Retroactive Proposal for Incognitee: Privacy Sidechains on Polkadot Asset Hub

Polkadot Treasury Proposal by Integritee AG (Ref 1518)

Integritee has deployed its privacy sidechain technology on Polkadot Asset Hub.
Try it now at: https://app.incognitee.io

After years of development, our sidechain has been field tested in May 2024 with a public user testing campaign where a total of 200k PAS have been moved by 95 accounts performing 969 shielding and 3291 unshielding actions during two weeks.

In November 2024, we launched our first productive Incognitee Sidechain on Integritee Network with more than 5'000 events until 31.03.2025.

At the end of January 2025, we launched our first productive Incognitee Sidechain on Polkadot Asset Hub with a total of 1000 events and tokens worth more than 25'000 USD shielded to L2.

With this, Integritee has shown that its technology delivers on its goal to enable privacy-enhanced transfers of any fungible token in the Polkadot ecosystem.
We ask the Polkadot treasury retroactively for

171'498 CHF ≃ 201'140 USD ≃ 201'140 **USDT**
(Exchange rate CHF/USD on 7.4.2025 =1.17284)

Table of Contents

Motivation **2**
Work Done **3**
Concept **6**
Compliance 7
Incognitee Feature Overview **8**
Usage Analysis **12**
Roadmap **13**
Future Stages 🏳 14
Soft-Loan Agreement **16**
Payment Conditions **16**

Motivation

Recent regulatory actions regarding privacy-enhancing technology (PET) have led several privacy projects to halt their activities or face sanctions. This situation highlights a polarized perspective where individuals are seen as having either nothing to hide or being potential criminals. The technological debates reflect this polarization, with arguments often favoring either complete privacy or full transparency.

Privacy is a fundamental human need and should be the default, especially for everyday activities. However, there is a societal requirement for mechanisms to reduce privacy when necessary to enforce the law.

Integritee's Incognitee product aims to balance privacy with legal compliance. It ensures privacy by default but implements measures to reduce privacy protections when required by law enforcement, adhering to democratic standards.

The Dotsama ecosystem is highly transparent nowadays. The information, who is transacting with whom and how much, who you nominate, how you vote, and whom you elect to the council is publicly visible to anyone. While this does have its advantages when it comes to accountability, it is not a sound setup for everyday actions.

The inherent linkability of everything that happens on transparent blockchains prohibits a wide range of use cases — or would you really want to disclose personal identity attributes on i.e. KILT in order to gain access to a certain service, if you know that this information can be linked back to your original DOT presale participation and trading history? Or your votes on a controversial topic on any other parachain, linkable through XCM? Follow the money and you'll be able to retrieve a lot of personal sensitive information way beyond token balances.

Because of transaction fees, you can't just start with a new account out of nothing. You need a minimum amount of tokens in order to get active on Dotsama chains — and most blockchains in general. This means you have to send funds from an existing account to your new one. Thereby, you're linking all future events back to that original account with very weak deniability. You can use centralized exchanges to make it harder to link both of your accounts by following the money. But the linkable information then resides on that exchanges' servers and is subject to arbitrary access by law enforcement or, occasionally, hackers.

Work Done

All sidechain and dApp code is open source under Apache 2 license and is usable by anyone, on any substrate based chain on Kusama, Polkadot or Solo in unpermissioned manner.

Successful previous proposal:

Work completed from Proposal #617

Concept & Specification Specify a privacy sidechain that can interact with any para-or relaychain without modifying their runtime Artifacts: • Original Proposal with task breakdown • Blog post • Presentation	7 PD (tech spec only)
Preparing to support two light clients in a single enclave into two different substrate-based chains • PR 1288 • PR 1223	14 PD
Shielding and Unshielding with Target Chain Event Listener (to not rely on custom pallets present in runtimes on L1) • PR 1272 • PR 1378 • PR 1502 foreign L1 shield/unshield • PR 1499 CI shard vault • PR 1498 rpc ShardVault	28 PD
Integritee Network Runtime enhancements • PR 201 introduce ShardConfig (incl. Maintenance mode and upgradability)	10 PD
TOTAL	59 PD x 160CHF/h x 8h/PD = **75'520 CHF**

