**Digital Asset**

# A Privacy-First Approach to DLT

Accelerating innovation to address old and new problems with Daml

## Craig Blitz, Chief Product Officer, Digital Asset

**Digital Asset**

## AGENDA

# Digital Asset

## Digital Asset
## At-a-Glance

| | | | |
|---|---|---|---|
| **2014** | **7** | **$300M** | **4 April** |
| DA FOUNDED | GLOBAL OFFICES | SERIES A, B, C, D | Daml Day |

London
UK

Zurich
Switzerland

New York
USA

Budapest
Hungary

SBI & Digital Asset
Joint Venture

Tokyo
Japan

Hong Kong
China

Sydney
Australia

## DA INVESTORS

ABN·AMRO

accenture

CME Group

DEUTSCHE BÖRSE GROUP

Goldman Sachs

vmware

DTCC
Securing Today. Shaping Tomorrow.™

SAMSUNG

IBM

J.P.Morgan

Broadridge

ELDRIDGE

citi

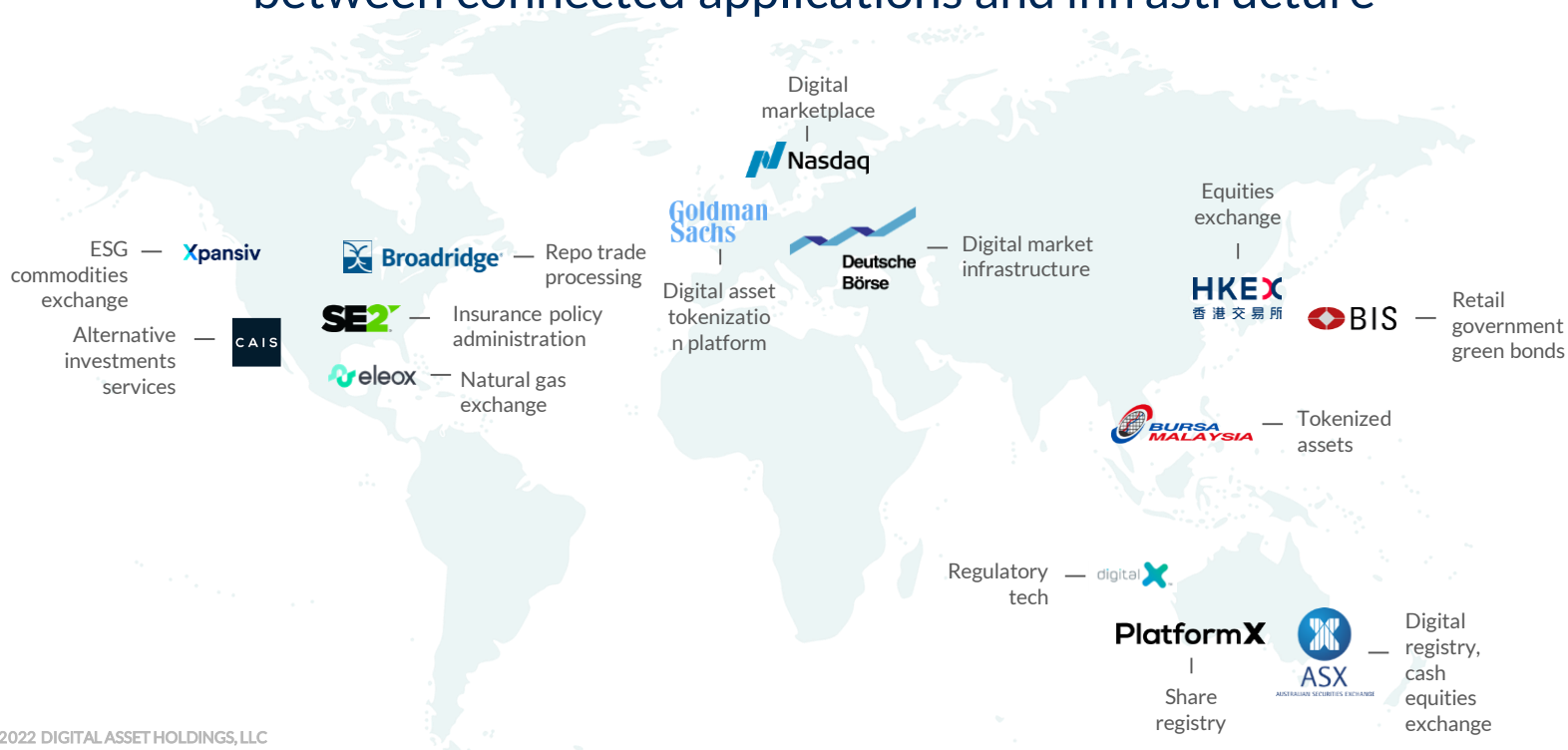**Digital Asset**

# We are building a global network of networks and Daml is the interface
## between connected applications and infrastructure

