

# Daml: A Smart Contract Language for Securely Automating Real-World Multi-Party Business Workflows

Alexander Bernauer, Sofia Faro, Rémy Hämmerle, Martin Huschenbett, Moritz Kiefer, Andreas Lochbihler, Jussi Mäki, Francesco Mazzoli, Simon Meier, Neil Mitchell, Ratko G. Veprek  
Digital Asset  
Switzerland

## Abstract

Distributed ledger technologies, also known as blockchains for enterprises, promise to significantly reduce the high cost of automating multi-party business workflows. We argue that a programming language for writing such on-ledger logic should satisfy three desiderata: (1) Provide concepts to capture the legal rules that govern real-world business workflows. (2) Include simple means for specifying policies for access and authorization. (3) Support the composition of simple workflows into complex ones, even when the simple workflows have already been deployed.

We present the open-source smart contract language Daml based on Haskell with strict evaluation. Daml achieves these desiderata by offering novel primitives for representing, accessing, and modifying data on the ledger, which are mimicking the primitives of today’s legal systems. Robust access and authorization policies are specified as part of these primitives, and Daml’s built-in authorization rules enable delegation, which is key for workflow composability. These properties make Daml well-suited for orchestrating business workflows across multiple, otherwise heterogeneous parties.

Daml contracts run (1) on centralized ledgers backed by a database, (2) on distributed deployments with Byzantine fault tolerant consensus, and (3) on top of conventional blockchains, as a second layer via an atomic commit protocol.

## 1 Introduction

Automation through distributed applications can increase the efficiency and reduce the cost of conducting business between multiple entities operating in different trust domains. Distributed ledger technologies (DLT), also known as blockchains for enterprises, promise to significantly reduce the high cost of building such automation, by providing a digital ledger with shared execution logic, as well as atomicity and consistency guarantees for processing the shared data across all participating parties. The shared logic is typically defined by user-supplied programs called smart contracts, written in specialized programming languages. To deliver

on the promise of easily building such automation, we argue a smart contract language should satisfy three desiderata:

**Real-world adequacy.** All business workflows execute in the context of one or more backing legal systems, whose law code defines the foundational rules for conducting business. For example, most law code requires contracts to be formed via offer and acceptance [32], and defines remedies and damages when the contract terms are violated. The language should provide concepts to capture such rules, so that they can be seamlessly automated.

In particular, the view “the code is the law” is incompatible with the legal systems used to date [19]: Unless society can be convinced to agree that the DLT state represents what people intended to happen, the state on the ledger cannot be enforced in a court. While there exist attempts to adjust the legal system accordingly (for a narrow range of use cases), the alternative solution requires a DLT to support manual intervention to rectify the situation in the event of an unforeseen real-world eventuality [25], even if this violates the encoded rules. The smart contract language should therefore make explicit where, how and by whom intervention can happen during the execution, without requiring apriori knowledge of the exact type of intervention and without relaxing any of the promised security guarantees.

**Security.** Smart contracts present a large attack surface for malicious DLT participants. This is demonstrated by a long and growing list of publicly known smart contract vulnerabilities [3, 8]. We argue that a secure smart contract language should implement the following requirements:

- Clean language semantics without surprising corner cases helps programmers avoid common security pitfalls. For example, unexpected executions such as reentrancy on the Ethereum virtual machine (EVM) are an ongoing security concern.
- Proper authorization checks for changes to the data ensure that misbehaving entities cannot mess with the shared data beyond the intended scope. The authorization policy should be specified along with the

smart contract code so that they can be easily kept in sync.

- The language should be designed for confidentiality such that specific access policies for stored data are easily defined naturally and the smart contract programmer can easily understand and maintain them.

**Composability.** It should be easy to unilaterally extend the ledger functionality by composing pre-existing workflows into more complex ones. Composability fosters organic growth of DLT solutions and helps to manage complexity. We have identified three challenges here:

- Composition must work even for workflows that have already been deployed and started on a ledger.
- Delegation of authority is needed so that one entity can execute subworkflows that others have pre-authorized.
- Validation for a workflow must automatically focus on the relevant subtransaction and ignore the context.

