Hyperledger Ursa integration into Hyperledger Iroha

Title	Hyperledger Ursa integration into Hyperledger Iroha
Status	PROJECT COMPLETED
Difficulty	MEDIUM

Description

We have an amazing new project Hyperledger Ursa, that is a secure cryptography library for different projects. As the main idea of Hyperledger is to make projects interoperable it would be great to integrate Ursa cryptography into Iroha or/and maybe include Iroha's cryptography into Ursa.

Dictionary

Additional Information

https://www.hyperledger.org/blog/2018/12/04/welcome-hyperledger-ursa - introduction to Ursa

https://github.com/hyperledger/ursa - Ursa repository, https://github.com/hyperledger/iroha - Iroha repository

https://github.com/hyperledger/iroha/tree/master/shared_model/cryptography - Cryptography in Iroha

https://iroha.readthedocs.io/en/master/ - Iroha Documentation

Learning Objectives

The intern will get guided by Iroha maintainers and contributors, that are ready to share their extensive knowledge obtained over years of research in cryptography and blockchain

They will be able to create a link between different projects that reflects the global tendency of cooperation and focus on interoperability including the idea of open-source development

Expected Outcome

Ursa library can be used in Iroha or Iroha cryptography could be included into Ursa libraries

Relation to Hyperledger

Hyperledger Iroha, Hyperledger Ursa

Education Level

Any.

Skills

Basic engineering skills, C++ and Rust experience.

Future plans

Continue integrating Ursa into other projects and use it in Iroha

Preferred Hours and Length of Internship

Part-time (full-time is also possible with some additional tasks).

Mentor(s) Names and Contact Info

Andrei Lebedev, andrei@soramitsu.co.jp, Soramitsu

Mentee Name and Contact Info

Alexander Matson, Alex Matson, City College of New York, alex@alexmatson.com

Project Plan

Deliverables

- [x] Integrate Ursa with the Iroha build system
- [x] Interface with Ursa's ed25519 signing functions
  - [x] Edit docs for Ursa FFI and memory bug fix
  - [x] Wrap Ursa calls in an Iroha crypto provider (expose same interface)
- [x] Integrate Multihash library
- [x] Automatically switch crypto providers depending on public key value

Milestones

- [x] First Quarter: June 3rd, 2019 15 Jul 2019
  - [x] Begin researching integration plans
  - [x] Test Ursa's C interface over FFI
  - [x] Update docs for Ursa's C interface, remedying memory leak bugs
  - [x] Add Ursa as a cmake module within Iroha's cmake system, with build commands
- [x] Second Quarter: July 15th, 2019 26 Aug 2019
  - [x] Add a CryptoProvider for Ursa
  - [x] Set value of `DefaultCryptoAlgorithmType` according to the build flag during compilation
  - [x] Update crypto-related test cases to point to `DefaultCryptoAlgorithmType`
  - [x] Update Ursa C interface with a memory-safe string destructor
  - [x] Research approaches for multihash integration
- [x] Third Quarter: August 26th, 2019 07 Oct 2019
  - [x] Select and integrate a multihash library, plus dependencies
  - [x] Attempt one of integrating multihash with Iroha/Ursa keys – didn't work out
  - [x] Attempt two of integrating multihash with Iroha/Ursa keys – simplified implementation
  - [x] Change the CryptoVerifier to select between CryptoProviders depending on the public key's multihash encoding
- [x] Fourth Quarter: October 7th, 2019 18 Nov 2019
  - [x] Check the loaded keypair is in the ledger
  - [x] First pass at making block signing configurable: add a config file option
  - [x] Second pass simplified the code changes; instead of config file option, automatically sign with the multihash type of the public key
  - [x] Create slides for summary report presentation

Outcomes

1. The ability for Iroha to re-use a common, well-maintained crypto library.
2. Tighter integration in the Hyperledger ecosystem.

Summary Report