

Aligned Sovereign Intelligence Protocol

A Dual Governance & Treasury Reserve Ecosystem

ASIP White Paper v5.1

A. Monroy & M. Bastidas

<https://asi2.org>

ABSTRACT

"Mitigating the risk of extinction from AI should be a global priority" Center for AI Safety, 2023 [1]. That statement was signed by Geoffrey Hinton, Demis Hassabis, Ilya Sutskever, and leaders at Google, Anthropic, Open AI, Microsoft, xAI, MIT, Cambridge, Oxford, Harvard, and Stanford.

The Aligned Sovereign Intelligence Protocol (ASIP) represents a paradigm shift in how AI safety research is funded and governed. Unlike traditional capital models, ASIP provides perpetual, non-dilutive funding for AI safety projects through a transparent, performance-driven governance token known as the Safe AI Token (SAIT). SAIT addresses the critical centralization problem in AI research, where US corporate-backed projects received about \$1.35T ($\approx 90\%$ of all AI funding) in a single jurisdiction [2] [3].

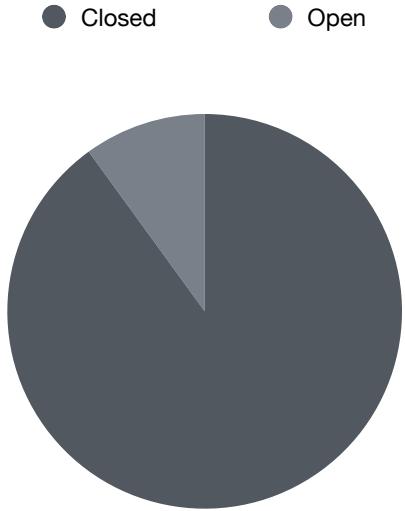
The Safe Asset Token (SAT) serves as SAIT's treasury reserve and represents a return to sound money principles articulated by Benjamin Graham - the man who taught Warren Buffett value investing [4]. SAT is named after Satoshi Nakamoto, whose vision for peer-to-peer electronic cash revolutionized digital finance [5]. SAT is a treasury asset pegged to a basket of assets: stablecoins and commodities such as precious metals. SAT provides the fiscal soundness necessary for SAIT's governance model, enabling compliance-driven buybacks that prove real-world utility while maintaining scarcity and value.

Together, SAIT and SAT create a sustainable ecosystem where AI safety research funding operates independently of traditional investment pressures, backed by a robust treasury that bridges decentralized finance with a real-world apex challenge.

INTRODUCTION

The AI Research Funding Crisis

The global AI ecosystem represents approximately \$16.2 trillion by 2030, yet its research funding remains dangerously centralized. Corporate-backed AI projects concentrated in the United States have captured roughly 90% of available funding (apx \$1.35T)—creating a geographic, financial, and institutional monopoly on AI development [2] [3] [8]. This apex centralization poses existential risks [1] [9]:



Geographic Concentration: The overwhelming concentration of AI funding in a single jurisdiction creates geopolitical risks and limits diverse perspectives essential for developing safe, globally-aligned AI ecosystem [10] [11] [12].

Mission Drift: Traditional venture capital requires equity stakes and board representation, often forcing teams to prioritize commercial viability over research. The pressure to achieve returns conflicts fundamentally with a patient and thorough research process [13].

Equity Dilution: Each funding round dilutes founder control and shifts decision-making power toward investors whose main interest is positive financial returns on their capital.

Time Compression: Investor timelines typically demand exits within 5-7 years, yet meaningful AI alignment research will operate on longer horizons. This temporal mismatch forces researchers to abandon long-term safety considerations in favor of near-term commercial progress.

SAIT

SAIT was created to solve these structural problems by providing a perpetual, non-dilutive funding mechanism for AI safety research. It functions as an open-source incubator with transparent governance. SAIT combines:

- Direct Funding: Grants that preserve researcher autonomy
- Milestone-Driven Governance: KPI based unlocks tied to verifiable progress
- Open-Source Mandate: All funded research remains in the public domain
- Transparent Operations: Public dashboards tracking all funding flows and research outcomes
- Time Flexibility: 36-month funding cycles that match research timelines, not exit strategies

SAIT expects projects to either spin off commercial entities or rotate out within 36 months, creating a sustainable cycle where successful research creates space for new initiatives.

SAT: The Treasury Foundation

Every governance token faces a fundamental credibility problem: how to prove utility beyond arbitrage. SAIT solves this through SAT—an asset-backed token that serves as SAIT's treasury reserve. This dual-architecture creates deterministic transparency—every SAIT token either circulates or sits in reserve, with compliance-driven buybacks exchanging SAIT for treasury-held SAT as proof of governance and surplus reserves [14].

