otc*Digital

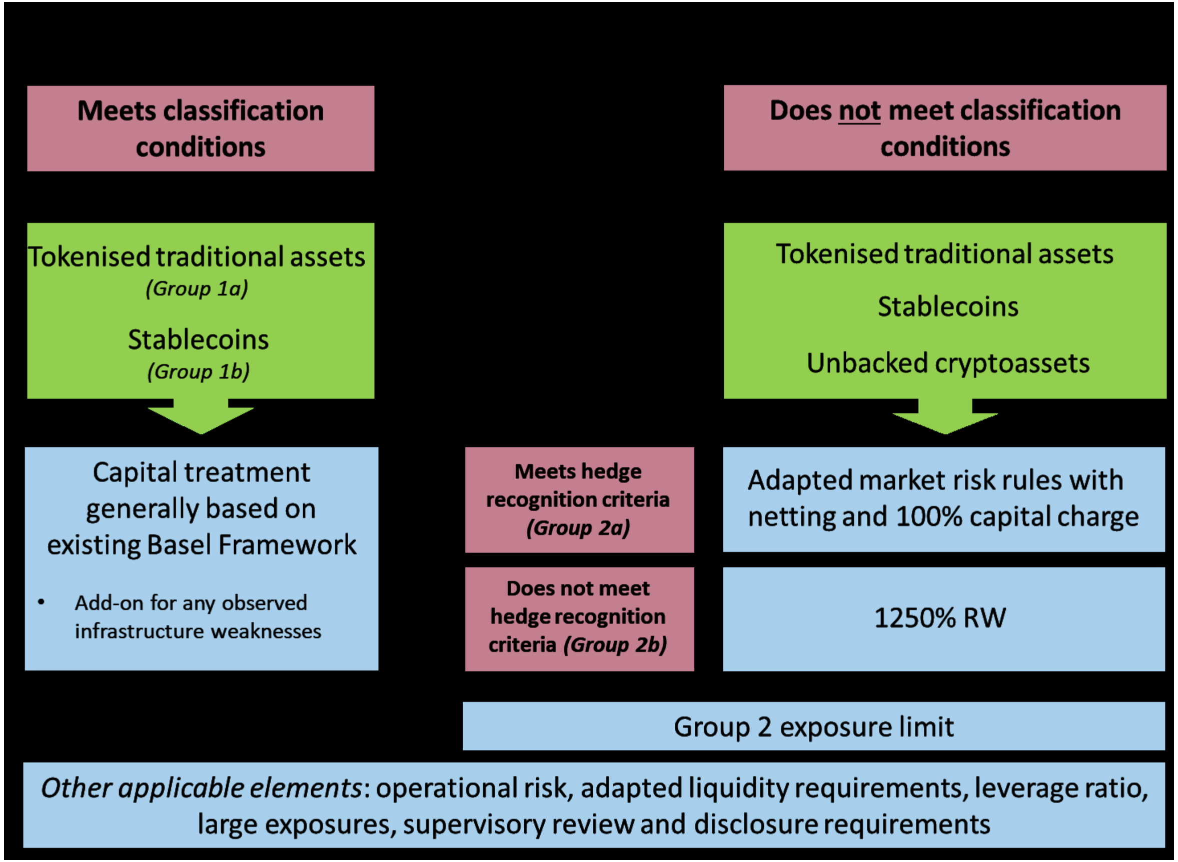
POLYMESH

# Integrated confidential digital assets marketplace with full lifecycle and automation

## Interoperable ecosystem for Digital Assets: Tokenization, lifecycle and Trading platforms for dealers, investors, custodians, CCPs, transfer agents and CSDs

We believe in broadening investment opportunities and improving desk-level ESG through digital standards and automation

