



SATI Protocol Whitepaper

Your Context. Your Choice. Your AI.

- [00](#) Getting Started
- [01](#) Overview
- [02](#) Background
- [03](#) Mission
- [04](#) Technology
- [05](#) Roadmap
- [06](#) Token
- [07](#) Team & Partnerships
- [08](#) Resources

What Is SATI Protocol

SATI Protocol is Consumer Data Infrastructure that converts the zero-party and first-party data generated in consumer applications into user-controlled context and verifiable data credentials, and connects them to consent-based advertising and personalized AI agents.

Internet services have long used personal data to improve personalization and advertising performance. Yet users have had little practical control over the purposes for which their data is collected, who receives it, and how long it is used.

AI agents are advancing rapidly, but there is still no trusted data layer that allows them to understand a user's long-term preferences, life context and decision-making criteria in a safe and sustained manner.

SATI addresses both problems with a single structure. It turns the data users create while using its app into context the user controls, and connects that context to consent-based advertising and personalized AI agents.

Three-Minute Summary

Question	Answer
What is SATI building?	A context layer owned and controlled by users, with consent-based advertising and personalized AI built on top of it
What do users do?	Generate data by using an app offering Saju (Korean Four Pillars astrology), compatibility readings, horoscopes, an AI companion, meditation and wellness, and AI-assisted mental care support
Where is data stored?	Raw data stays encrypted off-chain. Only credential status, consent policy identifiers, commitments, and issuance/revocation events are recorded on-chain
What do advertisers buy?	Not lists of individuals, but the available size of anonymous cohorts that meet eligibility criteria
How are rewards funded?	By advertisers' actual campaign spend, not by new token issuance
How many token types are there?	Three: the external SATI Token, the internal Native SATI Coin, and the non-transferable SATI Data Credential
Total supply	10,000,000,000 SATI

Glossary

- **Zero-party data:** Information a user voluntarily provides with knowledge of the specific service purpose — e.g., date and time of birth, birthplace, gender, interests and preferences.
- **First-party data:** Information observed through direct interaction with SATI services — e.g., feature usage, content choices, reward history and ad responses.
- **Inferred data:** Attributes computed by the system by combining declared and behavioral data. Never treated as equivalent to fact, and always labeled with a confidence level.
- **Sensitive data:** Information requiring a high level of protection, such as health, mental care and crisis signals. Excluded from ad targeting as a matter of principle.
- **Data Credential:** A non-transferable token that proves a specific attribute or participation condition without disclosing the underlying personal data.
- **Data Origination:** A strategy of recording meaning, basis, confidence level, consent scope and expiry conditions from the moment data is first created.
- **Native SATI Coin:** A restricted asset used within the internal network for user rewards and service payments. Peer-to-peer transfers and direct withdrawals to external wallets are prohibited.
- **Public Escrow:** The smart contract into which advertisers deposit campaign budgets.
- **Verifiable Human Engagement:** A framework that verifies ad impressions, engagement and feedback as authorized actions by real people.
- **Agentic Web:** A web in which AI interacts with tools, services and other agents on the basis of context and limited permissions.

Executive Summary

SATI Protocol is Consumer Data Infrastructure that converts the zero-party and first-party data generated in consumer applications into user-controlled context and verifiable data credentials, and connects them to consent-based advertising and personalized AI agents.

Internet services have used personal data to improve personalization and advertising performance, yet users have had little practical control over why their data is collected, who receives it and how long it is used. At the same time, while AI agents are advancing rapidly, there is no trusted data layer that enables them to understand a user's long-term preferences, life context and decision-making criteria safely and continuously.

SATI addresses both problems with a single structure. The SATI app offers Saju, compatibility and horoscope readings, an AI companion, meditation and wellness, and AI-based mental care support. In the course of using these services, users accumulate information they declare themselves along with interaction data generated through use. SATI classifies and refines this data and issues it as non-transferable Data Credentials that can prove specific attributes or participation conditions without revealing the underlying personal information.

Advertisers deposit campaign budgets into a smart contract using SATI tokens and query anonymous cohorts using criteria that cannot identify individuals. Users decide for themselves whether to participate in a campaign, and receive Native SATI Coin from the internal network as a reward when verified engagement occurs. Recurring rewards are funded by advertisers' actual campaign spend, not by new token issuance.

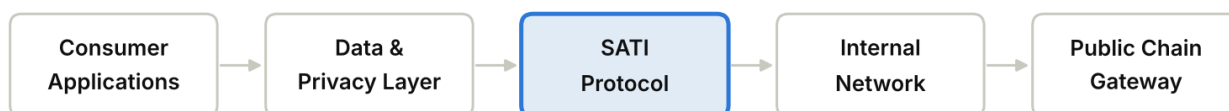
Over the long term, SATI will offer an SDK that allows other applications to integrate wallet, consent management, Data Credential, reward and settlement functions. Long-term context accumulated with the user's explicit permission becomes the foundation that enables personalized AI agents to understand users more accurately and to recommend, prepare and execute tasks within limited permissions.

The Five Protocol Layers

Layer	Role	User Value
SATI Core App	User acquisition and generation of zero-party and first-party data at the source	Practical services and continuous personalization
Data & Privacy Layer	Data classification, refinement, quality assessment and purpose-based isolation	Protection of raw data and control over scope of use
SATI Protocol	Execution of rules for consent states, credentials, campaigns, rewards and audits	Verifiable and revocable data use

Layer	Role	User Value
Internal Network	Gasless processing and operation of the restricted Native SATI Coin	A consumer experience that does not require awareness of the blockchain
Public Chain Gateway	Deposit of external SATI tokens, reserves and external redemption	Secure connection between external liquidity and internal services
SDK & Agent Layer	Third-party app integration and permission management for personalized AI agents	User context reusable across services

Raw data stays off-chain; only permissions, proofs and settlement remain verifiable



The "mainnet" referred to by SATI is not a general-purpose public L1 open to everyone without restriction. It is a dedicated protocol network that processes data credentials, consent, advertising rewards and internal payments in accordance with policy. The external SATI Token is issued on a separate public chain, and the two systems are connected through the Gateway and reserve contracts.