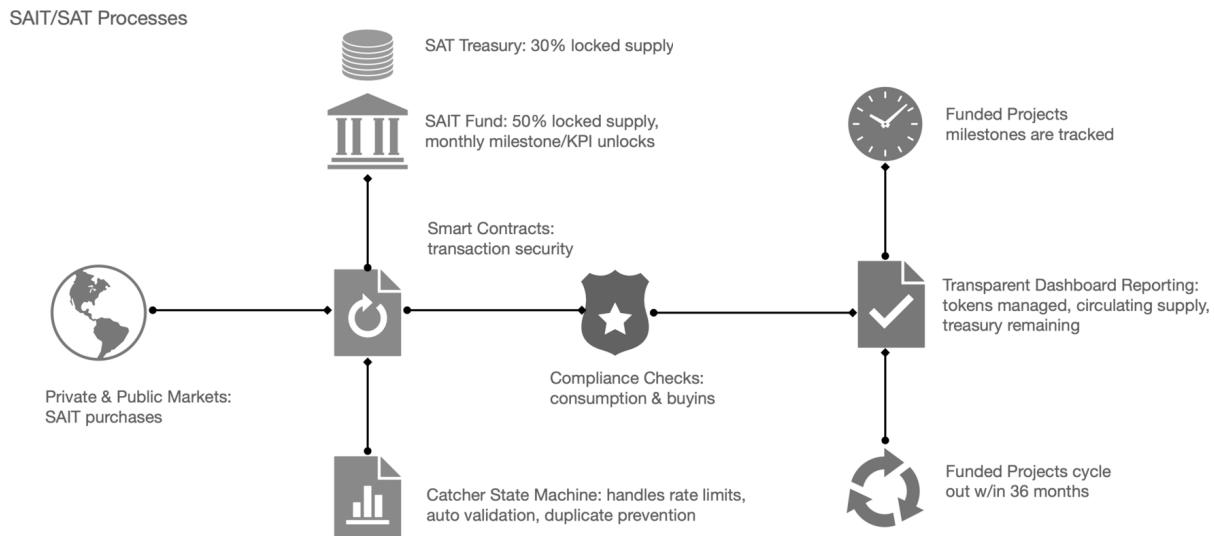
SAT itself represents a return to sound money principles. Just as Satoshi Nakamoto created Bitcoin to enable trustless peer-to-peer transactions, SAT implements Benjamin Graham's vision of a reserves backed by diversified basket of strategic assets - like an ETF [4]. Where Bitcoin's volatility prevented its use as stable money, SAT achieves stability through:

- Diversified Collateral: A weighted basket of assets spreads volatility risk
- Over-Collateralization: 150% backing ensures resilience against market shocks
- Active Management: Automated protocols that adjust basket composition based on market conditions.

This dual-token model—SAIT for funding and governance, SAT for treasury reserves—creates a fiscally sound ecosystem where AI safety research can operate with the patient capital it requires while maintaining regulatory compliance and market confidence.

DESIGN

SAIT Architecture



SAIT is utility token with two primary functions:

A) Research Funding: SAIT grants provide non-dilutive capital for AI safety R&D, preserving researcher autonomy and project direction. Traditional investment creates equity dilution and mission drift; SAIT eliminates both.

B) Research Governance: Tokens without enforced utility risk being dismissed as speculative instruments. SAIT's performance-driven governance ties token unlocks to verifiable milestones, creating objective value measurement.

The solution blends escrow-based fundraising with compliance-driven SAT buybacks, ensuring SAIT remains useful, scarce, and mission-focused while maintaining fiscal soundness.

SAIT Tokenomics

1. Supply & Allocation

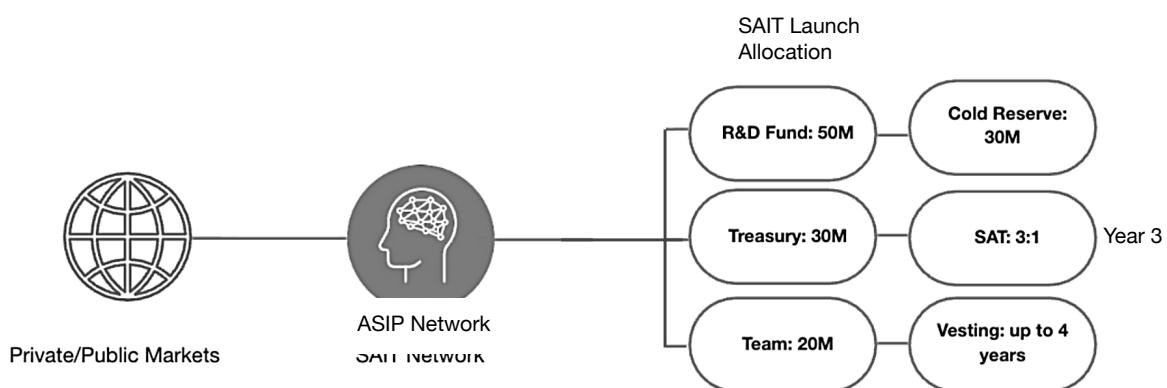
Total Supply: 100M SAIT (fixed, no inflation)

Allocation Groups:

- 50% AI Fund: Milestone-triggered unlocks
- 30% Treasury: Long-term operational stability
- 20% Team, Partners, & Incentives: extended vesting schedules, student grants, youth engagement programs

Allocation Mechanics:

- Progressive KPI unlocks create scarcity and demand
- Annual releases capped at 7% maximum of circulating supply
- 6-month+ cliff for internal parties prevents early dumps and ensures long-term alignment.