In this paper, we present Daml, a functional smart contract language designed to satisfy the above desiderata. Daml is open-source and can be obtained from [daml.com](https://daml.com). It is derived from Haskell and thereby inherits many of its language features such as algebraic datatypes, typeclasses, parametric polymorphism, monads, and higher-order functions.

Daml adds novel primitives for representing, accessing, and modifying data on the ledger. When designing these primitives, we took inspiration from the principles behind the legal systems in force today, so that we can be confident that common business workflows can be represented in Daml naturally. Moreover, we deliberately do not attempt to introduce new concepts without a corresponding concept in today's legal systems. For example, trustless bearer tokens and global state invariants have no correspondence in the world of pen-and-paper contracts and are therefore unsupported.

In Daml, the authorization and access policies are specified along with the data and smart contract code as part of the primitives. The programmer annotates every piece of ledger data with a set of owners and a set of controllers who may change the data according to the smart contract code. The semantics then ensures that all owners are guaranteed to see the changes. Moreover, we obtain a clean language semantics by encapsulating the primitives in an Update type constructor with monadic operations; like the IO monad in Haskell, the Update monad helps with separating local pure computations from code that depends on and updates the ledger state.

Daml is compiled to the core language Daml-LF, which is based on Girard's System  $F_\omega$  [13]. The compiler reuses the Glasgow Haskell Compiler (GHC) frontend to parse, type-check, and desugar the Daml code. Unlike Haskell, Daml uses strict call-by-value evaluation that is easier to reason

about and to implement; in a DLT setting, laziness has little benefit as frequent synchronization would trigger evaluation anyway. Daml-LF code is organized in modules and packages, which can be used from Daml with modular compilation. Code is referenced using content-based addressing, i.e., a cryptographic hash to uniquely identify the referenced code.

The ledger interprets the Daml-LF code using the Daml runtime, implemented as a CEK machine with external ledger state. Update statements result in a transaction tree, a hierarchical description of the ledger state changes. The tree structure enables workflow composition at the semantics level: the trees of existing workflows become the subtrees of the combined workflow. For transaction validation, each constituent workflow can focus on its own subtree and ignore the rest.

Daml runs on a variety of ledger implementations while guaranteeing application portability across all of them. Centralized implementations backed by a relational database systems (e.g., Postgres, Oracle) offer a low barrier to adoption and short development cycles. For decentralized deployments, Byzantine fault tolerant state machine replication is available for Daml on VMware Blockchain [29] based on the SBFT protocol [14], for Hyperledger Fabric [2], and for Hyperledger Besu [18], an enterprise version of Ethereum based on IBFT [26], as well as Corda [24]. At the time of writing, Daml smart contracts deployed on such ledgers are used by leading companies in the financial services, healthcare, and supply chain management sectors, processing USD 100b+ in daily transaction volumes. This indicates that the Daml language is fit for purpose. Moreover, Daml provides application portability across these different technologies because the same Daml smart contracts run on all those implementations.

Our main contributions are the following:

- The primitives for smart contracts in Daml and Daml-LF that abstract the principles found in today's legal systems. They enable programmers to easily encode real-world business workflows in smart contract code.
- Daml-LF's approach to data ownership and its authorization rules for ledger changes, which simplify defining write and read access controls for on-ledger data.
- Transaction trees as a model for ledger changes to enable workflow composition after deployment.
- A Daml implementation suitable for use in production.

The paper is organized as follows: We introduce the salient features of Daml by examples in [Section 2](#). Daml-LF's syntax, type system, semantics, and authorization rules are given in [Section 3](#). We explain implementation aspects of the Daml compiler, the Daml runtime, and Daml

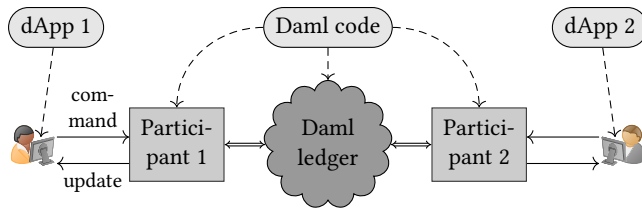


Figure 1. System model for Daml ledgers

ledgers in Section 4. Section 5 discusses related work; Section 6 concludes.

