Nomisma | Architecture & Integration Case Study

Confidential

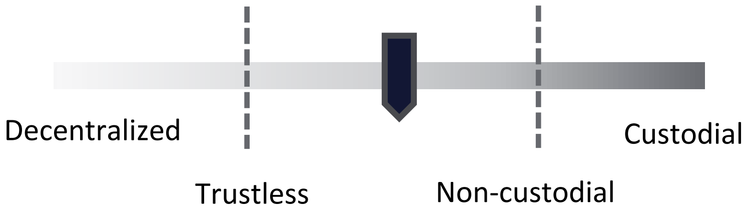
Technology

Nomisma Architecture

- Blockchain Ethos
- Enterprise Grade Performance & Reliability

Trust Continuum Optionality

- Decentralized
- Hybrid ‘trustless’ (described below)
- Non-Custodial but ‘trusted’
- (Any Custody Solution)



‘ Trustlessness’ definition

1. Rule enforcement is not controlled or permissioned by a single entity.
2. Transactions are signed client side.
3. Collateral is held autonomously in escrow, Nomisma does not have access to it.
4. Transparency (where preferred over privacy).

1. Functions which do not pertain to a single entity may be executed by anyone on the blockchain. In executing a function, the step-by-step procedures are pre-determined by Nomisma and immutable once implemented. The functions are also atomic, meaning a function cannot partially execute. When a user ‘executes’ a function, she sends a message to “turn it on” which will then run its predetermined, immutable process.

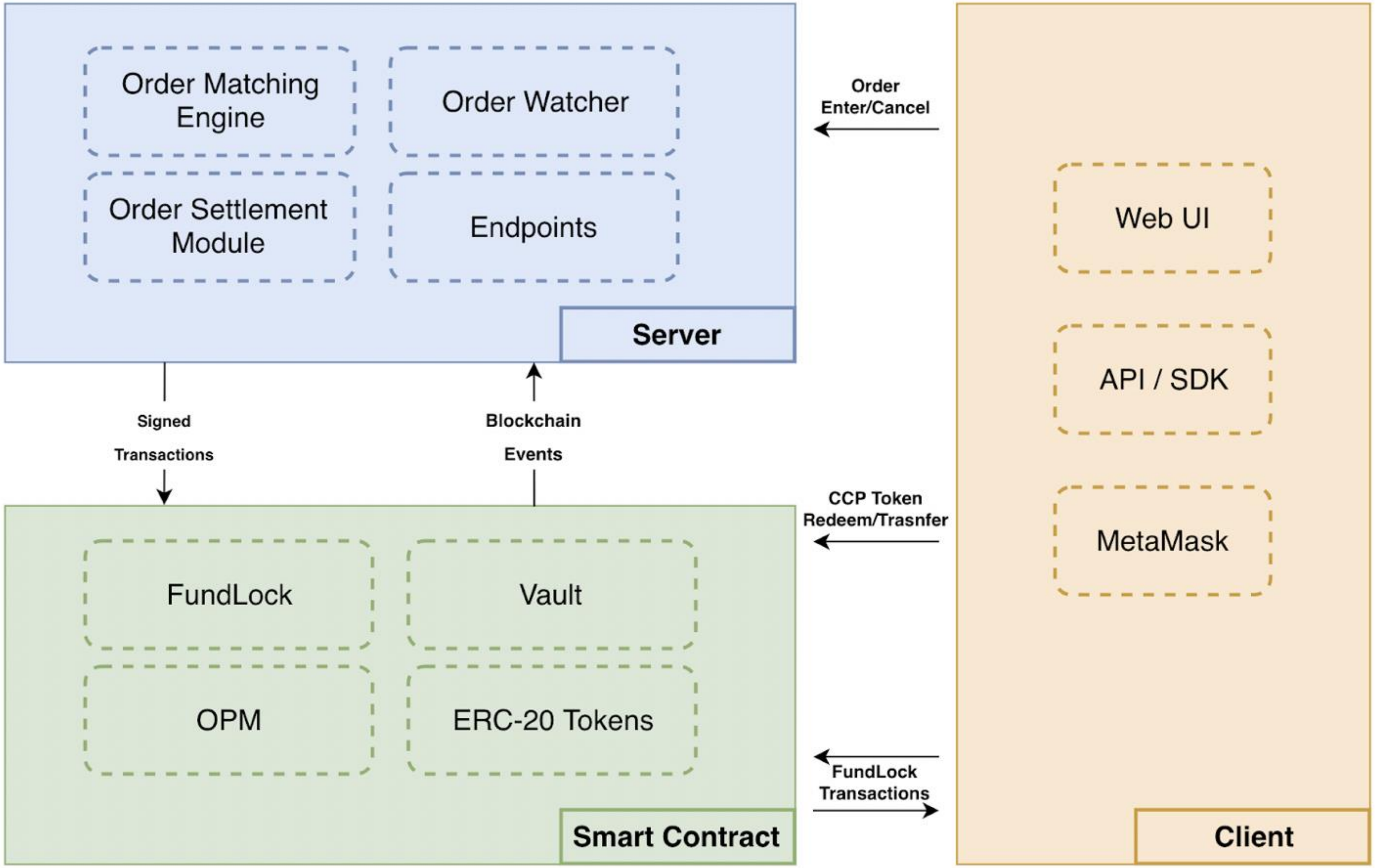
2. The frontend proposes a transaction to the user through his wallet. Transactions are signed by the client and therefore cannot be modified by our servers. The client can choose to view data directly from the blockchain, it is not sent and therefore cannot be modified, by Nomisma servers.