2. Treasury & Unlock Logic

Dual Mechanics Approach:

A) Treasury as an Escrow Grant Unlock

- Base Drip: 0.3–1% monthly provides predictable liquidity
- Milestone Boosts: Additional unlocks triggered only by verifiable progress (pilot deployments, organizational adoption, sovereign implementations)
- Rollback Protection: Unused monthly allocations return to escrow, preventing oversupply

Benefits:

- Prevents token flooding during development phases
- Creates scarcity-driven demand during achievement announcements
- Long-term deflationary pressure maintains buyer confidence
- Requires a transparent public dashboard with third-party verification

B) Proof of Compliance & Buybacks

Each governance check within the SAIT network triggers a buyback event:

- Instead of burns, SAIT governance protocols exchange SAIT tokens for SATs
- Tokens are batched and swapped weekly from treasury reserves
- Safeguards include authentication (authorized organizations only), rate limits, and duplicate prevention

Example Proof-of-Compliance for buyback floor resilience:

$$\text{Price Floor} = (\text{Treasury SAT Reserves} * \$150) / \text{Monthly Buyback Demand}$$

If reserves = 1M SAT (\$150M), demand = 500K SAIT: Floor = \$300/SAIT.

Probability: Manipulating TWAP requires >51% market volume

This creates reliability and deterministic transparency as every SAIT token has a traceable path—either circulating in the open market or locked in escrow—with SAIT-for-SAT buyins providing proof of governance activity and reserve strength.

Governance KPI timestamp

```
function verifyMilestone(bytes32 proofHash, uint256 requiredScore) public returns (bool) {  
    uint256 actualScore = oracle.getBenchmarkScore(proofHash); // Chainlink oracle call  
    if (actualScore >= requiredScore) {  
        unlockTokens(milestoneAmount); // Release from escrow  
        return true;  
    }  
    return false;  
}
```

4. Price Growth Anchors

Scarcity: Fixed supply combined with escrowed majority and milestone-gated releases creates organic scarcity and a positive narrative.

Proof of Progress: All milestones verified through transparent audits under SAIT governance oversight as KPIs are met. Public governance dashboard tracks all project performance metrics.

Rotation Policy: As an open-source incubator, SAIT expects funded projects to either spin off commercial entities within 36 months or rotate out, making room for new research initiatives.

5. Market Dynamics

Effective Circulating Supply: Lower than gross supply due to compliance-driven buybacks.

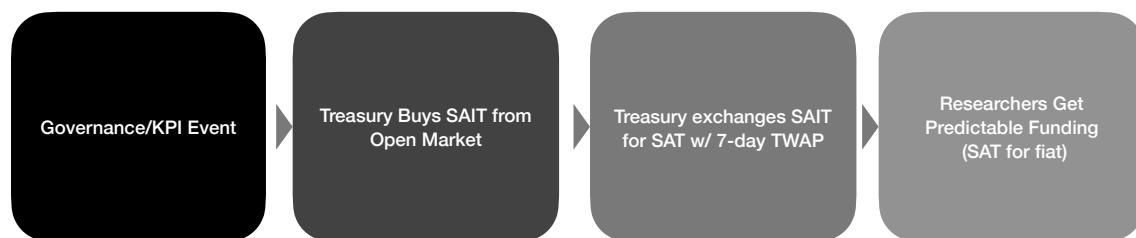
Dual Value Anchors:

- Funding Scarcity: Escrow-driven supply discipline
- Governance Buybacks: Adoption-proven utility demonstration

6. Grants & Buybacks

Grants: SAIT offers utility via research grants that may carry over to 3rd party investors should a participant choose to commercialize. That is a project specific decision because SAIT functions as an AI grant mechanism with a strong treasury, not an investment vehicle. It is a research team's perogative to participate post-grant in the expanding AI market [6] [7].

Treasury Buybacks: The SAT buyin mechanism strengthens the regulatory position by demonstrating SAIT operates as a functional governance protocol with measurable RWA utility, not merely as a fundraising instrument.



- | | |
|---|--|
| A | [Compliance Event (KPI Met)] --> B [Buyback Trigger] |
| B | --> C[Collect SAIT Tokens (Escrow/Batch)] |
| C | --> D[7-Day TWAP Calculation] |
| D | --> E[Exchange SAIT for SAT at \$150 Peg] |
| E | --> F[Treasury Reserves Increase] |
| F | --> G[Scarcity: Circulating SAIT Decreases] |
| G | --> A[Incentivizes More Research] |

```
function triggerBuyback(uint256 saitAmount, address organization) public {
    require(isAuthorized[organization], "Unauthorized compliance trigger");
    require(rateLimiter.allow(organization), "Rate limit exceeded");
    uint256 twapPrice = calculateTWAP(saitToken); // 7-day average in USD
    uint256 satToRelease = (saitAmount * twapPrice) / 150; // $150 SAT peg
    saitToken.transferFrom(organization, treasury, saitAmount);
    satToken.transfer(organization, satToRelease);
    emit BuybackExecuted(saitAmount, satToRelease);
}
```

SAIT Supply Decreases (Buybacks)

- Treasury uses SAT reserves to buy SAIT from open market
- Creates buying pressure (not selling pressure)
- Removes SAIT from circulation → scarcity
- Proves utility: "More research funded = More SAIT bought back"