Digital marketplace
| Nasdaq

ESG commodities exchange — Xpansiv

Broadridge — Repo trade processing

Goldman Sachs
|
Digital asset tokenization platform

Deutsche Börse — Digital market infrastructure

Equities exchange
|
HKEX 香港交易所

BIS — Retail government green bonds

Alternative investments services — CAIS

SE2 — Insurance policy administration

eleox — Natural gas exchange

BURSA MALAYSIA — Tokenized assets

Regulatory tech — digital X

PlatformX
|
Share registry

ASX AUSTRALIAN SECURITIES EXCHANGE — Digital registry, cash equities exchange

4

# The Business Problem: Legacy Transaction Technology

What do legacy systems and outdated business processes all have in common across financial transactions?

**Multi-party workflows** with increasing internal and external sharing needs.

**Complex trust requirements between systems** requiring no unknown participants in the system.

**Burdensome privacy and regulatory requirements** around transaction and participant data.

**Results in heavy reconciliation and inaccurate data sharing**

# What does this mean for **many organizations?**

**Manual reconciliation & inaccurate data sharing leads to:**

**Large overhead** in building and maintaining systems

**Expensive data** breaches

**Slow innovation** that is non-existent in some cases

**Hits to trust** and reputation

Organizations are aware of these problems, but
**are stunting growth via decision paralysis**

- **Old and new problems to solve** and companies are aware and trying to do something about it, but they are paralyzed

- **Reconciliation and operational inefficiencies** continue to haunt financial transactions involving multiple parties  capitalizing on new regulations

- **Competitive threats from nimble startups** and a rapidly evolving ecosystem of asset classes and products in market threaten the status quo of the larger organizations

What if companies could address old problems—without ripping out legacy infrastructure—and still innovate toward the future of decentralized economic networks?

Digital Asset

# Enterprise blockchains can enable large transactions across multiple parties
# while ensuring privacy of participants and transactions. Enter Daml.



