Privacy on Solana:

A Full-Spectrum Approach for the Modern Enterprise

2026

SOLANA

Privacy on Solana for the Modern Enterprise

When building enterprise applications, privacy is a core requirement. It's needed to protect commercial sensitive information, preserve user data, transact without exposing details, and more. Applications need capabilities that only effective privacy implementations can enable, such as selective disclosure and compliance auditability.

The challenge, however, is that applications are unique in their privacy needs. A banking app that processes payroll must keep each employee's salary hidden from the public. An institutional trading desk must execute orders without signaling intent to the market. And a supply chain consortium must verify inventory across partners without exposing pricing.

Each is a different privacy problem, with different technical requirements and different regulatory constraints. Privacy is a complex decision: one involving a wide spectrum of options and requirements.

For enterprises, privacy is a spectrum, not a switch.

To meet these needs, it's become critical to build on a platform that supports the full privacy spectrum, not just one mode. Just as important as understanding the nuances, technology, and regulations around privacy, is building on the right foundation.

> **In this report, we'll look at the details of building privacy into applications. We'll map privacy across two axes—what's visible and who's visible—creating a matrix of four distinct privacy modes. We'll explore what each of these modes protects and what it reveals. We'll look at the specific use cases for each mode and which ecosystem solution best serves that purpose. And finally, we'll look at the native features and products on Solana that support each mode, giving real-world examples, and touch on the technical details behind them.**

Why Solana?

Before we dive into the privacy matrix, let's first take a brief look at Solana and how it implements privacy. As we walk through the matrix we'll use Solana features and protocols to help us understand the differences and options. A brief background will help with our analysis.

What is Solana?

- **Solana** is a high-performance Layer 1 (L1) **blockchain network** that processes **thousands of transactions per second**, **over 100 million transactions per day**, with confirmation times as low as 200 milliseconds[1], all while maintaining median fees at a **fraction of a cent**.
- It's a scalable foundation for both decentralized applications and major enterprise institutions.
- For a great overview on why teams and developers choose Solana, check out the official article, **Why Solana?**

Solana's privacy implementation

On Solana, privacy is core and based on a simple premise: auditability where required, privacy where desired. This approach avoids the extremes of default obscurity or total exposure, instead approaching privacy as a spectrum of offerings.

Privacy on Solana is composable, offering auditability where required, privacy where desired.

With Solana, an enterprise client can toggle between levels of privacy (such as basic confidentiality or full cryptographic secrecy) by selectively using the technologies and protocols that meet their unique privacy requirements. For example, fundamental building blocks like **token extensions** offer a variety of features teams can use, such as encrypted balances, selective disclosure, and permissioned access.

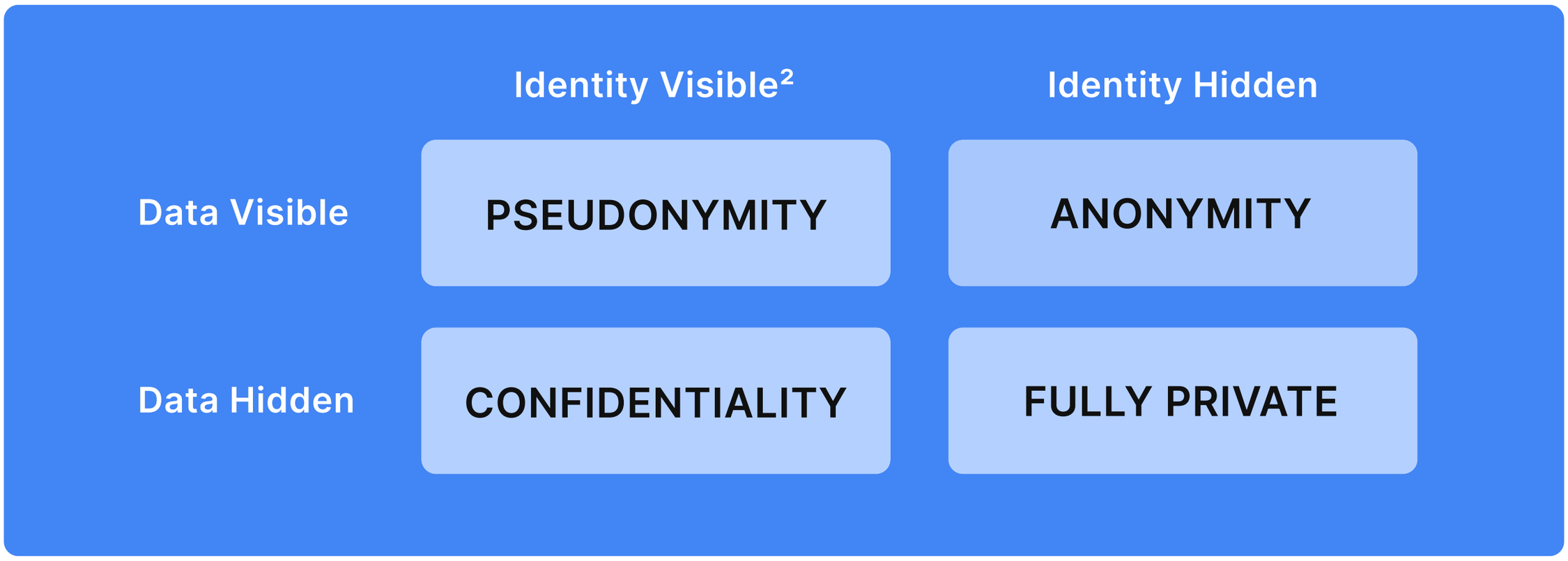
[1]With the forthcoming Alpenglow upgrade

