



aphanite

THE COMPLETE GUIDE

How to use Aphanite.

Everything the platform does, in one place — signing in with your wallet, private messaging, sending crypto in chat, groups, verification, backup, and every privacy control. Written for real people, not cryptographers.

DOCUMENT

User Guide & Feature Manual

REFLECTS

Current app build

DATE

July 2026

AUDIENCE

Everyone

How to use Aphanite.

Everything the platform does, in one place — signing in with your wallet, private messaging, sending crypto in chat, groups, verification, backup, and every privacy control. Written for **real people**, not cryptographers.

DOCUMENT	REFLECTS	DATE	AUDIENCE
User Guide & Feature Manual	Current app build	July 2026	Everyone

CONTENTS

- | | |
|--|--|
| 01 Welcome to Aphanite | 09 Verifying People |
| 02 Getting Started | 10 Backup & Restore |
| 03 Your Identity & Handles | 11 Security & Privacy Controls |
| 04 Devices & Keys | 12 Paid Features & Pricing |
| 05 Messaging | 13 Developer API |
| 06 Requests & Consent | 14 Privacy, Explained |
| 07 Groups | 15 FAQ & Glossary |
| 08 Sending Crypto in Chat | |

SECTION 01

01 · Welcome to Aphanite

Aphanite is a private messenger built around your crypto wallet. Your address is your identity, your messages are readable only by you and the people you talk to, and there is nothing to sign up for.

If you have used a normal messaging app, Aphanite will feel familiar — you have conversations, groups, requests, and settings. What is different is underneath. There is no phone number or email tied to your account; you sign in by proving you control a wallet address. Every message you send is encrypted on your own device before it leaves, so the servers that carry it only ever see scrambled data they cannot read. And because Aphanite is wallet-native, you can also send and receive crypto right inside a conversation.

THE ONE BIG IDEA

Free private core, paid perimeter. Private messaging — one-to-one and in groups — is free forever and always end-to-end encrypted. The only things that ever cost money are optional extras around the edges (a custom @name, a verified badge, bigger groups, encrypted cloud backup, a developer API). None of those can read your messages, and Aphanite never makes money from your content or your contacts.

What you can do with Aphanite

- **Message privately** — end-to-end encrypted direct messages and group chats.
- **Be reached by your address or a handle** — no phone number to hand out.
- **Send crypto in chat** — transfer funds to someone mid-conversation and view recent on-chain history.
- **Stay in control of who reaches you** — first contact from strangers waits in a Requests queue.
- **Verify who you are talking to** — safety numbers and a live in-chat identity check.
- **Protect your history** — optional encrypted backup that only you can unlock.
- **Tune your privacy in depth** — a large, private-by-default settings panel.

SECTION 02

02 · Getting Started

Setup takes a couple of minutes and a wallet. Prefer to look around first? The homepage offers a demo identity that works without a real wallet.

1. **Connect your wallet.** Click Connect Wallet and pick your wallet (MetaMask, or any compatible injected wallet). This only shares your public address — it gives Aphanite no power to move funds.
2. **Sign in — no gas, no spend.** Your wallet signs a one-time, domain-bound message (Sign-In With Ethereum). This proves the address is yours. It is free, off-chain, and never creates a transaction. The rule is simple: **sign, never spend.**
3. **Authorize this device.** Aphanite creates a messaging key for this device and asks your wallet to sign a short authorization for it. That signature links the device to your identity so this device — and only this device — can read your messages here.
4. **Pick a name (optional).** You can ride free using your address, or claim a permanent @handle (3–20 characters: a–z, 0–9, underscore). A custom handle is a paid, one-

time extra that writes your name into the public directory; new accounts also get a free random alias by default.

5. **Make it yours.** Everyone gets a unique avatar generated from their address, or you can upload your own. Choose a light or dark theme and an accent colour, and set your preferred network for sending crypto in chats. All of this is changeable later in Settings.

6. **Say hello.** Add a few people by @handle or address to get started — Aphanite sends them a first-contact request. You can invite people any time.

JUST BROWSING?

Use **Try with demo identity** on the homepage to explore the full experience without a real wallet. Open two browser profiles to try a two-person chat with yourself. Demo transfers are simulated — nothing leaves your device.

SECTION 03

03 · Your Identity & Handles

Your wallet address is your account. Handles, ENS names, directory visibility, and linked wallets all sit on top of that single root identity.

Handles. A handle is a permanent, human-readable @name — like @alice — that maps to your address so people can find and reach you without copying a long hex string. Handles are unique, one per address, and are written into Aphanite's public transparency log. Claiming a custom one is an optional paid extra; without it, you are still fully usable by your address or your assigned alias.