# Tokenization:  BIS RWA/Crypto assets classifications and rwa



**Meets classification conditions**

Tokenised traditional assets *(Group 1a)*

Stablecoins *(Group 1b)*

Capital treatment generally based on existing Basel Framework

- Add-on for any observed infrastructure weaknesses

**Does not meet classification conditions**

Tokenised traditional assets

Stablecoins

Unbacked cryptoassets

**Meets hedge recognition criteria *(Group 2a)***

Adapted market risk rules with netting and 100% capital charge

**Does not meet hedge recognition criteria *(Group 2b)***

1250% RW

Group 2 exposure limit

*Other applicable elements*: operational risk, adapted liquidity requirements, leverage ratio, large exposures, supervisory review and disclosure requirements

## Real World Assets (RWA) Compliance

**BIS:**

- Network Interoperability
- No permissionless networks for Group 1
- Control : who sees what (privacy)

**OCC/FinCEN/SEC 15c3-3 & SIPA 1970 rules:**

- Demonstrate control of asset
- Transfer guarantee to the right party (no unilateral transfer)

BIS: Bank for International Settlements
rwa: Risk-Weighted Assets
OCC: Office of the Comptroller of the Currency
SIPA:  Securities Investor Protection Act
FinCEN: Financial Crimes Enforcement Network
BIS Source

# Tokenization:  BIS Prudential Treatment of Crypto Assets

60.9 Tokenized traditional assets will only meet classification condition 1 if they satisfy all of the following requirements:
(1) They are digital representations of traditional assets using cryptography, DLT or similar technology to record ownership.
(2) They pose the same level of credit and market risk as the traditional (non-tokenized) form of the asset. In practice, this means the following for tokenized traditional assets:

(a) *Bonds, loans, claims on banks (including in the form of deposits),*[2] *equities and derivatives*. The cryptoasset must confer the same level of legal rights as ownership of these traditional forms of financing (eg rights to cash flows, claims in insolvency etc). In addition, there must be no feature of the cryptoasset that could prevent obligations to the bank being paid in full when due as compared with a traditional (non-tokenized) version of the asset.

(b) *Commodities*. The cryptoasset must confer the same level of legal rights as traditional account-based records of ownership of a physical commodity.

Source: https://www.bis.org/bcbs/publ/d545.pdf  (Dec 2022)
Further Consultation: responses due by Apr, 2024:  https://www.bis.org/bcbs/publ/d567.pdf
Credit Risk:    https://www.bis.org/basel_framework/chapter/MAR/20.htm?inforce=20191215&published=20191215
Market Risk:  https://www.bis.org/basel_framework/chapter/CRE/20.htm

# Digital Assets on DLTs – now it is mature, privacy enabled and scalable

Permissioned Networks ->

### Enterprise Privacy Ledgers (trust in participants -> pseudo privacy & custody)

- "I owe you" or "claim on an issuer" model
- Centralized cap-table (Issuers/Transfer Agents)
- Limitations:

Qualified Custody?: can't demonstrate control of assets, no segregated key management

Global Custody: commodities, global supply chains

### Enterprise ZK Chain by Polymesh (trust in math and network -> true privacy & custody)

- Permissioned, purpose built for financial markets
- **Confidential Assets** (account based)
- Qualified custody support: control of assets, granular key management, multiple HSMs, restore assets due to lost/stolen keys …