## 2 Daml by Example

Daml is an open-source functional smart contract language with Haskell-like syntax. In this section, we briefly sketch the system model for Daml ledgers (Section 2.1) and then present the core concepts and ideas behind the Daml language through a simple model of cash IOUs (“I Owe You”) (Sections 2.2–2.5). The official documentation with full details is available online at [docs.daml.com](https://docs.daml.com).

### 2.1 System Model

Figure 1 shows the system model of a typical Daml ledger. We distinguish between the shared rules and the users’ strategies of a distributed application (dApp). Only the shared rules are implemented in Daml, whereas every user decides on their own how to express and maintain their strategy for acting on the ledger. The strategy part including the dApp frontend is typically implemented in a mainstream language such as Java or TypeScript. Users interact with the Daml ledger by sending Daml commands to a ledger client, called a participant. The participant interprets such a command by running the Daml smart contract code to produce a ledger update, which is then forwarded to the Daml ledger. The Daml ledger is responsible for enforcing the Daml semantics subject to its trust assumptions. More precisely, the Daml ledger (1) validates that ledger updates conform to the Daml semantics and (2) informs the participants affected by a successful ledger update, which in turn notify their users’ dApps. We discuss Daml ledger implementations in Section 4.3. For now, it suffices to think of a Daml ledger as the participant API endpoints that are synchronized.

### 2.2 Data Modelling

We start the Daml overview with how to model IOUs in Daml. We represent cash amounts using the record type `Cash` defined below using the keyword `data` with record constructor `Cash` and two fields: the `currency` of type `Text` (i.e., strings) and the `amount` of type `Decimal`, i.e., a fixed-point number with 28 digits before and 10 digits after the decimal point.

```

data Cash = Cash with
  currency : Text
  amount   : Decimal
  
```

An IOU is represented as an instance of a smart contract definition, a Daml **template**. Templates are parametrized with the data that is stored in the contract instance, the contract arguments. For a `SimpleIou`, this data consists of the issuer of the IOU, the current owner of the IOU, and the cash that the issuer owes to the owner. The **ensure** clause specifies an invariant on the contract arguments, namely that the cash amount must be positive.

The Daml type `Party` represents an identity that can act on the ledger, in the sense that they can sign contracts and submit transactions. How such actions of parties are cryptographically recorded, verified, and evidenced depends on the implementation. Generally, all Daml ledgers must link any transaction to some cryptographic evidence for authorization and non-repudiation purposes. Linking the evidence to real-world entities is a separate problem, which can be implemented as Daml workflows. This way, we can support the diverse requirements in this field that can not be satisfied with a single approach.

```

template SimpleIou with
  issuer : Party
  owner  : Party
  cash   : Cash
where
  ensure cash.amount > 0.0
  observer owner
  signatory issuer

choice SimpleTransfer : ContractId SimpleIou with
  newOwner : Party
  controller owner
  do create this with owner = newOwner
  
```

The **observer** and **signatory** clauses specify the notification and authorization rules, resp., for the contract instances of a template: The observer parties are notified when a contract instance is created or archived. The non-empty set of signatories specifies the parties whose authority is required to create or archive a contract. In general, Daml ledgers guarantee that a party is notified whenever their authority is used. For `SimpleIou`, the issuer is the signatory and the owner is an observer. There is no need to specify the issuer as another observer because signatories are notified about creations and archivals anyway, as their authority is used.

### 2.3 Encoding Business Logic

In our example, the IOU owner may transfer the IOU to another party. Yet, Daml contracts use a modified UTXO model and are therefore immutable. So an IOU transfer archives the old `SimpleIou` instance and creates a new `SimpleIou` instance for the new owner, atomically within one Daml transaction. Yet, the owner needs the authority of the issuer for both the archival and the creation, because

the issuer is the signatory for `SimpleIou`s. To that end, the `SimpleIou` template defines a `choice SimpleTransfer`. Choices are code entry points for smart contracts and define the rules prescribing how a contract instance can evolve. Here, the `SimpleTransfer` choice returns a `ContractId SimpleIou`, i.e., the identifier of the newly created `SimpleIou` contract instance. The choice takes the new owner as an argument and the keyword `controller` says that the owner’s authority is needed for exercising this choice, i.e., calling this entry point. The `do` block contains the implementation, namely creating a copy of the current IOU `this` with the `owner` field updated to `newOwner`. The `create` function returns the contract ID the ledger assigns to the newly created instance.