The Privacy Matrix

With that base understanding, let's now dive into the details of privacy.

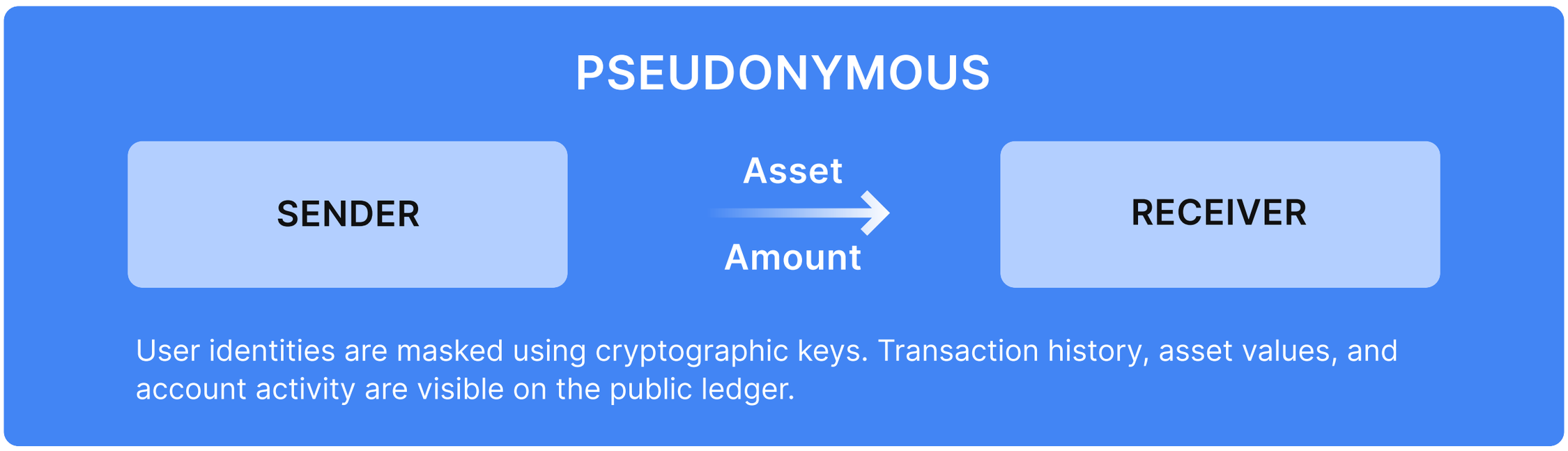
Privacy is a spectrum, with many nuances, choices, and often trade-offs to be made. One financial flow may need to hide how much was sent, another may need to hide who sent it, and yet another may need full participant anonymity to function at all. It's important to understand the choices and distinctions.

For our paper, we'll divide privacy into four modes. Each mode serves different privacy requirements, different regulatory requirements, and different use cases.



