SwissNex - Web3 Synergy

Swiss Consulate | Osaka

ZK-ACTUS

Verifiable Financial Contracts

Mark Conway-Greenslade

Casper Association | IEEE | CEBRA

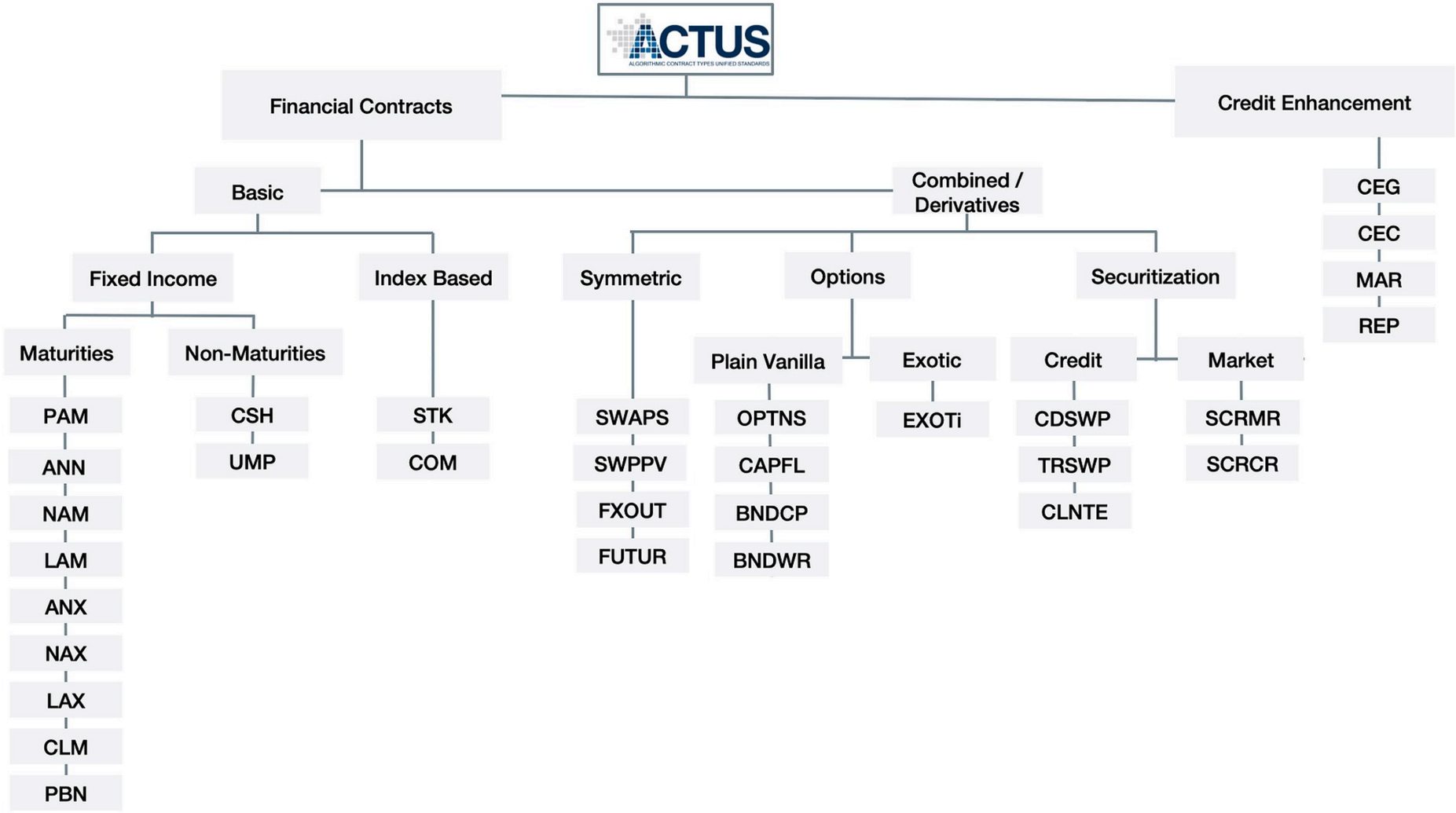
Dr. Willi Brammertz

Ariadne Analytics | ACTUS Foundation

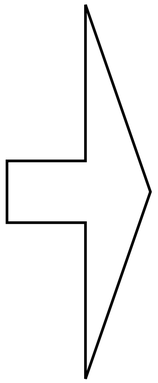
Part 1: ACTUS

An Emerging Financial Standard

actusfrf.org


ACTUS
ALGORITHMIC CONTRACT TYPES UNIFIED STANDARDS
Financial Contracts
Credit Enhancement
Basic
Combined / Derivatives
CEG
CEC
MAR
REP
Fixed Income
Index Based
Symmetric
Options
Securitization
Maturities
Non-Maturities
Plain Vanilla
Exotic
Credit
Market
PAM
ANN
NAM
LAM
ANX
NAX
LAX
CLM
PBN
CSH
UMP
STK
COM
SWAPS
SWPPV
FXOUT
FUTUR
OPTNS
CAPFL
BNDCP
BNDWR
EXOTi
CDSWP
TRSWP
CLNTE
SCRMR
SCRCR

```
{
    "contractType": "ANN",
    "contractID": "ann01",
    "contractRole": "RPA",
    "contractDealDate": "2012-12-28T00:00:00",
    "initialExchangeDate": "2013-01-01T00:00:00",
    "statusDate": "2012-12-30T00:00:00",
    "notionalPrincipal": "  5000",
    "cycleAnchorDateOfPrincipalRedemption": "2013-02-01T00:00:00",
    "nextPrincipalRedemptionPayment": "434.866594118346",
    "dayCountConvention": "A365",
    "nominalInterestRate": "0.08",
    "currency": "USD",
    "cycleOfPrincipalRedemption": "P1ML0",
    "maturityDate": "2014-01-01T00:00:00",
    "rateMultiplier": "1.0",
    "rateSpread": "0.0",
    "fixingDays": "P0D",
    "cycleAnchorDateOfInterestPayment": "2013-02-01T00:00:00",
    "cycleOfInterestPayment": "P1ML0"
}
```


```
{
        "eventDate": "2013-01-01T00:00",
        "eventType": "IED",
        "payoff": "-5000.0",
        "currency": "USD",
        "notionalPrincipal": "5000.0",
        "nominalInterestRate": "0.08",
        "accruedInterest": "0.0"
    },
    {
        "eventDate": "2013-02-01T00:00",
        "eventType": "PR",
        "payoff": "400.8939913786",
        "currency": "USD",
        "notionalPrincipal": "4599.1060086213",
        "nominalInterestRate": "0.08",
        "accruedInterest": "33.9726027397"
    },
    …etc
```


Term Set (ANN)

Algorithm

Event Sequence

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**

Part 2: ACTUS + ZK + DLT

Verifiable Financial Contracts

VFC Integrity

VFC Tokenisation

VFC Payments

ACTUS + ZK + DLT

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)

ACTUS + ZK + DLT

ACTUS Cash Flow

(Timestamp, Direction, Amount, Denomination, Obligor)

Payments Engine

(Verify, Calculate, Open, Close, Default, Notify)

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 + ZK + DLT

ACTUS

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

Cryptographic Proofs

(Signatures, Attestations, Fingerprints, ZK-Proofs)

DLT

(Smart Contract)

ZK-Proofs

f(x,w) → {True,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

Thank You !

SwissNex - Web3 Synergy

Swiss Consulate | Osaka

ZK-ACTUS

Verifiable Financial Contracts