### Fix reconciliation problems
Address existing problems and get ready for the future without an expensive reset
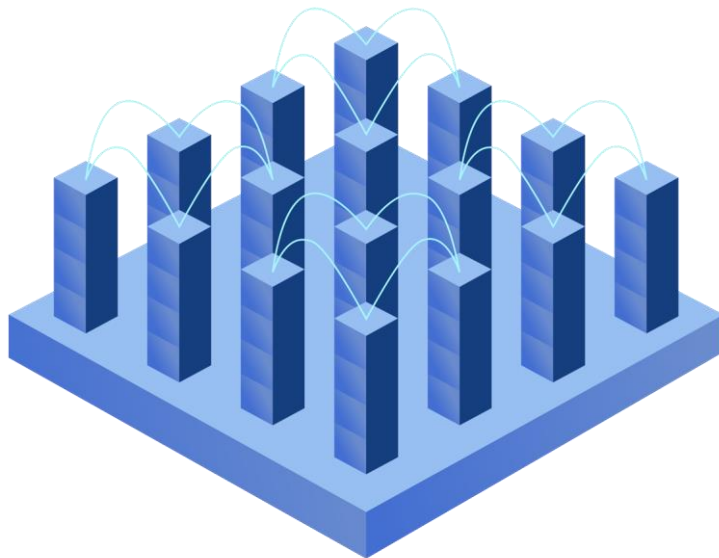
### Reduce cost and risk
Reduce delays in transactions while reducing counterparty risk and spend on fixing issues or regulatory compliance
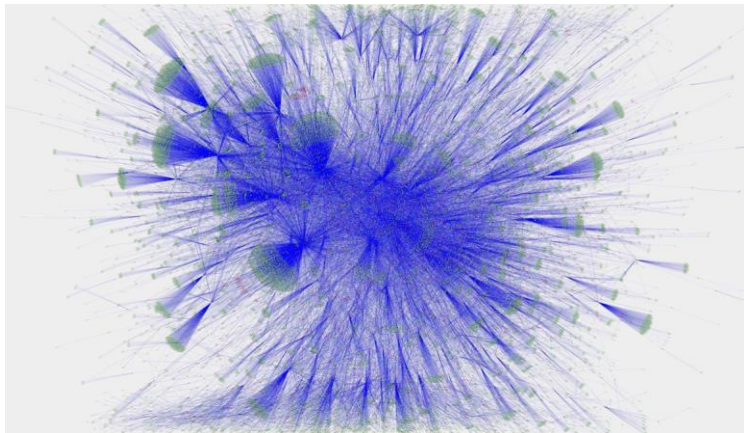
### Focus on innovation
Spend more time and resources in delivering new innovative products and services and growing your economic network
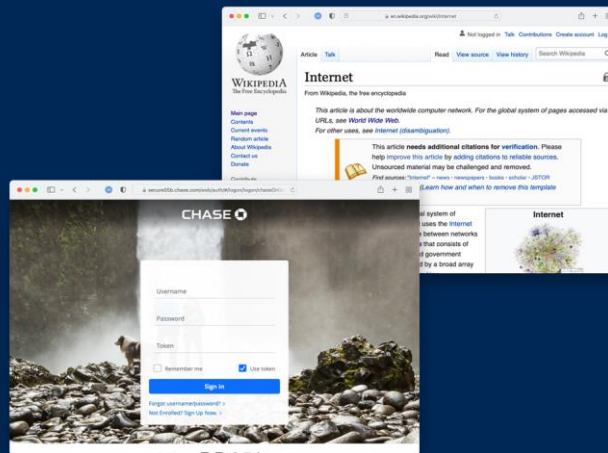
# Our Vision: **The Global Economic Network**

A seamless layer of infrastructure that connects networks in order to compose frictionless multi-party applications while retaining privacy guarantees.

**Digital Asset**

The Internet is an incredibly complex network-of-networks.



But users can browse **from public Web pages to private banking information seamlessly**, without worrying about the underlying infrastructure.

# THE SOLUTION

A platform that lets you forge seamless connectivity across business boundaries.

Daml is the leading platform for building and running multi-party applications. Companies can create solutions that transform disparate silos into synchronized networks, eradicating latency and errors by guaranteeing consistent, shared, and trusted data and workflows.

# THE SOLUTION

Daml is the leading platform for building and running sophisticated, multi-party applications.

---

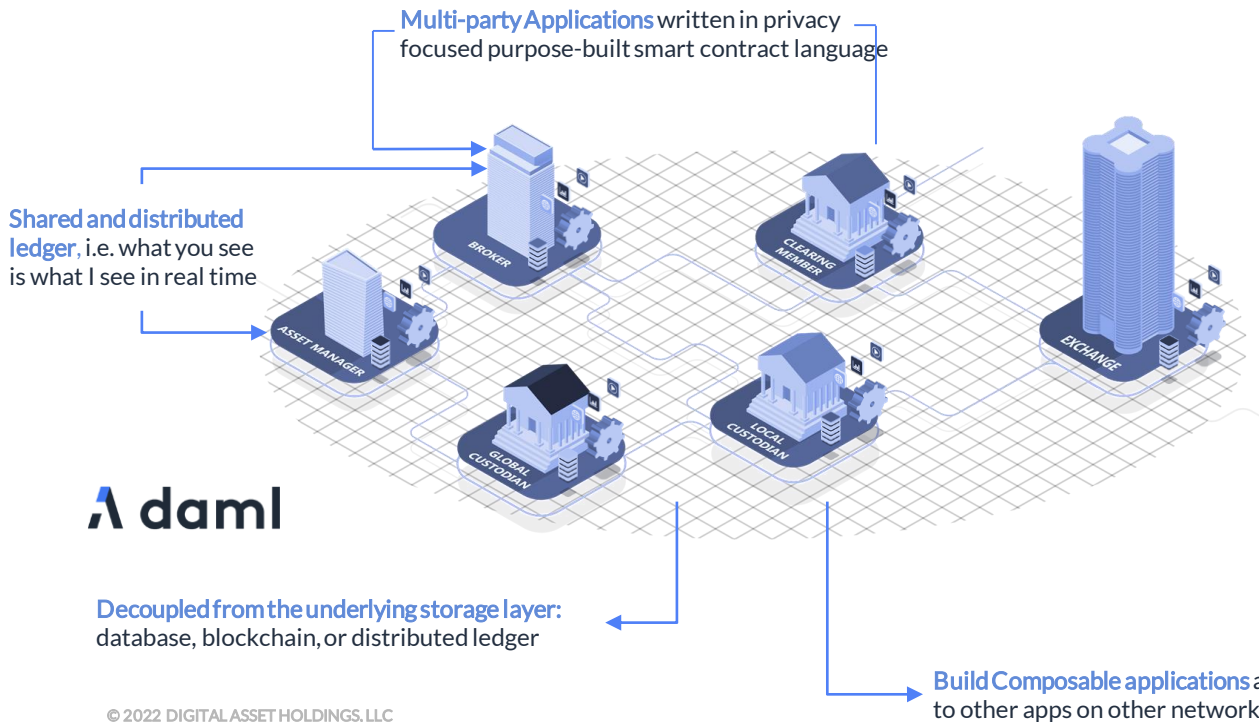Daml contains two core innovations: the Daml Language and Canton.

