Hyperledger AnonCreds

Key Characteristics

AnonCreds ZKP verifiable credentials provide capabilities that many see as important for digital identity use cases in particular, and verifiable data in general. These features include:

- A full implementation of the Layer 3 verifiable credential “Trust Triangle” of the Trust over IP Model.
- Complete flows for issuing verifiable credentials (Issuer to Holder), and requesting, generating and verifying presentations of verifiable claims (Holder to Verifier).
- Fully defined data models for all of the objects in the flows, including verifiable credentials, presentation requests and presentations sourced from multiple credentials.
- Fully defined applications of cryptographic primitives.
- The use of Zero Knowledge Proofs (ZKPs) in the verifiable presentation process to enhance the privacy protections available to the holder in presenting data to verifiers, including:
  - Blinding issuer signatures to prevent correlation based on those signatures.
  - The use of unrevealed identifiers for holder binding to prevent correlation based on such identifiers.
  - The use of predicate proofs to reduce the sharing of PII and potentially correlating data, especially dates (birth, credential issuance /expiry, etc.).
  - A revocation scheme that proves a presentation is based on credentials that have not been revoked by the issuers without revealing correlatable revocation identifiers.

AnonCreds was initially part of the Hyperledger Indy project, but has always been largely agnostic to the ledger/data store where AnonCreds objects are stored. The shift of AnonCreds from Indy to being an independent project reflects that reality – that AnonCreds can use any number of platform for the storage of materials needed for issuing, holding, proving and verifying AnonCreds verifiable credentials.

Specification

The current version working draft AnonCreds specification can be found here, along with the related AnonCreds Methods Registry. The AnonCreds Specification Working Group manages the specification and registry in these GitHub repositories: AnonCreds Specification, AnonCreds Methods Registry.

Implementations

There is a currently one Rust implementation of AnonCreds in the project, with wrappers for use in other languages.

Communication

Mailing List

Information about the mailing list for Hyperledger AnonCreds is available here: https://lists.hyperledger.org/g/anoncreds, including guidance on subscribing to the list and access to the mailing list archives.

Discord Chat (for questions and ephemeral discussions)

We encourage anyone interested in Hyperledger AnonCreds to join the Hyperledger Discord (here's an invitation to join), and go to the main AnonCreds channel. You'll find a friendly community and lots of people happy to answer your questions!

Meetings
History

Hyperledger AnonCreds was accepted as project at the Hyperledger Foundation in October, 2022. However, AnonCreds within Hyperledger dates back to the the start of the Hyperledger Indy project in 2017. The motivation in taking AnonCreds out of the Indy project was to simplify the technology for use beyond Indy, enabling its use with any public data storage mechanism—making AnonCreds “ledger-agnostic.” Any Verifiable Data Registry (VDR) that allows an issuer to publish the necessary objects such that holders and verifiers can access (resolve) those objects, supports AnonCreds. That definitely includes Indy (of course!), but that also allows others to take advantage of the extremely important privacy-protecting capabilities of AnonCreds independent of an Indy ledger implementation.

The history leading to AnonCreds goes back much further than Indy, tracing back (at least) to pioneering “blind signatures” work published by famed “e-cash” cryptographer David Chaum in 1983. Jan Camenisch and Anna Lysyanskaya (the “CL” of “CL-Signatures” in AnonCreds) published their academic papers on the underlying algorithms in AnonCreds starting in 2001, taking ZKP capabilities from ideas to reality. Between then and the 2016 creation of Indy, there was at least one other full implementation of the CL-Signatures cryptography in an IBM product called IDMixer. And in 2022, after 5+ years as a key component of Indy, AnonCreds was accepted as standalone project at Hyperledger, available for use in conjunction with Indy and with many other types of ledgers, blockchains and even centralized databases or file systems.

Recent space activity

Stephen Curran
2024-05-20 AnonCreds Working Group Meeting updated May 20, 2024 view change
2024-05-13 AnonCreds Working Group Meeting updated May 13, 2024 view change

Ry Jones
Hyperledger AnonCreds updated Apr 23, 2024 view change

Space contributors

- Stephen Curran (16 days ago)
- Ry Jones (43 days ago)
- Steve McCown (44 days ago)
- Sean W. Bohan (121 days ago)
- Artem Ivanov (183 days ago)
- ...