ENS names & avatars. If you use ENS, Aphanite can display ENS names and pictures for addresses. This is **off by default** because looking up ENS sends addresses to a public resolver; turn it on in Settings → Account & Identity if you want it.

Directory visibility. By default your handle is Listed so others can find you in the people directory. Switch to Unlisted in Settings to stay hidden from search while remaining reachable by anyone who already knows your handle or address.

Linked wallets. Hold more than one address? You can link additional wallets to a single identity so signing in with any of them lands in the same account. Each link is a signature from the wallet being linked, and every link is recorded in the transparency log. Manage links under Settings → Account & Identity → Linked wallets.

SECTION 04

04 · Devices & Keys

Each device you use gets its own messaging key, authorized by your wallet. This is what makes multi-device and key rotation possible without ever exposing your wallet key.

Adding another device. To use Aphanite on a second device, open it there, connect the same wallet, and authorize the new device's key with a wallet signature. On the new device you'll see a 64-character device key; the authorization ties it to your account. From then on, anyone messaging you seals a copy for each of your active devices, so every device stays in sync.

Fingerprints & transparency proofs. Under Settings → Devices & Keys you can reveal this device's **key fingerprint** for out-of-band verification, and view the cryptographic **inclusion proof** that your key really is in the public registry. These are the tools that let a careful user confirm nothing has been tampered with.

Rotation & revocation. Device keys can rotate on a schedule (Manual, Monthly, or Quarterly) for stronger forward secrecy. If you lose a device or no longer trust it, revoke it from the devices list; the revocation is written to the transparency log so your contacts can see the change.

KEY-CHANGE ALERTS

Aphanite can warn you when a contact's safety number changes — the tell-tale sign of a possible impersonation or a device change. This alert is **on by default** and nothing about it leaves your device. For high-risk situations, you can also require re-verifying a contact before you can message them again after their key rotates.

SECTION 05

05 · Messaging

Direct messages are end-to-end encrypted with the Signal protocols — X3DH to start a conversation, then the Double Ratchet for every message. The same protocol that powers Signal and WhatsApp. You just type; the encryption is automatic and invisible.

The basics. Open a conversation, type, and send. By default Enter sends and Shift+Enter makes a new line (you can flip this in Settings). Double-tap a message for a

quick reaction; your default reaction emoji is configurable.

Editing, unsending & deleting. You can edit or unsend a message for a window after sending it — off, 5 minutes, 1 hour, or 1 day. Deleting a message can remove it for everyone: Aphanite sends a private "delete" instruction over the same encrypted channel, so the server never sees the content involved.

Disappearing messages. Turn on a **disappearing timer** so messages auto-delete after a set time — 10 seconds up to a week. You can set a default for all new chats in Settings and override it per conversation. There is also a best-effort screenshot notice (it cannot be fully enforced, and Aphanite is honest about that).

Drafts & composing. Unsent drafts are saved locally so you don't lose a half-written message. Text size, chat wallpaper, and other composing preferences live under Settings → Chats & Messaging and Appearance.

Send later. Tap the clock in the composer to schedule a written message — in 30 minutes, an hour, 8 hours, or tomorrow. The message stays on your device until the moment it sends (keep the app open at that time), then goes out through the normal encrypted path. Pending sends show above the composer, where you can cancel them.

WHY YOUR MESSAGES ARE SAFE

Every direct message is encrypted with keys that exist only on your devices and your contact's devices. Aphanite's servers move a sealed envelope they cannot open. Even Aphanite cannot read your messages or hand their contents to anyone — there is no back door, by design.

SECTION 06

06 · Requests & Consent

Because anyone can reach an address, Aphanite keeps strangers out of your inbox until you say yes. First contact lands in a Requests queue — you decide what gets through.

How first contact works. When someone you haven't talked to messages you, their message arrives in **Requests**, not your main inbox, carrying an encrypted intro. Accept it and you both become contacts — messages flow normally from then on. Decline it and it goes away. This one design choice is what keeps a permissionless, address-based messenger usable.

Who can message you. In Settings → Privacy you choose who may start a conversation: Everyone (still via Requests), Contacts of contacts, or Allowlist only. You can also auto-accept people your existing contacts already talk to, if you prefer less friction.

Anti-spam. Nobody pays to message you, and nobody can pay their way in. Spam control is consent-based: first contact always lands in Requests until you approve it, marking a sender as **spam** silently stops their messages — only you can lift that mark — and per-sender rate limits stop anyone from flooding your Requests queue. A hard block cuts a sender off entirely.