### The Daml Language

Daml contains a smart contract language and tooling that defines the schema, semantics, and execution of transactions between distributed parties.

### The Canton Ledger

A privacy-enabled distributed ledger that is enhanced when deployed with complementary blockchains and provides secure synchronization between multiple parties on a wide range of technologies.

**Digital Asset**

# Accelerate business transformation with **Daml and Canton**

**Multi-party Applications** written in privacy focused purpose-built smart contract language

**Shared and distributed ledger,** i.e. what you see is what I see in real time

**Decoupled from the underlying storage layer:** database, blockchain, or distributed ledger

**Build Composable applications** and connect to other apps on other networks

**Write multi-party applications** in Daml ensuring privacy and transparency for only authorized parties

**Create a shared virtual ledger** Canton simplifies secure data sharing between organizations while preserving privacy and authorization

**Leverage existing infrastructure** No need to retire your existing infrastructure to run decentralized and distributed apps

**Grow your Economic Network** Scale your network and get future-ready by adding new participants and letting others create new decentralized applications

ASSET MANAGER
BROKER
GLOBAL CUSTODIAN
LOCAL CUSTODIAN
CLEARING MEMBER
EXCHANGE

∧ daml

# Canton domains can be centralized or decentralized to suit application needs

Canton nodes synchronize through domains. Transactions are encrypted so the domain operator never sees confidential data.
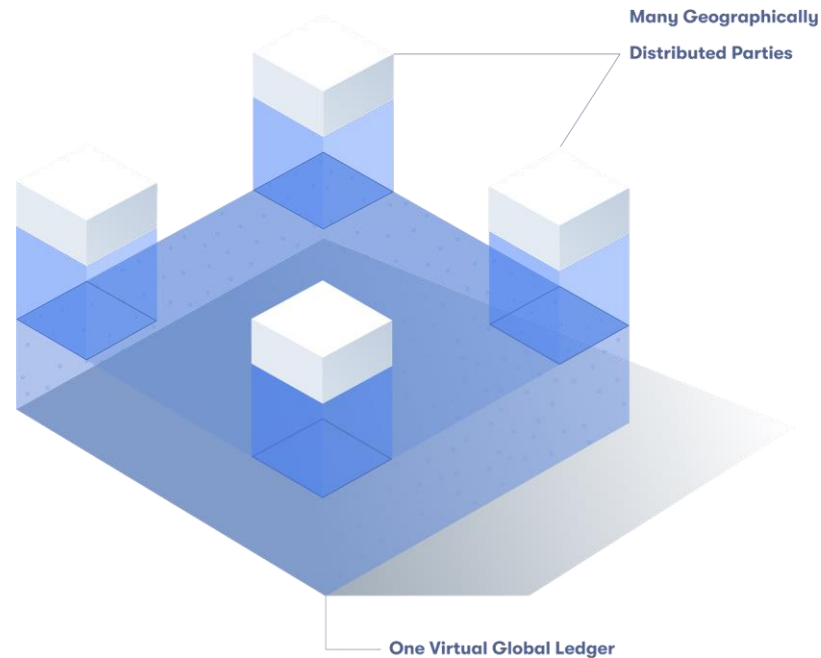
Canton domains can run backed by a relational database or a blockchain if decentralization is required.

