WHITEPAPER · V1.0

Cloak

A Private Activity Layer for On-Chain Life

Put a cloak over anything.

Cloak November 2026

ABSTRACT

Public ledgers make every payment, trade, and settlement observable. Cloak lets you send, swap, settle OTC, and launch from private balance on Solana, addressed by Cloak ID or X @handle, with optional reputation that never publishes bag size. Private balances run on Helius Solana Privacy Rings.

Contents

1 Introduction
2 System architecture
3 Private balance layer: Helius Rings
4 Identity
5 Cloaked Send and Slips
6 Dead Drop OTC
7 The Book
8 Cloaked Launch
9 Private swap and bridge
10 Security and privacy model
11 Threat model
12 Multichain
13 Conclusion

1. Introduction

Fast blockchains solved throughput. They did not solve discretion. Any transfer that touches a public wallet becomes a durable record: counterparties, amounts, timing, and often intent. Indexers and social screenshots turn that record into a permanent dossier.

People do not live in base58. They tip, invoice, and settle against Cloak IDs and X @handles. Cloak is the layer between social addressing and private settlement.

Cloak is an application layer. Send, swap, OTC, and launch run private by default. When reputation matters, the Book publishes status without leaking size.

Put a cloak over anything. Privacy by default. Disclosure by choice.

1.1. Design goals

- Address people as Cloak ID or X @handle.
- Keep payment and settlement amounts off public receipts.
- Pay someone who has not joined yet, without claim-link chores.
- Settle size trades with encrypted terms and dual private locks.
- Launch tokens under the same privacy model.
- Publish reputation without publishing bag size.
- Ship on Solana first; extend the same standard across chains.

2. System architecture

Cloak separates four concerns: who you are, what you hold privately, how settlement is authorized, and what the world can see.

- User: Operates Cloak through the browser client.
- External wallet: A Wallet Standard Solana wallet. Authenticates the Cloak ID session and signs public funding legs (deposits, fee top-ups).
- Cloak ID: Durable account identity across Send, OTC, Launch, Book, and portfolio. Shown as Cloak ID labels (Cloak ID 0001). Can link to an X @handle.
- Private account: Browser-held Ed25519 key distinct from the external wallet. Owns shielded notes. Passphrase-protected backup is available.
- Helius Solana Privacy Rings (SPR): The private-balance substrate. Cloak deposits into, spends from, and withdraws through Helius Rings for shielded notes, note encryption, client proofs, and pool transfers.
- Settlement program: On-chain Cloak program for private_pay, slip_fund / claim / refund, deal_lock / seal / return, and related circuits, settling against Rings private balance.
- API and worker: Sessions, intents, finality verification, relays. Never store user spending or viewing keys.
- Book: Public print surface for verified outcomes without size.

Note. Figure 1: External wallet authenticates Cloak ID. Private account keys drive Helius Rings balances and Cloak settlement-program proofs. Send, Slips, Dead Drop, and Launch settle under that program against Rings notes. Book prints publish status without amounts.

The client builds proofs and produces public transaction bytes. The backend verifies signatures, program expectations, and finalized chain effects. Witnesses and decrypted balances stay in the browser.

2.1. Trust boundary

Cloak's server is an availability and verification plane, not a custodian of private keys. It stores account mappings, encrypted backups when the user opts in, operation records, and public wire bytes required for reconciliation. It does not receive plaintext private keys, viewing keys, or decrypted note sets.

The browser origin is a trust boundary. Device vaults wrap seeds with non-exportable Web Crypto keys. That is trusted-browser storage, not hardware isolation. Users treat recovery material with the same care as a seed phrase. Cloak cannot reset a lost passphrase.

---

3. Private balance layer: Helius Rings

Cloak's private balances run on Helius Solana Privacy Rings (Solana Privacy Router, SPR). Cloak uses Rings as the balance substrate and builds settlement, identity, Launch, and the Book on top.

> **DEFINITION: HELIUS SOLANA PRIVACY RINGS**
>
> Helius's shielded-pool infrastructure on Solana: encrypted notes (private UTXOs), pool transfers, client proving, and indexed encrypted material. Cloak uses Rings for private balance. It does not re-implement that cryptography.