The amount of funds granted was 75'520 CHF ≃ 87'377 US Dollars ≃ **11'655 DOT**

Work completed from Proposal #997

From February-June 2024

Paseo Deployment (move from Rococo to Paseo)	5 PD
Frontend development for user campaign	14 PD
Frontend development demo wallet	9 PD
Immunefi Bug Bounty Setup (excl bounty allocation in TEER)	3 PD
TOTAL	31 PD x 160CHF/h x 8h/PD = **39'680 CHF**

The amount of funds worth the work **39'680 CHF**

Work completed not covered yet by Treasury

From July 2024 - March 2025

Implement Session Keys support for sidechain Improving UX by reducing the number of signing interactions • PR1655	11 PD
Frontend for Session Keys Use role-based session keys to authorize reading balance, reading messages, writing messages or even sending funds. • PR 100	14 PD
Support native and foreign Assets on Asset Hub Customization for assets on Asset Hub systemchain, needed for USDC, USDT, ETH , WBTC aso. • PR 1652 asset hub customizations • PR 1689 shield assets • PR 1703 • PR 1705 USDT.e • PR 1710 ETH + WBTC	29 PD
Frontend development for handling Asset Hub assets • PR 126 • Testing with multiple non-dev people & fixing	9 PD
Implement private messaging using Polkadot address Transactions can have a private note attached (i.e. invoice number). • PR 1642 core functionality • PR 1645 cli + testing helpers	14 PD
Frontend development for private messaging Chat with Polkadot People registry discovery • PR 88 • PR 92	12 PD

Maintenance mode and shard retirement: In an emergency, this allows refunding (unshielding) all assets from L2 back to L1 • PR 1693 • Tests on Paseo	16 PD
Frontend development for vouchers Vouchers are a feature for easy onboarding: Send tokens by sending a url to a temporary wallet. No setup needed • PR 93	4 PD
Immunefi Bug Bounty maintenance and report evaluation	5 PD
Deployment, monitoring setup	15 PD
TOTAL	129 PD x 160CHF/h x 8h/PD = **165'120CHF**

The amount of funds worth the work **165'120 CHF**

Operational Expenses for Incognitee Asset Hub Polkadot

Until 31.3.2025 (More nodes to be added in the near future)

Infrastructure for beta sidechain (minimalistic setup with one failover node). All on OVH: • 1x scale-i1 (SGX, high-performance) 380.66€/mt • 1x advance-1 (SGX, weaker) 80.66€/mt • 1x rise-game-1 (relay node) 75.62€/mt	536.94€/mt x 2mt **1027 CHF**
Infrastructure for staging environment on Paseo Asset Hub (weaker SGX machine on OVH). Charging from one month prior to beta deployment • 1x advance-1 (SGX, weaker) 80.66€/mt	80.66€/mt x 3mt **231 CHF**
Maintenance 16h/mt à 160 CHF/h	2'560CHF/mt x 2mt **5120 CHF**
TOTAL	**6'378 CHF**