| DATABASES | PostgreSQL | ORACLE DATABASE | |
|-----------|------------|-----------------|---|
| BLOCKCHAINS | vmware | HYPERLEDGER FABRIC | HYPERLEDGER BESU |

**Many Geographically Distributed Parties**

**One Virtual Global Ledger**

# PUBLIC CHAINS WILL NOT GET US THERE

Digital Asset

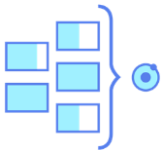None of the most popular chains support the necessary privacy to run commercially sensitive enterprise transactions or even allow for a heterogeneous application ecosystem.

| | Name | Price | 24h % | 7d % | Market Cap |
|---|---|---|---|---|---|
| ☆ | Bitcoin 1 BTC | $41,822.83 | ▲ 0.64% | ▼ 10.35% | $792.00B |
| ☆ | Ethereum 2 ETH | $3,111.37 | ▲ 0.15% | ▼ 18.64% | $370.82B |
| ☆ | Tether 3 USDT | $1.00 | ▼ 0.00% | ▲ 0.02% | $78.29B |
| ☆ | BNB 4 BNB | $449.43 | ▲ 3.70% | ▼ 12.66% | $74.87B |
| ☆ | USD Coin 5 USDC | $0.9998 | ▼ 0.05% | ▼ 0.04% | $43.92B |
| ☆ | Solana 6 SOL | $135.50 | ▼ 2.66% | ▼ 20.98% | $42.22B |
| ☆ | Cardano 7 ADA | $1.14 | ▼ 0.64% | ▼ 14.42% | $38.32B |
| ☆ | XRP 8 XRP | $0.7391 | ▼ 0.37% | ▼ 11.48% | $35.21B |
| ☆ | Terra 9 LUNA | $71.50 | ▲ 3.41% | ▼ 19.57% | $25.56B |
| ☆ | Polkadot 10 DOT | $23.95 | ▼ 1.54% | ▼ 19.95% | $23.64B |
| ☆ | Dogecoin 11 DOGE | $0.1592 | ▲ 6.62% | ▼ 7.09% | $21.22B |

**Digital Asset**

# Daml is designed to offer **Secure Synchronization between parties**

| DATA OWNERSHIP | STRONGLY PERMISSIONED | HIGH PRIVACY | TRUSTLESS & FAULT-TOLERANT |
|---|---|---|---|

Every party owns their data, located in their SoR. Data with a single owner can be modified freely.