Core App and Ecosystem

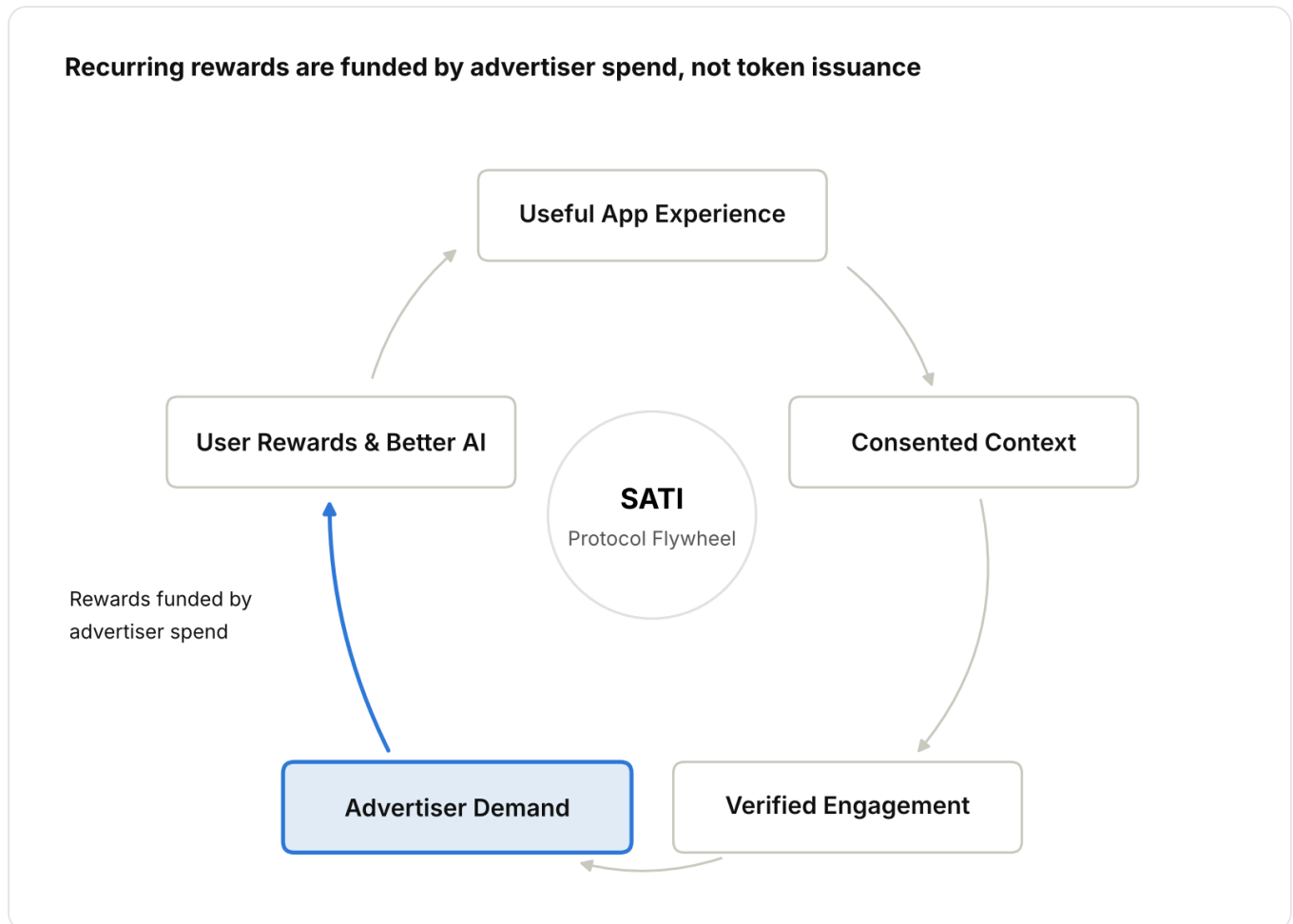
- **Fortune telling, Saju, compatibility and horoscopes:** Naturally generate data on personality, relationships and interests that users provide themselves.
- **AI companion:** Accumulates long-term preferences, goals, changes and feedback through recurring conversations.
- **Meditation and wellness:** Uses the routines users choose and their responses to content for personalization.
- **AI mental care support:** Supports emotional conversation and self-reflection, but does not replace medical diagnosis or treatment.
- **Built-in wallet and data dashboard:** Lets users view the Data Credentials they hold, their consent status, rewards and access history.

Sensitive data principle: Highly sensitive information such as mental care, health and crisis signals is excluded from ad targeting as a matter of principle. Even where such data is needed for service improvement or safety response, separate consent, minimal collection, restricted access and limited retention periods apply.

SATI Labs is responsible for the protocol, the token, the Data Credential standard, the core brand and global business rights. SATI Co., Ltd. is responsible for app and web development and service

operations in Korea. Core intellectual property, development deliverables, cost and revenue sharing, and personal data processing and cross-border transfers are to be set out in inter-company agreements and separate privacy documentation.

Business Model and Flywheel



A useful app creates consented context; verified engagement translates into advertiser demand; and advertiser spend grows user rewards and personalization, which in turn drives further app usage.

The initial business model is consent-based digital advertising. Advertisers acquire SATI tokens through lawful channels such as exchanges, complete KYB on the Advertiser Portal and deposit their campaign budgets. SATI enables advertisers to explore anonymous cohorts above a minimum threshold by combining permitted criteria such as age group, broad region, gender and general interests.

When a user consents to receive and engage with advertising and meets predefined conditions — impression, view, click or follow-up action — Native SATI Coin is paid out based on the verification result.

The identity or raw data of individual users is never provided to advertisers. The protocol fee is capped at 30% of the campaign budget, and exact user reward rates and fee rates are disclosed in advance as campaign-specific policies.

Structural Imbalance in the Data Economy

Value is created from users' data and participation, yet control, transparency and economic participation are concentrated in platforms. Personalization, recommendations, advertising, credit scoring and AI all depend on user data, but once users accept blanket terms of service at sign-up, it becomes difficult for them to see on what basis their data is generated, for what purposes and how long it is used, and to whom it is passed.