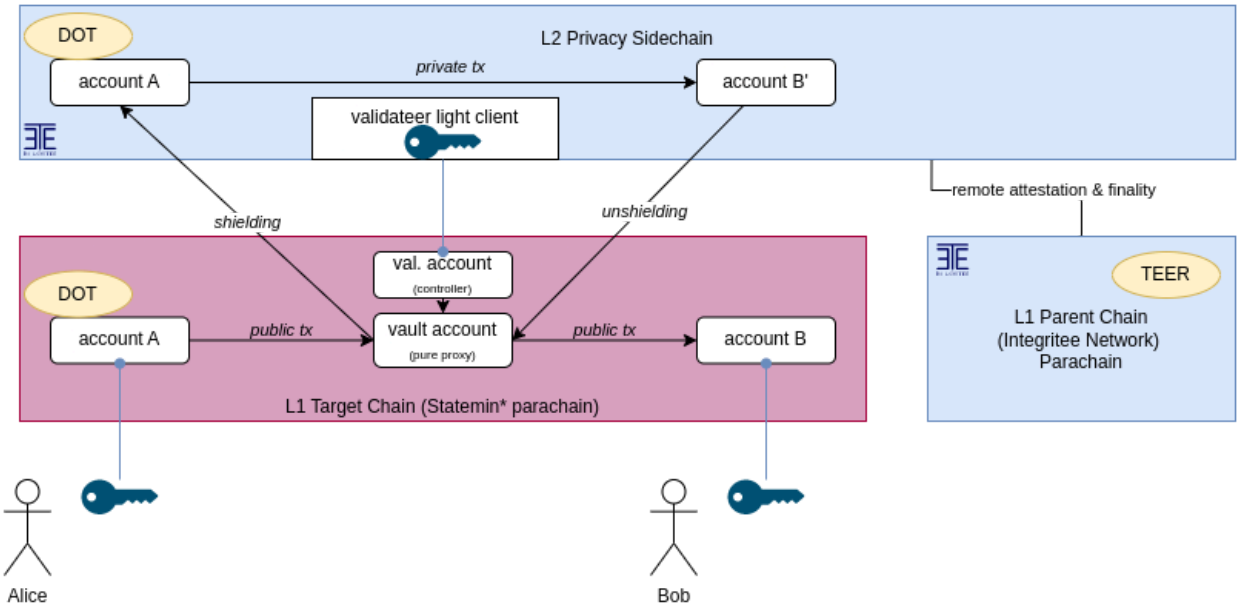
Summary

Total proposed retroactive treasury spend for Asset Hub Polkadot privacy sidechain

Development	165'120 CHF
Operational Expenses	6'378 CHF
TOTAL	**171'498 CHF**

Concept

For context and the bigger vision, we suggest you read our blog article. Here we will focus on the tasks that need to be done based on our SDK to realize Pilot 1 & 2 in our blog.



Alice would like to transfer funds from her account to Bob's privately. She sends DOT tokens to the sidechain's vault account. The sidechain's light client will subscribe to all transfers to its vault account and will endow the sender's account with the amount received. Then, Alice can trigger all kinds of transactions on L2. In our example, she directly transfers tokens from her shielded account to Bob's. Bob can then trigger unshielded tokens to his L1 account. After this process, there is no way to directly link information on L1.
In order to gain practical unlinkability, one has to avoid the linkability of amounts or timing of the process. Mixers can be used to hide the exact time and amount of transfers. This means that the degree of privacy enhancement depends on the number of users that are simultaneously active on our sidechain. The more users sending similar amounts, the better the k-anonymity. Thanks to the Trusted Execution Environments (TEE) technology, not even the operators of the sidechain "validateers" can learn anything about L2 transactions on our sidechains. Validateers are validators operating our second-layer sidechains – the block production and validation happen inside TEEs. This means validateers can trust each other based on remote attestation and the consensus protocol is greatly simplified.

In this example, the fees to be paid by the user are:

1. *Shielding fee* [DOT]: a percentage of the shielded amount plus the extrinsic fee on L1
2. *Private-tx fee* [DOT]: a fixed fee
3. *Unshielding fee* [DOT]: a fixed fee, enough to cover L1 extrinsic fees for unshielding plus markup

Fees to be paid by the sidechain validateers (mostly unrelated to user traffic) are:

1. Remote attestation fee [TEER]
2. Sidechain block finality fee [TEER] depending on block period

Compliance

Incognitee aims for privacy-by-default while being compliant with AML as well as data-protection laws.

During Beta

While in beta, we limit shielding amounts to values inferior to 1000 USD which makes us irrelevant for money laundering attempts and laws.
We do offer higher limits subject to KYC/KYB already during beta phase, which is compliant because Incognitee isn't decentralized yet at this stage

Future Compliance Measures

Once validating Incognitee is decentralized, we need other compliance measures in place which will allow law enforcement access to prosecute money laundering and other criminal activity. Defining the solution to balance requirements of all stakeholders is an ongoing process which we can't pursue alone but needs deliberation and finally ratification. Our current proactive suggestion is outlined here:

https://docs.incognitee.io/compliance

With this, we hope to contribute to a constructive dialogue with society beyond today's web3 community.

