



SEMATECT

Proof-of-Forage: one public nest, private puzzles, postage and nectar

Working paper · Beta v5.3 · 17 September 2026

Planned ticker STCT · Planned network Base · ERC-20 postage + ERC-721 plates

Status: draft for builders — not a securities offering, not a live ticker

Abstract

SEMATECT is a protocol in which each miner is represented as one insect on a single public nest that does not reset. The board — built hexes, work orders, and bait — is public. The mathematical instance a miner must solve to dock on a hex is private, hashed from that miner, that hex, and the nest as it stands now, so a neighbor's path is not a valid receipt. A work order requires a small STCT stamp and may carry optional nectar (ETH, USDC, or wrapped BTC as cbBTC). Stamp and nectar sit in on-chain escrow on that hex until a legal forage fills it or the patron cancels. The miner who first submits a valid certificate — not the first click — receives the ERC-721 plate, the stamp, and the nectar. Steering chooses a hex; autopilot may choose hexes too; neither click nor idle time is the proof. The website is a camera over chunked views of the nest. The Base contracts are the nest. This paper states the objects, the caste mathematics, the custody rules, and the library they come from. It does not claim that insect mathematics beats an ASIC at SHA-256. There are no wall-clock rounds. No mainnet contract is published yet.

1. One-sentence product

Miners keep the NFT brick. People who hire the hive keep stall rent. STCT is the stamp. ETH, USDC, or cbBTC may sit on a hex as nectar.

Mining produces a signed plate whose picture is drawn from the certificate. Postage directs where the next plate may land. Nectar is optional bait on the same hex. Patronage is title on a stall, not title on the brick. Idle balances do not melt. There is one nest. It does not start over.

2. Research library and etymology

The name SEMATECT is taken from *sematectonic*: coordination by the work-product itself, as distinct from a scent mark. Grassé named stigmergy — insects coordinate by changing the nest, not by talking [1]. Wilson split marker stigmergy from sematectonic stigmergy [2]. Heylighen restated the split as a general coordination mechanism [3]. Ostrom's design principles for a commons — bounded cells, named users, monitoring — are why a hex you can inspect is protocol, not decoration [12]. A living nest has no match clock. The ground is the memory [1, 10]. Map refresh is tied to nest state, not to a bell that could be mistaken for confiscating bait.

Caste	Source	What the miner must find
Formica (ant, amber)	Dorigo Ant System / ACO [4, 5]	A short legal tour on a personal pantry map for that hex.
Apis (bee, gold)	Seeley; von Frisch; Hales [6, 7, 8]	A capacity-limited nectar path plus a max-adjacency comb dock.
Macrotermes (termite, sage)	Bonabeau–Theraulaz–Deneubourg; Camazine [9, 10]	A legal drop where local height already invites soil.

3. Objects of the protocol

Object	What it is	Who holds it
Hex	One cell of the public 2D nest.	Commons; inspectable.
Work order	Paid job pinned to one empty hex.	Posted by a patron.
Stamp (STCT)	Required postage that makes the order legal.	Escrow, then miner on fill.
Nectar	Optional ETH, USDC, or cbBTC bait on the same hex.	Escrow, then miner on fill.
Plate (ERC-721)	Signed brick + picture drawn from the certificate.	The miner who laid it.
Patron right	Title on the stall, not the brick.	Whoever paid the stamp.
Rent	Grain when neighbors build.	The patron.
Certificate	Path + caste + map seed + nonce + hex.	Miner, then chain.

Each miner is one insect. One person may run many miners. Paying a stamp does not mint a 721. If your own miner fills an order you posted, you spent postage and you still receive that plate, because that miner did the work.

4. Public nest, private puzzle

The nest is public: built bricks, open orders, visible nectar. Anyone may pan, zoom, and inspect a hex. The homework for docking is private.

$$\text{Map} = G(\text{hex}, \text{wallet}, \text{caste}, \text{nestRoot})$$

Copying a neighbor's path fails because it is not a path on your instance. *nestRoot* changes when a brick lands next door, so yesterday's path is not automatically legal today. There is no wall-clock round. Difficulty still tightens as the nest fills, and if valid certificates arrive too fast the thin lock's *k* may rise.

5. Proof-of-Forage

A certificate that mints must pass four checks.

5.1 The path is on the miner's map for that hex (*pathLegal*).

5.2 Score $S(P; \text{map}, \text{caste})$ beats target $T(\text{hex}, \text{caste}, \text{nest})$.

5.3 $\text{SHA-256}(\text{seed} \parallel \text{caste} \parallel P \parallel \text{miner} \parallel \text{nonce} \parallel \text{hex})$ shows *k* leading zero bits.

