

# DaDFiR3 Workshop

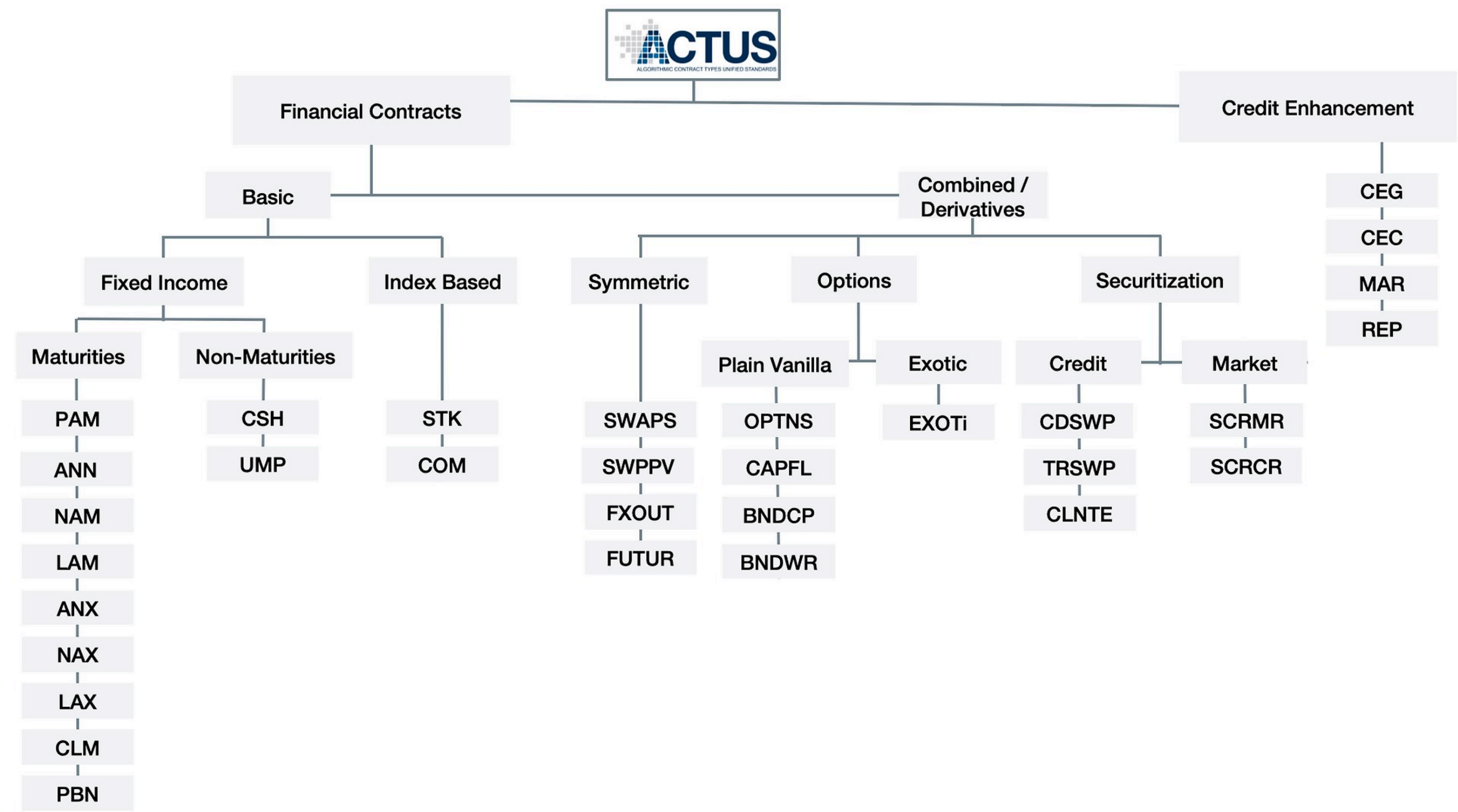
2nd International Workshop on Automated Regulatory Financial Reporting  
Feb '24 University of Zurich

## ZK-ACTUS

## Verifiable Financial Contracts

# Part 1: ACTUS

## An Emerging Financial Standard



**Dictionary**

**Taxonomy**

**Contract**

**Term**

**Term Set**

**Applicability**

**Enum**

**Scalar Type**

**Function Type**

## Algorithms

- **Types**
  - **Utility Functions**
  - **State Transition Functions**
  - **Payoff Functions**
- **Inputs**
  - **Machine readable termsets**
  - **Terms are composable**
  - **Hetereogenous**
- **Output**
  - **Event Sequence (1..N)**
  - **Equivalent to cash flows**
  - **Homogeneous**

**JAVA**

(reference)

**RUST**

(WIP)

**HASKELL**

**PYTHON**

(WIP)