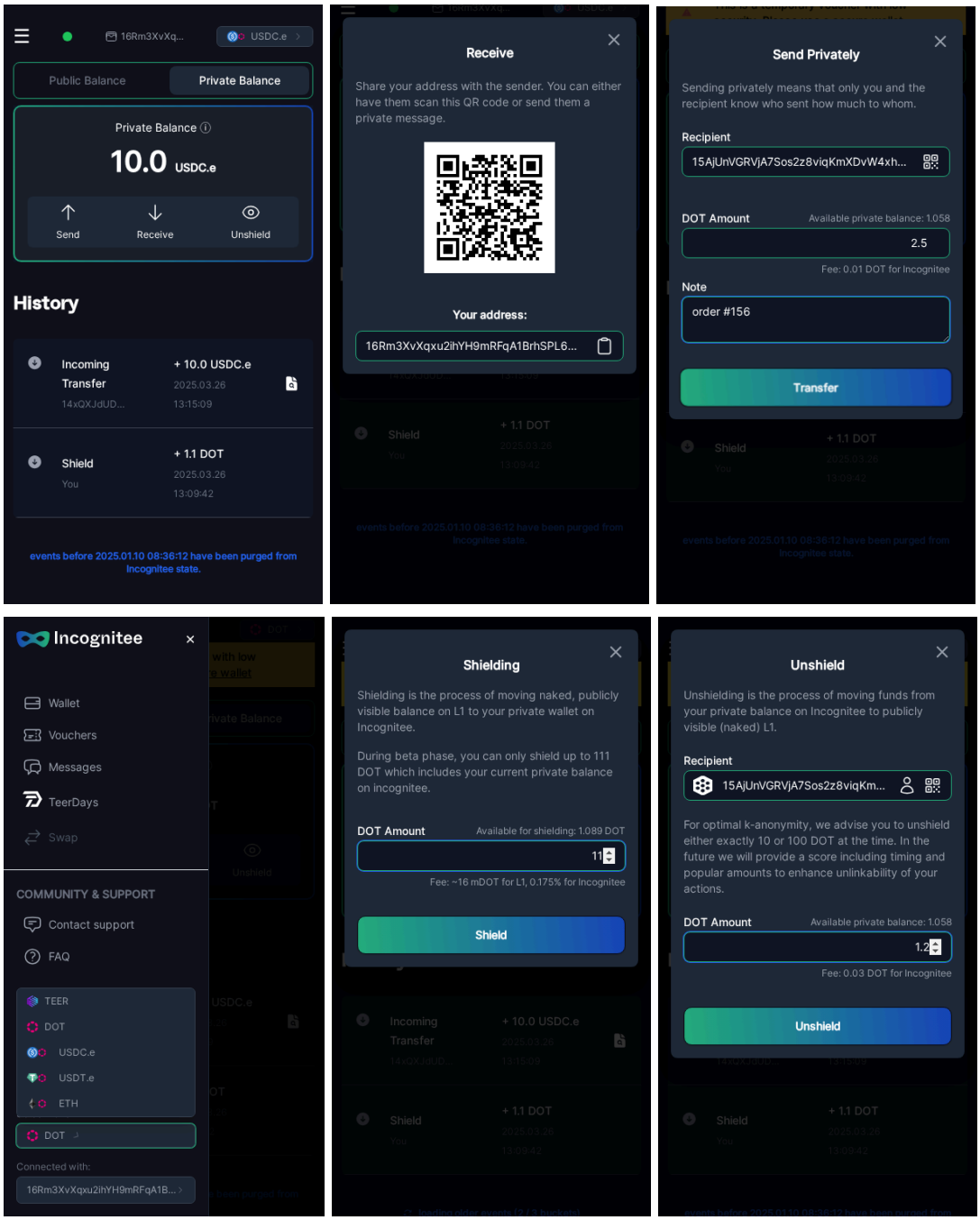
Future Plans

We expect that the sidechain on Polkadot Asset Hub will be self-sustaining through collecting fees in DOT/USDC/USDT at a certain point. Anyone can launch a competing sidechain at that point based on our Apache2 licensed source code and tutorials, so competition is guaranteed. Moreover, we will onboard third party validateers to the sidechains we launch to make our sidechains unstoppable. Also, wallet integrations via API are planned to avoid reinventing the wheel and fractionalizing the wallet landscape.