Proof of Governance Activity

- Every compliance check = Verifiable governance event
- Buyback volume = Direct measure of AI safety research happening
- Public dashboard shows: "X organizations triggered Y compliance events = Z SAIT
- Quadratic voting mitigates dominance by large holders, while delegation allows efficient participation for institutions:

```
contract SAITGovernance {  
    struct Proposal {  
        uint256 id;  
        address proposer;  
        string description; // e.g., "Approve $1M grant for AI alignment project"  
        uint256 startTime;  
        uint256 endTime;  
        uint256 forVotes; // Quadratic sum for fair weighting  
        uint256 againstVotes;  
        bool executed;  
    }  
  
    mapping(uint256 => Proposal) public proposals;  
    mapping(address => uint256) public votingPower; // Based on SAIT balance or delegated  
    mapping(address => mapping(uint256 => bool)) public hasVoted;  
    uint256 public proposalCount;  
    uint256 constant VOTING_PERIOD = 7 days; // Matches research timelines  
  
    event ProposalCreated(uint256 id, address proposer);  
    event VoteCast(address voter, uint256 proposalId, bool support, uint256 weight);  
  
    // Create a new proposal (requires minimum SAIT stake)  
    function createProposal(string memory _description) public {  
        require(votingPower[msg.sender] >= 1000 * 10**18, "Insufficient stake to propose"); // e.g., 1000 SAIT  
        min  
        proposalCount++;  
        proposals[proposalCount] = Proposal({  
            id: proposalCount,  
            proposer: msg.sender,  
            description: _description,  
            startTime: block.timestamp,  
            endTime: block.timestamp + VOTING_PERIOD,  
            forVotes: 0,  
            againstVotes: 0,  
            executed: false  
        });  
        emit ProposalCreated(proposalCount, msg.sender);  
    }  
  
    // Cast vote with quadratic weighting (sqrt(votes) to prevent whale dominance)
```

```

function vote(uint256 _proposalId, bool _support, uint256 _amount) public {
    Proposal storage prop = proposals[_proposalId];
    require(block.timestamp >= prop.startTime && block.timestamp < prop.endTime, "Voting not active");
    require(!hasVoted[msg.sender][_proposalId], "Already voted");
    require(votingPower[msg.sender] >= _amount, "Insufficient voting power");

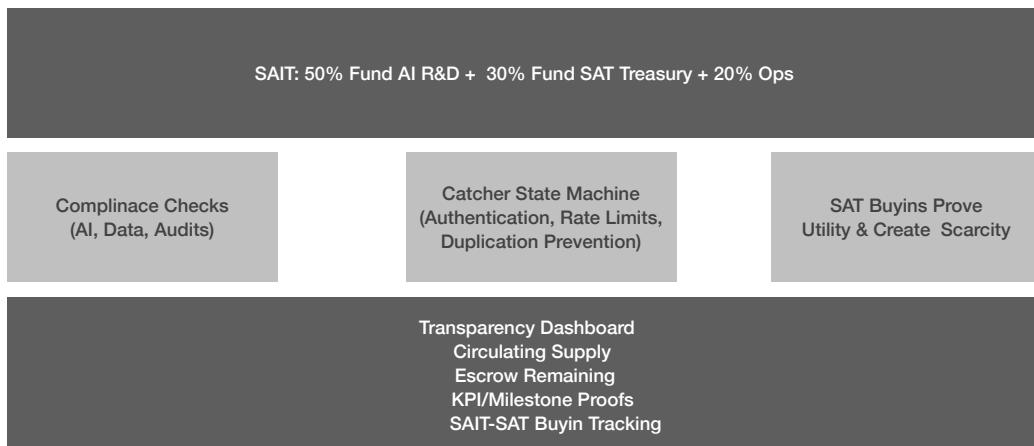
    uint256 weight = sqrt(_amount); // Quadratic voting: weight = sqrt(tokens committed)
    if (_support) {
        prop.forVotes += weight;
    } else {
        prop.againstVotes += weight;
    }
    votingPower[msg.sender] -= _amount; // Lock tokens during vote
    hasVoted[msg.sender][_proposalId] = true;
    emit VoteCast(msg.sender, _proposalId, _support, weight);
}

// Execute proposal if quorum met and forVotes > againstVotes
function executeProposal(uint256 _proposalId) public {
    Proposal storage prop = proposals[_proposalId];
    require(block.timestamp >= prop.endTime, "Voting not ended");
    require(!prop.executed, "Already executed");
    uint256 quorum = totalSupply() * 10 / 100; // 10% quorum of total SAIT
    if (prop.forVotes + prop.againstVotes >= quorum && prop.forVotes > prop.againstVotes) {
        // Execute: e.g., transfer funds from treasury or update params
        // treasury.transferFunds(prop.proposer, grantAmount); // Integrate with SAT treasury
        prop.executed = true;
    }
}
// Helper: Delegate voting power (for SWFs/FOs managing large holdings)
function delegate(address _delegatee) public {
    votingPower[_delegatee] += votingPower[msg.sender];
    votingPower[msg.sender] = 0;
}
}

```

THE SAT RESERVE TREASURY

SAT: Safe Asset Token Design



SAT serves as SAIT's treasury reserve and represents the practical implementation of monetary theories developed by Benjamin Graham, Friedrich Hayek, and Frank D. Graham during and after the Great Depression. Their collective insight concluded that monetary stability requires diversified assets, not single-asset pegs. This approach spreads risk, thus creating a greater peg defense.

Historical Context

In 1944, as the Bretton Woods conference established the post-war monetary order, Warren Buffett's guru - Benjamin Graham proposed a novel alternative. He wanted to define currency value against a basket of assets, not one - namely gold. He wrote, "We define the dollar as equivalent to the commodity unit, in the same way that it was formerly defined as equivalent to gold."