Let's look in detail at each.

PSEUDONYMITY (Data Visible, Identity Visible)



[2]Identity here refers to onchain address, not necessarily real-world identity

→ PSEUDONYMITY

Pseudonymity is the default state of most blockchains, and the starting point for understanding the privacy spectrum. When a user sends tokens from one wallet to another, everyone can see that Wallet A sent tokens to Wallet B. But they don't know who controls those wallets.

Pseudonymity is often misunderstood. It's not anonymity. A determined person (or AI) can often connect pseudonymous wallets to real-world identities through onchain behavior patterns, exchange KYC records, and transaction graph analysis.

But for many use cases, pseudonymity provides just the right balance: public verifiability of the transaction, hidden identity of the parties involved.
Applications that need to hide both identity and data can combine pseudonymity with confidentiality, which we'll cover next.

USE CASE:
Interbank Settlement

When a bank settles a transaction with another bank, the public benefits from knowing that the settlement occurred and the funds moved. This transparency makes blockchain useful for financial infrastructure. But the identities of the counterparties should not be visible to competitors or to the general public.

Native to Solana

Standard SPL tokens on Solana operate at the pseudonymity mode by default. Every transaction is public: amounts, flows, and timestamps are on the ledger. But the party behind each wallet address is pseudonymous by design. No real-world name is attached to a public wallet/key.

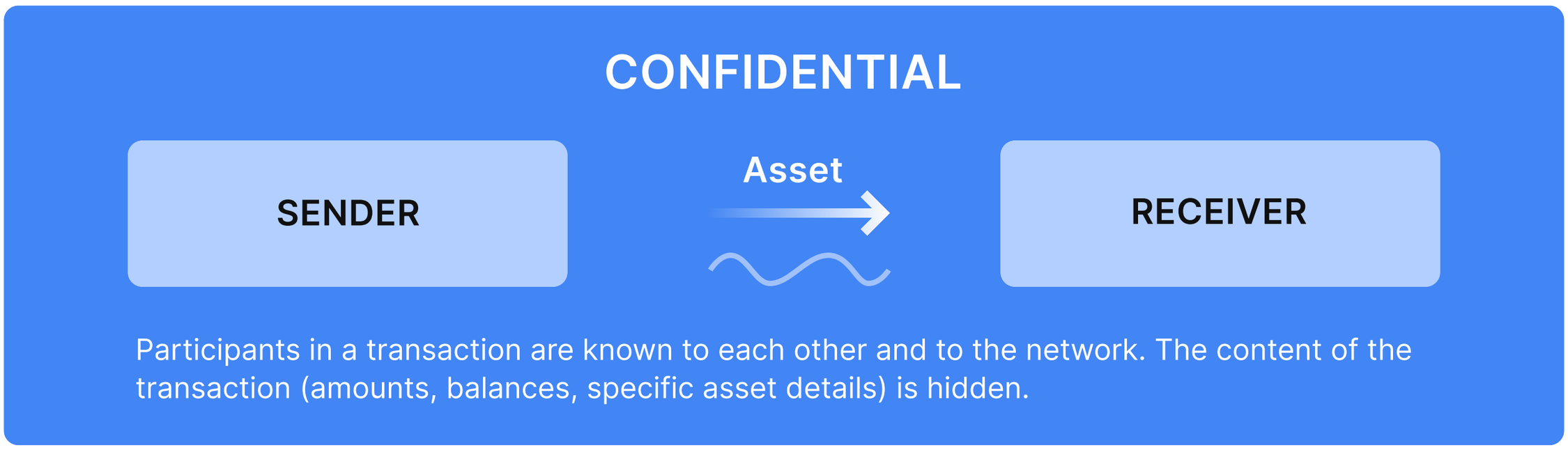
For institutions that need structured pseudonymity, token extensions provide two tools.

- **DefaultAccountState** allows token issuers to freeze all new accounts by default until a counterparty has been verified offchain. KYC happens outside the ledger. The ledger records only that an address was approved to transact. The identity stays offchain, while the settlement stays onchain.

- **MemoTransfer** requires every inbound transfer to include a reference memo, enabling payment reconciliation against internal records. This is the same function as a wire reference number, but without broadcasting deal terms to competitors or the public. A memo can be encrypted or in clear text as desired.