The owner’s authority suffices to exercise the `SimpleTransfer` choice on the IOU, but creating the transferred IOU requires the issuer’s authority (as the issuer is the signatory). So this demonstrates a form of authority delegation: When the old IOU was created, the issuer has pre-authorized the consequences of the choices in the template. Therefore, the issuer’s authority is available in the choice implementation and the workflow thus well-authorized.

Every template implicitly defines a parameter-less `Archive` choice with all signatories as controllers that simply archives a contract instance. By default, user-defined choices such as `SimpleTransfer` also archive the contract instance they are being exercised on. Archival means that no further choices can be exercised on the contract. This `Archive` choice ensures that every contract instance can in principle be archived and later deleted from a ledger, i.e., there are no “stuck” Daml contracts. So the signatories can mimic any real-world intervention on the ledger state by jointly archiving obsolete contract instances and appropriately creating new ones.

Yet, this `Archive` choice allows the issuer to unilaterally archive a `SimpleIou` at any time because the issuer is the only signatory. Ideally, the owner should consent if an IOU is taken away from them—or if an IOU is given to them, following the propose-accept pattern of contract formation. We can model this in Daml by making the owner also a signatory of the IOU, as shown in the `Iou` template. `Iou` differs from `SimpleIou` in two points:

- The owner is also a signatory.
- The choice `Transfer` has two controllers, the old and the new owner.

The joint authority of both controllers is needed to exercise the choice. This ensures that enough authorization is available for the `create` of the new IOU in the choice implementation: the issuer and the new owner are signatories.

```
template Iou with
  issuer : Party
  owner  : Party
  cash   : Cash
```

```
where
  ensure cash.amount > 0.0
  signatory issuer, owner

  choice Transfer : ContractId Iou with
    newOwner : Party
    controller owner, newOwner
    do create this with owner = newOwner
```

## 2.4 The Offer-Accept Pattern

The `Iou` contract instance represents a proper bilateral agreement, equivalent to a legal contract on paper. To reach this agreement, the issuer can propose the agreement and the future owner can accept the proposal. We model such a workflow in Daml as a separate template `IouProposal` where only the issuer is a signatory. The terms of the IOU are a template parameter of type `Iou`, which is the record of the contract arguments of the homonymous template. The owner of the proposed IOU controls two choices: `Accept` creates the `Iou` and returns its contract ID; and `Reject` merely archives the proposal returning the singleton `()`. The implicit `Archive` choice allows the issuer to retract its proposal if the issuer neither accepts nor rejects the proposal.

```
template IouProposal with
  iou : Iou
where
  observer iou.owner
  signatory iou.issuer

  choice Accept : ContractId Iou
    controller iou.owner
    do create iou

  choice Reject : ()
    controller iou.owner
    do pure ()
```

For a `Transfer`, the old and new owner to the IOU could run a similar proposal workflow to gather their joint authority for exercising the choice. For frequent transfers, it is more convenient to setup the workflow once in a role contract template such as `IouSendRole`. Here, the receiver agrees to being transferred any `Iou` from the given sender, using the `Send` choice. The keyword `nonconsuming` means that the `Send` choice does not archive the `IouSendRole` contract instance so that it can be used any number of times. Nonconsuming choices help to reduce contention in UTXO-like models. If `Send` was consuming, the choice body would have to recreate the role contract so that another `Iou` can be transferred. Then, the sender could not send several IOUs concurrently, as they have to wait until they see the fresh contract ID assigned to the recreated role contract.