Incognitee Feature Overview

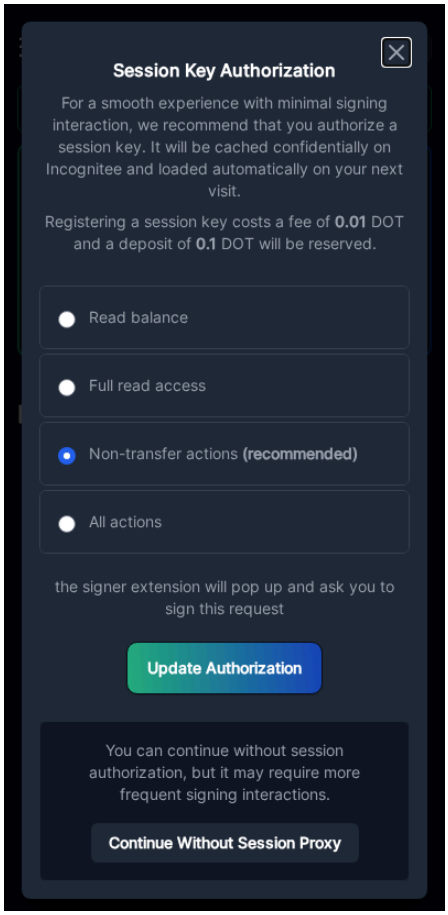
At https://app.incognitee.io

Our current live version handles DOT, USDC.e, USDT.e, TEER and ETH



Basic User Story for DOT

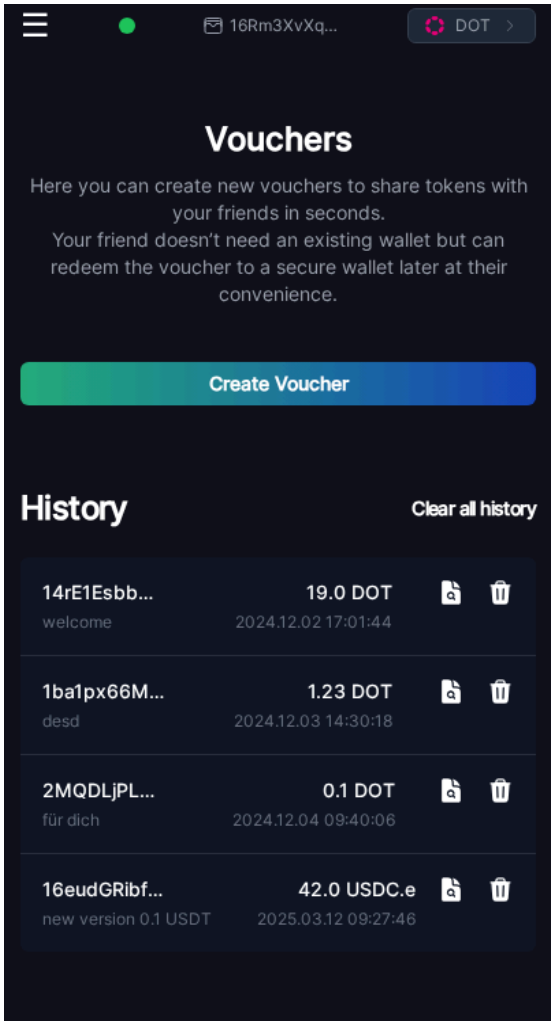
1. When opening the wallet dapp, you will be able to sign in with your favorite wallet as known from other dapps.
2. You can either obtain DOT from exchanges or start right away, but make sure to teleport your DOT from the relaychain to the AH first.
3. By **shielding** the DOT, you are transferring them to the Incognitee private L2.
4. You can **privately send** and receive DOT on Incognitee L2.
5. If you'd like to go back to L1, you can also **unshield** the DOT.

