five signers must verify its **democratic legitimacy** before execution can proceed. This verification does not concern the substance of the proposal, that has already been established by the voting community, but its procedural integrity: was the required quorum correctly reached? Does the action being proposed for execution correspond faithfully to the text that was voted on? Did the voting window close without detectable anomalies in on-chain participation? Only after this attestation does the governor activate the Protocol Timelock, which records the change publicly on-chain and initiates the standard 48-hour public review window before final execution.

In this architecture, the multisig does not function as a political veto body. It functions as a guardian of constitutional process. Just as a constitutional court does not judge whether a law is desirable, but whether it was enacted according to the procedures the system has defined, the signers verify that the community's will was expressed and captured in full conformity with the protocol's own rules.

This distinction matters: no signer can block a proposal because they personally disagree with it, but any signer can flag, and with the agreement of the required threshold, halt an execution that presents documented procedural irregularities.

The threshold for expanding the multisig from its current 3-of-5 configuration to more distributed arrangements, such as 5-of-9 or 7-of-12, is not defined in advance by fixed TVL targets or active token-holder counts. That decision will itself be made through DAO governance, at the point when the community determines that the protocol's maturity and the breadth of participation justify a further

distribution of signing authority. This choice, delegating to the DAO the timing of its own progressive replacement of founder-controlled keys, is itself a structural element of the constitutional design.

5. Summary

The multi-signature governance framework can be understood by analogy to a constitutional system of checks and balances:

SYTN Role	Analogy	Power	Check
Operator	Civil servant	Executes daily operations.	Cannot make policy.
Governor	Legislature	Proposes and enacts	48-hour public review

		changes.	before any change takes effect.
Default admin	Supreme court	Emergency authority, constitutional override.	Requires 3-of-5 independent parties to agree.

No single individual, no single key, and no single organisation can unilaterally control SYTN. Every action at every level is either constrained by code, delayed for public review, or requires multi party consensus. This is not a trust-based promise, it is a set of rules enforced by the smart contracts themselves, verifiable by anyone, at any time, on the public blockchain.

This document constitutes version 1.1 of the SYTN Protocol multisig-model, published May 2026 by SYTN Foundation. All prior drafts and informal summaries are superseded by this version.

For institutional inquiries, partnership discussions, and access to supplementary technical papers:
founder@sytnfinance.com| **chief.architect@sytnfinance.com**

Document integrity verified on-chain. Notarify certificate available upon request.

NOTARIFY
DIGITAL CERTAINTY

Certificate of authenticity

This is to certify that the document referred hereunder was notarized by our company at the date and time printed down below.

File hash

3cfa7a4c7a2b0d5c578b1daed0e8da05327c1e04f5f065f5da199e112154e858

CERTIFIED BY **NOTARIFY**

File Id	d0b7401f3693438e9520c7eba49b2b69.pdf
Combined Hash	pending
URL Notarify	https://app.notarify.io/d/eaaf6f

Notarify Timestamp

Friday, May 29,
2026 18:53 UTC+2

Certified by

Notarify

NOTARIFY
DIGITAL CERTAINTY

Signatures

Signer	Timestamp	Typology	Signature hash	Document hash
SYTN protocol	Friday, May 29, 2026 18:53 UTC+2	Graphic	-	3cfa7a4c7a2b0d5c578b1daed0e8da05327c1e04f5f065f5da199e112154e858

Date and time

Friday, May 29,
2026 18:54 UTC+2

Certified by

Notarify

NOTARIFY
DIGITAL CERTAINTY

File logs

Full name	E-mail	Timestamp	Event
SYTN protocol	founder@sytnfinance.com	Friday, May 29, 2026 18:53 UTC+2	View

Date and time

Friday, May 29,
2026 18:54 UTC+2

Certified by

Notarify