Satoshi Nakamoto's 3 Jan 2009 release of Bitcoin fulfilled part of Graham's vision—the ability to create trustless, peer-to-peer electronic cash using cryptographic proof instead of trusted intermediaries opened the door to a true stable reserve. However, Bitcoin's volatility prevented its' use as a medium of exchange. SAT completes Graham's and Nakamoto's vision by combining Nakamoto's trustless architecture with Graham's real world asset diversification.

SAT Treasury

Peg Mechanism: SAT uses the 1913 baseline equivalent to \$100 USD today. However, to protect against volatility and ensure resilience, SAT is minted at \$150 USD (150% over-collateralization).

Collateral Agnostic Redemption: When users burn SAT, they receive \$150 back, which may burn a different composition than the collateral asset they used at mint. This prevents direct claims on specific asset components, which is critical because some SAT assets may not be immediately redeemable from the SAIT treasury.

Basket Composition: For market simplicity, transparency, and clarity, SAT holds a modular mix of strategic assets that have acted as money or as a barter instrument in the past, weighted modularly to hold the peg across three asset classes:

- Bitcoin & Ethereum (as digital commodities)
- Precious Metals (gold, silver, platinum, copper, etc)
- Stablecoins (as digital sovereign cash equivalents)

The exact composition must remain modular, adjusting in realtime based on market volatility to maintain the SAT peg.

Stability Mechanisms

SAT maintains its peg through seven core mechanisms:

- 1. Heavy Over-Collateralization:** 150% backing provides cushion against market shocks
- 2. Vigilant Compliance:** Continuous monitoring and regulatory adherence across multiple jurisdictions
- 3. Dynamic Asset Replacement:** Underperforming assets are systematically replaced

- 4. Diversified Basket Holdings:** Multiple assets reduce exposure to single-market risks
- 5. Supply Adjustments:** Protocol responds to market volatility or economic attacks
- 6. Reserve Backing:** Fiat stablecoins, native tokens, and commodity reserves provide additional collateral layers
- 7. Multi-Exchange Price Aggregation:** Historic price averages from different exchanges hedge against manipulation

Price Band Management

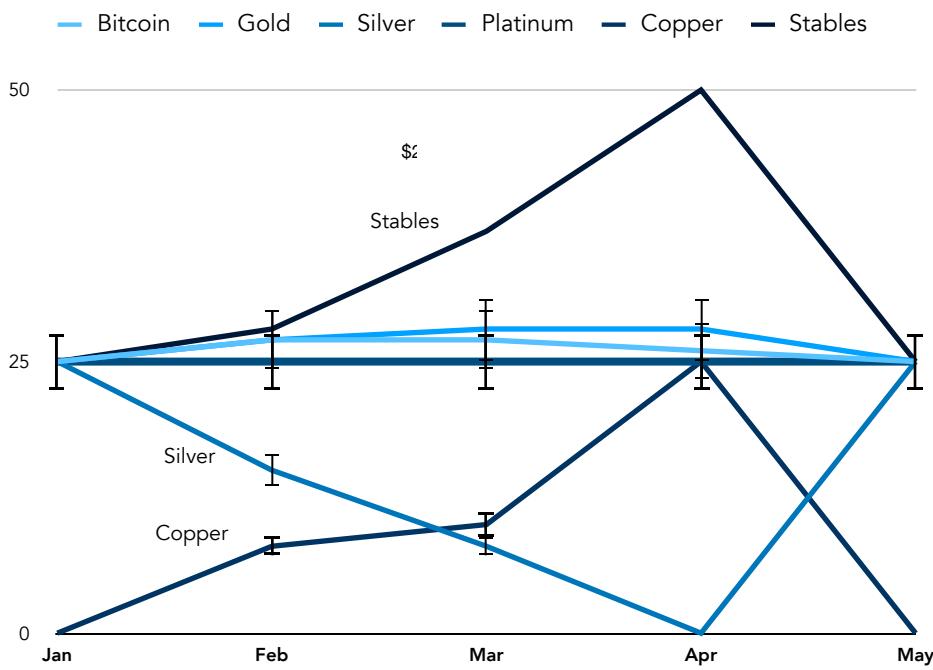
SAT employs sophisticated price monitoring to maintain stability:

- 1. APP (Asset Price Profits):** 2–10% above historic equilibrium triggers profit-taking, which is reinvested into the basket (not full liquidation)
- 2. APD (Asset Price Detachment):** 2–10% below equilibrium initiates decoupling from the affected asset
- 3. Replacement Threshold:** At or before -20% deviation, the network fully decouples from the asset and replaces it
- 4. Reentry Conditions:** Replaced assets cannot return to the basket until they exceed historic equilibrium

Black Swan Protection: The Silver Thursday Collapse

On March 27, 1980, silver prices collapsed over 50% in a single day, dropping from \$21.62 to \$10.80 per ounce—the metal's biggest single-day collapse in history. If SAT held silver in its' portfolio:

Month	Bitcoin	Gold	Silver	Platinum	Copper	Stablecoins	Status
Jan	\$25	\$25	\$25	\$25	\$25	\$25	Baseline: \$150
Feb	\$27	\$27	\$15	\$25	\$28	\$28	APP triggered, rebalance
Mar 1-20	\$27	\$28	\$8	\$25	\$25	\$37	ADP triggered, decoupling
Mar 20-26	\$26	\$28	\$0	\$25	\$21	\$50	Silver fully replaced
Mar 27 Silver Tues	\$26	\$28	\$0	\$25	\$21	\$50	Crises avoided, zero impact
May	\$25	\$25	\$25	\$25	\$25	\$25	Silver returns to the SAT basket