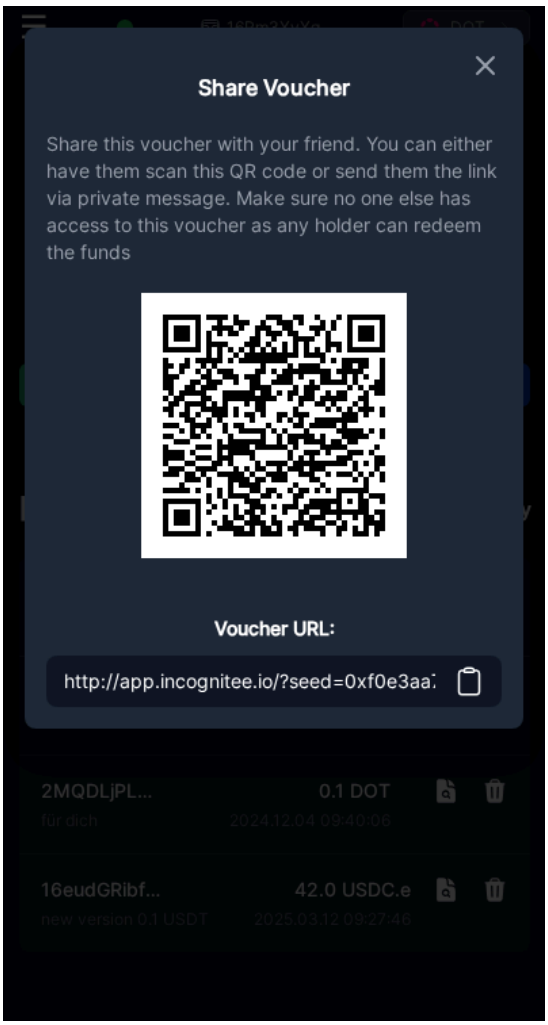


Session Keys improve UX by reducing the necessary interactions with signer extensions. Because everything is private on Incognitee, users must authenticate even for reading their balance. Session keys ensure a smooth experience nevertheless.

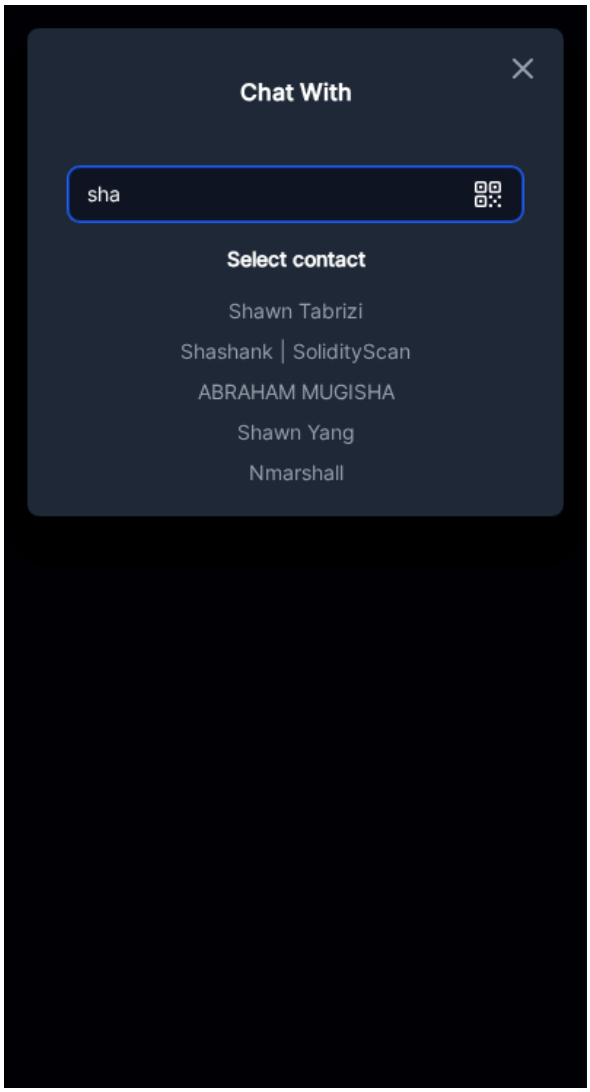
https://docs.incognitee.io/5.-technology/session-proxies

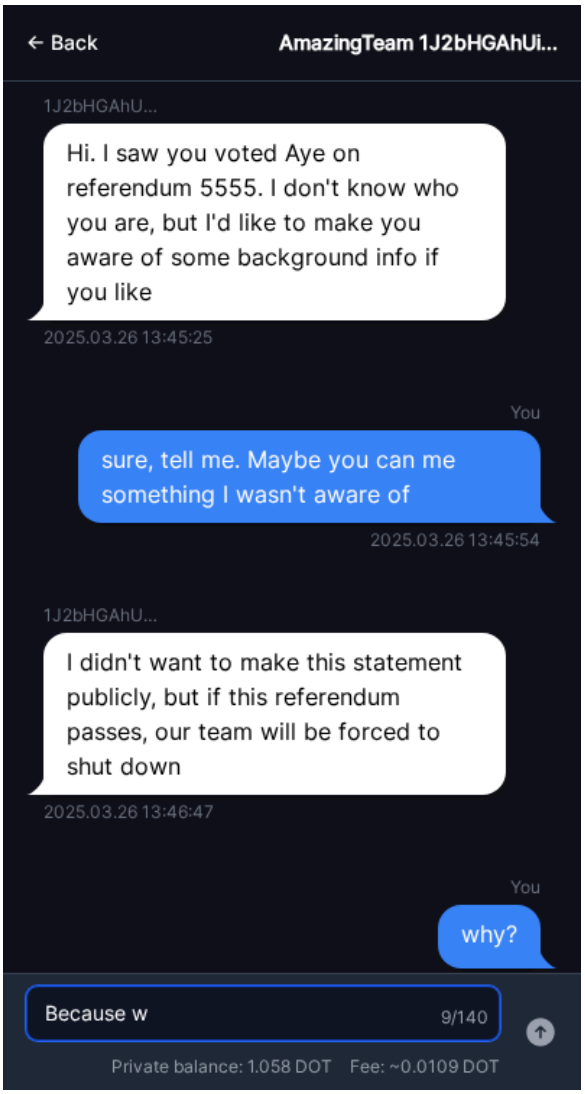
Vouchers allow easy onboarding of people who don’t have a wallet set up already.
https://docs.incognitee.io/5.-technology/vouchers