Blocking & muting. Block an address to stop it reaching you entirely, or mute a conversation to silence it without blocking. Manage both under Settings → Privacy → Blocked & muted.

SECTION 07

07 • Groups

Group chats bring several people together with the same privacy guarantees as one-to-one. Group messages are sealed to each member individually, so bodies stay end-to-end encrypted.

Creating a group. Create a group with a name (2–40 characters) and an optional avatar. Choose whether it is **public** (anyone can discover and join) or **private** (invite-only and hidden from discovery), and optionally set a join **password**. Add members by @handle or address.

Joining & discovering. Browse public groups by name and join them (entering the password if one is set). Verified, official groups carry a checkmark and appear at the top of discovery. Private groups require an invite.

Managing a group. The group creator can set the avatar, invite people, and delete the group; any member can leave at any time. Each group also has an `id` that developers can use with the API to build bots and integrations for that group.

Encrypted polls. Tap the chart icon in a group's composer to ask the group a question with 2–6 options. Votes update live on the poll card — and because both the question and every vote travel as sealed messages, **the server can see neither the question nor the results**. One vote per member; your choice locks once cast.

GROUP SIZE & LIMITS

Free accounts can host groups up to a standard member cap. The optional **Larger groups** feature raises the limit for groups you create. Because group messages are sealed to every member's devices, very large groups are intentionally bounded.

SECTION 08

08 • Sending Crypto in Chat

Aphanite is wallet-native, so you can send a transfer to someone right inside a conversation — and check recent on-chain activity — without leaving the chat.

Sending a transfer. Open the transfer control in a conversation, enter an amount, and confirm. There's a handy Tap to use max that keeps a little back for gas. The transfer is a **real on-chain transaction signed by your wallet** — not by Aphanite. Aphanite never holds or moves your funds; your wallet does, and you approve every transfer.

Requesting crypto. Flip the payment sheet to **Request** to ask instead of send: the other person receives a tap-to-pay card with the amount and an optional note, and one tap opens their wallet with everything prefilled. No funds move until they approve the payment in their own wallet.

Choosing a network. You set a preferred network during setup and can switch per transfer. If your wallet is on a different network, Aphanite will prompt it to switch before sending.

Transaction history. From within a chat you can view an address's recent on-chain transaction history, so you can confirm a payment landed or get context on who you're dealing with.

GOOD TO KNOW

On-chain transfers are **public on the blockchain** — the amount, the addresses, and the transaction are visible to anyone, and permanent. That is a property of the blockchain itself, not Aphanite. If a transfer is cancelled in your wallet or your balance is too low, Aphanite will tell you and nothing is sent. In demo mode, transfers are simulated and nothing leaves your device.

SECTION 09

09 · Verifying People

Encryption protects your message in transit; verification confirms you're encrypting it to the right person. Aphanite gives you two easy ways to check.

Safety numbers. Every conversation has a **safety number** derived from both parties' keys. If you and your contact see the same number — compared in person, over a call, or through another trusted channel — you can be confident no one is sitting in the middle. If a contact's safety number ever changes unexpectedly, Aphanite flags it.

Live identity check. For an in-the-moment confirmation, use the **live verification** in a chat: you challenge your contact, and their wallet signs a one-time message proving they control the address you think they do. If the signature matches, you'll see Identity verified; if it doesn't, Aphanite warns you to treat that identity with caution. Verified contacts get a badge in the conversation.

The transparency log. Under the hood, the mapping from handles to keys lives in a public **key-transparency log**. Your client can check a cryptographic inclusion proof that a key really is in the log, so the directory can't quietly swap someone's key for an impostor's without leaving a visible record. Key changes are surfaced to you.

SECTION 10

10 · Backup & Restore

Your history lives on your devices. Optional encrypted backup lets you restore it later — protected by a passphrase only you know, so even Aphanite can't read it.

How encrypted backup works. When you turn on hosted backup, Aphanite encrypts everything on your device using a key derived from your passphrase (with Argon2id, a deliberately slow, brute-force-resistant method), and uploads only the resulting **ciphertext**. The server stores bytes it cannot decrypt. Restoring on a new device re-creates your exact identity and immediately decrypts your history.