3. The collateral, once transferred to the smart contract, cannot be manipulated against the rules of the contract by Nomisma or any other party in the absence of a security exploit in the contract or the underlying Ethereum blockchain.

4. All transactions are recorded permanently and transparently and as a single source of truth on the blockchain.

A non-custodial but trusted implementation of the architecture, may not need to retain any of the 4 criteria, although any of them could be included as desired.

Technology



Server

Order Matching Engine

Order Watcher

Order Settlement Module

Endpoints

Signed Transactions

Blockchain Events

Smart Contract

FundLock

Vault

OPM

ERC-20 Tokens

Client

Web UI

API / SDK

MetaMask

Order Enter/Cancel

CCP Token Redeem/Trasnfer

FundLock Transactions

Degree of trustless execution is tuned by controlling the weight of development on the centralized backend relative to the smart contracts.

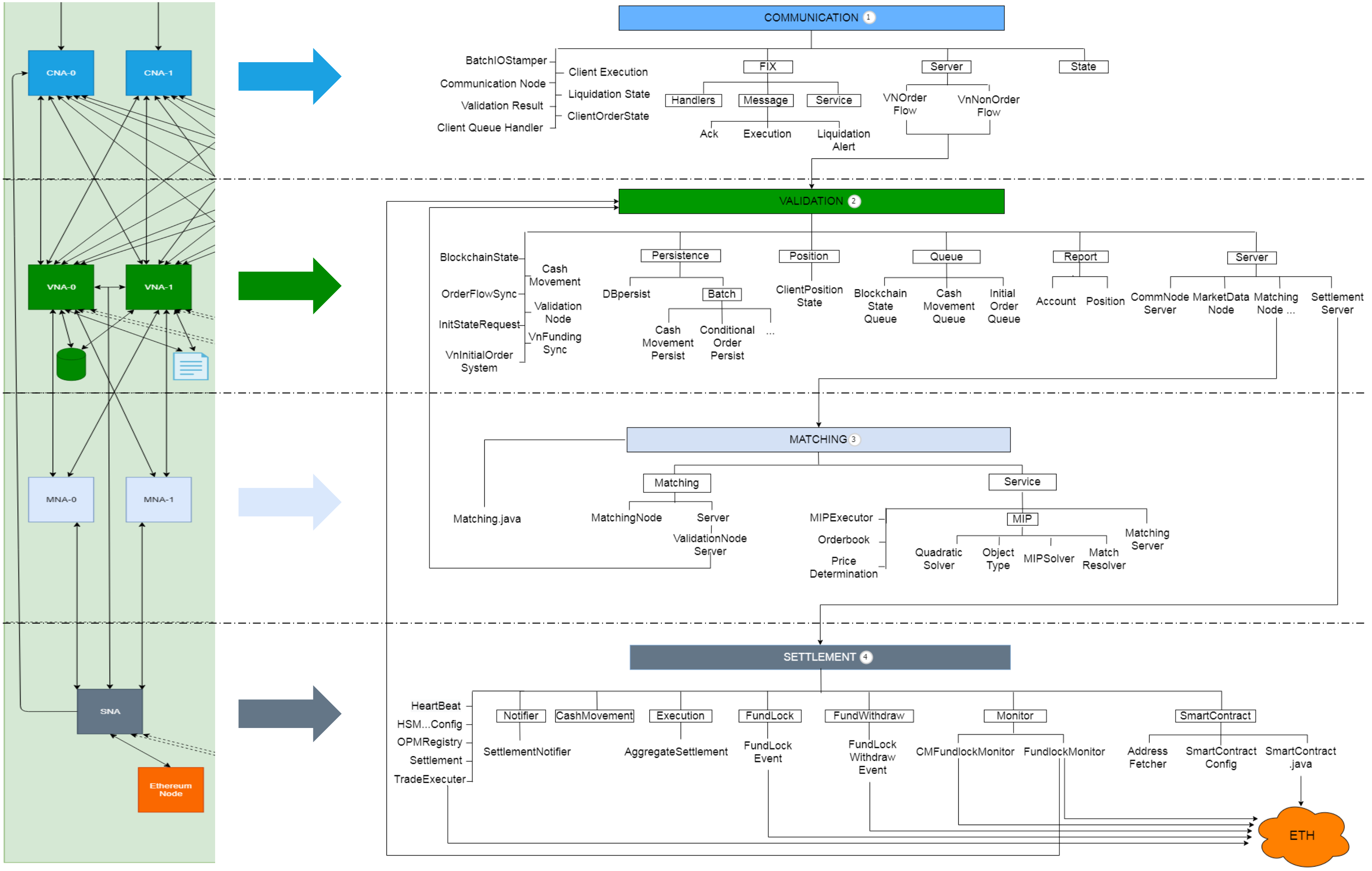
Architecture

Communication Tier

Validation Tier

Matching Tier

Settlement Tier



CNA-0

CNA-1

VNA-0

VNA-1

MNA-0

MNA-1

SNA

Ethereum Node

COMMUNICATION 1

BatchIOStamper

Communication Node

Validation Result

Client Queue Handler

Client Execution

Liquidation State

ClientOrderState

FIX

Handlers

Message

Service

Ack

Execution

Liquidation Alert

Server

VNOrder Flow

VnNonOrder Flow

State

VALIDATION 2

BlockchainState

OrderFlowSync

InitStateRequest

VnInitialOrder System

Cash Movement

Validation Node

VnFunding Sync

Persistence

DBpersist

Batch

Cash Movement Persist

Conditional Order Persist

...

Position

ClientPosition State

Queue

Blockchain State Queue

Cash Movement Queue

Initial Order Queue

Report

Account

Position

Server

CommNode Server

MarketData Node

Matching Node ...