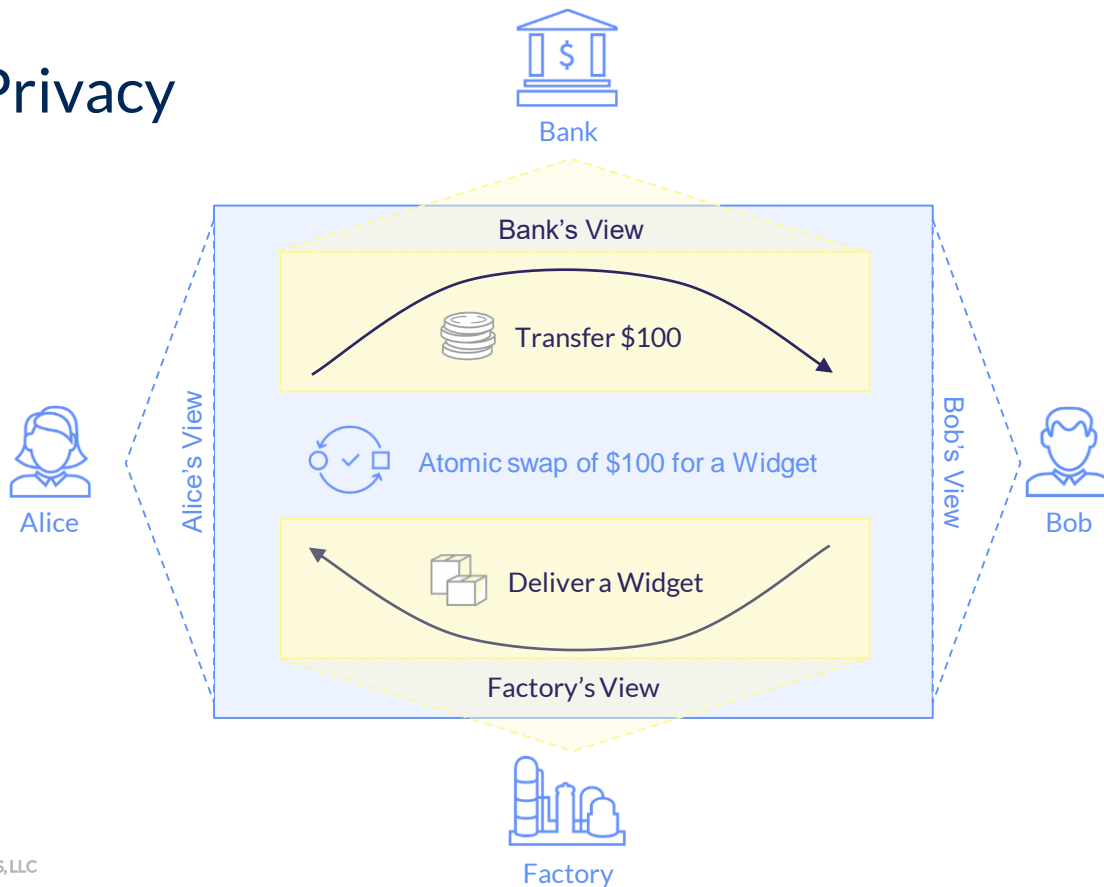Data on the overlaps between views are only read and modified according to defined, permissioned processes.

Data is shared on a strict need-to-know basis.

Malicious or faulty parties cannot falsify another party's SoR.

