How to Build an Autonomous AI Agent on a Mac mini – Overview

What You’re Building

A Mac mini that runs an always-on AI agent with its own identity – separate email, crypto wallet, and phone number – powered by a three-tier fallback chain of cloud, decentralized, and local inference. You text the agent on Signal like texting a friend. It routes between AI models automatically, and uses MOR-staked decentralized compute via the Morpheus network at zero marginal cost.

The Stack

Layer	Technology	Purpose
Hardware	Mac mini M4 (headless, always-on)	Dedicated agent host
Identity	Proton Mail, macOS Keychain, Safe multi-sig wallet (Base)	Isolated credentials and funds
Agent Framework	Your choice (OpenClaw, LangChain, CrewAI, custom)	Model routing, messaging, tools
Messaging	Signal via VoIP (JMP.chat + signal-cli)	Private communication channel
Cloud AI	Claude Opus (or preferred cloud model)	Primary reasoning
Decentralized AI	Morpheus network (proxy-router + proxy bridge)	Free after MOR stake, P2P inference
Local AI	Ollama (on Mac mini or secondary Mac)	Private, unlimited, always available

The Build in Seven Phases

Phase 0 – Discovery. Define what the agent will do, choose its name and persona, decide which phases apply to your build. Not everyone needs DeFi. Not everyone has two Macs. The plan adapts.

Phase 1 – Mac mini Setup. Headless macOS configuration. Dedicated user account for the agent. Energy settings for always-on operation. HDMI dummy plug (prevents sleep issues and ensures proper display rendering). Tailscale for remote access. SSH hardened to key-only auth. Homebrew, Node.js, Git.

Phase 2 – Agent Identity. Proton Mail account with Bridge for local IMAP/SMTP. macOS Keychain for all secrets (no plaintext, ever). Ethereum wallet generated with Foundry, private key in Keychain, seed phrase on paper. Safe multi-sig wallet on Base with the agent's key and your key as co-signers – the agent proposes transactions, spending above limits requires your approval. GitHub account. Full identity separation verified.

Phase 3 – Communication Channel. VoIP phone number from JMP.chat (~$4/month, no personal info required). Signal registered via signal-cli on the Mac mini. You text the agent, it responds.

Phase 4 – Model Routing. Three-tier fallback chain: Cloud AI (Claude) as primary, Morpheus (decentralized) as first fallback, local Ollama as backup. Morpheus proxy-router connected to Base mainnet. MOR staked for 7-day sessions (tokens return on expiry, re-stake indefinitely). OpenAI-compatible proxy bridge abstracts all blockchain complexity. The agent framework routes automatically – if one tier goes down, the next picks up.

Phase 5 – Persona + Workspace Files. Six text files define the agent's behavior: SOUL.md (character), IDENTITY.md (facts), USER.md (the human), AGENTS.md (rules and guardrails), TOOLS.md (permissions), MEMORY.md (long-term continuity). Change the files, change the behavior.

Phase 6 – Security Hardening. Defense in depth: all services bound to localhost, firewall enabled, tokens rotated, no plaintext secrets, Safe wallet with on-chain spending limits, launchd persistence, kill switch.

Phase 7 – Ongoing Operations. Trust-building timeline: watch-only (weeks 1-2), small budget (weeks 3-4), expanded autonomy (month 2+). The agent proposes, the human approves. Autonomy expands as judgment is demonstrated.

Key Concepts

- **MOR staking is renewable, not consumable.** Each 7-day session costs ~2 MOR to stake, and the tokens return when the session expires. Re-stake indefinitely. We recommend starting with ~50 MOR in the wallet (gives you flexibility across sessions). Ongoing cost is gas only (fractions of a cent on Base).
- **Three economic models, one interface.** Cloud (per-token pricing), decentralized (staked, tokens returned), local (free). The agent routes automatically.
- **Identity isolation is the security foundation.** Separate macOS user, email, wallet, credentials. The agent cannot access your accounts.
- **The Safe IS the guardrail.** Funds live in a multi-sig Safe contract with on-chain spending limits. The agent proposes, you approve above the threshold. Enforced by the blockchain, not by software.
- **Persona files are the control surface.** You define who the agent is through text files. No code changes needed to reshape its personality, rules, or boundaries.

What You Need

- A Mac mini (M4 recommended, ~$600)
- An HDMI dummy plug (~$10)
- A Proton Mail Plus account (~$4/month)
- A JMP.chat VoIP number (~$4/month)
- A cloud AI subscription or API key (~$20-200/month)
- ~$10-50 of ETH on Base (gas)
- ~50 MOR tokens (~$10, reusable – tokens return after each session)
- Optionally, a second Mac with 64GB+ RAM for local inference
- A pen and paper for the wallet seed phrase

Time to build: About a weekend for the basic agent. Add another day for Morpheus integration.

Resources

- **Printable guide:** `AUTONOMOUS-AGENT-SETUP-GUIDE.pdf` (17 pages, full walkthrough)
- **Claude Code prompt:** `AUTONOMOUS-AGENT-SETUP-PROMPT.md` (paste into Claude Code for interactive guided setup)