At the infrastructure level, the **Solana Attestation Service** allows institutions and KYC providers to issue signed, verifiable credentials linked to wallet addresses. A wallet can prove accreditation or compliance clearance without the verifying application ever learning who holds the wallet. And once a wallet verifies, it can reuse the credential across the ecosystem.

CONFIDENTIALITY (Data Hidden, Identity Visible)



→ CONFIDENTIALITY

Confidentiality is the traditional enterprise privacy baseline. Encrypting data at rest, enforcing Transport Layer Security (TLS) in transit, or building access controls around sensitive fields are all common examples of implementing confidentiality. It's the table stakes required by GDPR, CCPA, and most financial regulations.

On a public blockchain, adding confidentiality would mean that accounts and transactions are still visible on the public ledger, but balances and transfer amounts are encrypted. The network can verify that a transfer is valid without knowing how much was moved. This is similar to today's commerce: a customer can't see the financial statements of their neighborhood coffee shop just because they buy coffee there every morning. Applications should work the same way.

USE CASE:

Payroll and Vendor Payments

A company pays its employees onchain. The network needs to confirm that the payment was authorized and that the funds were moved. But each employee's individual salary should not be visible to anyone browsing the ledger.

Native to Solana

Solana supports confidentiality through **Confidential Balances**, a set of token extensions that use **zero-knowledge (ZK) proofs** and encryption to shield token balances and transfer amounts.

Launched in 2025 as the first encrypted token standard built on a major L1 for institutional compliance, Confidential Balances include three core capabilities:

→ **Confidential Transfers:** Transfer tokens between accounts while encrypting the amount. The network verifies validity through a suite of cryptographic proofs without ever seeing the underlying value.

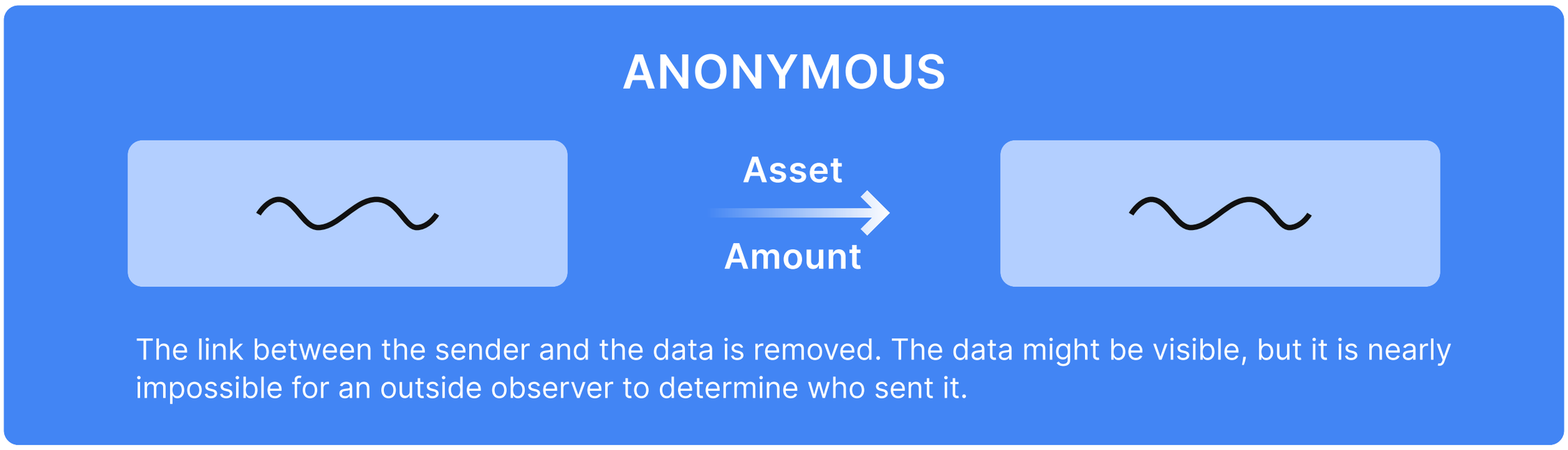
- **Confidential Mint and Burn:** Token issuers can create or destroy tokens without revealing quantities. The supply of tokens stays private.