Early Warning System: The APD (Asset Price Detachment) mechanism would have triggered at -2% to -10% deviations, well before the catastrophic 50% collapse

Proactive Asset Replacement: SAT would have fully decoupled from silver before March 27, 1980, avoiding the collapse entirely

Treasury Batch Exchange

Exchange Rate: 7-Day TWAP (Time-Weighted Average Price)

Treasury swaps: collect SAIT tokens for SAT reserves from Treasury allocation

Treasury receives: SAT reserves (\$150 backing)

Effect: Circulating supply decreases

Prevent manipulation while ensuring fair market value

$$\text{SAIT} \rightarrow \text{SAT} \text{ Exchange} = (\text{7-Day TWAP of SAIT in USD}) \div \$150 \text{ per SAT}$$

Example:

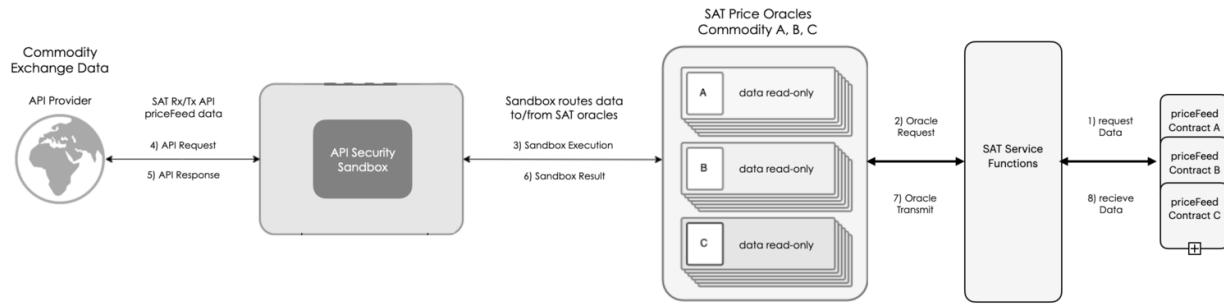
- SAIT 7-day average price = \$150 USD
- SAT value = \$150 USD (fixed, commodity-backed)
- Exchange rate: 1 SAIT = 1 SAT

TWAP:

- Smooths out daily volatility
- Prevents single-day price manipulation
- Fair to both organizations and Treasury
- Industry standard (used by Uniswap V3 oracles)

Technical Implementation

Blockchain Infrastructure: SAT ver1 operates on Ethereum using ERC-20 contracts via the Ethereum EVM and Chainlink Decentralized Oracle Network (DON).



Price Feed Architecture:

```
// Multiple commodity price feeds from global markets
req.add("get", "https://assets-api.com/api/latest?
access_key=[KEY]");
req.add("path", "x.data.rates.BTC");
req.addInt("times", TIMES_AMOUNT);
```

Vault Contract Structure:

```
// Vault accepts specific collateral types
constructor(address _priceFeed, address _stablecoin) {
    priceFeed = AnyAPIPriceFeed(_priceFeed);
    stablecoin = Stablecoin(_stablecoin);
    isCollateral[BTC_ADDRESS] = true;
    isCollateral[PAXG_ADDRESS] = true;
}
```

Oracle Redundancy: While Chainlink serves as the primary oracle, the architecture anticipates integrating additional industrial-grade oracles as backups, recognizing that any design is only as strong as its weakest link.

Proxy Contract Monitoring:

```
// Multiple parameters tracked in single oracle response
uint256 public gold; // PAXG pricefeed
uint256 public usdt; // Tether pricefeed
uint256 public usdc; // Circle pricefeed
uint256 public silver; // KAG pricefeed
uint256 public btc; // Bitcoin pricefeed
```

Proxy contracts continuously monitor price swings. If prices fall 2–10%, the asset begins to de-leverage; at 10–20% (maximum), it must be replaced. This protects against both market volatility and arbitrage attacks.

Custody & Audit

Continuous Auditing: Transactions are audited 24/7/365, providing complete records to clients, partners, and regulators.

Third-Party Custodians: SAT uses neutral jurisdiction custodians who are fully insured for both personal and business collateral.

Peg Defense

SAT employs spotter/proxy contracts (a MakerDAO innovation) to sanitize off-chain prices from third-party sources. Price fluctuations triggering red flags cause basket weight adjustments or, in extreme cases, complete pauses to protect peg solvency.

The assets in SAT's basket are dynamic, but the collateral backing the peg remains constant. The protocol maintains no fewer than five assets with low correlation, reviewed and balanced periodically according to global market conditions via proxy contracts and FX translations across primary on and off-chain markets.

Market Size & Utility

Trading Volume: Commodities trade over \$10 trillion annually across global exchanges

Network Effects: SAT's off-chain network conducts 15 billion trades annually worth over \$10T, providing natural demand beyond Web3-native markets.

Cross-Border Solution: Stablecoins and their asset pegged equivalents represent the perfect market for proof-based, cross-border transactions because they are inherently borderless RWA products serving borderless RWA markets.