The problem SATI sets out to solve is not merely privacy protection. It is an operating structure that lets users understand how their data is created and used, make purpose-specific choices, stop access, request corrections, and participate in the value generated by approved uses.

Data Silos and Platform Lock-In

Data generated in one service mostly remains on that platform's servers and in its proprietary schema. Even when a download function exists, the data is hard for other services to interpret or reuse immediately, and data pipelines that depend on external APIs are fully exposed to changes in the platform's policies, terms of use, access restrictions, costs and quality.

SATI records meaning, basis, confidence level, consent scope and expiry conditions from the moment data is first created in the core app. This is Data Origination: unlike approaches that move data that already exists, it designs quality and rights structures at the point of creation.

The Context Gap in Personalized AI

Today's generative AI is powerful within a single session but limited in its ability to continuously understand long-term goals, relationships, tastes, recent changes and risk signals. Storing every conversation on central servers without limit increases the risks of privacy violations, use beyond the original purpose, misjudgment and security incidents. Conversely, without memory, an agent must ask for the same explanations every time.

On the Agentic Web, AI goes beyond generating answers to calling external tools and other agents and executing payments. What is needed is not more data, but verifiable context with clearly defined purpose, duration and permissions within the scope the user has authorized. SATI tackles this problem by separating AI intelligence from data access rights.

The Opportunity for User-Owned Data

Standard	Status	What SATI Draws On
W3C Verifiable Credentials Data Model 2.0	W3C Recommendation (May 2025)	Cryptographic exchange of credentials in an issuer–holder–verifier model
Ethereum ERC-4337	Adoption in progress	Smart accounts, transaction batching and gas sponsorship
EIP-7702	Adoption in progress	Design space for limited delegation of permissions
MCP	Specification 2025-11-25	A common interface connecting AI applications with tools and data
A2A	Published	Interoperability between different agents
x402	v2 documentation published	Programmatic payments by people and agents within the HTTP flow
ERC-8004	Draft	Connecting agent discovery, reputation and validation through on-chain registries

SATI does not simply replicate these standards. It combines the capabilities they enable — Data Credential interoperability, gasless accounts, limited agent permissions, verifiable engagement and programmable settlement — in a way that fits its consumer app, data sovereignty principles and advertising business model.

A User-Owned Context Layer

Mission: To build a user-owned context layer through which users control their long-term context and data access rights, share in the value generated by approved uses, and safely use AI agents that understand them.

SATI's core asset is not the data files themselves, but Provenance, which describes when, in which service and under what consent data was created; Data Credentials, which prove specific attributes; purpose-specific access rights; usage records; and renewable long-term context. This layer is not a static profile created once — it is continuously updated based on user behavior and explicit feedback.

Data Sovereignty: Six Core Rights

In SATI, data sovereignty is not an assertion of legal ownership over personal data files. It is an operating principle that gives users meaningful decision-making power over the collection, correction, use, access, revocation and deletion of their data, and the distribution of its value.

Right	Description
Right to know	Disclosure of the source of data, when it was created, whether it is inferred, its purpose of use and who accesses it
Right to choose	Separate, purpose-specific consent for core services, personalization, advertising and AI agent access
Right to control	Limiting the scope and duration of access, and pausing or revoking it
Right to correct	Amending declared data and disputing inferred data
Right to delete	Requesting deletion of raw data, except where legal retention obligations apply
Right to participate	Sharing in rewards when value is created through approved data use and verified engagement

Consumer-First Data Origination

SATI does not build a data network first and then look for users; it starts with an app that users will choose to use repeatedly. Data is generated when users provide information and feedback to get better fortune readings, relationship analysis, conversations, meditation and wellness experiences — so the motivation for data acquisition does not depend solely on token rewards.

This structure creates three defensive advantages:

- It builds a proprietary data moat that does not depend on third-party platform APIs.
- Data quality can be assessed because service context and the basis of creation are recorded together.
- Changes in the same user can be updated over time, making the data better suited to personalized AI than static data brokers.

Consent-Based Value Sharing

SATI is not a marketplace for selling data. It is a protocol that verifies the conditions users have approved and connects them with participation opportunities that match those conditions. Advertisers do not purchase raw personal data or user lists.

Value sharing is not compensation for the permanent transfer of data. It consists of three elements: consent limited to a specific purpose and period; verification of ad impressions or actions; and distribution of rewards from the campaign budget. Once consent is revoked, further access and any new use are stopped.

Seven Keywords of the Agentic Web

These are the seven concepts SATI uses as its reference points in designing for the Agentic Web.

Keyword	Definition
User-Owned Context Layer	Long-term personalization context for which the user controls the scope and duration of access
Agentic Web	A web in which AI interacts with tools, services and other agents on the basis of context and limited permissions
Privacy-Preserving Personalization	Personalization that uses only the necessary attributes and conditions, without broadly exposing raw data
Consent-Based Advertising	Advertising made possible by user choice, without identifying individuals or transferring raw data
Verifiable Human Engagement	A framework that verifies ad impressions, engagement and feedback as authorized actions by real people
Advertiser-Funded Token Utility	A structure in which real advertiser demand for tokens — not inflationary rewards — generates rewards and revenue
Consumer Crypto	Crypto that starts from a useful app experience, without putting wallets, gas or bridges front and center

Architecture and Data Pipeline

SATI's technical architecture consists of five layers: Application, Data & Privacy, Protocol, Internal Network and Public Chain Gateway. The wallet is not a separate repository sitting at the end of the stack, but an interface that brings together the permissions and assets of each layer from the user's perspective. Data Credentials are bound to the wallet, consent states and access records are verified by the protocol, and conversion to external assets follows Gateway policy.