- **Auditor Keys:** An optional compliance mechanism that allows a designated party such as a regulator or auditor to decrypt and view confidential transactions. This enables privacy for users while maintaining transparency for oversight.

As an example, by using Confidential Balances a stablecoin issuer could deploy a token where every transfer amount is encrypted and every balance is shielded, yet an auditor could still decrypt the transaction[3].

Beyond these protocols, enterprises can build their own custom privacy logic using ZK circuits and encryption primitives directly on Solana, tailoring the privacy mode to their exact requirements.

ANONYMITY (Data Visible, Identity Hidden)



→ ANONYMITY

With anonymity, privacy moves from hiding the data to hiding the participants. This is also the mode where organizations often question implementation. Anonymity can sound like the opposite of compliance.

But it doesn't have to. Anonymity is not inherently suspicious. After all, it's how cash, voting, and sending a letter through the mail without a return address all work today. Much of the world has long recognized that people have a legitimate need to act without being identified.

The question for most teams becomes: can their app provide anonymity … while still meeting regulatory obligations?

[3]Note that Confidential Balances, per the expected behavior for anonymity, do not hide transaction timing or the identities of transacting parties.

In December 2025, SEC Chair Paul Atkins addressed this question directly at the Crypto Task Force Roundtable on Financial Surveillance and Privacy.

> *"This technology allows for privacy-preserving tools that the analog world could not provide, such as zero-knowledge proofs, selective disclosure, and wallet designs that allow users to prove compliance without handing over their entire financial history or personal details to intermediaries or to the government."*
>
> **Paul Atkins,**
> SEC Chair, Crypto Task Force Roundtable, December 15, 2025

Atkins warned that if regulators "treat every wallet like a broker, every piece of software as an exchange, every transaction as a reportable event," the result would be a "financial panopticon." The government's appetite for surveillance data, he said, is **"obviously—and fundamentally—incompatible with the kind of free society that has made America great."**

The simple truth is privacy-preserving technology and regulatory compliance can co-exist, and they have to for institutional adoption on blockchain to be scalable.

USE CASE:

Anonymous Charitable Donations

A donor wants to support a charity without revealing identity. The charity receives the funds and can verify that the donation was legal, but the donor's identity remains hidden on the public ledger.

Native to Solana

Yona allows users to trade SOL and other tokens privately through Jupiter, Solana's leading DEX aggregator, using a shielded pool. The trade is untraceable by external observers, who can see that the swap happened, but not who executed the trade. Using zero-knowledge proofs, transactions can be validated without exposing amounts or participants.

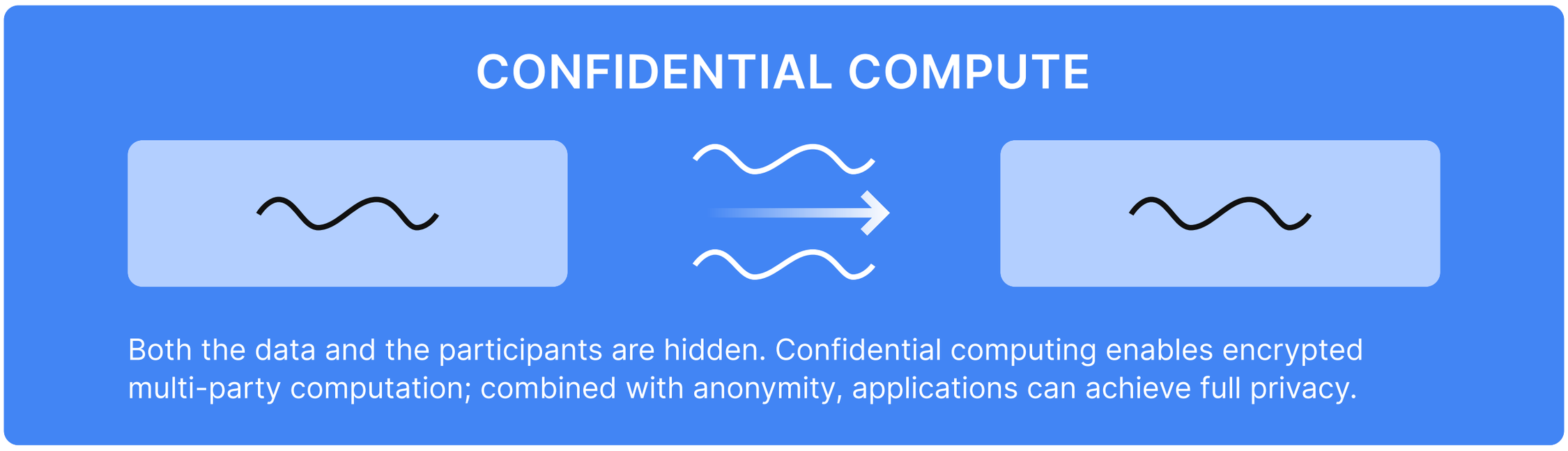
Noctura[4] takes a dual-mode approach with its wallet so that users can decide what mode of privacy they need:

