ACTUS ZK Rollup

Verifiable Financial Contracts

casper

Morgan Thomas | Mark Greenslade

June ‘23

Introduction

Leveraging DLT to service ACTUS compliant financial contracts is the R&D team's focalising use case. It is an activity well suited to a tightening regulatory environment in which 'crypto' is deemed a regulated activity.

ACTUS algorithms must be formally and operationally verifiable. In respect of operational verifiability, the R&D team is building a special purpose ZK infrastructure to service ACTUS financial contracts at scale.

DLT will be used to publish set of cryptographic proofs encompassing the entire lifecycle of a financial contract. Such proofs include standard constructs such as data fingerprints (i.e. hashes) as well as ZK proofs pertaining to the verifiably correct execution of ACTUS algorithms.

The bedrock of published proofs represents an integrity layer upon which tokenisation & payment systems may be established.

ACTUS ZK Rollup

Solution Elements

API Gateway

ZK Provers

Data Availability

DLT Contracts

Timeline

2023

Q1 Design work begins. Workshops held in Zug.

Q2 Initial team build. Prototyping commences.

Q3 Team extended. Design enhanced. Prototyping continues.

Q4 Test platform established. Engineering commences.

2024

Q1 Engineering continues. SDK development commences.

Q2 Product hardening. Alpha Soft Launch.

Q3 Product hardening. Beta Soft Launch.

Q4 Production Launch.

ACTUS ZK Rollup

Verifiable Financial Contracts

casper

Morgan Thomas | Mark Greenslade

June ‘23

Gateway

Permissioned access to the system will be granted by the API gateway. A set of SDKs will streamline process of interacting with the gateway in the programming language of customer choice.

ZK compute node operators will be able to register with the API gateway, registration incurs a fee. The same applies to data available operators.

ZK Provers

TODO

Data Availability

TODO

DLT Contracts

TODO

Endpoints

ACTUS ZK Rollup Gateway Endpoints I

register-operator

Header
api-access-token

In
operator-info
service-fee-tx

Out
registration-token

Synopsis

1. Validate api-access-token
2. Validate input params
3. Generate registration token
4. Enqueue input params

register-node

Header
api-access-token

In
node-info
service-fee-tx

Out
registration-token

Synopsis

1. Validate api-access-token
2. Validate input params
3. Generate registration token
4. Enqueue input params

get-registration-status

Header
api-access-token

In
registration-token

Out
registration-status
Null | True | False

Synopsis

1. Validate api-access-token
2. Validate input params
3. Query registration store
4. Parse & return query result

ACTUS ZK Rollup

Gateway Endpoints II

process-termset

Header
api-access-token

In
termset-info
service-fee-tx

Out
execution-token

Synopsis

1. Validate api-access-token
2. Validate input params
3. Generate execution token
4. Enqueue input params

get-termset-status

Header
api-access-token

In
registration-token

Out
registration-status
Null | True | False

Synopsis

1. Validate api-access-token
2. Validate input params
3. Query registration store
4. Parse & return query result

ACTUS ZK Rollup

Verifiable Financial Contracts

casper

Morgan Thomas | Mark Greenslade

June ‘23