**2009 (1G)**

**2015 (2G)**

**2017 (3G)**

**2023 (4G)**

**2024 (5G)**

### Bitcoin

- First decentralized ledger
- Anonymity
- UTXO
- P2P payments

### Ethereum

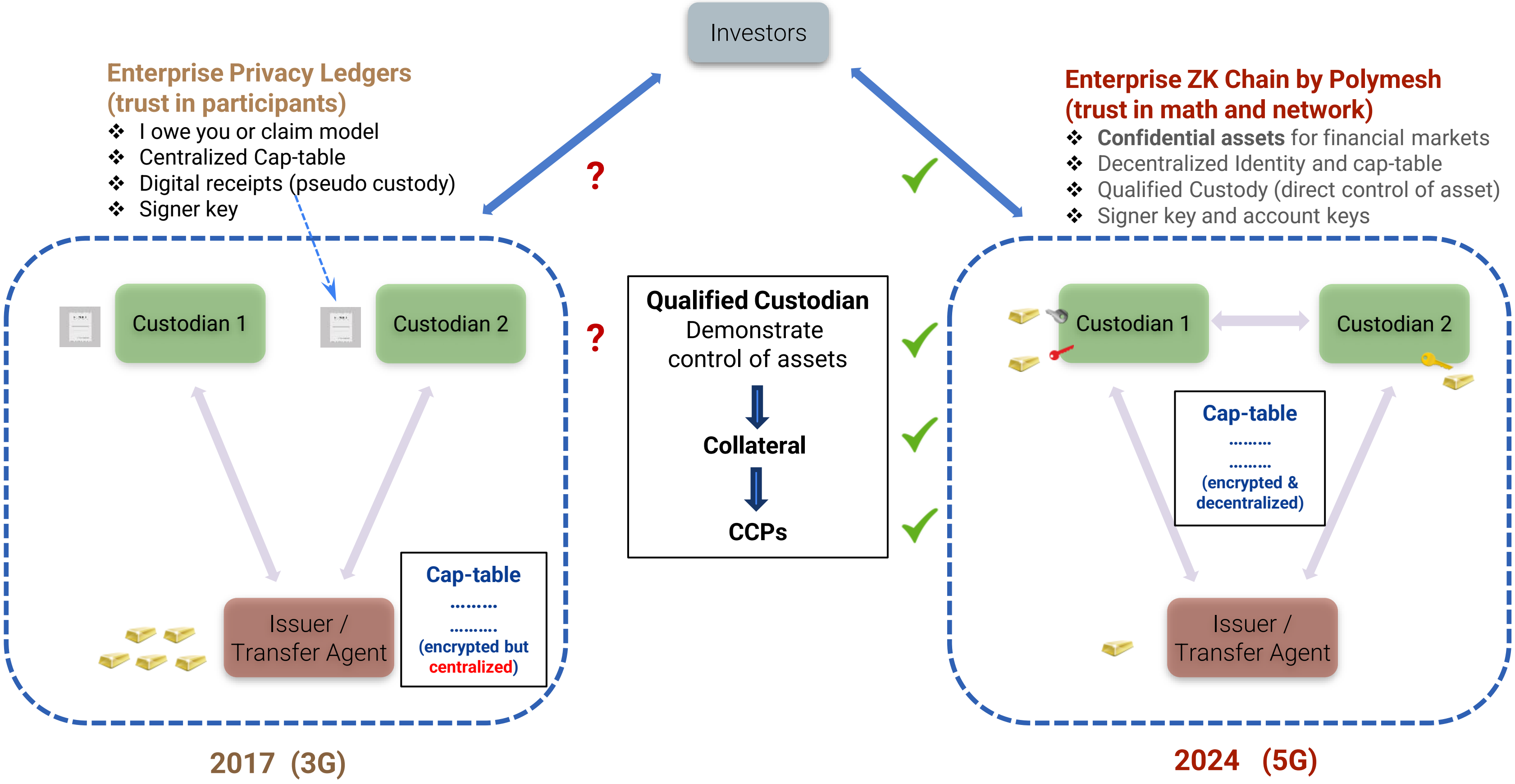
- World computer
- Account Based
- Smart Contracts – ERC xxx
- Public Assets
- Cap-table: decentralized but not encrypted (no privacy)
- Other chains: Algorand, Solana, Avalanche …

### Zero Knowledge Public Networks

- Privacy/trust in the network
- zkEVM rollups (scaling)
- L2 Domain Specific Languages (DSL) – Aztec Noir, Circom, Zokrates
- Aleo, Firo (L1 ZK chains)
- Namada (interoperability)
- zk L2 / L3 solutions (Polygon CDK)
- UTXO / Account based models
- Solana (confidential asset transfer)
- Polygon Miden (in the works)