- **Transparent Mode:** Assets interact normally with standard Decentralized Finance (DeFi) protocols. Noctura has full composability with lending, trading, and liquidity provision across the Solana ecosystem.
- **Shielded Mode:** Assets are anonymized. Transactions become untraceable on the public ledger.

[2]Identity here refers to onchain address, not necessarily real-world identity

Both Noctura modes are compliance-first. Users can generate audit trails and compliance documentation to prove transaction history to a regulator, even for shielded transactions. Both of these protocols show how composability is key on Solana. Applications and users can lend on a DeFi protocol in transparent mode, earn yield, then re-shield assets upon withdrawal. Privacy and DeFi coexist on Solana.

FULLY PRIVATE (Data Hidden, Identity Hidden)



⟶ FULLY PRIVATE

Much of the financial system depends on collaborative computation using private data: credit checks, fraud detection, portfolio risk aggregation, order matching. In all of these cases, the parties need the output of a shared calculation—but don’t want to reveal their inputs.

And in many cases, the parties don't want to reveal themselves either. A bank contributing exposure data to a cross-institution risk calculation needs to hide both its numbers and its identity. A trader placing an order in a dark pool needs the order to execute without anyone knowing the size, the price, or who placed it.

Fully private applications hide both: what was computed and who computed it.

Achieving full privacy (hiding both the data and the participants) requires adding confidential computing to the above mode of anonymity. Solana's composable architecture makes this possible: a confidential computation can accept inputs submitted through an anonymity layer, producing a system where neither the data nor the participants are exposed.

And Solana’s speed makes this all practical for the first time. Previously, privacy computations were too expensive to be practical. ZK proofs take time to generate, and multiparty computation requires coordination rounds. On traditional flows, this overhead slows down the transaction to the point where it’s impractical. But Solana’s sub-second confirmation speed changes this. On Solana, privacy proofs can be verified at speeds nearing standard web requests.

USE CASE:

Cross-Bank Credit Scoring & Fraud Detection

Three banks need to determine whether a shared client is over-leveraged. Each bank holds a portion of the client's debt, but none can legally or competitively share their loan books with the others.

With confidential computing, all three contribute their encrypted exposure data to a multiparty computation. The result (total client leverage) is revealed to all three. But the individual inputs from each bank are never exposed.

USE CASE:

Dark Pools

An institutional trader needs to place a large buy order without the market seeing the order size or price limits. On a transparent order book, high-frequency bots detect pending large trades and front-run them for profit. In a confidential order book, however, orders are matched inside an encrypted environment. The trades execute, the prices are fair, no outside observer can see the order details. Combined with anonymity tools, the identity of who placed the order is also hidden.

Native to Solana

Solana's ecosystem offers multiple paths to fully private mode. The following protocols provide the confidential computing foundation. Combined with anonymity-layer tools like Yona or Noctura, they enable fully private applications.

Contra, built by the Solana Foundation, uses a private execution environment running the Solana Virtual Machine. This provides privacy through restricted access rather than cryptographic computation. With Contra, institutions get private transaction ordering, no public mempool, zero per-transaction fees within channels, and customizable access controls. The final settlement states publish to Solana mainnet as public data.

Arcium operates a decentralized confidential computing network using MXEs (Multiparty eXecution Environments) that run MPC protocols for confidential computation.