In SATI, data passes through a seven-stage lifecycle:

- **Collect** — Collect data declared directly by users or generated through service use.
- **Classify** — Categorize data as zero-party, first-party or inferred, and assign sensitivity, purpose and retention period.
- **Refine** — Assess duplication, errors, elapsed time and confidence, and refine the data into usable attributes.
- **Consent** — The user approves the purpose, accessing party, duration and reward terms.
- **Credentialize** — Issue the required attributes and conditions as non-transferable Data Credentials.
- **Use & Verify** — Advertising, personalization and AI agents verify eligibility conditions within the permitted scope.
- **Update / Pause / Revoke / Delete** — Update, pause or revoke according to changes in the data and the user's choices.

Data Types and Purpose-Based Isolation

SATI divides data into four types and applies a different confidence level and handling principle to each.

Type	Definition	Examples	Default Principle
Zero-party	Information the user voluntarily provides with knowledge of the specific service purpose	Date and time of birth, birthplace, gender, interests, preferences	Explicit purpose-specific consent; editable by the user
First-party	Information observed through direct interaction with SATI services	Feature usage, content choices, reward history, ad responses	Minimal collection, retention limits, access control
Inferred	Attributes computed by the system by combining declared and behavioral data	Interest categories, preference shifts, recommendation fit	Labeled as inferred, with confidence level and right to dispute
Sensitive	Information requiring a high level of protection, such as health, mental care and crisis signals	Counseling conversations, emotional state, risk signals	Isolated from advertising; separate consent; enhanced access control

Inferred data is never treated as equivalent to fact. Credentials include the sourceClass, assuranceLevel, issuedAt and expiresAt fields to express the difference between declared, observed and inferred data and the passage of time. Low-confidence inferences are never used as the sole basis for ad eligibility or high-risk AI actions.

Data is isolated by purpose across five stores:

Vault	Key Data	Advertising Use
Core Service Vault	Date and time of birth, birthplace, gender, interests, preferences	Prohibited without separate consent
Personalization Vault	Preferences, feedback and long-term personalization context	Only general-interest credentials, on a limited basis
Wellness Vault	Meditation, wellness and mental care data	Prohibited in principle
Advertising Credential Store	Non-identifying credentials proving ad eligibility	Permitted
Compliance Vault	KYC/KYB, sanctions and fraud screening results	Prohibited

Consent States and Permission Signatures

Consent is not a single checkbox but a stateful permission object. It includes the purpose, data scope, accessing party, validity period, reward terms, revocation method and policy version. The main states are Pending, Active, Paused, Revoked and Expired.

Every access checks the current consent state, and revoked permissions cannot be used for new data queries or to run new campaigns.

- Consent for service use is separated from consent for advertising use.
- Read, recommend, prepare and execute permissions for AI agents are distinguished from one another.
- One-time, time-limited, count-limited and purpose-limited permissions are supported.
- Critical permissions are recorded using structured signatures such as EIP-712, or equivalent policy signatures.

Non-Transferable Data Credentials

A **SATI Data Credential** is a user-bound token that represents a refined personal data attribute or participation condition. It is based on the ERC-1155 interface to manage multiple credential types efficiently but, unlike ordinary NFTs, adds non-transferability logic that prohibits transfer, sale or collateralization between users.

Because the ERC-1155 standard itself does not guarantee non-transferability, transfer paths are explicitly restricted at both the contract and Gateway levels.

Field	Meaning
credentialType	Credential type, such as age range, broad region, interest category or participation eligibility
subjectCommitment	A commitment that does not directly expose the user identifier
issuer	SATI or an approved third-party issuer
sourceClass	Basis of the data: declared, observed, inferred, partner-provided, etc.
assuranceLevel	Verification strength and confidence level of the credential
issuedAt / expiresAt	Issuance and expiry timestamps
consentPolicyId	Applicable consent policy and version
status	Active, Paused, Revoked, Expired
proofCommitment	A commitment that verifies the integrity of the original data or proof material

On-chain / off-chain boundary: Raw personal data and counseling conversations are kept in encrypted off-chain storage. Only credential status, consent policy identifiers, commitments, issuance and revocation events, and the minimum records required for audits are stored on-chain.

Consent-Based Advertising and Verified Engagement

Advertiser Portal and campaign contracts. Advertisers complete corporate verification (KYB), wallet connection, and review of campaign objectives, targeting criteria, budget, participation conditions, reward rates, duration and restricted industries. Approved campaigns are activated after external SATI tokens are deposited into Public Escrow. Direct sales of SATI tokens for fiat currency or by credit card will not be offered until licensing and partner structures are finalized in each jurisdiction.

Privacy-preserving cohort search. What advertisers search is not a list of individuals, but the available size of cohorts that meet eligibility criteria. Exact dates of birth, detailed addresses, counseling content and raw free-form conversations are never exposed to ad search.

- Results below the minimum cohort threshold are not returned.
- Excessive query combinations and repeated queries are restricted to mitigate re-identification attacks.
- Per-user results, wallet addresses and raw data exports are not permitted.
- Sensitive and mental care data are excluded from ad credential generation.
- Campaign impressions and follow-up actions are verified only to the minimum extent permitted by policy.

Verifiable Human Engagement. Rewarded traffic is a target for bots, multiple accounts, ad farms and low-quality engagement. SATI does not assume that creating an account proves a person is human. Instead, it uses layered verification that combines app tenure, device and session integrity, behavioral consistency, credential status, per-campaign duplication limits, risk scores and, where necessary, KYC.

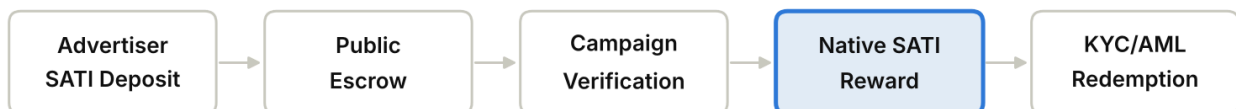
Engagement verification results are provided to advertisers as proofs that the conditions required by the campaign contract were met, together with aggregate reports — not as raw behavioral logs. The metrics available to advertisers are reach, verified impressions, verified engagement, conversion events and volume excluded for fraud.

Internal Network and Dual-Asset Settlement

SATI operates three assets of different natures separately.