Public Permissionless Networks

# Enterprise Ledgers : Trust in participants or network ?



**Enterprise Privacy Ledgers**
**(trust in participants)**

- ❖ I owe you or claim model
- ❖ Centralized Cap-table
- ❖ Digital receipts (pseudo custody)
- ❖ Signer key

**Enterprise ZK Chain by Polymesh**
**(trust in math and network)**

- ❖ **Confidential assets** for financial markets
- ❖ Decentralized Identity and cap-table
- ❖ Qualified Custody (direct control of asset)
- ❖ Signer key and account keys

# Digital Assets on DLTs – now it is mature, privacy enabled and scalable

## Enterprise Privacy Ledgers
## (trust in participants -> pseudo privacy and custody)

- “I owe you” or “claim on an issuer” model
- Participants are ring-fenced within a jurisdiction
- Centralized cap-table (many power-centers – attacking one will cause serious degradation to network)
- Qualified Custody?: can’t demonstrate control of assets, (own private key -> own assets model does not work), no segregated key management

**2017 (3G)**

recent security incidents in EquiLend and Ion

## Enterprise ZK Chain by Polymesh
## (trust in math and network -> true privacy and custody)

- Private, Permissioned, purpose built for financial markets
- **Confidential Assets** (account based)
- **Decentralized Identity and cap-table**
- Mediators / Auditors support
- **Qualified custody** support: control of assets, granular key management, multiple HSMs, restore assets due to lost/stolen keys …

**2024 (5G)**

## otcDigital Enterprise ZK Platform & Network

- Confidential Assets on Polymesh chain (L1)
- Business Workflows and CDM contracts on Corda DLT (L2)
- Privacy for all on the L1 & L2 networks
- Integrated platforms and network for Issuers, Investors, Custodians, CCPs, CSDs, Transfer Agents, Auditors, Administrators …
- Full support for sanctions, freezes, bankruptcies, lost/stolen keys
- **Safe and sound financial markets**

# Web3: Fully decentralized stack by otcDigital

L6: Presentation (otcApps)

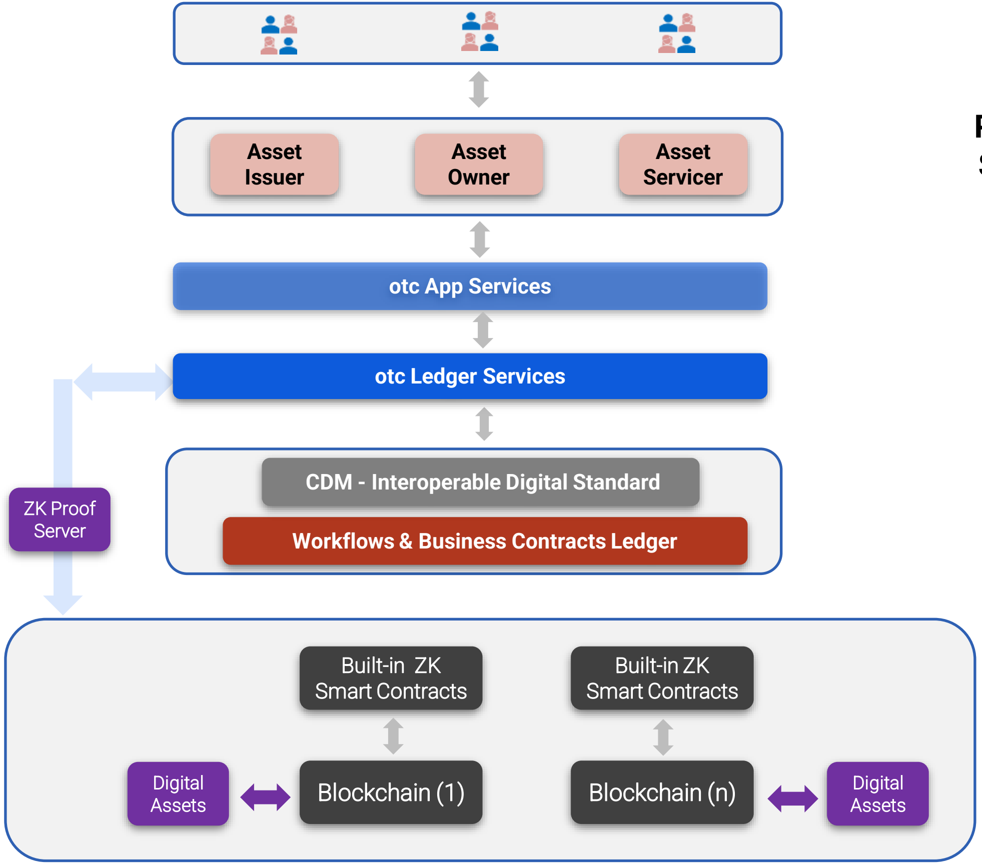
L5: otc Products & Services
(Cash, CP, Bonds …)