Settlement Server

MATCHING 3

Matching.java

Matching

MatchingNode

Server

ValidationNode Server

Service

MIPExecutor

Orderbook

Price Determination

MIP

Quadratic Solver

Object Type

MIPSolver

Match Resolver

Matching Server

SETTLEMENT 4

HeartBeat

HSM...Config

OPMRegistry

Settlement

TradeExecuter

Notifier

SettlementNotifier

CashMovement

Execution

AggregateSettlement

FundLock

FundLock Event

FundWithdraw

FundLock Withdraw Event

Monitor

CMFundlockMonitor

FundlockMonitor

SmartContract

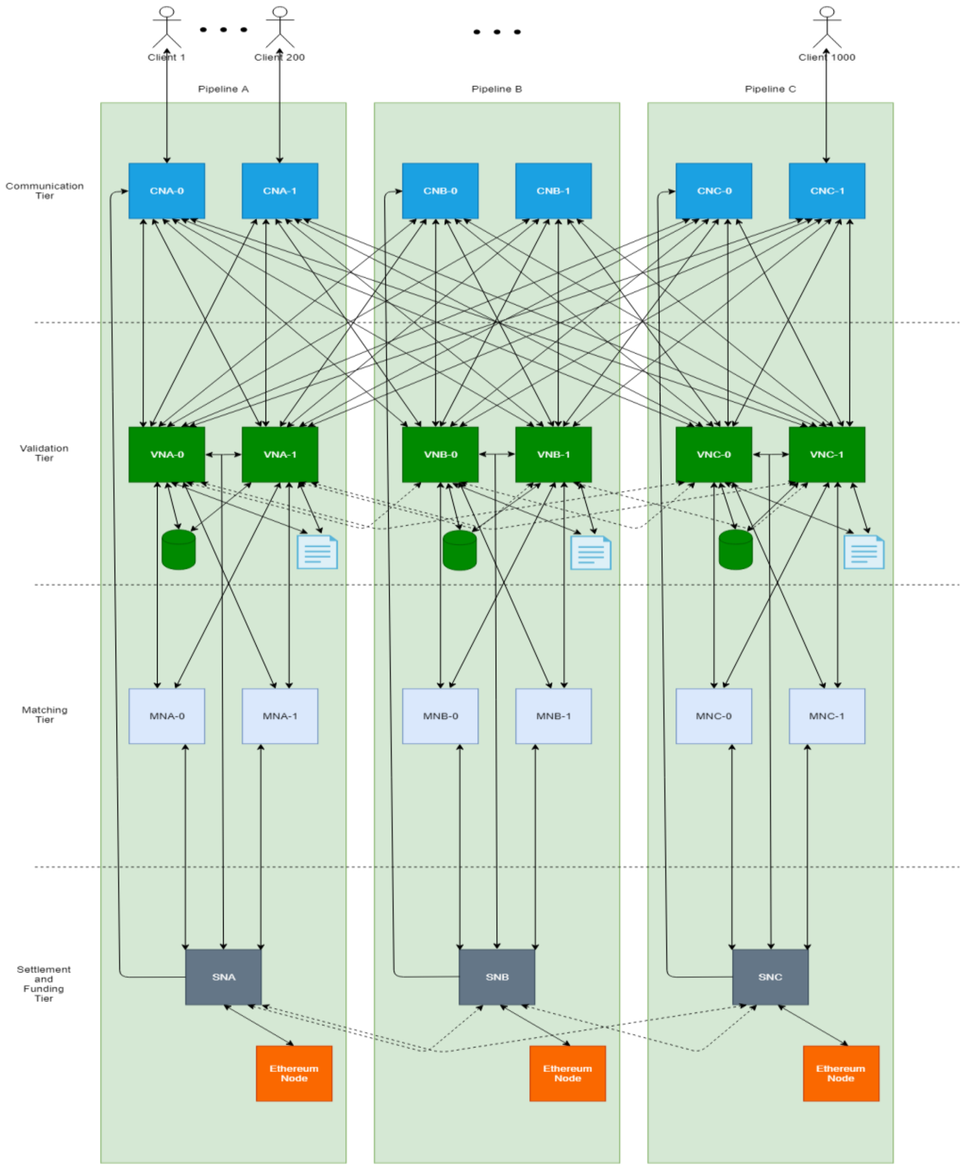
Address Fetcher

SmartContract Config

SmartContract .java

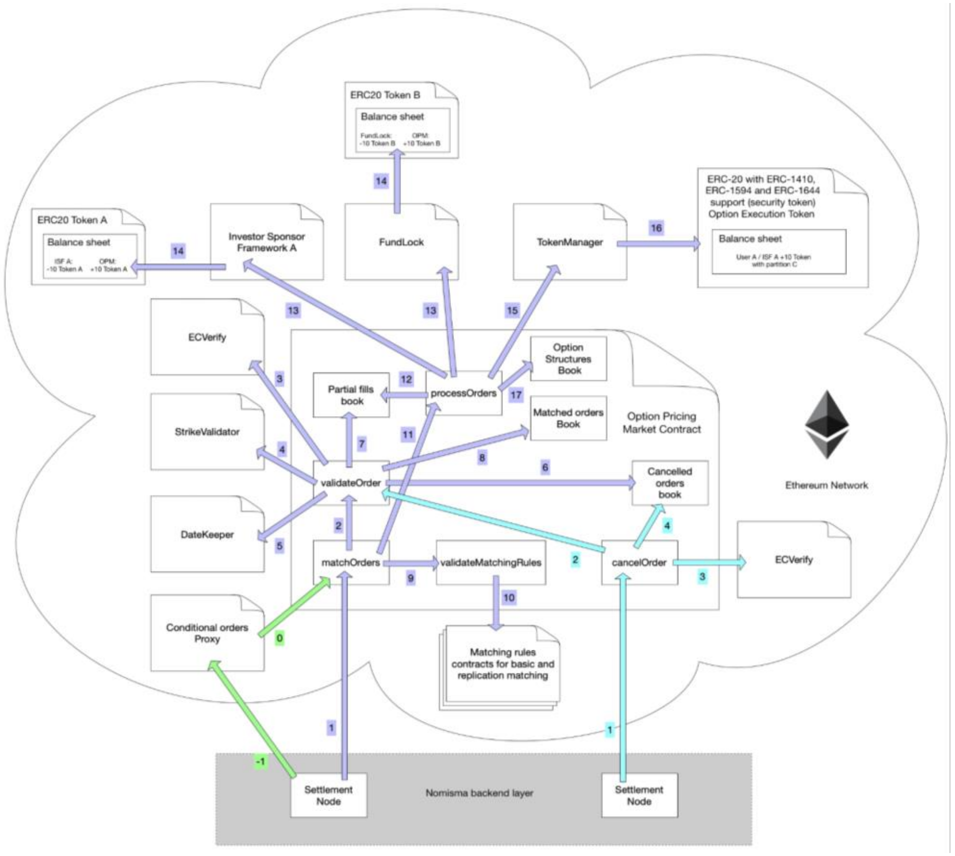
ETH

Technology



Centralized backend: implemented in Java.