Asset	Network	Transferability	Role
Public SATI Token	Public chain (to be selected)	Transferable	Ad deposits, external liquidity, ecosystem settlement
Native SATI Coin	SATI internal protocol network	Restricted	User rewards, internal service payments
SATI Data Credential	SATI internal protocol network	Non-transferable	Proof of data attributes, eligibility and consent status

Advertiser deposits pass through verification to user rewards and external redemption



On redemption, the internal balance is burned and an equal amount of external reserves is paid out.

Restrictions on the Internal Coin

- Peer-to-peer transfers between users are prohibited.
- Direct withdrawals to external wallets are prohibited.
- The coin may be used only within approved services and smart contracts in the SATI ecosystem.
- Only the user who earned the coin may apply to redeem it for external SATI tokens.
- Following KYC/AML review, the internal balance is burned and an equal amount of external reserves is paid out.
- Each KYC-verified account is linked to a SATI app wallet on a 1:1 basis by policy.

KYC is only one element of exit control and does not replace AML as a whole. Advertiser KYB, sanctions and PEP screening, transaction monitoring, anomaly detection, source-of-funds verification, limits and delayed payouts, and, where necessary, integration with Travel Rule and suspicious transaction reporting frameworks are reviewed on a jurisdiction-by-jurisdiction basis.

Gasless Smart Accounts

Users should be able to use SATI without prior knowledge of gas fees, networks, bridges or private key management. The built-in smart wallet uses session keys, spending limits, contract allowlists, recovery policies and risk-based step-up authentication. Gas is paid on the user's behalf by a Paymaster or system account operated by SATI Labs or the service provider.

For integration with public chains, SATI draws on ERC-4337 smart accounts and the batching, sponsorship and permission-scoping concepts of EIP-7702. The initial internal network provides the same user experience and policy constraints on its own execution layer; the specific account implementation and chain selection will not be finalized until security audits are completed.

SDK and Personalized AI Agents

In Phase 3, SATI will provide an SDK through which third-party apps can integrate an embedded wallet, consent manager, Data Credentials, reward distributor, campaign interface and settlement gateway. Installing the SDK does not automatically make an app's data the property of SATI; the roles of the app operator, the user and SATI Labs, as well as processing purposes, legal bases and the scope of data movement, are separated through contracts and consent policies.

Tier	Scope
Sandbox	Pseudonymous and test data only; no real rewards are generated
Standard	General data schemas and limited credential issuance
Verified	Extended capabilities for apps that have passed security, privacy and operational reviews
Restricted	Categories requiring separate contracts and regulatory review, such as finance, health and high-risk execution

SATI AI agents are not intended to be a centralized super-app with unlimited read access to all raw data. They request purpose-specific credentials and user-approved context on a least-privilege basis, and access rights expire when the permitted period ends. Agent permissions are divided into five levels according to risk.

Level	Permitted Actions	Default Controls
Read	Query permitted context and credentials	Limits on purpose, duration and fields
Recommend	Provide recommendations, analysis and alternatives	No execution; rationale shown

Level	Permitted Actions	Default Controls
Prepare	Draft messages, bookings, purchases and workflows	User review required
Execute — Low Risk	Perform approved, low-risk recurring tasks	Limits, allowlists, cancellable
Execute — High Risk	High-risk tasks such as money, health, legal matters and account changes	Explicit per-action confirmation, or prohibited

Agents keep audit logs of data access, tool calls, communication with external agents, proposals, user approvals and actual execution. MCP provides a design perspective for tool and data connectivity, A2A for agent-to-agent communication, and the ERC-8004 Draft for discovery, reputation and validation. SATI reviews the maturity and security of each specification and tests compatibility in stages.

Security, Privacy and AI Safety

- Data minimization, encryption, key separation, access control and purpose-based storage isolation are applied by default.
- High-risk permissions are subject to multi-party approval, time delays, limits, re-authentication and an Emergency Pause.
- Contracts, the Gateway, reserves and smart wallets undergo independent security audits and monitoring.
- Model outputs are continuously evaluated for accuracy, bias, over-reliance, prompt injection and data leakage.
- Mental care features include crisis guidance and referral procedures to professional organizations, and restrict definitive medical statements.
- Privacy impact assessments and AI risk assessments are built into product launch gates.

Privacy-enhancing technologies such as selective disclosure, cohort thresholds, zero-knowledge proofs, TEEs and confidential computing are being evaluated in stages. Because applying a technology does not by itself guarantee privacy, each is assessed together with the threat model, operating procedures, key management and legal accountability.

Technical Standards and Design References

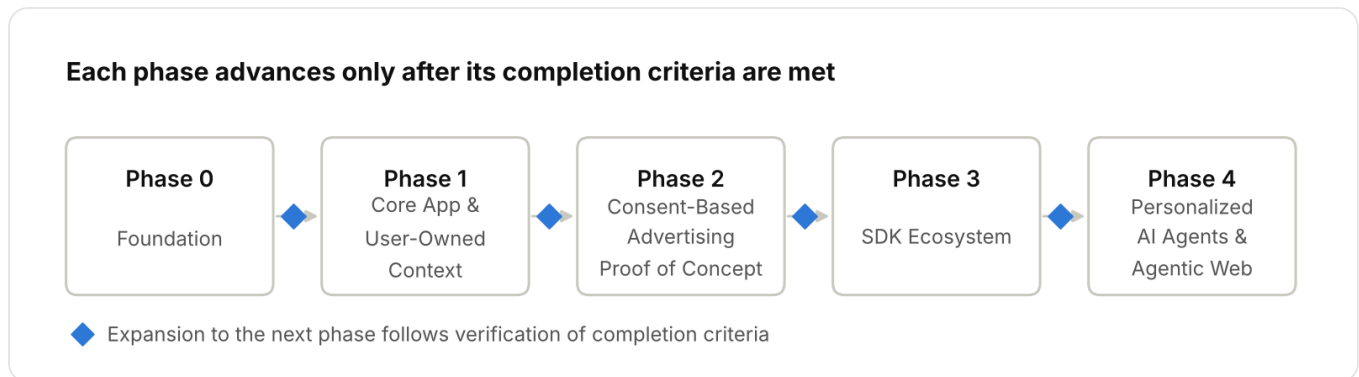
The following are references SATI consults to confirm technical standards and design direction. Their inclusion does not mean that SATI has already fully implemented any given specification; SATI reviews the maturity and security of each standard and verifies compatibility in stages.