What's included in a backup

- Message history across all conversations
- Every setting and preference
- Any purchased paid features
- Verified contacts & safety numbers

- Pinned/muted chats, drafts, and read state
- Your device keys — so a restore is the same identity and decrypts right away

YOUR PASSPHRASE IS THE ONLY KEY

Use a passphrase of at least 8 characters and keep it safe. If you lose every device and your backup passphrase, your history cannot be recovered — there is no reset link and no back door. That's the deliberate cost of messages only you can read. You can also export an encrypted archive of your local data at any time.

SECTION 11

11 · Security & Privacy Controls

Aphanite ships with a deep settings panel, and every default is the most private option. Anything that would share more data is off until you turn it on. Use the search box at the top of Settings to jump to any control.

Locking the app. Set an **app lock (PIN)** to require a code to open Aphanite on this device — the PIN is stored only as a salted hash and never leaves the device. Pair it with an auto-lock timeout, hide the app's contents in your device's app switcher, and auto-clear copied addresses and keys from your clipboard.

Sessions & anti-phishing. View every active login session and revoke any you don't recognize (or sign out everywhere else in one tap). Keep **domain-binding warnings** on so Aphanite alerts you if a sign-in request comes from an unexpected site — your defence against phishing clones.

Duress wipe. For high-risk situations you can configure a **panic / duress** code that instantly wipes local data when entered. Use with care — it is irreversible when triggered.

CONTROL	WHAT IT DOES	DEFAULT
Read receipts	Whether contacts see when you've read a message	Off
Typing indicators	Whether contacts see you typing	Off
Last-seen / online	Who can see your activity status	Nobody
Link previews	Off avoids leaking your IP or the URL	Off
Proxy / Tor routing	Hide your IP address from the relay	Off — opt in
Cover traffic (experimental)	Decoy traffic to blunt timing analysis	Off
Usage analytics	Anonymized stats — collected only if you opt in	Off

Privacy toggles worth knowing — every default is the private option.

Network & routing. Choose which relay carries your (encrypted) envelopes, or point at your own custom relay. For extra privacy you can route through a proxy or Tor to hide your IP from the relay, and experiment with cover traffic to blunt timing analysis. These trade a little speed for more privacy and are there when you want them.

SECTION 12

12 • Paid Features & Pricing

Messaging is free. A few optional extras carry a one-time on-chain fee — and none of them can read your messages. You pay from your own wallet; Aphanite simply records the payment.

FEATURE	WHAT YOU GET	ONE-TIME FEE
Custom handle	A permanent @name in the public directory — short names are rare and priced accordingly (3 characters 0.05, 4 characters 0.01, 5 characters 0.003)	from ~0.00093 ETH
Verified / business account	A verified badge next to your name everywhere	0.05 ETH
Larger groups	A higher member limit for groups you create	0.002 ETH
Encrypted backup & sync	Hosted, unreadable-to-us cloud backup	0.0012 ETH
Developer API keys	Build bots & integrations on Aphanite	0.003 ETH
Priority relay	A lower-latency delivery lane	0.001 ETH
Link another wallet	Attach an extra address to your identity	0.0008 ETH
Creator groups	Charge an entry fee for groups you create — joiners pay you directly, wallet-to-wallet; Aphanite never holds the money	0.01 ETH

Fees are indicative and set in the app at time of purchase. Payment is a normal on-chain transaction from your wallet — on Ethereum, Base, Arbitrum, or Optimism — and Aphanite verifies it on-chain (right recipient, right amount, your wallet, never reused) before anything unlocks. Nothing is charged unless you approve it in your wallet. Any paid feature (except handles) can also be gifted to another user — you pay the same fee, they get the unlock and a sealed alert naming you.

THE PRINCIPLE BEHIND PRICING

Every paid feature lives at the perimeter — identity, capacity, storage, and developer tooling. Not one of them requires reading a message. That's how Aphanite can charge for extras while keeping the promise that your content is yours alone.

SECTION 13

13 · Developer API

Builders can integrate with Aphanite through a REST API that resolves public directory data and routes already-encrypted envelopes. The API never sees message plaintext.

Getting a key. Unlock Developer API access (a paid perimeter feature), then create an API key under Settings → API Settings. The secret (an `sk_live_...` token) is shown once at creation and never retrievable again, so store it safely. Keys can be named and revoked at any time.

What the API can do. Authenticate requests with an `Authorization: Bearer` header. The endpoints let you confirm your identity, resolve public handles and device keys, browse the public directory, and submit or pull **already-sealed** envelopes — the same encryption guarantee, offered to developers.