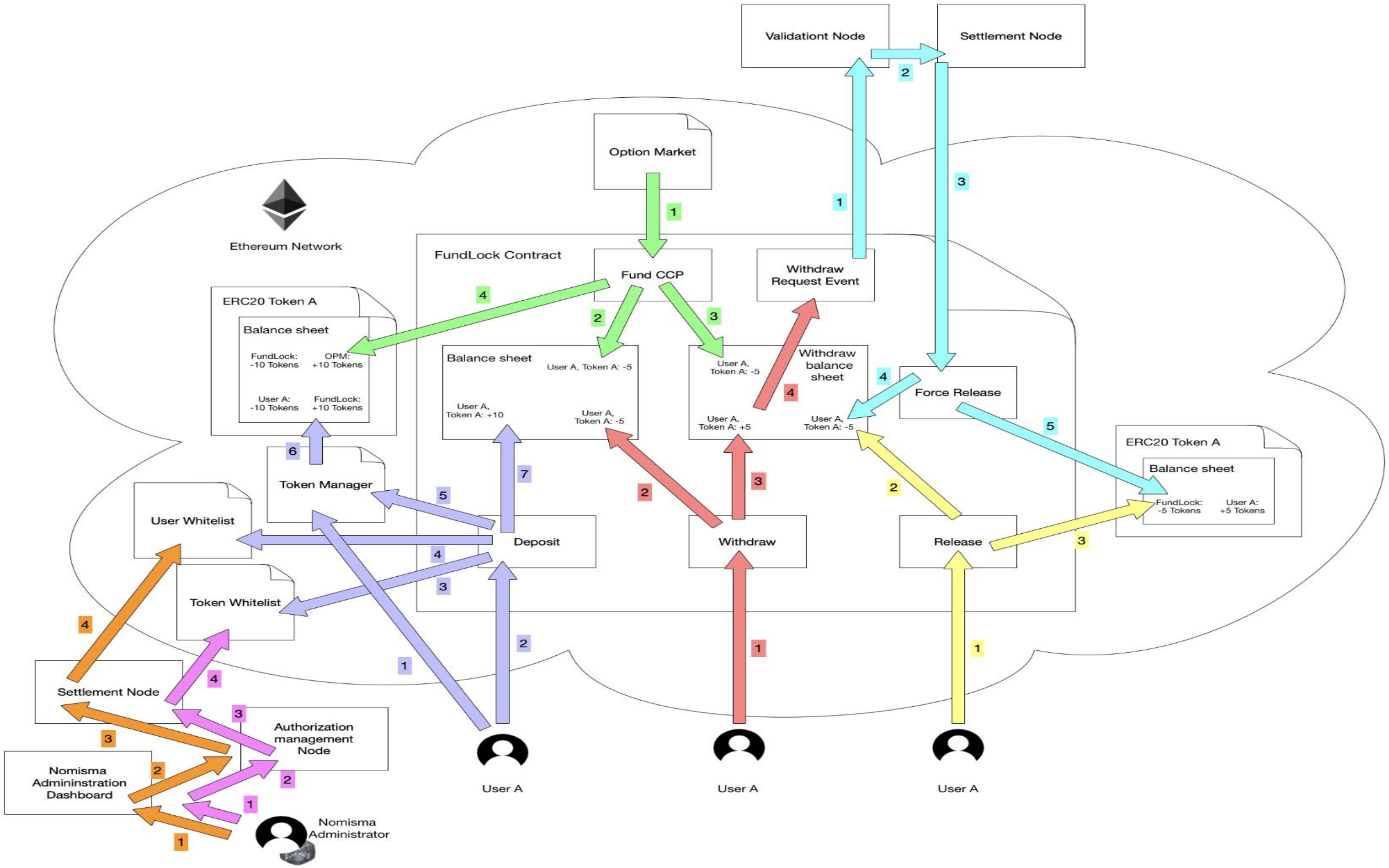
Modular ‘Mesh’ design:
Enterprise grade reliability in a cloud hosted environment.
‘Settlement and Funding Tier’ connects to the Ethereum blockchain and is integrated with a separate smart contracts’ architecture.