> **DEFINITION: PRIVATE BALANCE**
>
> The set of spendable shielded notes owned by a Cloak private account in the Helius Rings pool on a given cluster.

> **DEFINITION: PRIVATE ACCOUNT**
>
> A browser-generated Ed25519 identity that owns Rings notes. It is separate from the external wallet used for session login and public funding.

3.1. How Cloak uses Helius Rings

Every cloaked payment, Slip, Dead Drop lock, and private-balance spend settles against Helius Rings notes:

1. Deposit: the user's external wallet funds the Helius Rings pool. Value becomes encrypted notes owned by the Cloak private account.
2. Hold: private balance is the spendable set of those Rings notes, decrypted only in the browser with the user's keys.

3. Spend: Cloak settlement circuits (private_pay, slip_fund, deal_lock / seal, and related paths) authorize application outcomes; pool proofs and note spends go through the Helius Rings / SPR prover path.
4. Transfer: pool transfers move value between private addresses inside Rings without publishing amounts on the public receipt.
5. Withdraw: notes exit the Rings pool to a public wallet.

- The client uses the Helius privacy SDK / SPR stack for note management, proving, and pool interaction.
- Cloak connects to Helius privacy RPC and related services for the cluster.
- Cloak's on-chain settlement program is the product layer; the shielded pool is Helius Rings.
- Cloak is an independent product. Helius builds and operates the Rings infrastructure Cloak uses for private balance.

3.2. Notes and proofs

- Value is held as encrypted notes in the Helius Rings shielded pool.
- Spends require client-side proofs that authorize the transfer without revealing note contents to the public ledger.
- Pool transfers move value between private addresses inside Rings.
- Indexers return encrypted payloads; decryption happens locally with the user's keys.
- Application circuits for Cloak settlement (private_pay, deal_seal) run in the browser; pool proofs use the Helius Rings / SPR prover path.

3.3. Custom Rings

Helius Rings keeps private-note amounts off public receipts for in-pool activity. Deposits into the pool, withdrawals to a public wallet, and some settlement signer metadata remain public on the shared Rings path.

Helius is shipping custom Rings that make transactions fully anonymous end to end. When that lands, Cloak rolls it out on the same Helius substrate. Send, Slips, Dead Drop, Launch, and private swap move onto custom Rings for private balance and settlement. Cloak does not build a separate anonymity stack.

- Shared Helius Rings / SPR: private balances and product settlement.
- Helius custom Rings: fully anonymous transactions.
- Cloak identity, Book, Launch, and settlement UX stay Cloak; anonymity upgrades ride Helius Rings.

> **Note.** Cloak does not ship a competing privacy prover. Full anonymity comes with Helius custom Rings, and Cloak adopts them.

3.4. Public edges

Deposits into Helius Rings and withdrawals to a public wallet expose wallet addresses, asset, amount, and timing on-chain. Matching a public deposit amount to a soon-to-follow private lock is a linkage risk. Cloak documents this and recommends buffers, waiting, and avoiding exact-amount choreography around deals.

Network fees, certain settlement signer metadata, and advertised listing fields are also public on the shared Rings path. Helius custom Rings close those edges; Cloak adopts them when they ship.

3.5. Account lifecycle

1. User authenticates with an external Solana wallet (or an embedded-wallet path) and opens a Cloak ID session.
2. The client creates or restores a private account for that Cloak ID and cluster.
3. Online backup encrypts private key material under a user passphrase (PBKDF2-SHA256, AES-256-GCM) bound to address and network.
4. Deposits move from the external wallet into Helius Rings private balance; withdrawals reverse that edge.
5. Private spends are signed by the private account, proven against Rings, and verified after chain finality.

One private account maps to one Cloak ID per cluster. Replacement of an existing mapped account is refused. Reconnecting the external wallet alone does not restore notes.

---

4. Identity

> **DEFINITION: CLOAK ID**
>
> The durable account identity used across Send, OTC, Launch, Book, and portfolio. Shown as a Cloak ID label (Cloak ID 0001).