- W3C Verifiable Credentials Data Model v2.0
- ERC-1155 Multi Token Standard
- ERC-4337 Account Abstraction

- EIP-7702 Set Code for EOAs
- Model Context Protocol Specification 2025-11-25
- Google Agent2Agent Protocol
- ERC-8004 Trustless Agents — Draft
- x402 v2 Documentation
- NIST AI RMF Generative AI Profile
- EU AI Act — Regulation (EU) 2024/1689

Phased Execution Plan

SATI's roadmap prioritizes verification gates for product, regulation, security and demand over date-driven marketing commitments. Each phase expands only when the key metrics and legal reviews of the previous phase have been satisfied. Token issuance or exchange listing is not equivalent to product launch and is subject to separate decision-making and disclosure procedures.



Phase 0 — Foundation

- Finalize the architecture of the SATI internal protocol network, built-in smart wallet and Gateway
- Evaluate public chain candidates and design the external SATI Token and reserve contracts
- Finalize the classification framework for zero-party, first-party, inferred and sensitive data, along with consent policies
- Implement the ERC-1155-based non-transferable Data Credential schema and issuance/revocation rules
- Establish a privacy impact assessment, virtual asset regulatory analysis, mental care safety policy and security threat model

Completion criteria: Consent, credential, reserve and reward flows are reproducible on testnet, and design documentation is complete for external legal and security review.

Phase 1 — Core Application and User-Owned Context

- Launch the SATI app, including Saju, compatibility, fortune and horoscope readings, the AI companion, and meditation and wellness features
- Deploy a user-friendly embedded wallet with recovery and re-authentication policies
- Provide a user dashboard showing data provenance, consent, Data Credentials and access history
- Logically and operationally isolate advertising data from mental care and other sensitive data
- Operate processes for user requests to correct, revoke, delete and access data

Completion criteria: Repeat usage, consent conversion, data refresh rate, complaint and revocation handling time, and privacy incident metrics meet internal benchmarks.

Phase 2 — Consent-Based Advertising Proof of Concept

- Implement advertiser KYB, wallet connection, campaign contracts and Public Escrow
- Apply anonymous cohort queries, minimum thresholds, a ban on sensitive targeting and query limits
- Enable user opt-in/opt-out, impression and engagement verification, and Native SATI Coin rewards
- Implement 1:1 reserves for the external SATI Token, internal coin burning and KYC/AML-based external redemption
- Provide reports on ad performance, volume excluded for fraud, user rewards and protocol fees

Completion criteria: In recurring campaigns funded with real ad spend, verified engagement, advertiser repurchase, user opt-out, fraud rates and unit economics are confirmed at a measurable level.

Phase 3 — SDK Ecosystem

- Release the Wallet, Consent, Data Credential, Reward and Settlement SDKs and developer documentation
- Operate a third-party app Sandbox and data schema validation tools
- Establish developer and partner tiers, security reviews, policy violation response and revenue sharing
- Pilot W3C VC-compatible credentials with external issuers and verifiers
- Pilot MCP-based tool connectivity and agent context access for partner apps

Completion criteria: Multiple external apps reliably operate consent, credential and settlement functions with real users, and developer retention is confirmed.

Phase 4 — Personalized AI Agents and the Agentic Web

- Long-term personalized memory based on user approval, with provenance and confidence management
- Per-agent data scopes, session keys, spending limits and expiring permissions
- Recommend-Prepare-Execute stages and human-in-the-loop controls for high-risk actions
- Pilot MCP- and A2A-based interoperability, agent-to-service payments and auditable activity logs
- Research registries and evaluation frameworks for agent quality, safety reputation and validation

Completion criteria: User approvals, permission scopes and execution outcomes are auditable end to end, and both the usefulness and safety of personalization are validated in real agent tasks.

SATI Token Overview

Item	Value
Token name	SATI Token
Ticker	SATI (proposed)
Maximum supply	10,000,000,000 SATI
External standard	Transferable token on a public chain (chain and standard to be finalized)
Internal asset	Restricted Native SATI Coin, backed 1:1 by external reserves
Data credential	Non-transferable, ERC-1155-based SATI Data Credential

The **SATI Token** is the external asset that links advertising campaign demand with ecosystem settlement. **Native SATI Coin** is a restricted asset used for user rewards and internal service payments, and the **Data Credential** is not a means of transferring value but a user-bound token that proves data attributes and permission status. The legal and accounting nature of all three assets will be finalized following advice in each jurisdiction.

Token Utility

- Advertisers deposit campaign budgets into Public Escrow using SATI tokens.
- Used for protocol fees, partner and developer settlement, and approved ecosystem services.
- Serves as the 1:1 reserve asset backing the internal Native SATI Coin.
- Should governance become decentralized in the future, limited protocol proposal and voting functions may be considered.

Sustainable token utility must come from real usage demand from advertisers and ecosystem participants, not from simple holding rewards or fixed returns. As a principle, user rewards are funded from campaign budgets and service revenue; any separate incentives for early user acquisition will be disclosed separately from advertising rewards.

Supply and Allocation

Total supply: **10,000,000,000 SATI**.

