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

01 Who we are at Digital Asset
02 What problem we are solving
03 Introduction to the Global Economic Network
04 Meet Daml 2.0
05 Daml use cases
Digital Asset

Digital Asset At-a-Glance

2014 DA FOUNDED
7 GLOBAL OFFICES
$300M SERIES A, B, C, D
4 April Daal Day

Digital Asset

GLOBAL OFFICES

London UK
Zurich Switzerland
Budapest Hungary
New York USA
Hong Kong China
Sydney Australia

DA INVESTORS

ABN AMRO
Accenture
CME Group
Deutsche Börse Group
Goldman Sachs
DTCC
IBM
SBI & Digital Asset Joint Venture
SAMSUNG
vmware
J.P. Morgan
Broadridge
ELDRIDGE
CITI
We are building a global network of networks and Daml is the interface between connected applications and infrastructure.
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What do legacy systems and outdated business processes all have in common across financial transactions?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?
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.
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.
Accelerate business transformation with **Daml and Canton**

- **Decoupled from the underlying storage layer**: database, blockchain, or distributed ledger
- **Build Composable applications** and connect to other apps on other networks
- **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
- **Create a shared virtual ledger**: Canton simplifies secure data sharing between organizations while preserving privacy and authorization
- **Write multi-party applications** in Daml ensuring privacy and transparency for only authorized parties
- **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
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.
PUBLIC CHAINS WILL NOT GET US THERE

None of the most popular chains support the necessary privacy to run commercially sensitive enterprise transactions or even allow for a heterogeneous application ecosystem.
Daml is designed to offer **Secure Synchronization between parties**

---

**DATA OWNERSHIP**

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

---

**STRONGLY PERMISSIONED**

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

---

**HIGH PRIVACY**

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

---

**TRUSTLESS & FAULT-TOLERANT**

Malicious or faulty parties cannot falsify another party's SoR.
Desired Privacy in DvPs

Bank's View
- Transfer $100

Factory's View
- Atomic swap of $100 for a Widget
- Deliver a Widget

Alice's View
- Alice

Bob's View
- Bob

Bank
Factory
Digital Asset

Widget Coding example

```plaintext
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)
```

© 2022 DIGITAL ASSET HOLDINGS, LLC
Only Canton supports sub-transaction-level privacy

<table>
<thead>
<tr>
<th>Ledger</th>
<th>Granularity of privacy</th>
<th>Transactions are composable across privacy sets</th>
<th>Transactions preserve contract privacy</th>
<th>Transactions preserve historical privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canton</td>
<td>Smart Contract</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>A DLT Platform</td>
<td>Transaction</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Everything else</td>
<td>Channel (semantic variants include zkRollups, Subnets, etc)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

*While technically possible it leaks all contracts to all transaction stakeholders*
What’s next?
Daml 1.0 - Daml 2.0 - Daml 3.0

Daml 1.0

Smart contract framework with direct integrations that offered integrity, but no privacy or security against the ledger operator.

Daml 2.0

Added sophistication with the way Canton integrates Daml with underlying ledgers. Adds real privacy against the ledger operator. Opens the door to ever stronger fault tolerance and prepares us for Daml 3.

Daml 3.0

All about open networks and laying the technical foundation for a global economic network; full fault tolerance and interoperability.
Daml in the real world
Use cases for Daml-driven applications

**CLEARING & SETTLEMENT**
Enable users to optimize data use

**TOKENIZATION & ISSUANCE**
Create truly smart assets

**LIFECYCLE MANAGEMENT**
End-to-end management, across technology infrastructures

**PAYMENTS**
A shared, virtual system of record

**CUSTODY & SAFEKEEPING**
With privacy and efficiency

**SUPPLY CHAIN**
Balance responsiveness and efficiency
For more information, visit digitalasset.com
To get started learning (more about) Daml, visit digitalasset.com/developers/learn
Questions?

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