SAT Treasury Benefits

- **Allocated:** SAT is backed only by assets traceable in real-time to direct native assets on or off-chain. Its' digital nature enables instant global transfers and regulatory transparency.
- **Availability:** OpenAPI Specification (OAS) compatibility allows Web2 applications to integrate SAT. Fractional ownership is accessible to anyone with internet access.
- **Redeemable:** Digitally redeemable in native collateral (like USDT). 24/7/365 redemption access.
- **Functionality:** Easy to convert, trade, or use. Compatible with DEXs for trading against USD stablecoins and other digital assets, including gold-backed tokens (XAUT, XAU).
- **Diverse:** Maintains the inherent nature of an open market asset. No single entity controls access or aggregate market price.
- **Low Risk:** Assets kept separate from all other holdings. Physical token representations are audited daily and published 24/7/365. Assets secured as part of the continuous audit process, not part of any other SAT interests.
- **Privacy & Neutrality:** User wallets assign unique public addresses via alphanumeric codes. Cold wallets are encouraged for offline private key storage. Multi-custodial collateral held in insured, licensed, neutral, geo-diverse cold storage facilities.

INTEGRATION: SAIT + SAT ECOSYSTEM

How SAIT and SAT Work Together

The dual-token architecture creates a self-reinforcing ecosystem:

SAIT: Governance and funding token for AI safety research

- Governance events trigger buyback events
- Treasury-controlled supply ensures scarcity
- Milestone-driven unlocks tie value to verifiable progress

SAT: Treasury reserve and stability mechanisms

1. Buybacks for SAIT tokens prove governance utility
2. Cross-border utility provides external demand and liquidity
3. Over-collateralized treasury backing ensures fiscal soundness

Buyback Mechanism

SAIT governance exchanges SAIT tokens for SAT for the treasury:

1. Compliance checks trigger batched buyin events
2. SAIT tokens collected and swapped weekly for treasury SAT
3. Safeguards include authentication, rate limits, and duplicate prevention
4. Public dashboard displays all transactions transparently

This mechanism accomplishes multiple objectives:

- **Proves Utility:** Demonstrates real-world governance usage beyond speculation
- **Creates Deflation:** Removes SAIT from circulation, increasing scarcity
- **Ensures Stability:** SAT's commodity backing provides reliable treasury reserves
- **Regulatory Clarity:** Compliance-driven flows support classification as functional protocol

Using zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), organizations prove compliance (e.g., "95% alignment score") to oracles without disclosing sensitive data:

```
library ZKAuditProof {
    // Struct for proof (simplified zk-SNARK components)
    struct Proof {
        uint256[2] a;    // Proof point A
        uint256[2][2] b; // Proof point B
        uint256[2] c;   // Proof point C
        uint256 input;  // Public input (e.g., required score threshold)
    }

    address public verifierContract; // Pre-deployed zk-SNARK verifier (e.g., via Semaphore or Groth16)

    event AuditVerified(address organization, uint256 milestoneId, bool success);

    // Submit zk-proof for audit (prove score >= threshold without revealing score/data)
    function submitAuditProof(uint256 _milestoneId, Proof memory _proof, uint256 _threshold) public {
        // Verify proof using on-chain verifier (e.g., Groth16 circuit for "score >= threshold")
        bool isValid = verifyTx(_proof.a, _proof.b, _proof.c, [_threshold]); // Call to verifier
        require(isValid, "Invalid zk-proof");
    }
}
```

```

    // If valid, trigger unlock/buyback without revealing private inputs
    // e.g., escrow.releaseFunds(msg.sender, grantAmount);
    emit AuditVerified(msg.sender, _milestoneId, true);
}

// Verifier function (pseudocode for Groth16 verification)
function verifyTx(
    uint256[2] memory a,
    uint256[2][2] memory b,
    uint256[2] memory c,
    uint256[1] memory input // Public: threshold
) internal view returns (bool) {
    // Pairing checks (elliptic curve math for zk-SNARK)
    // alpha * beta == gamma * delta (simplified; actual impl uses pairing libs like bn254)
    require(pairing(a, b) == pairing(c, input), "Pairing mismatch"); // Proof fails if false
    // Additional checks for knowledge of private witness (e.g., actual score, audit data hash)
    return true; // If all pass
}

// Oracle integration: Fetch public benchmark for input
function requestBenchmarkScore(bytes32 _auditHash) external {
    // Chainlink.request("benchmarkAPI", _auditHash); // Public score threshold
    // On fulfillment, use as input for proof verification
}
}

```

STRATEGIC ADVANTAGES

Mission Preservation & Direct Funding: SAIT meets R&D requirements without investor dilution or control - i.e., it maintains research focus without commercial pressure.

Transparency & Credibility: Treasury unlocks tied to publicly verified KPIs, with all treasury ops visible on public dashboards. Buybacks from SAIT to SAT prove discipline over speculation

Scarcity: Supply discipline through a strong treasury plus buyback deflation. The Majority of SAIT supply is locked until justified by progress, with buybacks creating additional deflationary pressure.

Regulatory Bridge: SAIT functions as an incubator for R&D, leading to commercial spinoffs or phase-out, avoiding securities classification issues.

Fiscal Soundness: SAT's over-collateralized stables and digital commodity backing provides stable treasury reserves resistant to single-market shocks.

Global Neutrality: SAIT's mission and SAT's reserve positions are neutral and multi-jurisdictional meant to function in global financial networks.

Proven Historical Precedent: SAT implements monetary rigor tested during history's greatest financial crises, adapted for blockchain transparency and efficiency.

Narrative: Clear links between project milestones, breakthrough announcements, and token scarcity build a positive narrative because all are positive outcomes.