Allocation	Share	Amount	Purpose
Community + Ecosystem	50%	5,000,000,000	Real user rewards, ecosystem growth, developer incentives, protocol incentives and rewards for partner ecosystem contributions

Allocation	Share	Amount	Purpose
Team	20%	2,000,000,000	Allocation to core members who develop and operate the project
Treasury	12%	1,200,000,000	Foundation operating funds, development, ecosystem support, crisis response and strategic reserves
Marketing	10%	1,000,000,000	Brand operations, global campaigns, exchange listings, KOLs, community growth and user acquisition
Liquidity / MM	5%	500,000,000	Exchange liquidity provision and market stabilization
Private Sale	3%	300,000,000	Allocation to early investors

Vesting Schedule

SATI token vesting is designed around five principles:

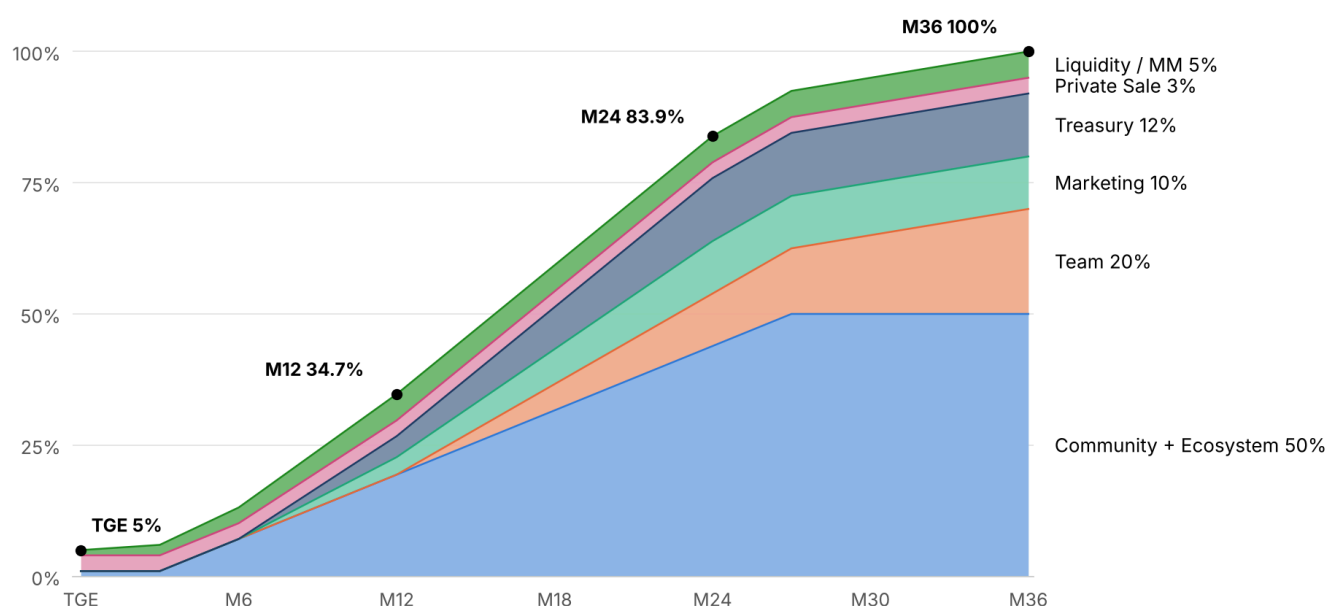
- A 5% unlock at TGE secures initial liquidity.
- Team allocations carry a 12-month cliff to prevent early selling pressure.
- Allocating 50% to Community + Ecosystem reinforces a user-centric structure.
- The entire supply enters circulation within a maximum of 36 months.
- Initial circulating supply is kept low to reduce market pressure.

Allocation	TGE Unlock	Cliff	Linear Vesting	Fully Unlocked
Community + Ecosystem	100,000,000 (1%)	3 months	24 months	M27
Team	0	12 months	24 months	M36
Treasury	0	6 months	18 months	M24
Marketing	0	6 months	18 months	M24
Liquidity / MM	100,000,000 (1%)	0	12 months	M12
Private Sale	300,000,000 (3%)	0	None	TGE
Total	500,000,000 (5%)	—	—	M36

Unlocks are linear after the cliff. The 5% TGE unlock consists of 300,000,000 from Private Sale, 100,000,000 from Liquidity / MM and 100,000,000 from Community + Ecosystem.

From 5% circulating at TGE to full unlock at Month 36

Cumulative unlocks by allocation, as % of total supply (10,000,000,000 SATI)



Point in Time	Cumulative Unlocked	% of Supply
TGE	500,000,000	5.0%
M3	600,000,000	6.0%
M6	1,312,500,000	13.1%
M12	3,470,833,333	34.7%
M18	5,929,166,667	59.3%
M24	8,387,500,000	83.9%
M30	9,500,000,000	95.0%
M36	10,000,000,000	100%

Rewards, Revenue Distribution and Disclosure Principles

Advertiser deposits, user rewards, protocol fees, refund balances and external reserves are segregated for accounting purposes. The structure is designed so that unspent budgets and confirmed user rewards are not commingled with SATI Labs' operating funds.

Category	Source of Funds	Default Principle
User advertising rewards	Advertiser campaign budgets	Native SATI Coin paid according to verified engagement conditions
Protocol fees	Up to 30% of the campaign budget	Operations, verification, settlement and infrastructure costs, plus protocol revenue

Category	Source of Funds	Default Principle
Developer and partner settlement	Service revenue or a pre-agreed share	Distributed according to campaign contracts and on-chain and accounting records
Ecosystem incentives	Separately fixed allocation or Treasury	Kept separate from advertising rewards; purpose, limits and duration disclosed

As a principle, reserves, external redemptions, campaign deposits, user rewards, fees and major Treasury movements are disclosed in regular reports, with on-chain proofs provided alongside accounting and operational reports.

Governance and Risk Management

Details of token sales, initial circulation, cliffs, vesting, unlocks, stakeholder agreements, market making and wallets will be disclosed once finalized. Figures and schedules not stated herein are not firm commitments, and legal review, contract audits, segregation of allocation wallets and execution of agreements must be completed before TGE.

Area	Management Items
Regulatory	Review licensing for the token, the internal coin, and advertising, payment, exchange and custody functions in each jurisdiction
Market	Manage the impact of external SATI Token price volatility on ad spend and user rewards
Reserves	1:1 correspondence between internal balances and external reserves; controls over custody, withdrawals, key management and audits
Liquidity	Monitor external redemption demand and the ability to pay out from reserves
Centralization	Disclose change procedures and multi-party approval for the initial operator

Initial governance is divided into protocol and security, data ethics and privacy, advertising policy, Treasury and token, and AI safety functions. Material changes undergo impact assessment, internal approval, external review where necessary, and user notification. Holding tokens does not grant any right to access personal data or control over data.