Private Messaging with other Polkadot accounts. Just enter a Polkadot address or discover by name using the Polkadot People registry and start chatting.
https://docs.incognitee.io/5.-technology/private-messaging





Future planned features:

- Private Governance and Voting
- Private Swaps
- Private AI Chats
- Private AI Agent payments

Usage Analysis

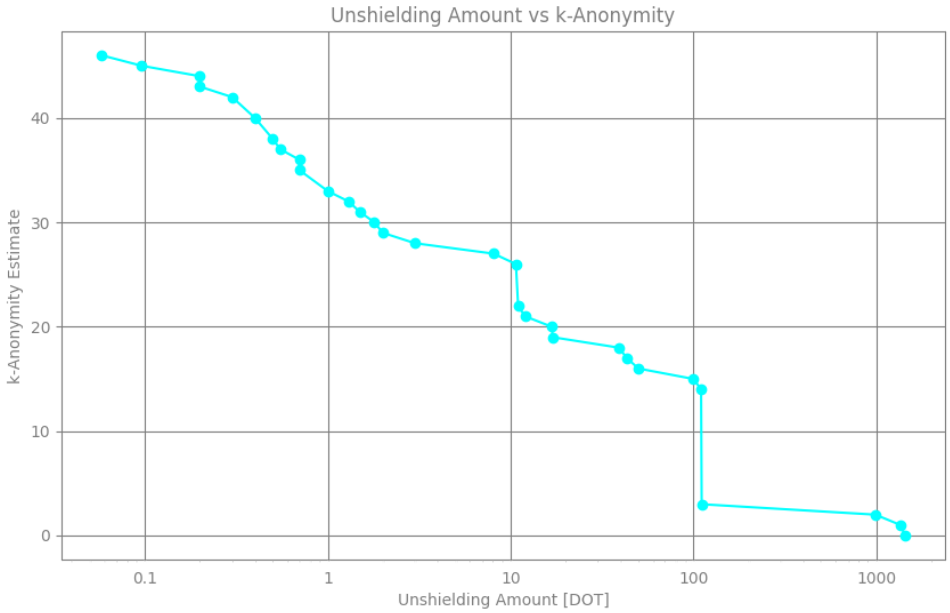
We have successfully launched Incognitee and it is slowly gaining traction, even in its limited beta version. This early phase allows us to gather as much feedback as possible from the community to refine and enhance the product. We're also in discussions with other ecosystem projects for potential integrations, which will further expand its reach and impact.

Publicly verifiable statistics: (from 28.1.2025 until 27.3.2025)

	Shielding events	Total shielded	Unshielding events	Total unshielded	TVL [USD]
DOT	76	5757 DOT	39	649 DOT	23000 $
USDC.e	10	1036 USD	4	5.3 USD	1030 $
USDT.e	6	106 USD	1	2 USD	115 $
ETH	7	0.5033	3	0.0007	1000 $
total	**99**	**-**	**47**	**-**	**25145 $**

Unique accounts: 57
Newly created accounts (when unshielding): 14

All ethereum-bridged tokens are newly supported and didn't see much traction yet.



K-Anonymity for DOT, depending on the amount you'd like to unshield.

One use case of Incognitee is account hygiene, as explained by brenzi in his forum post. We also published an introductory medium article to anonymity in the context of web3.