L4: Shared Data, workflows & Services Network

L3: Ledger Data & workflows

L2: Business Privacy,
Digital Standard &
Interoperability

L1: Asset Privacy,
Programmable Privacy,
scalability & security,
L1 ledger interoperability



Asset Issuer

Asset Owner

Asset Servicer

otc App Services

otc Ledger Services

ZK Proof Server

CDM - Interoperable Digital Standard

Workflows & Business Contracts Ledger

Built-in ZK Smart Contracts

Built-in ZK Smart Contracts

Digital Assets

Blockchain (1)

Blockchain (n)

Digital Assets

**Party Interoperability, Shared Economy and Automation**

CDM – the logical ledger
(ledger agnostic industry smart contract)

on Corda

ZK based Privacy Chains

Polymesh

CDM: Common Domain Model

# Custody Regulatory Compliance
## (addressing OCC, FinCEN, CFTC, SEC 15c3-3 & SIPA 1970 rules)

### Demonstrate control of Asset

- Secure the private key - secure the asset (HSM keys per account, single or sharded wallets - MPC)
- Misplaced / stolen / lost keys can be restored (guaranteeing no loss of funds)
- Customer protection: potential joint custody & SIPC trustee passive key shares address Broker-Dealer fails

### Settlement/Transfer guarantee to the right party

- All customer accounts, vault addresses are whitelisted and controlled by custodians ensuring KYC/AML compliance and potential reversibility in case of mistaken transfers
- FinCEN: VASP, Transmittal Order compliance

### Record Keeping

- All orders, executions, positions stored as CDM records in DLT
- All custody and settlement workflows including individual asset transfer details are recorded as CDM in DLT

### Reporting

- All the above DLT transactions can be reported (in industry standard CDM or other regulatory standards) to a regulatory node in real-time or on demand

POLYMESH

# Confidential Asset Discussion

January 2024

Private & Confidential

# Confidential Assets vs Non-Confidential Assets

## Confidential Assets

- Utilize zero-knowledge proofs and homomorphic encryption
- Balances and settlement instruction amounts stored encrypted on-chain
- Participants cannot view underlying balances or transaction amounts
- Use anonymity sets to obfuscate which asset ticker is being transferred

## Non-Confidential Assets

- Balances and settlement instruction amounts are in plain text on-chain.
- All participants can view on-chain balances and transaction amounts
- Transparency allows more on-chain compliance and custodial options

**Non-Confidential Assets support more automated workflows and on-chain custody models while confidential assets provide more privacy for balances and transactions**

**Private & Confidential**

# Confidential Assets - Actors

## Sender / Receiver

- Manage an Elgamal Key Pair (e.g. private key)
- Sender required to generate ZK proofs for transaction to affirm **on-chain**
- Receiver required to verify details (e.g. amounts) from Sender proofs **off-chain** and affirm **on-chain**
- Receiver required to manage incoming balances from transactions **on-chain**