Technology

Granular Fundlock box expansion (arrow #13)

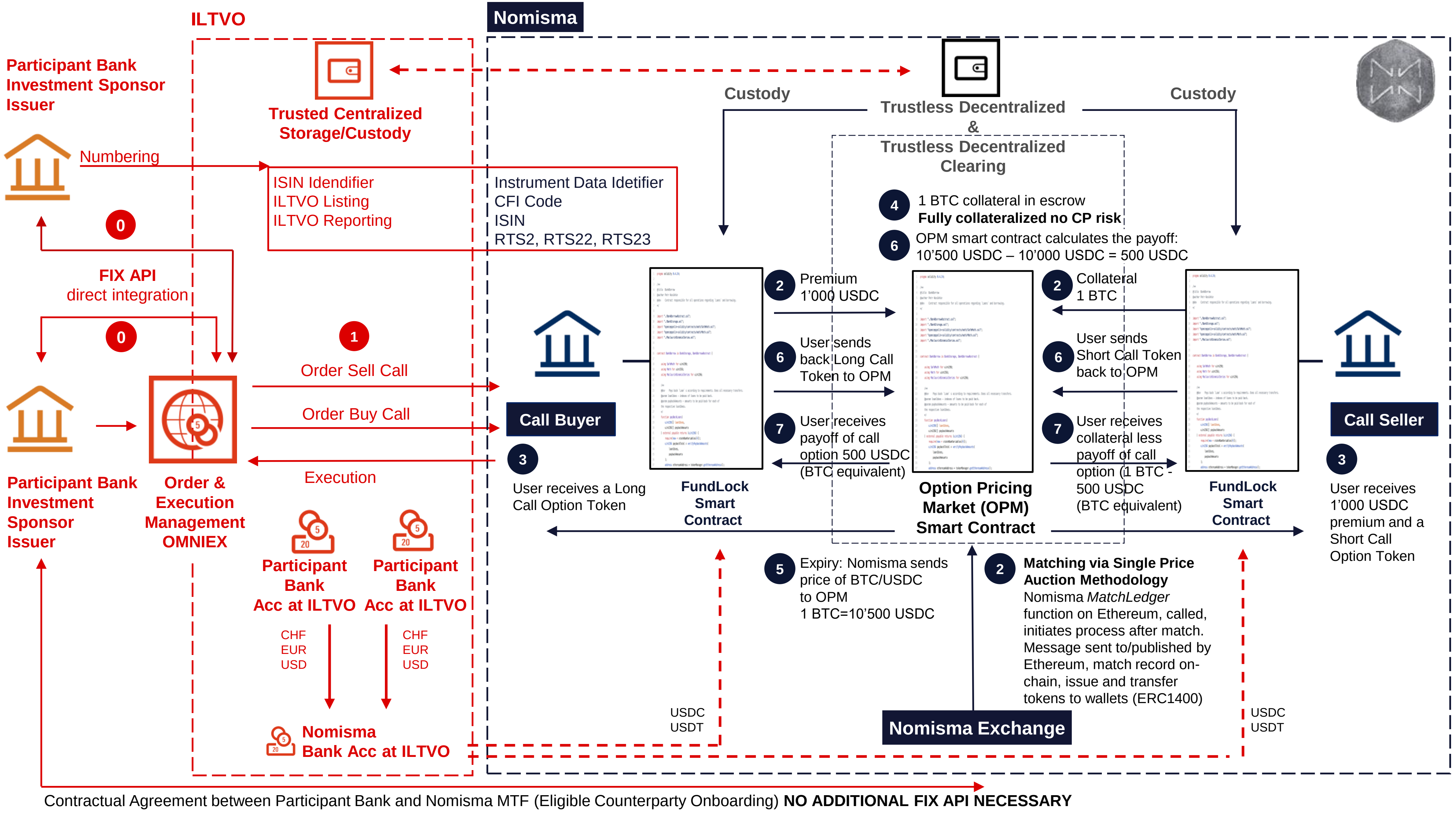
- FundLock is Nomisma’s trustless on-chain account management architecture.



