1RPC

Web3 relay that protects users from the exposure and harvesting of their personal metadata. RPC serves as the gateway that unites off-chain users with the on-chain universe. As data, including queries and transactions, pass through this gateway, machine-level metadata, such as IP addresses, device information, and timestamps, are appended, making them transparent to providers.

The rise in Account Abstraction adoption has broadened visibility into the intent of UserOps, which are the potential state transition pathways implemented to execute user transactions. Providers can now identify these intentions and assist with transaction finalization and delivery.

Currently, the combination of intent and transaction accounts only form a marginal portion of the requests coursing through RPC. The majority of requests are merely queries or "signals" showing your latent activity related to a specific wallet or smart contract. As AI improves in prediction, these "signals" expose potential vulnerabilities to providers keen on predicting your future intentions or transactions. This scenario echoes the Web2 environment, notorious for enormous data harvesting and collection by centralized entities.

1RPC harnesses secure enclaves as an RPC proxy between clients and RPC providers. This system ensures robust integrity and privacy, guaranteeing that no metadata will be stored by the operator nor communicated to the RPC providers. Anyone can validate this guarantee through an attestation process that evaluates the complete stack of hardware and software implemented in the system.

1RPC has protected over 20 billion relays and has over 10 million monthly active users , with a one-click connection supporting 50+ networks.

Private RPC Relay vs. Self-hosting Node

The primary cause of RPC privacy issues is the escalating reliance on RPC providers as opposed to utilizing self-hosted blockchain nodes, a more decentralized approach. The growing complexity and burgeoning costs associated with owning a blockchain node, be it an extensive full node with a complete set of data or a lightweight node housing only the latest data, have largely contributed to this trend.

Given that all data is stored and managed locally, the risk of metadata exposure is mitigated. Although metadata may still be revealed to other peers via transaction broadcasting, this risk is considerably less than direct connections to endpoints of centralized RPC providers.

Since only a select number of users possess the ability to self-host nodes, a relay model has been introduced. This model provides a more pragmatic and economical solution to users. From a user’s perspective, there is little to no difference between employing a RPC relay and connecting directly to RPC providers. The relay operates with full transparency in transmitting payload information (minus metadata) and only introduces minuscule overhead by adding one more step in the connection process.

RPC Relay with and without Secure Enclave

Numerous open-source implementations of RPC relays exist, many of which support JSON-RPC, a widely adopted RPC standard by many blockchains. In addition, they also support generic HTTPS, WebSocket, and several others. Establishing an RPC relay service that assures users no data will be collected is certainly achievable. However, this traditional model lacks a measurable and provable guarantee that users can verify.

A considerable enhancement would be to run the relay within a secure enclave. This type of technology, used to protect sensitive personal information on mobile phones, is often referred to asTEE or Trusted Execution Environment in server-side applications. By leveraging Secure Enclave technology, several vital properties beneficial to RPC users can be achieved:

- End-to-End Encryption
- : This allows for an industry-standard TLS connection to be established between the user and the enclave, as well as between the enclave and the RPC providers, without compromising the secure protections that prevent network-level eavesdropping.
- Code Integrity and Zero Tracking
- : The code executed within the secure enclave can be measured and demonstrated to users with high verifiability, thus ensuring strict adherence to the privacy-preserving design of the RPC relay. When coupled with full attestation from open-sourced software or hardware implementations and reproducible builds, users can be confident that they are connecting to a genuine RPC relay.
- Private Execution
- : The handling of user requests cannot be monitored by the relay node operator because the secure enclave provides an isolated execution environment. This ensures that even a malicious operator cannot view the execution or read the memory region that holds the sensitive data for each request.
-

Attestation Enabled by Automata 2.0

The implementation of Private RPC Relay requires two main types of attestations.

Attestation on Software Build

The build has to create a reproducibleMRENCLAVE value when rebuilding the code in a base builder docker hosted in AWS Nitro Enclave. Find more details inSoftware Build Attestation .

Because the whole compilation is reproducible and the attestation is provided by the builder docker which is already attested by the AWS Nitro Enclave, we leverage the root of trust from the AWS Nitro Enclave and choose optimistic attestation, which does not provide a challenge method during this attestation.

Attestation on Hardware

Currently, 1RPC is hosted in Azure, which usesIntel DCAP to complete the TEE attestation, ensuring that the hardware execution environment and the running code are matched as expected.

Since the Intel DCAP Quote verification is quite complicated and will incur significant gas fees, we choose to use consensus-based attestation which invites certain trusted parties' attestors to validate the correctness of the quote uploaded by the1RPC server.

Previous Attestation Report Next L2Faucet Last updated2 hours ago

Was this helpful?