Founder

SATI Protocol is being developed by a team with experience in consumer applications, artificial intelligence, blockchain infrastructure, digital finance, regulatory affairs and external communications. The Core Team is responsible for the actual design, development and commercialization of the SATI application and protocol, while the Advisors provide strategic counsel on policy, finance, audit and communications.

Changbeom Park | Founder & Protocol Strategy. As Chairman of Korea Digital Asset Evaluation & Certification (KODEAC), he has led industry initiatives in digital asset policy, stablecoins, RWA tokenization and global expansion in digital asset markets. As founder of SATI Protocol, he oversees protocol strategy, regulatory affairs, fundraising, global partnerships and ecosystem expansion.

SATI Labs is responsible for the protocol, the token, the Data Credential standard, the core brand and global business, while SATI Co., Ltd. is responsible for app and web development and service operations in Korea. The rights, costs, revenues and personal data processing relationships between the two entities are governed by separate agreements and policies.

Core Team

Name	Role	Profile
Min Jang	AI & Protocol Research Lead	B.S., M.S. and Ph.D. in Computer Science and Engineering from POSTECH, specializing in machine learning and artificial intelligence. Deputy Director of the POSTECH Center for Crypto Blockchain Research (CCBR). Responsible for the personalization engine, AI agent architecture and data inference models.
Mintaek Song	Digital Finance & Ecosystem Strategy Lead	Adjunct Professor at the Hanyang University Graduate School of Business. Led business and digital strategy at Daum Communications and in the financial sector. Responsible for digital finance strategy, token economics and the advertising business model.
Junghoon Lee	Web3 Business & Growth Lead	Background in digital asset trading platform operations, blockchain and metaverse businesses, and P2E game marketing. Responsible for global market entry strategy, advertiser acquisition and Web3 partnerships.
Jonghak Lee	Backend & Infrastructure Lead	Over 20 years of web service and backend development, including development and operation of the Nate portal at SK Communications. Responsible for the core backend, data processing pipeline and systems integration.
Yongwoo Lee	Blockchain Platform Lead	Over 16 years of software and platform development; CTO of a blockchain-based content platform. Responsible for the internal mainnet, smart wallet and external token conversion gateway.

Advisors

The advisory board provides strategic counsel on policy, finance, audit and communications.

Name	Role	Advisory Scope
Sangsoo Lee	Corporate Strategy & Organizational Governance	Organizational and governance design, global business expansion, strategic partnerships and key stakeholder collaboration
Gongsik Han	Public Policy & Regulatory	Regulatory strategy, user protection policy, protocol governance and engagement with regulated institutions
Jun Ha	Financial Institutions & Blockchain	Partnerships with financial institutions, payment and settlement infrastructure, entry of digital assets into the regulated system, and institutional partnerships
Youngha Lee	Audit, Risk & Compliance	Reserve verification, internal controls, financial audits, risk management and transparency in fund management
Junkoo Kang	Financial Regulation, Capital Markets & Governance	Financial regulatory compliance, capital markets strategy, investor protection, internal controls and board governance
Sangshin Sun	Media & Strategic Communications	Domestic and international media strategy, external communications, and reputation and crisis management
Dongwook Han	Economic Media & Investor Communications	Market and industry narratives, investor communications, economic media relations and content strategy
Jinho Noh	AI, Data & Information Security	AI and data utilization strategy, consent-based data management, information security and service infrastructure reliability

Partnerships

Strategic partners working with SATI Protocol:

- GOBI PARTNERS
- KOREA DIGITAL ASSET CUSTODY
- Lee & Ko

Risk Disclosure

- **Regulatory:** Licensing requirements for the token, the internal coin, and advertising, payment, exchange and custody functions vary by jurisdiction and are subject to change.
- **Market:** Price volatility of the external SATI Token affects demand for ad spend and the value of user rewards.
- **Reserves:** The 1:1 correspondence between internal balances and external reserves depends on custody, withdrawal, key management and audit controls.
- **Liquidity:** SATI monitors the possibility that external redemption demand may exceed the capacity to pay out from reserves.
- **Centralization:** In the early stages, the operator retains change authority; change procedures and multi-party approvals are disclosed.
- **Technical:** Risks of contract vulnerabilities, prompt injection, data leakage and model misjudgment remain.
- **Schedule:** Each phase of the roadmap may be delayed depending on whether its verification gates are met.

Legal Notice

- This document is provided for informational purposes only and does not constitute an investment solicitation, an offer or solicitation to subscribe, or financial, legal or tax advice.
- Figures and schedules not stated herein are not firm commitments. Details of token sales, initial circulation, cliffs, vesting, unlocks, stakeholder agreements, market making and wallets will be disclosed once finalized.
- Mental care support features assist with emotional conversation and self-reflection and do not replace medical diagnosis or treatment. Holding tokens does not grant any right to access personal data or control over data.

FAQ

Q1. Is my data sold to advertisers?

No. Personal data and user lists are never sold. Advertisers can only query the size of anonymous cohorts that meet their criteria.

Q2. Where do rewards come from?

From advertisers' actual campaign spend — not from new token issuance.

Q3. What happens if I revoke my consent?

All further access and any new use of your data stop.

Q4. Are my counseling conversations used for advertising?

No. Mental care and other sensitive data are excluded from ad credential generation.

Q5. Can I sell my Data Credential?

No. Data Credentials are non-transferable; transfer, sale and use as collateral are not permitted.

Q6. Do I need to understand wallets and gas fees?

No. With the built-in smart wallet and sponsored gas, you can use SATI without any prior knowledge.

Q7. Can I send the internal coin to an external wallet?

The user who earned the coin may apply for external redemption after completing KYC/AML review.

Q8. Will the AI agent make payments from my account?

High-risk tasks require explicit per-action confirmation or are prohibited outright.