> **DEFINITION: X @HANDLE ADDRESSING**
>
> A linked X identity. Counterparties send to the X @handle without a wallet address and without knowing whether the recipient has joined yet.

Session authentication proves control of the external wallet. Linking X uses OAuth. Handle lookup for payments is a directory function only. It does not grant spending authority.

Social addressing is how people find each other in Cloak. Wallet addresses are for deposits and withdrawals, not for naming counterparties.

---

5. Cloaked Send and Slips

Send is a first-class product area, not nested under OTC. The user selects a recipient (Cloak ID or X @handle), an asset from Helius Rings private balance, and an amount, then approves once.

> **DEFINITION: CLOAKED SEND**
>
> A private payment from the sender's Rings private balance to a recipient identity, authorized by the settlement program's private_pay or slip_fund path, and recognized only after verified finality.

5.1. Recipients on Cloak

When the recipient already has a Cloak ID and private account, settlement targets their shielded address through private_pay against Helius Rings. Amounts stay off public receipts. The sender can Print status to the Book without publishing size.

Protocol fee for direct cloaked sends is 0%. Network fees and rent are separate. Supported assets spend from Rings private balance.

5.2. Slips for recipients who have not joined

> **DEFINITION: SLIP**
>
> A time-bounded private hold funded from Rings for an intended X recipient who may not yet have a Cloak ID. The recipient claims after linking identity. The sender may cancel before claim or refund after expiry with a valid proof.

The sender never manages claim links. After slip_fund finalizes, the client publishes a claim capsule and a server-sealed invitation so delivery is automatic for the sender. The hold window is seven days.

1. Sender enters an X @handle and amount, then approves once.
2. Funds lock in the Slip under the settlement program, funded from Rings private balance.
3. Invitation and claim material are published for the intended recipient.
4. Recipient joins, links X, and claims into Rings private balance.
5. If unclaimed through expiry, sender refunds with a fresh proof.

5.3. Finality

A submitted signature is not success. The worker verifies network, program instruction and events, immutable scope and terms, finality, and the linked Helius Rings private-pool operation before the product marks the send complete. Pending signed bytes are retained for exact retry. They are not overwritten by a second spend.

---

6. Dead Drop OTC

Dead Drop is Cloak's OTC rail: discover enough to find a counterparty, negotiate privately, settle from Helius Rings private balance.

> **DEFINITION: DEAD DROP**
>
> An OTC flow where terms are encrypted to counterparties, both sides lock from Rings private balance, and settlement is a co-signed program seal verified on finality.

- Public listings and quote requests expose discovery fields (ticker, status), not sealed size and price.
- Encrypted terms pass only between intended Cloak IDs.
- Both sides lock from Helius Rings private balance, then co-sign settlement.
- Listing publication costs a fixed private fee (0.01 SOL) from private balance.
- Sealed deals charge a 0.4% settlement fee on the seller side.

6.1. Lifecycle

1. Discovery: public listing or request for quotes.

2. Negotiation: encrypted offers and reservations between Cloak IDs.
3. Lock: each side funds its leg from Helius Rings private balance.
4. Seal: both parties approve one settlement transaction.
5. Verification: worker confirms finality, program effects, and linked Rings operations.
6. Book print or void for reputation, when chosen.

On the shared Rings path, the two signers of a Deal Seal and their transaction timing are public. Helius custom Rings make that settlement class anonymous; Cloak adopts them when they ship.

---

7. The Book

Privacy by default still leaves room for a verified public signal. The Book is that surface: disclosure without bag size.

> **DEFINITION: PRINT**
>
> A public Book record of a verified outcome: Cloak IDs, ticker, and status, without bag size or wallet addresses.

> **DEFINITION: VOID**
>
> A Book record that a deal did not complete. It keeps reputation honest without inventing size.

Payment senders choose whether to publish receipts. The Book is selective disclosure against private rails, not an explorer dump.

---

8. Cloaked Launch

Launch creates and trades tokens without turning every move into a public wallet story. It uses the same product language as Send, Swap, and OTC, and the same Helius Rings private balance.