Desired Privacy in DvPs

Bank

Bank's View

Transfer $100

Atomic swap of $100 for a Widget

Deliver a Widget

Factory's View

Alice's View

Bob's View

Alice

Bob

Factory

# Widget Coding example

```
TX 5 1970-01-01T00:00:00Z (Main:53:11)
  #5:0
  │   known to (since): 'AliceCo' (5), 'BobCo' (5)
  └─> 'AliceCo' exercises AtomicallySwap on #4:4 (DeliveryVersusPayment:WidgetDeal)
            with
      children:
      #5:1
      │   known to (since): 'AliceCo' (5), 'BobCo' (5), 'FactoryCo' (5)
      └─> 'BobCo' exercises TransferWidget on #4:3 (Widget:LockedWidget)
              with
          children:
          #5:2
          │   known to (since): 'AliceCo' (5), 'BobCo' (5), 'FactoryCo' (5)
          └─> create Widget:Widget
              with
                owner = 'AliceCo';
                producer = 'FactoryCo';
                sku = "Widget321"

      #5:3
      │   known to (since): 'AliceCo' (5), 'BobCo' (5), 'BankCo' (5)
      └─> 'AliceCo' exercises TransferCash on #3:3 (Cash:LockedCash)
                with
                  newOwner = 'BobCo'; newAccount = "Bob/USD@Bank"
          children:
          #5:4
          │   known to (since): 'AliceCo' (5), 'BobCo' (5), 'BankCo' (5)
          └─> create Cash:Cash
              with
                account = "Bob/USD@Bank";
                owner = 'BobCo';
                bank = 'BankCo';
                currency = "USD";
                amount = 15000.0000000000
```

```
template WidgetDeal
  with
    buyer          : Party
    seller         : Party
    sku            : Sku
    producer       : Party
    cost           : Decimal
    currency       : Currency

    lockedWidget   : ContractId LockedWidget
    sendToAccount  : Account
    lockedCash     : ContractId LockedCash

  where
    signatory buyer, seller

    choice AtomicallySwap: (ContractId Widget, ContractId Cash)
      controller buyer
      do
        widgetOfBuyer <- exercise lockedWidget TransferWidget
        cashOfSeller <- exercise lockedCash TransferCash
          with
            newOwner = seller
            newAccount = sendToAccount

        return (widgetOfBuyer, cashOfSeller)
```
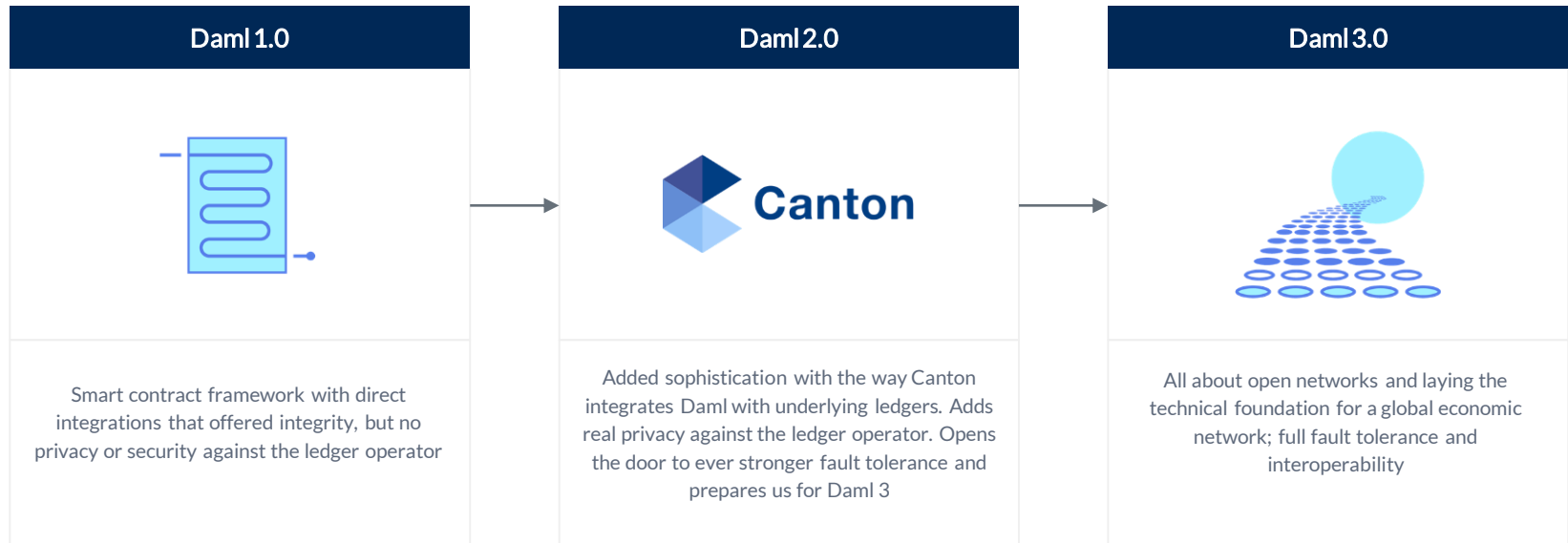
18

# Only Canton **supports sub-transaction-level privacy**

| Ledger | Granularity of privacy | Transactions are composable across privacy sets | Transactions preserve contract privacy | Transactions preserve historical privacy |
|---|---|---|---|---|
| Canton | Smart Contract | ✓ | ✓ | ✓ |
| A DLT Platform | Transaction | —* | ✕ | ✕ |
| Everything else | Channel (semantic variants include zkRollups, Subnets, etc) | ✕ | ✕ | ✕ |

*While technically possible it leaks all contracts to all transaction stakeholders*

**Digital Asset**

# Daml in the real world
## Use cases for Daml-driven applications

| **CLEARING & SETTLEMENT** | **TOKENIZATION & ISSUANCE** | **LIFECYCLE MANAGEMENT** |
|---|---|---|
| Enable users to optimize data use | Create truly smart assets | End-to-end management, across technology infrastructures |

| **PAYMENTS** | **CUSTODY & SAFEKEEPING** | **SUPPLY CHAIN** |
|---|---|---|
| A shared, virtual system of record | With privacy and efficiency | Balance responsiveness and efficiency |

**Digital Asset**

# For more information, visit digitalasset.com
To get started learning (more about) Daml, visit
digitalasset.com/developers/learn

HYPERLEDGER WEBINAR

**Digital Asset**

# Questions?

Digital Asset has a team of industry and technology experts to assist with all questions and POC requests

HYPERLEDGER WEBINAR