

PKIA 2023

Invited Talk 7

ZK-ACTUS

Verifiable Financial Contracts



Mark A. Greenslade

- **Full stack, clean-code, open-source, polyglot technologist**
- **Chair of the IEEE (CH) Working Group on Decentralised Systems**
- **Member of the Central Bank Research Association**
- **Head of R&D @ Casper Network**



Part 1: ACTUS

An Emerging Financial Standard

actusfrf.org

- **Taxonomy**
- **Technical Specification**
- **Dictionary**
- **Demo Application**
- **Test Fixtures**

Algorithms

- **Inputs**
 - Machine readable termsets
 - Terms are composable
 - Heterogeneous
- **Output**
 - Event Sequence (1..N)
 - Equivalent to cash flows
 - Homogeneous

JAVA

RUST

HASKELL

**PYTHON
(WIP)**

TYPESCRIPT

R

Part 2: ACTUS + ZK + DLT

Verifiable Financial Contracts

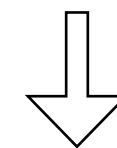
**VFC
Integrity**

**VFC
Tokenisation**

**VFC
Payments**

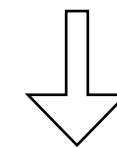
ACTUS

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



Cryptographic Proofs

(Signatures, Attestations, Fingerprints, ZK-Proofs)

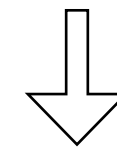


DLT

(Smart Contract)

Minting

(Identifiers, Direction, Counter Parties, Units, Metadata)



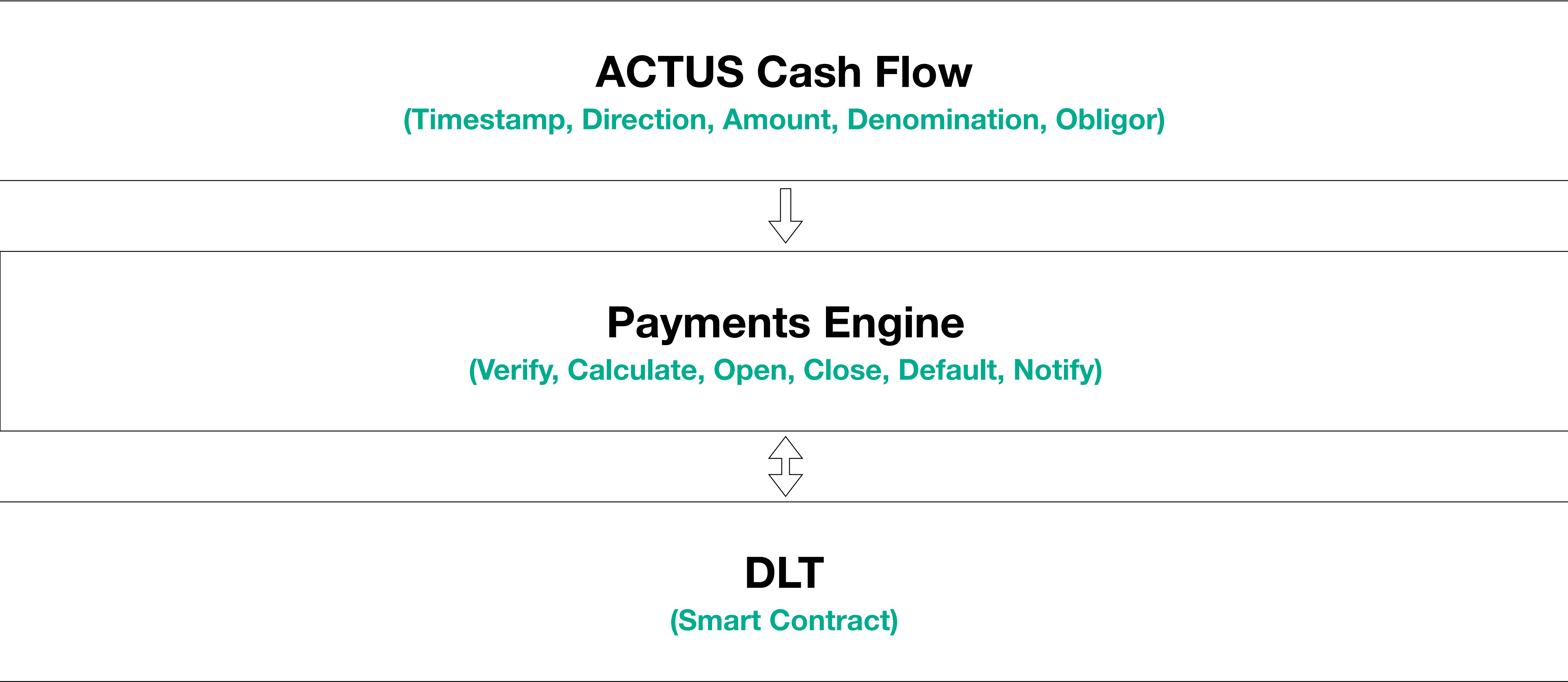
DLT

(Smart Contract)



Servicing

(Auditors, Rating, Regulators, Markets)



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

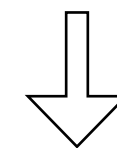
- **Regulatory Certitude**
Robust. Nuanced. Adaptive.
- **Counter-Party Risk**
Identity -> KYC/AML. Defaults -> ???
- **Post Quantum Security**
Cryptography equivalent to Y2K
- **Jurisdictional Anchoring**
Smart Legal Contracts
- **Technological Flux**
Multi-Decadal Platforms

Part 3: ZK Proofs

Computational Integrity

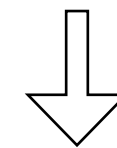
ACTUS

(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

Probabilistic
Succint
Expensive to compute
Cheap to verify

Elements

Arithmetic Circuit
Constraint System
Polynomial
Polynomial Commitment

Developers

Virtual Machines
E-DSLs
Rollups
Applications

PKIA 2023

Invited Talk 7

ZK-ACTUS

Verifiable Financial Contracts

casper

Mark Greenslade September '23