Bonsol moves heavy computation offchain, generates ZK proofs of execution, and publishes those proofs onchain for verification. Bonsol can prove that a computation was performed correctly without requiring validators to re-execute it. For full input confidentiality where no party sees the raw data, Bonsol can be combined with encryption or MPC.

Encrypt brings Fully Homomorphic Encryption (FHE) to Solana, enabling computation on encrypted data without ever decrypting it. Unlike MPC, FHE requires no coordination between parties. A single party can process encrypted inputs and produce encrypted outputs.

MagicBlock creates Trusted Execution Environment (TEE)-secured ephemeral rollups using Intel Trust Domain Extensions (TDX)—temporary, high-speed, offchain validators that process transactions inside hardware-secured enclaves, then sync results back to Solana.

MagicBlock relies on hardware attestation rather than mathematical proof, which carries different trust assumptions than ZKP-based approaches. In this way, MagicBlock can enable hardware-attested confidentiality for order books, payment rails, and high-frequency applications. It allows privacy to be added to any existing Solana program without code rewrites.

Table: Confidential computing on Solana

Protocol	Technology	Key Use Cases
Arcium	MXEs	Dark pools, sealed auctions, C-SPL tokens, private lending
Contra	Private execution environment (Solana Foundation)	Private payment channels, institutional settlement
Bonsol	ZK proofs (mathematical verification)	Heavy/private computation with onchain proof verification
MagicBlock	TEE ephemeral rollups (Intel TDX)	Confidential order books, real-time trading, gaming

Compliance in Every Mode

A common concern with privacy is ensuring that solutions meet regulatory requirements. Solana has built-in compliance mechanisms that address three core regulatory requirements: the Travel Rule, OFAC sanctions screening, and auditability.

The table below maps how Solana addresses each requirement across the four modes of our matrix.

Table: Compliance on Solana at each mode

	Pseudonymity	Confidentiality	Anonymity	Fully Private
Travel Rule	Travel rule data is transmitted via a separate VASP-layer. A memo in the transfer can include an ID or encrypted information for further verification.	Auditor keys let compliance teams verify amounts against thresholds.	Selective disclosure provides post-transaction auditability. Real-time Travel Rule transmission requires additional VASP-layer integration or onchain shared encryption scheme within memos.	Combination of auditor keys and selective disclosure. ZK proofs, MPC or TEEs could be used to prove whether the transaction is subject to travel rule requirements.
OFAC Screening	Pseudonymous addresses screened against SDN list; SAS (Solana Attestation Service) links verified identity.	Addresses remain visible. Standard SDN screening applies.	Pre-transaction screening is not natively supported onchain. Offchain compliance tooling required.	Depends on protocol, ranges from full screening (Contra) to application-defined (Arcium).
Aduitability	Onchain transaction graph fully visible.	Onchain transaction graph visible. Full transfer amount history available via auditor key.	Post-transaction auditability via selective disclosure.	Application-defined audit mechanisms.

Note: Institutions should evaluate each mode's compliance tooling against their specific regulatory requirements.

The Privacy Decision

Privacy is a market requirement. Customers expect it and applications require it.

On Solana, you choose your privacy level, from encrypted balances to zero-knowledge anonymity to multiparty confidential computing. Each level maps to a compliance path, and each is composable with the broader ecosystem. The privacy stack is here. The next step is choosing where your applications belong.

For more information and to get started building today visit
launch.solana.com/products/contra

Disclaimer

The information contained in this material, either pertaining to the Solana Foundation (“Foundation”) or otherwise (together, the “Information”), is for general informational purposes only and does not constitute and offer to sell or a solicitation of an offer to buy any securities, options, futures, or other derivatives related to securities in any jurisdiction, nor should not be relied upon as advice to buy, sell or hold any of the foregoing. The information is not and does not contain tax, legal or investment advice or opinion. Foundation and its agents, advisors, council members, officers and employees (the “Foundation Parties”) make no representation or warranties, expressed or implied, as to the accuracy of the Information and Foundation expressly disclaims any and all liability that may be based on such information or any errors or omission therein. This email and the Information is intended only for the persons to whom it is transmitted. The Foundation Parties shall have no liability whatsoever, under contract, tort, trust or otherwise, to any person arising from of related to the Information or any use of the Information by you or any of your representatives.