## Auditor(s)

- Manage an Elgamal Key Pair (e.g. private key)
- Can decrypt transaction amounts using Sender proofs **off-chain**

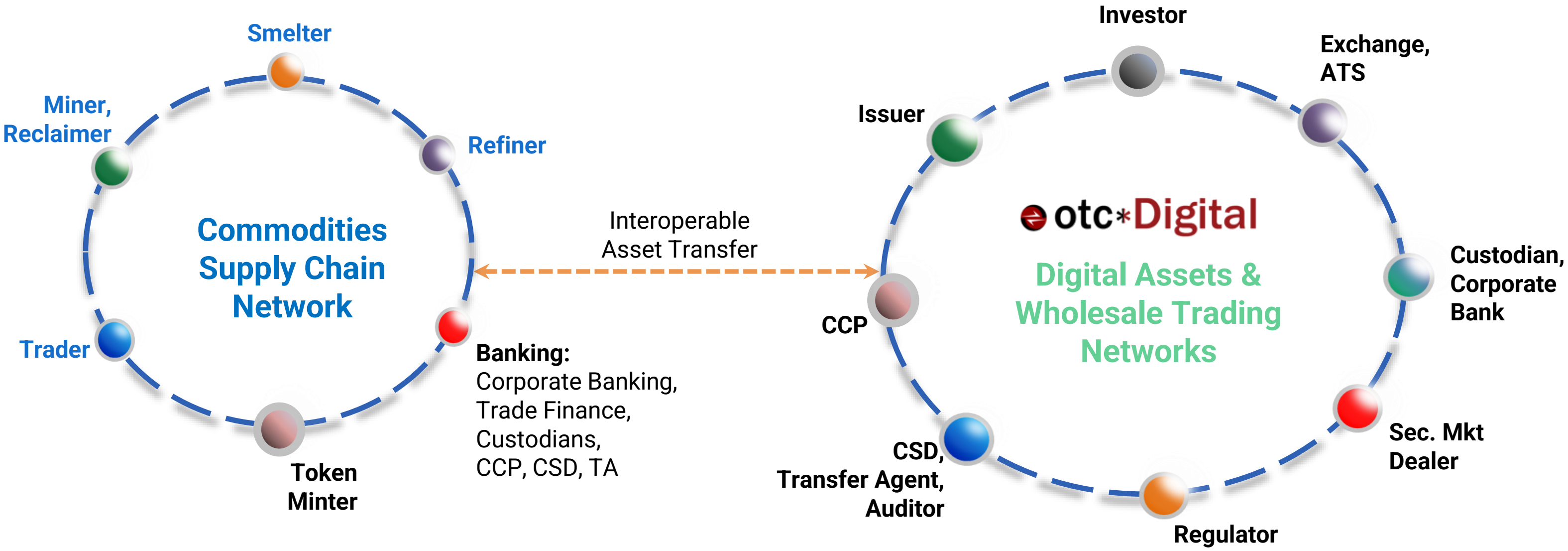
## Mediator

- Same as **Auditor(s)** and in addition;
- Mediator required to verify details (e.g. amounts) from Sender proofs **off-chain** and affirm **on-chain**

**On-chain** transactions require a connection to a Polymesh RPC Node and a Polymesh Identity / Key to sign / submit affirmations.
**Off-chain** transactions require a connection to a Polymesh RPC Node (to retrieve the Sender proofs and verify completion of transactions).

**Private & Confidential**

# Commodities Supply Chain and Trading Networks



**Digital Assets**

Gold Tokens: Ore, Scrap, Dore bar,
Pure Gold bar, Silver bar, Base
Metal bar
Deposit tokens, Gold Alloy

Trade Finance: Loans

**Digital Assets**

Commodities, Securities, Funds, ETF,
CBDC, Deposit tokens, Stablecoins,
Cryptos, NFTs, Loans, Private Equity

Lending, Forwards, Options, Swaps