ISSUANCE AND BUSINESS PROCESS

Comparison

Incumbent Legacy Trading Venue Operator (ILTVO)		ILTVO vs. NOMISMA	NOMISMA	
ILTVO treats derivatives as financial instruments		FINANCIAL INSTRUMENTS ✓ **Same**		Nomisma (and the Regulator) treats derivatives on digital assets as financial instruments
ILTVO Participants originate and upload Instrument Reference Data		INSTRUMENT REFERENCE DATA ✓ **Same**		Nomisma Participants define financial instrument via API, FIX or web application
ILTVO Numbering	ILTVO reserves and assigns ISIN received from ANNA to the financial instrument	INSTRUMENT REFERENCE DATA ✓ **Same**	Nomisma applies for ISIN at Association of National Numbering Agencies (ANNA) Nomisma submits Regulatory Technical Standards (RTS) for the financial instrument to FIRDS (ESMA, NCA)	Nomisma
ILTVO Participants book ISIN in their Core Banking System (Avaloq, Temenos, Finnova)		PARTICIPANTS BOOKING ✓ **Same**		Nomisma Participants book ISIN in their Core Banking System (Avaloq, Temenos, Finnova)
ILTVO Listing	ILTVO Listing enables financial instruments to be immediately admitted to trading	ADMISSION TO TRADING ✓**Same**	Financial instruments created under the protocol are immediately admitted to trading	Nomisma admission to trading
ILTVO Reporting	Reporting Members send reports via the Reporting Tool (web interface) for Trade & Transaction Report and Transaction File Interface (Transaction Report)	REPORTING PRE-TRADE AND POST-TRADE TRANSPARENCY ✓ **Same/Similar**	Nomisma reports to National Competent Authority (NCA) or ESMA, or uses an APA (Approved Publication Arrangement) and an ARM (Authorized Reporting Mechanism)	Nomisma Reporting Obligations Pre-Trade and Post Trade Transparency MiFiD EU 600/2014; MiFiR; Commission Delegated Regulation (EU) 2017/583
Issuer responsible for data maintenance post-issue (triggers, etc)	Issuer is responsible for all triggers	TRIGGER MANAGEMENT Centralized vs Decentralised ! **Different**	ERC1400 Tokens, Smart Contracts record all relevant data, payoff, triggers, conditions	Nomisma, Ethereum Blockchain
ILTVO Trade Matching	Multilateral Non-Discretionary	MATCHING ENGINE TRANSACTION EXECUTION ✓**Same /** ! **Different**	Multilateral Non-Discretionary Nomisma MatchLedger function is called after trade match, transaction is broadcasted on Ethereum Blockchain, ERC1400 Tokens are minted, Tokens as well as collateral are transferred to the respective Participants' wallets	Nomisma Matching Engine
ILTVO Clearing & Settlement	ILTVO manages collateral	COLLATERAL MANAGEMENT ! **Different**	Nomisma Ethereum based Fund Lock Smart Contract manages collateral	Ethereum Smart Contract
ILTVO Clearing & Settlement	ILTVO manages netting and settlement	SETTLEMENT ! **Different**	Nomisma MTF sends Expiration Reference Price to OPM Ethereum Smart Contract that calculates payoff, after validation, buyer/seller send long/short token to OPM and receive validated payoff/collateral minus validated payoff	Nomisma Ethereum based settlement protocol



ILTVO

Nomisma

Participant Bank
Investment Sponsor
Issuer

Numbering

Trusted Centralized
Storage/Custody

ISIN Idendifier
ILTVO Listing
ILTVO Reporting

Instrument Data Idetifier
CFI Code
ISIN
RTS2, RTS22, RTS23

0

FIX API
direct integration

0

Custody

Trustless Decentralized
&
Trustless Decentralized
Clearing

Custody

4 1 BTC collateral in escrow
Fully collateralized no CP risk

6 OPM smart contract calculates the payoff:
10'500 USDC – 10'000 USDC = 500 USDC

1

Order Sell Call

Order Buy Call

Execution

Participant Bank
Investment
Sponsor
Issuer

Order &
Execution
Management
OMNIEX

Call Buyer

3

User receives a Long
Call Option Token

2 Premium
1'000 USDC

6 User sends
back Long Call
Token to OPM

7 User receives
payoff of call
option 500 USDC
(BTC equivalent)

FundLock
Smart
Contract

Option Pricing
Market (OPM)
Smart Contract

2 Collateral
1 BTC

6 User sends
Short Call Token
back to OPM

7 User receives
collateral less
payoff of call
option (1 BTC -
500 USDC
(BTC equivalent)

FundLock
Smart
Contract

Call Seller

3

User receives
1'000 USDC
premium and a
Short Call
Option Token

Participant
Bank
Acc at ILTVO

Participant
Bank
Acc at ILTVO

CHF
EUR
USD

CHF
EUR
USD

Nomisma
Bank Acc at ILTVO

USDC
USDT

5 Expiry: Nomisma sends
price of BTC/USDC
to OPM
1 BTC=10'500 USDC

2 **Matching via Single Price
Auction Methodology**
Nomisma *MatchLedger*
function on Ethereum, called,
initiates process after match.
Message sent to/published by
Ethereum, match record on-chain, issue and transfer
tokens to wallets (ERC1400)