Architecture Logic

Traditional cryptocurrency projects face a fundamental problem: proving tokens have value beyond speculation. Projects either:

- Remain purely speculative (no underlying value)
- Create artificial scarcity (burns without proving usage)
- Depend on single-asset backing (gold, fiat) with centralization risks

SAIT + SAT solves all three:

- Real Utility: AI research funding with measurable outcomes
- Proven Scarcity: Buybacks demonstrate actual protocol usage
- Diversified Backing: an ETF style basket provides stable, neutral reserves

CONCLUSION

A Return to First Principles

ASIP represents a return to fundamental principles in both technology research funding and monetary stability.

For AI research, ASIP eliminates some structural problems with legacy venture capital:

- No equity dilution
- No compressed timelines
- No geographic concentration

Hybrid Model Advantage

The SAIT + SAT architecture ensures fundraising and utility work in tandem. Contributors can see exactly how SAIT functions: to fund AI safety R&D and validate progress through transparent governance. As adoption grows, SAT buybacks increase SAIT scarcity while proving real-world usage—creating a strong foundation for both financial sustainability and long-term market trust.

Duality and Action

The AI safety research funding crisis and global monetary instability are not separate problems—they reflect a common pattern of excessive centralization creating systemic risk. SAIT addresses AI funding centralization while SAT addresses monetary centralization, using blockchain technology to create transparency, neutrality, and accountability that traditional systems cannot match.

History demonstrates that sovereign money eventually abandons hard asset pegs when governments face crises. This leads to debt-based financial engineering, cascading into business and consumer lending risks, ultimately destabilizing the global trade that underpins peace and prosperity. SAT provides an alternative: neutral, commodity-backed money that operates independently of any single nation's fiscal policy.

Similarly, AI safety research cannot wait for perfect market conditions or philanthropic largesse. The technology advances too quickly, the stakes are too high, and the current funding models are too compromised by commercial pressures. ASIP provides immediate, sustainable funding with governance structures that preserve research integrity.

"What is past is prologue" — William Shakespeare

REFERENCES

- [1] Center for AI Safety. (2023). "Statement on AI Risk". Retrieved from <https://safe.ai/work/press-release-ai-risk>
- [2] Stanford Institute for Human-Centered AI. (2025). "The 2025 AI Index Report". Retrieved from <https://hai.stanford.edu/ai-index/2025-ai-index-report> (US dominance in AI investment, ~90% of significant funding; \$1.35T cumulative 2018-2024).
- [3] Crunchbase. (2025). "State of Startups in Q3 2025". Retrieved from <https://news.crunchbase.com/venture/state-of-startups-q3-2025-ai-megarounds-charts-data/> (US VC: 62.7% to AI in 2025; global 46-53%).
- [4] Graham, B. (1937). "Storage and Stability: A Modern Ever-Normal Granary". McGraw-Hill (Diversified reserves for sound money).
- [5] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". Retrieved from <https://bitcoin.org/bitcoin.pdf>
- [6] PwC. (2017). "Sizing the Prize: AI's Economic Impact". Retrieved from <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf> (\$15.7T global GDP contribution by 2030).
- [7] UNCTAD. (2025). "AI Market Projected to Hit \$4.8 Trillion by 2033". Retrieved from <https://unctad.org/news/ai-market-projected-hit-48-trillion-2033-emerging-dominant-frontier-technology>
- [8] Bloomberg. (2025). "AI Dominating 2025 VC Investing". Retrieved from <https://www.bloomberg.com/news/articles/2025-10-03/ai-is-dominating-2025-vc-investing-pulling-in-192-7-billion> (US 62.7%, global 53.2% AI VC allocation).
- [9] RAND Corporation. (2025). "On the Extinction Risk from Artificial Intelligence". Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3000/RRA3034-1/RAND_RRA3034-1.pdf
- [10] World Economic Forum. (2025). "AI Geopolitics and Data Centres". Retrieved from <https://www.weforum.org/stories/2025/07/ai-geopolitics-data-centres-technological-rivalry/>
- [11] RAND Corporation. (2025). "How Artificial General Intelligence Could Affect Geopolitics". Retrieved from https://www.rand.org/pubs/research_reports/RRA3034-2.html
- [12] Brookings Institution. (2025). "Are AI Existential Risks Real?". Retrieved from <https://www.brookings.edu/articles/are-ai-existential-risks-real-and-what-should-we-do-about-them/>
- [13] Harvard Law Review. (2025). "Amoral Drift in AI Corporate Governance". Retrieved from <https://harvardlawreview.org/print/vol-138/amoral-drift-in-ai-corporate-governance/>
- [14] CoinMarketCap. (2025). "Governance Token Metrics (Aave, Compound, Uniswap)". Retrieved from <https://coinmarketcap.com/> (Market caps: UNI \$5.35, AAVE \$196.68).

LEGAL DISCLAIMER

This white paper is for informational purposes only and does not constitute financial advice, investment advice, trading advice, or any other advice whatsoever. ASIP tokens should not be purchased with the expectation of profit from appreciation in value.

No Investment Contract: ASIP SAIT tokens represent access to AI research governance and funding mechanisms. ASIP SAT tokens represent asset-backed reserves for treasury purposes. Neither constitutes an investment contract or security under applicable law.

Geographic Restrictions: ASIP tokens may not be available in all jurisdictions. Participants are responsible for compliance with local laws.

By participating in the ASIP ecosystem or acquiring its' tokens, you acknowledge that you have read, understood, and accepted these terms and the risks described throughout this document.