**TYPESCRIPT**

(WIP)

**SOLIDITY**

# Part 2: ACTUS + ZK + DLT

## Verifiable Financial Contracts

**VFC  
Integrity**

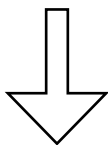
**VFC  
Tokenisation**

**VFC  
Payments**



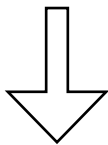
ACTUS

(Counter Parties, Term Set, Algorithm, Cash Flows)



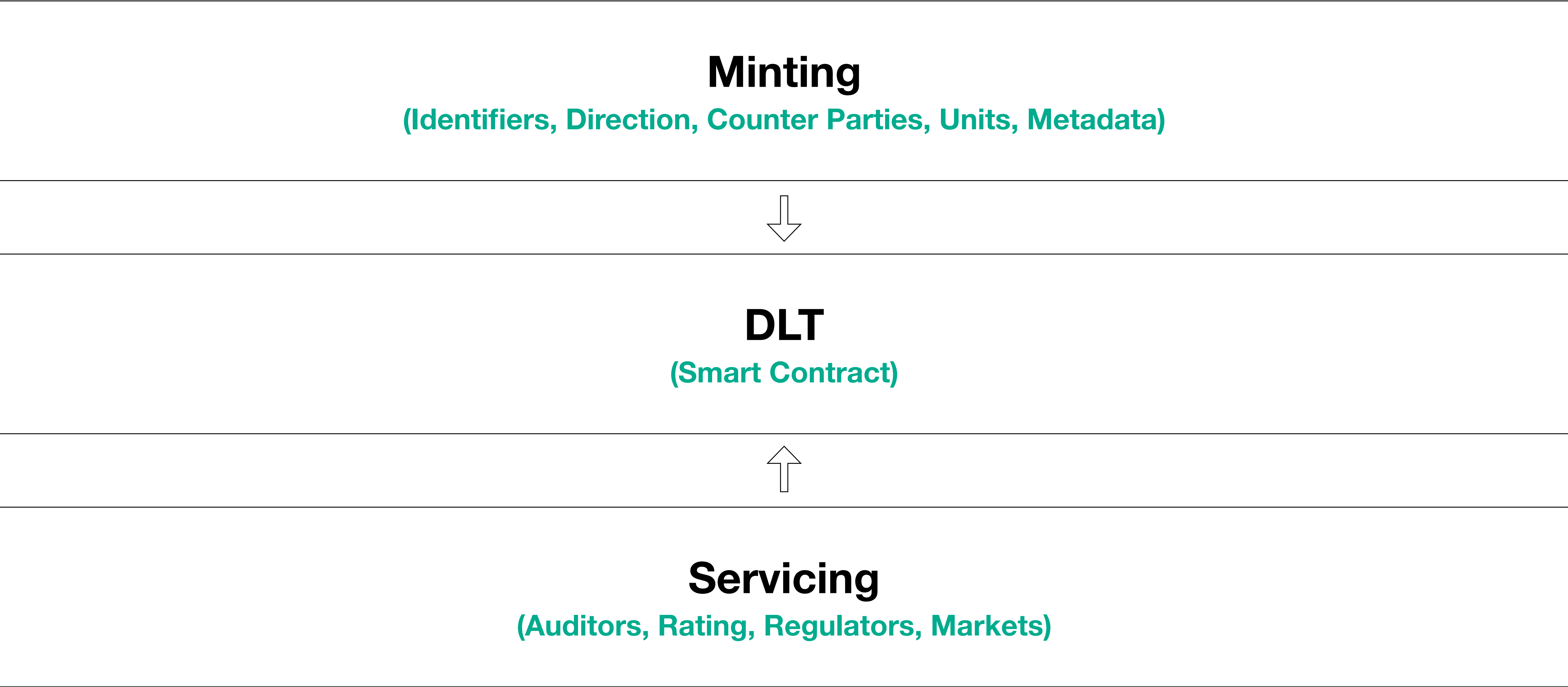
Cryptographic Proofs

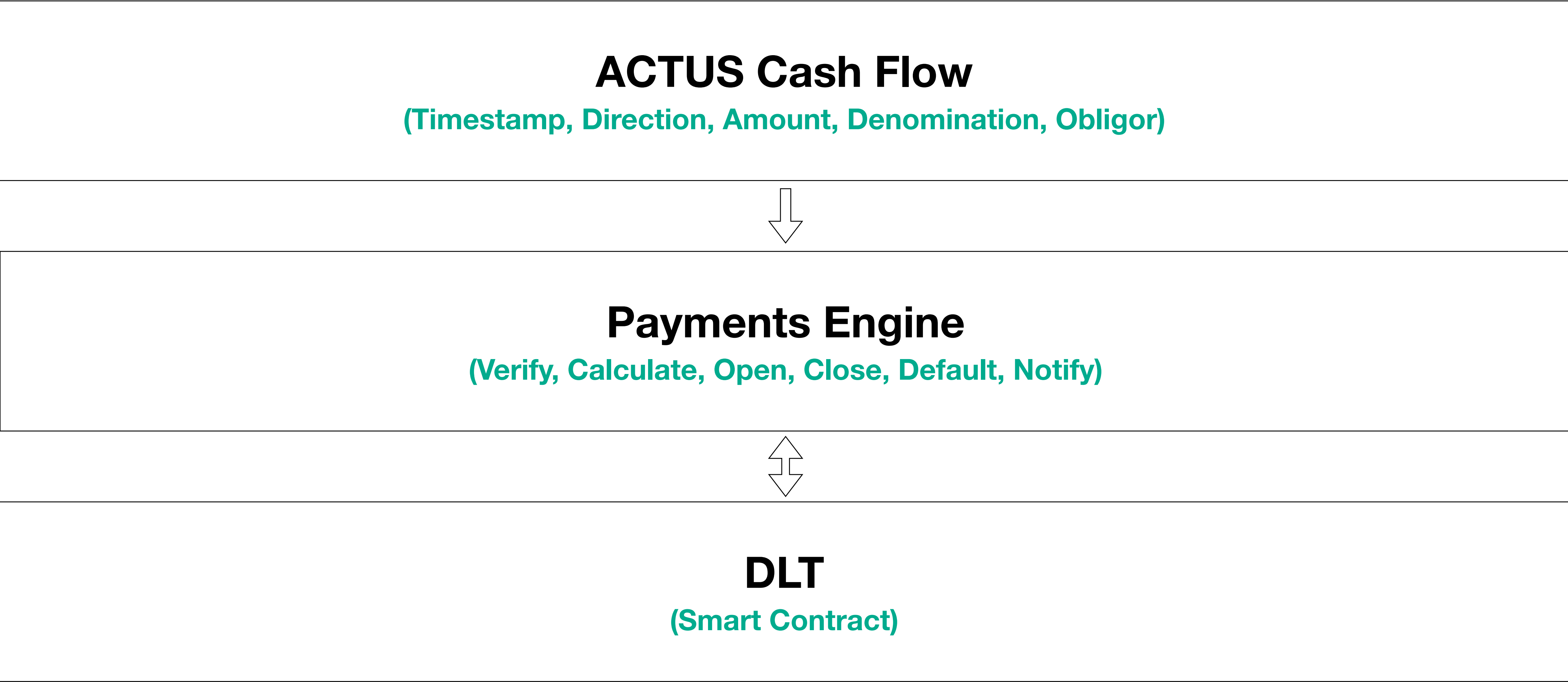
(Signatures, Attestations, Fingerprints, ZK-Proofs)



DLT

(Smart Contract)





## VFC Principles

- **Occams Razor**  
As Little As Possible, As Much As Necessary
- **Chain Agnostic**  
Standard Smart Contracts
- **Privacy Preserving**  
Who, What, When, Why
- **Trust But Verify**  
Cryptographic Proofs Everywhere

## VFC Challenges

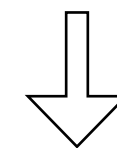
- **Regulatory Certitude**  
Robust. Nuanced. Adaptive.
- **Counter-Party Risk**  
Identity -> KYC/AML. Defaults -> ???
- **Post Quantum Security**  
Cryptography equivalent to Y2K
- **Jurisdictional Anchoring**  
Smart Legal Contracts
- **Technological Flux**  
Multi-Decadal Platforms

# Part 3: ACTUS ZK Proofs

## Computational Integrity

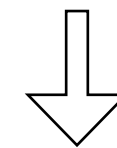
## ACTUS

(Counter Parties, Term Set, Algorithm, Cash Flows)



## Cryptographic Proofs

(Signatures, Attestations, Fingerprints, ZK-Proofs)



## DLT

(Smart Contract)

## ZK-Proofs

$f(x,w) \rightarrow \{\text{True}, \text{False}\}$

## Properties

Succint  
Sound  
Expensive to compute  
Cheap to verify

## Elements

Arithmetic Circuit  
Constraint System  
Polynomial  
Polynomial Commitment

## Developers

Virtual Machines  
E-DSLs  
Rollups  
Applications



# Part 4: ACTUS Gateway

L2 <-> L1 Infrastructure

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.

## Introduction

**API Gateway**

**ZK Provers**

**Data Availability**

**DLT Contracts**

# DaDFiR3 Workshop

2nd International Workshop on Automated Regulatory Financial Reporting  
Feb '24 University of Zurich

## ZK-ACTUS

## Verifiable Financial Contracts