> **DEFINITION: CLOAKED LAUNCH**
>
> Token creation and launch trading inside Cloak from private balance, with sealed and blind entry that blocks snipers and dump patterns.

Sealed and blind entry are the high bar on Launch: anti-sniper mechanics and dump-aware constraints. Cloak wins at launch by being quieter and more controlled.

- Create and trade under Cloak identity and privacy defaults.
- Keep launch activity on Helius Rings private balance.
- Enforce sealed and blind entry as real constraints.

9. Private swap and bridge

Private swap execution funds an operator's shared shielded pool from the user's Helius Rings private balance on mainnet. A unique public execution wallet runs the route over existing liquidity. Verified proceeds or refunds return through the private pool.

During execution the operator can see trade terms. User spending keys stay local. Execution amounts, fees, timing, and external bridge endpoints are public on the shared Rings path. This is a disclosed custody model, not an invisible swap.

If private routing is offline, Cloak says so and will not claim a private path. Bridge uses the same private-intent path. Full anonymity for swap legs arrives with Helius custom Rings (Section 3.3).

10. Security and privacy model

> **DEFINITION: PRIVACY OBJECTIVE**
>
> Observers without the user's private keys cannot read private note values, encrypted OTC terms, or unpublished payment amounts from Cloak's Helius Rings private rails.

> **DEFINITION: SECURITY OBJECTIVE**
>
> Private spends require the private account key. Session and public funding legs require the external wallet. The server cannot authorize a private spend from credentials it does not hold.

Finality, not a submitted signature, determines success. Workers re-verify program effects and linked Helius Rings private-pool operations before marking outcomes complete.

Surface	Private	Public
Payment amounts (Send / Slip)	Yes	Book status only, if printed
OTC terms and size	Yes (encrypted to parties)	Discovery fields only
Helius Rings note balances	Yes	No
Deposits / withdrawals	No	Address, asset, amount, time
Deal Seal signers	No	Signer set and timing
Private swap execution leg	Funding from Rings balance	Route amounts, fees, timing
Book print	Size withheld	Cloak IDs, ticker, status

Table 1. Visibility matrix on the shared Helius Rings path.

When Helius custom Rings ship, Cloak adopts them and the public column for in-pool and settlement flows shrinks. Table 1 is the shared Rings path.

11. Threat model

Threat	Control
Malicious counterparty	Encrypted terms to intended IDs; dual lock; co-seal; expiry refunds with proofs
Curious private-swap operator	Disclosed custody; temporary execution custody; keys stay client-side
Compromised browser profile	Passphrase backups; device vault warnings; no server-side key recovery
Funding linkage	Documented public edges on shared Rings; avoid exact-amount deposits before locks; Helius custom Rings when they ship
Overstated privacy	Status and disclosures state what is private on the live Rings path

Table 2. Primary threats and controls.

On the shared Rings path, Cloak does not promise invisible deposits or withdrawals, operator-blind private swaps, or hardware-enclave guarantees for browser keys. Full anonymity comes through Helius custom Rings, not a Cloak-owned prover.

12. Multichain

Cloak is a private activity standard, not a single-chain product. Solana is the first deployment, with live Helius Rings infrastructure.

> **DEFINITION: CLOAK STANDARD**
>
> On every supported network: (1) durable social identity, (2) private activity for payments and settlement, (3) public prints without size leakage. Chain adapters change under the hood. The product language stays the same.

- One Cloak ID and one Send model across networks.
- Launch and the Book under the same cloak language.
- Per-chain adapters and a clear capability matrix, not four disconnected apps.
- On Solana, private balances use Helius Rings, including custom Rings when they ship.
- X @handle and Cloak ID stay the human layer above chain addresses.

13. Conclusion

Crypto does not need another wallet. It needs a private activity layer that matches how people already address each other: privacy by default, disclosure by choice.

Cloak runs private balances on Helius Solana Privacy Rings, settles Send, Slips, and Dead Drops through its settlement program, ships Cloaked Launch, and keeps the Book for reputation without exposure. When

Helius ships custom Rings for fully anonymous transactions, Cloak rolls that out on Helius. Solana is first. Other chains inherit the same standard.

Put a cloak over anything.