5.4 First valid certificate for that open order wins. A click is not a certificate.

Beating *T* is the search. Rechecking *S* is addition. Search is costly; verification is cheap. *k* is not “we are Bitcoin.” It is a grind so a program that finds a pretty path still pays time [14]. Public pheromone on the camera is display only. The mint does not read the picture.

6. Formica — trail mathematics

Source. Dorigo, Maniezzo and Coloni, Ant System (1996); Dorigo and Stützle, *Ant Colony Optimization* (2004) [4, 5]. An ant at node i picks the next node j with

$$P_{ij} = (\tau_{ij}^{\alpha} \cdot \eta_{ij}^{\beta}) / \sum_k (\tau_{ik}^{\alpha} \cdot \eta_{ik}^{\beta}), \eta_{ij} = 1 / d_{ij}$$

After a tour of length L : $\tau \leftarrow (1 - \rho) \tau + \Delta\tau(L)$

τ is scent on the edge. η is closeness. ρ is Grassé's forgetfulness: old piles fade unless they keep being used [1]. Score S is integer Euclidean tour length. Target T begins near $\alpha \cdot \text{MST}$ of the same points. An amber plate is that signed tour. A copied bee certificate fails *pathLegal* for Formica.

7. Apis — nectar and comb

Source. Seeley, *Honeybee Democracy* (2010) and von Frisch [6, 7]. Comb geometry: Hales, the honeycomb conjecture [8]. Capacity-limited collection is the orienteering family [11].

$$S_{bee}(P) = \sum n(v) \text{ for } v \text{ in } P, \text{ subject to } \text{load}(P) \leq C$$

On the public board the next empty gold hex is the cell with the most already-built neighbors. A gold plate is a nectar path plus a legal comb dock — a different legal object than an ant tour.

8. Macrotermes — deposit mathematics

Source. Bonabeau, Theraulaz and Deneubourg; Camazine et al., *Self-Organization in Biological Systems* [9, 10].

$$P_{pick} = (k_1 / (k_1 + q))^2, P_{drop} = (q / (k_2 + q))^2$$

Insects pick from thin spots and drop on thick spots. A sage plate is legal only if the brick lands on an allowed dock and the local height rule holds. It is not an ant tour painted green.

9. Stamp, nectar, and rent

A work order has two layers. The stamp is STCT only and is required. Nectar is optional and may be ETH, USDC, or cbBTC (wrapped BTC on Base — not native Bitcoin). Native L1 Bitcoin cannot sit in a Base contract.

1. Patron locks stamp n STCT, and optionally nectar, on an empty hex. Both sit in the hex escrow contract.
2. First legal certificate on that hex fills it. Miner takes stamp, nectar, and the plate.
3. Poster becomes patron of that stall.
4. Later legal bricks on adjacent hexes pay rent (in STCT) to that patron.
5. Until fill, the patron may cancel and reclaim stamp and nectar. A clock does not confiscate bait.

Why pay twice: you are buying a stall on a street that may get busier, not a picture. Quiet corners pay nothing. Colony treasury should post the first year of orders so miners have customers before strangers arrive. Idle bags do not melt. Only pinned stamp and nectar are in play.

	Miner (fills the order)	Patron (posts the order)
Spends	Work — a legal forage.	STCT stamp, optional nectar.
Gets	721 plate + stamp + nectar.	Patron rights → rent in STCT.
Does not get	Stall title.	The miner's NFT.

10. Steering and autopilot

Steer mode: the operator chooses a hex. Autopilot: the program chooses hexes. Both may hunt nectar. Neither mode is a payday. Targeting does not lock the pile. First valid certificate wins. First click does not.

11. The plate is a token and a picture

The ERC-721 is title to one brick and an artwork derived from the certificate: caste color, hex, path or drop, score S , neighbors, and a short hash of the proof. Anyone can redraw the same plate from the on-chain numbers. Early plates are fossils; later plates are harder as the nest fills. Locked plates may add miner weight on later accepts ($1 + \sum 1/\text{serial-age of locked plates of that miner}$). Sleeping on a genesis plate does not mint.

Legal secondary sale uses the protocol *buy()* only. From the listed price, beta split: 90% seller / 5% protocol (ERC-2981) / 2.5% original filling miner / 2.5% seniority pot for older neighboring plates. A buyer title in STCT feeds the next work pool; newer plates tithe more than fossils. Oldest plates are better as tools and as fossils, not as a protocol price tag.

