Proof of Achievement

As the first milestone, we tasked ourselves with the following:

- Modules for arithmetic circuit generation for a JSON pattern match can be found in the repo
- Modules for checking signatures on HTTPS responses and circuit generation from those checks can be found in the repo

These are two sub-tasks that are key for implementing a prototype of a P2P on-ramp smart contract. The solution is split across many modules. The key ones are:

- https://github.com/zkFold/p2p-onramp/blob/main/src/ZkFold/P2P/Contract.hs
- https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Compiler/ArithmeticCircuit/Combinators.hs
- https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Compiler/ArithmeticCircuit/Instance.hs
- https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Compiler/ArithmeticCircuit/Internal.hs
- https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Compiler/ArithmeticCircuit.hs
- https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Compiler/Arithmetizable.hs

In addition, the first module contains an early prototype of our P2P on-ramp smart contract.

Relevant documentation:

- https://docs.zkfold.io/introduction/what-is-zkfold-symbolic
- https://hackage.haskell.org/package/zkfold-base-0.1.0.0/candidate