ENDPOINT	PURPOSE
<code>GET /api/v1/me</code>	Confirm your key and identity
<code>GET /api/v1/handles/{handle}</code>	Resolve a handle to its record
<code>GET /api/v1/keys/{address}</code>	Fetch an address's device keys
<code>GET /api/v1/directory</code>	Search the public directory
<code>GET · POST /api/v1/envelopes</code>	Pull your inbox · send sealed envelopes
<code>POST /api/v1/envelopes/ack</code>	Acknowledge decrypted envelopes
<code>GET /api/v1/groups · /{id}</code>	List groups · group + member keys

Groups and the developer API use per-message X25519 sealed boxes (the `box-v1` suite). Full REST docs and an OpenAPI description are available at api.aphanite.io.

SECTION 14

14 · Privacy, Explained

Here is the honest version of what Aphanite protects, what the server can see, and where the limits are — stated plainly rather than papered over.

WHAT'S PROTECTED

The **content** of your messages. Direct messages are end-to-end encrypted with X3DH and the Double Ratchet — the same protocol as Signal and WhatsApp; group and API messages use X25519 sealed boxes. Keys never leave your devices. Aphanite cannot read your messages and cannot produce their contents to anyone.

WHAT THE SERVER CAN SEE

The relay handles encrypted envelopes it cannot open — and for conversations you already have, it now sees far less of the outside of the envelope too. Once a direct conversation is established, your clients agree on secrets inside the encrypted channel and messages travel under rotating unlinkable mailbox tags — sealed sender — so the relay stores ciphertext under an opaque label with no sender, no recipient, and no device identity: it can't see who's talking to whom. Message sizes are padded to fixed buckets and clients check for mail on a jittered schedule. The honest limits: first contact (consent requests) and groups are still addressed by identity in v1, and the relay still sees your IP address and coarse timing — route through Tor or a VPN if that matters to you. Message content is never visible to Aphanite either way.

HOW YOU KNOW IT'S THE RIGHT PERSON

Handle-to-key bindings live in a public append-only transparency log, and your client can verify an inclusion proof before trusting a key — so the directory can't swap keys silently without leaving a visible record. You can also compare safety numbers and are alerted to key changes.

ON-CHAIN IS PUBLIC

Sign-in is off-chain and private, but any crypto transfer you send in chat is a public blockchain transaction — amounts and addresses are visible and permanent. That's the blockchain, not Aphanite.

THE COST OF REAL ENCRYPTION

There is no back door. If you lose every device and don't have an encrypted backup, your history can't be recovered. Set up backup if that matters to you, and keep your passphrase safe.

SECTION 15

15 · FAQ & Glossary

Quick answers to common questions, and a plain-language glossary of the terms you'll see around the app.

Do I need a crypto wallet?

Yes — signing in uses your wallet to prove you control your address; there's no password or email. To just look around, use the demo identity on the homepage.

Does signing in cost gas or move funds?

No. Sign-in is a gasless, off-chain signature (Sign-In With Ethereum). Aphanite never constructs a transaction to log you in — sign, never spend.

Can Aphanite read my messages?

No. They're encrypted with keys that never leave your devices. Aphanite cannot read them or hand them over.

Can I send crypto in a chat?

Yes — send a transfer directly in a conversation and view an address's recent on-chain history from the chat.

What if I lose my device or keys?

With no device and no encrypted backup, history can't be recovered — the trade-off for messages only you can read.

Is Aphanite free?

Messaging is free. Optional extras — custom handles, verified accounts, encrypted backup, larger groups, a developer API — are the only paid parts.

How do I contact the team?

Use the wallet-verified contact form on the homepage; your signature confirms it's really you and helps cut spam.

TERM	MEANING
End-to-end encryption	Only you and your contact can read a message; carriers see scrambled data.
X3DH + Double Ratchet	The Signal protocol used for direct messages — forward secrecy and self-healing keys.
SIWE	Sign-In With Ethereum — proving you own an address with a gasless signature.
Handle	Your @name, mapped to your address in the public directory.
Device key	The messaging key for one device, authorized by your wallet.
Safety number	A per-conversation code you can compare to confirm identities.
Transparency log	A public, append-only record of handle→key bindings with inclusion proofs.
Relay	The server that forwards your encrypted envelopes; it can't read them.
Request	A first-contact message waiting for your approval before it reaches your inbox.
dr-v1 / box-v1	The encryption suites: Double Ratchet for DMs; X25519 sealed boxes for groups & API.

About this guide — Aphanite · The Complete Guide, July 2026. Fees and feature availability are set in the app and may change; privacy properties are described as implemented, including their honest limits. For the underlying cryptography, see the Whitepaper and Protocol Specification.