Nomisma Exchange

USDC
USDT

Contractual Agreement between Participant Bank and Nomisma MTF (Eligible Counterparty Onboarding) **NO ADDITIONAL FIX API NECESSARY**

- Participant transfers funds to FundLock smart contract. These funds are then available for trading
- Participant enters order on Nomisma
- Nomisma validates availability of sufficient funds in Participants' FundLock smart contract
- Nomisma populates order in order book for matching

- Nomisma passes matched order data to network by calling 'pair' function in Option Pricing Market (OPM). Transaction settlement is confirmed once included in block on the network.
- OPM smart contract receives requisite funds for settlement from Participants' FundLock. Funds held in OPM until maturity of respective transaction to ensure payout at maturity (TradeLock smart contract)
- OPM sends token and premium, if applicable, to respective Participants of the trade.
- OPM holds collateral in smart contract until expiry. Contract fully collateralized, no CP risk to either party to the transaction.

- Participants send tokens representing trade back to OPM
- Nomisma sends the price of underlying at expiry to OPM
- OPM smart contract calculates final payoff of contract
- OPM smart contract transfers final payoff or collateral return less final payoff, to respective Participants of the trade

Smart Contracts

Protocol	Built upon Nomisma's native protocols (implemented in the smart contracts) as tokens on the Ethereum network.
Admission	Only digital asset Tokens that have been created by Nomisma or MTF Participants using Contingent Claims and Investment Sponsor protocol. A number of metrics are generated and automated by smart contracts eliminating the requirement of actions of the respective parties of the agreements
Automatic Decentralised	Required payoffs automatically made to the relevant parties. No centralized intermediary required to ensure payment or may intervene payment
Collateral	Collateral is held within smart contract and is always sufficient. Once conditions are fulfilled, smart contract automatically executes the payout function
Properties	The properties guarantee financial commitments to the relevant participants. Enforced as Solidity code as a combination of functions inside contracts executed by the Ethereum blockchain. Many functions are public, can be executed by any node in the network. The combination of publicly callable functions and the decentralized nature of Ethereum means the software can be operated without the requirement or authorization of a single party
Value	The value transacted is embodied as tokens or Ether and developed on or native to Ethereum Never "leaves" Ethereum and can be controlled and enforced by the contracts
FundLock	FundLock smart contract is a set of functions which Participants can define themselves (amount, maturity, strike price, validity of offer etc) Once defined, they are executed automatically upon conditions being met, conditions cannot be altered anymore and are executed autonomously.
Whitelisting	Tradable Tokens are whitelisted to guarantee the safety and resilience of the trading facility. When Nomisma's security test passed, Tokens are whitelisted for trading and checked by FundLock.
Deposit	FundLock, its address and deposit token are validated against the whitelist. Lack of whitelisting, leads to transaction being reversed and rejected
Withdrawal	FundLock smart contract checks if funds are sufficient and if there are any unconfirmed trade settlements. Sufficient funds and no unconfirmed trade settlements, status 'ready to be withdrawn'; Sufficient funds but unconfirmed trade settlements, a withdrawal delay of an hour starts to allow trade settlements to be confirmed on network. At the expiry of the withdrawal delay, the withdrawal request status is updated to 'ready to be withdrawn'. Insufficient funds, the withdrawal request is rejected.
Security	The derivative products consist not only of a single, but of many individual smart contracts, each with its own address. Overall functionality is ensured by the communication between the individual parts. If an address were compromised, the damage would be limited to the function in the affected address. If a manipulated smart contract were distributed to an existing address, the functional chain would be interrupted because this manipulated code does not recognise the addresses that depend on it. Due to the architecture of the system, the respective states and functions are kept separate. Once a smart contract has been created it can no longer be changed and is given a unique address. To manipulate and change the contract, a new smart contract would have to be created, which in turn would have its own address, which would not be linked to the other smart contracts