Roadmap

Stage 1: Prototype of Sidechain on Paseo with simple front-end support ✅
At this stage, we created a functional sidechain running on Paseo which supported a narrow use case to run a public user testing campaign with a specific action flow. A simple web campaign page as UI supported the actions performed by end users. On Paseo, we can already demonstrate the ability to do transfers on L2 fully private.

Stage 2: Fully functional Sidechain deployed on Paseo with a nice UI ✅
At this stage, we were able to demonstrate a fully functional sidechain running on Paseo with a nice UI to perform all the actions necessary to do transfers and check account balances with authentication.

Stage 3: Test Emergency Interventions on Paseo ✅
We ran different emergency scenarios on Paseo to show that recovery is possible and working as designed. Among the scenarios, we put the shard into maintenance mode (temporarily pausing state transitions) and shard retirement (force-unshielding all balances back to L1).

Stage 4: Battle-Test the Basics on Integritee Network ✅
The first productive incarnation is a functional privacy-preserving sidechain for transactions of TEER tokens only. Moreover, at this stage, we will only allow shielding of limited amounts. This is a precaution in the beta phase against both potential loss and legal issues. Limits are set high enough to endow accounts and be active, but low enough to hinder money laundering.

Stage 5: Beta Release on Polkadot Asset Hub ✅
After successful operations on the Integritee Network, we will deploy Incognitee on Polkadot Asset Hub. This will enable not only the support for DOT and also for other Parachain tokens on Assethub.

Stage 6: API Integration ✅
Our sidechain API can be already used to integrate with other dapps in the ecosystem.
The integration guide can be found in our docs for interested teams.

Stage 7: Sidechain Governance, Nomination, and External Validateers ⏳
We will soon introduce a Sidechain Governance mechanism that will allow a decentralized governance of several Incognitee sidechains independently from Integritee Network. Additionally, we will open up the permissionless operation of TEE-based Validateers for Incognitee sidechains with nominations from token holders. This will allow the distribution of Incognitee fees collected from operations in a decentralized way.

Stage 8: Security Audit 🏳️
Our implementation will be audited by a specialized and independent team before lowering the limitations of the beta version.

Future Stages 🏳️

Remove Limitations and add new features
Finally, we will remove certain limitations and add other features like private voting on Polkadot and Kusama and private token swaps.

API Integration
At this point, our sidechain API will be compatible with js/api json-rpc, and integrate well with established wallets. This may involve upstreaming our authentication procedure for queries, so we will be looking for collaborations with wallet teams to make private transactions as smooth as can be.

Release for other ecosystems
We are planning to expand to other ecosystems and offer the Incognitee solution to a broader user base.

Enabling Law Enforcement Access
We shall allow law enforcement to request selective disclosure of certain data concerning certain accounts. A governance process needs to be specified to ensure due auditing.

Snowbridge integration
We already leverage Snowbridge to bridge over assets from Ethereum like ETH, USDC, USDT and WBTC. But we want to improve the user experience and therefor directly integrate the bridging process into Incognitee via API.

AI private inference & payment
A new feature should allow Polkadot users to use AI services like ChatGPT or other LLMs with private crypto payments to overcome linkability between service usage and payment for the service in a first phase. In a second phase we would even extend this to offer private Inference.

AI Agents private payments
Our cutting-edge technology is uniquely designed to serve as the foundation for private transactions between AI agents, ensuring a decentralized, highly secure, and completely private payment infrastructure.

Soft-Loan Agreement

We do consider this a soft-loan which we will pay back to the treasury with a fraction of fee revenues which each shard of Incognitee earns as long as the target token is present on the Polkadot Asset Hub and can be spent by the treasury. **We commit to sending 30% of our gross fee revenue back to the treasury** automatically and regularly until we have repaid the soft-loan plus a **one-off premium of 10%.**

We will propose further soft-loans before having paid back this one. In that case, the payback target will simply be increased accordingly.

The payback logic will be hard-coded in Incognitee enclaves published by Integritee. This way we can ensure that the rules for payback are enforced without a choice left to 3rd party validateer operators.

Payment Conditions

This proposal requests the amount in USDT stablecoin.

The beneficiary address shall be: `14xQXJdUDC1pzyt8y3z27ANiUBgP7zTSaYutaLELJoyQrdLP (INTEGRITEE)`

owned and controlled by:

Integritee AG
Technoparkstr 1
8005 Zürich
Switzerland
CHE-311.131.116