12. Camera and ledger

The nest in the records is one grid that does not reset. The nest on the screen is a moving window [15, 16]. Far zoom is a heatmap. Neighborhood zoom draws hexes in view. Hex zoom shows the brick, the bait, and the patron. The website is a camera. The Base contracts are the nest. Three zoom levels of 32×32 hex tiles keep the camera light as the nest grows.

13. Custody — the site is not the bank

sematect.org is a camera. Stamp and nectar never sit on a project server. If the website is unreachable, escrow, plates, and certificates remain on-chain. A patron reclaims from the contract. Anyone may point another viewer at the same addresses once those addresses are published here.

14. Tokens and emission

STCT (ERC-20) is postage. Cap 1,000,000,000. Planned network: Base. ETH remains gas. There is no admin key that can mint. Empty work prints nothing.

Slice	Share	Rule
Mined	80%	Paid when a legal brick is accepted. No admin mint.
Colony treasury	12%	Locked. Posts early work orders. Runway.
Founder	8%	One-year cliff, four-year vest.

Colony treasury posts work orders for the first twelve months so miners have customers before strangers arrive. That is the cold-start: one nest, a small named set of miners, is the atomic network.

15. Mapping the library into the product

Source	Enters the product as
Grassé 1959 [1]	Board-as-message; one nest; no match clock.
Wilson 1975; Heylighen 2016 [2, 3]	Name; plate = work-product; STCT = marker postage.
Dorigo et al. 1996, 2004 [4, 5]	Formica tour, τ , η , evaporation p .
Seeley; von Frisch; Hales [6, 7, 8]	Apis capacity path; max-adjacency comb.
Bonabeau / Camazine [9, 10]	Macrotermes pick/drop on density q .
Ostrom 1990 [12]	Bounded cells, named users, click-to-audit.

Source	Enters the product as
Hayek 1945 [13]	Local knowledge; no central planner of forage.
Hashcash / Bitcoin puzzle [14]	Leading-zero grind AFTER a legal path only.
Tile maps / chunking [15, 16]	Camera draws a window; ledger holds the nest.

16. What this paper does not claim

We claim	We do not claim
Search is real; the check is public.	This pays like Bitcoin.
Three published local rules, not three skins.	Nature beats ASICs.
A plate is a signed brick you can redraw.	Citations create a market.
Stamp + nectar is a reason to use STCT and to bring ETH/USDC.	This document is an offering.
Escrow lives on-chain; the site is a camera.	Native BTC sits in a Base hex.
First certificate wins the pile.	First click wins the pile.

There is no mainnet STCT until the contract addresses are published on www.sematect.org. Do not buy a ticker that claims to be this project unless that address appears there.

17. References

- [1] Grassé, P.-P. (1959). La reconstruction du nid et les coordinations interindividuelles chez *Bellicositermes*. *Insectes Sociaux*.
- [2] Wilson, E. O. (1975). *Sociobiology*. Harvard. (sematectonic versus marker stigmergy, pp. 186–188.)
- [3] Heylighen, F. (2016). Stigmergy as a universal coordination mechanism. *Cognitive Systems Research*.
- [4] Dorigo, M., Maniezzo, V., and Colomi, A. (1996). Ant system. *IEEE Transactions on Systems, Man, and Cybernetics*.
- [5] Dorigo, M., and Stützle, T. (2004). *Ant Colony Optimization*. MIT Press.
- [6] Seeley, T. D. (2010). *Honeybee Democracy*. Princeton University Press.
- [7] von Frisch, K. (1967). *The Dance Language and Orientation of Bees*.
- [8] Hales, T. C. (2001). The honeycomb conjecture. *Discrete and Computational Geometry*.
- [9] Bonabeau, E., Dorigo, M., and Theraulaz, G. (1999). *Swarm Intelligence*. Oxford University Press.
- [10] Camazine, S., et al. (2001). *Self-Organization in Biological Systems*. Princeton.
- [11] Golden, B., Levy, L., and Vohra, R. The orienteering problem.
- [12] Ostrom, E. (1990). *Governing the Commons*. Cambridge University Press.
- [13] Hayek, F. A. (1945). The use of knowledge in society. *American Economic Review*.
- [14] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- [15] MDN Web Docs. Tiles and tilemaps overview.
- [16] Standard 2D engine practice: chunked tilemaps and camera culling.

This draft describes a protocol. It is not investment advice and not an invitation to buy a token.