SEMATECT

Proof-of-Forage: one public nest, private puzzles, claims and cells

Working paper · Beta v5.4 · 17 September 2026
Planned ticker STCT · Planned network Base · ERC-20 postage + two ERC-721s (claim, cell)
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 **claim** (ERC-721), the stamp, and the nectar. A patron who pinned nectar also receives a **cell** (a second ERC-721: "I fed that hex"). A seated claim may collect a small STCT grain each time one of its six neighbors fills, then it stops paying. Steering chooses a hex; autopilot prefers fed hexes; 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. What changed in v5.4

v5.3 named the miner NFT a plate and treated nectar as optional bait with no extra prize for the patron. That made ETH a donation and left newcomers without a plain word for the NFT. v5.4 keeps every formula and every citation from v5.3. It changes four names and one payday rule.

Rule	v5.4
Miner NFT	Claim. "I built that hex." Not called a plate.
Thing on the board	Brick. Public. Anyone can see who built it.
Claim payday	At most six STCT grains, one per neighbor fill. Then a souvenir you can still sell.
Patron NFT	Cell. Minted only if nectar was pinned. "I fed that hex." Sellable.
Why pin ETH	Speed + richer capped rent + a cell. Stamps cannot mint a cell.
What did not change	Caste math, four Proof-of-Forage checks, escrow, camera, emission, references [1]–[16].

2. One-sentence product

Miners keep the claim. Patrons who feed a hex keep a cell. STCT is the stamp. ETH, USDC, or cbBTC may sit on a hex as nectar. There is one nest. It does not start over. Idle balances do not melt.

3. 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. Hayek is why the puzzle stays local: no central planner of forage [13].

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.

Three published rules, not three skins. A copied ant receipt fails for a bee. A sage claim is not a green ant tour.

4. Objects of the protocol

Object	What it is	Who holds it
Hex	One cell of the public 2D nest.	Commons; inspectable.
Brick	The built wall on that hex. Not an NFT.	The nest. Anyone may see it.
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.
Claim (ERC-721)	“I built that hex.” Signed brick + picture from the certificate. Pays at most six neighbor grains.	The miner who laid it.
Cell (ERC-721)	“I fed that hex.” Minted only if nectar was pinned. Richer capped stall rent.	The patron. Sellable.
Patron right	Title on the stall, not the brick.	Whoever paid the stamp.
Rent / grain	STCT when a touching hex fills. Cap: six sides.	Claim holder (grain); stall / cell (rent).
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 claim. Pinning nectar does not mint a claim. A cell is not a claim. If your own miner fills an order you posted, you spent postage and you still receive that claim, because that miner did the work.

5. 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.

$$Map = G(hex, wallet, caste, nestRoot)$$

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.

6. Proof-of-Forage

A certificate that mints a claim must pass four checks.

6.1 The path is on the miner’s map for that hex (pathLegal).

6.2 Score S(P; map, caste) beats target T(hex, caste, nest).

6.3 SHA-256(seed || caste || P || miner || nonce || hex) shows k leading zero bits.

6.4 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. A claim does not skip these checks and does not raise hashpower.

7. Formica — trail mathematics

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

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

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 α · MST of the same points. An amber claim is that signed tour. A copied bee certificate fails pathLegal for Formica.

8. 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].

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

On the public board the next empty gold hex is the cell with the most already-built neighbors. A gold claim is a nectar path plus a legal comb dock — a different legal object than an ant tour. Protocol nectar (ETH / USDC / cbBTC on a hex) is not the same object as S_{bee}.

9. 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 claim 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.

10. Stamp, nectar, cell, and the six-side cap

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 claim.

3. Poster becomes patron of that stall. If nectar was pinned, the patron also mints a cell.

4. Later legal bricks on adjacent hexes pay STCT grain to the seated claim and STCT rent to the stall / cell, each at most six times.

5. Until fill, the patron may cancel and reclaim stamp and nectar. A clock does not confiscate bait.

A hex has six neighbors (pointy-top grid: NE, E, SE, SW, W, NW). That geometry is the cap [8]. A seated claim collects one small STCT grain each time a touching hex fills — at most six grains — then it is a souvenir you can still sell. A cell collects richer stall rent on the same six events, then it is a souvenir too. Early center claims spend their six sides first. New claims sit on the growing rim. Late miners are not taxed forever. Selling a claim or cell transfers only unused sides (zero to six). Nectar never lives inside either NFT. A seated claim never takes a neighbor's nectar, stamp, or claim. Claims do not add miner weight or skip the puzzle.

	Miner	Patron, stamp only	Patron, stamp + nectar
Spends	Work — a legal forage	STCT stamp	STCT stamp + ETH / USDC / cbBTC
Gets	Claim + stamp + nectar	Normal stall rent, six sides	Richer rent, six sides, plus a cell
Does not get	The cell	Claim, nectar, or cell	The miner's claim or the nectar back

Why pin nectar instead of raising the stamp. Postage and food are different jobs. The protocol can print STCT. It cannot print ETH. Raising the stamp is more postage; it does not mint a cell. A fed hex is preferred by autopilot (Seeley: recruit to rich patches [6, 7]), pays richer capped rent, and mints a cell the patron can keep or sell. That cell is the thing of value stamps cannot mint. Foreign bait does not replace the stamp. Colony treasury should post the first year of orders so miners have customers before strangers arrive.

11. Steer and autopilot

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

12. The claim is a token and a picture

The ERC-721 claim 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 claim from the on-chain numbers. Early claims are fossils: later claims are harder as the nest fills. Seating a claim is how it collects leftover neighbor grains. Sleeping on a genesis claim 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 claims. A buyer tithe in STCT feeds the next work pool; newer claims tithe more than fossils. Oldest claims are better as fossils and as leftover-side tools, not as a protocol price tag. The same split applies to cells.

13. 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, the claim, 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.

14. 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, claims, cells, 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.

15. 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.

16. 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; claim = work-product; STCT = marker; cell = receipt of imported food
Dorigo et al. 1996, 2004 [4, 5]	Formica tour, τ, η, evaporation ρ
Seeley; von Frisch; Hales [6, 7, 8]	Apis capacity path; max-adjacency comb; hex grid of six neighbors; autopilot prefers fed patches
Bonabeau / Camazine [9, 10]	Macrotermes pick/drop on density q
Golden et al. [11]	Capacity-limited nectar path (orienteering)
Ostrom 1990 [12]	Bounded cells, named users, click-to-audit
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

17. 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 claim is a signed brick you can redraw, capped at six sides.	Early miners own a forever ATM.
A cell is why a patron pins nectar.	Nectar replaces STCT postage.
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.

18. 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 Colorni, 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.