The choice body in the `do` block uses Haskell-style `do` notation for sequencing the operations on the ledger state. The `fetch` primitive looks up the contract arguments for a given contract ID `iouId`; it fails if the contract does not exist or has already been archived. The `assert` checks that the sender wants to transfer an IOU that they indeed own. And

the `exercise` calls the choice `Transfer` on the provided contract ID `iouId` with the given parameters; if the contract has already been archived, an `exercise` fails like the `fetch` primitive.

```
template IouSendRole with
  sender : Party
  receiver : Party
where
  observer sender
  signatory receiver

  nonconsuming choice Send : ContractId Iou with
    iouId : ContractId Iou
    controller sender
  do
    iou <- fetch iouId
    assert (iou.owner == sender)
    exercise iouId Transfer
      with newOwner = receiver
```

## 2.5 Composability

Daml code is organized in modules and packages, and packages can depend on other packages using the `import` keyword. This enables an open business architecture where entities can combine workflows from other entities like building blocks. For example, a financial institution A can provide the `Iou` smart contract with the `Transfer` choice in a module `BasicAssets` and publish it as a (compiled) Daml package `Basic`. Users can already create `Ious` and transfer them. Later, another entity B can build an atomic swap of two `Ious` in another package `Swap` by importing `Basic`. As soon as `Swap` is deployed, users can atomically swap their existing, unchanged `Ious`. In particular, A does not have to upgrade its services. This example demonstrates Daml’s composability property.

Suppose that two parties, the initiator and the responder, want to atomically exchange their `Ious`, say USD 100 issued by the Fed for CHF 90 backed by the Swiss national bank. Atomicity is important to reduce the counterparty risk: without atomicity, if one `Iou` is transferred before the other, the former owner incurs the risk that the other party defaults or goes out of business before transferring the second `Iou`; or commits fraud and never transfers the second `Iou`.

The `Transfer` choice already implements the transfer of a single `Iou`. So we merely need to compose two such transfers in a single Daml transaction. The `TradeProposal` template composes two such transfers, again following the propose-accept pattern. The initiator specifies the contract ID of its `Iou` and the `Iou` conditions it expects to receive in exchange. The responder, i.e., the owner of the expected `Iou`, can accept the trade proposal and immediately settle the trade with its own `Iou` with ID `respId`, where the two `exercise` calls to `Transfer` aggregate the two transfers into a single transaction. The keyword `pure` at the end defines the result of the body, namely the two new contract IDs.

```
template TradeProposal with
  initiator : Party
  initId : ContractId Iou
  expected : Iou
where
  let responder = expected.owner
  observer responder
  signatory initiator

  choice Settle : (ContractId Iou, ContractId Iou) with
    respId : ContractId Iou
    controller responder
  do
    responderIou <- fetch respId
    assert (expected == responderIou)
    newInitId <- exercise respId Transfer
      with newOwner = initiator
    newRespId <- exercise initId Transfer
      with newOwner = responder
    pure (newInitId, newRespId)

  nonconsuming choice DiscloseIou : Iou
  observer responder
  controller initiator
  do fetch initId
```

Before accepting the proposal, the responder should check that `initId` references an `Iou` of the initiator that the responder is willing to receive. Due to Daml’s confidentiality model, the responder cannot simply resolve a contract ID and look at the contract arguments, which may contain confidential business data. Instead, the initiator can disclose the `Iou` to the responder by using the nonconsuming choice `DiscloseIou` where the responder is declared as a choice observer. Daml ensures that choice observers are notified whenever the choice is exercised (similar to how observers declared on the template are notified about creation and archival). Accordingly, the responder observes the `fetching` of `initId` and thereby remembers the mapping from the contract ID to the contract arguments. This mapping is immutable and thus still valid when the `Settle` choice is executed; so there is no need to check that `initId` still refers to the same `Iou` terms.

This concludes the exposition of the Daml language features for this paper. Daml provides further primitive types such as strings, dates, timestamps, generic maps, and in particular various numeric types including non-serializable arbitrary-precision numbers for internal calculations. Other language features not covered in this paper are algebraic data types, Haskell-style typeclasses, exceptions with try-catch blocks, and contract keys for referencing contracts by value instead of by ID. They are documented on [docs.daml.com](https://docs.daml.com).

## 3 Daml-LF

Daml code is compiled into Daml-LF (LF stands for ledger fragment), which is interpreted by Daml ledgers. We now present the core features of Daml-LF, the semantic domain of transaction trees, and the authorization and visibility rules. The full specification of Daml-LF is available online at



$$\begin{array}{c}
\frac{x : \tau \in \Gamma}{\Gamma \vdash x :: \tau} \quad \frac{\Gamma, x : \tau \vdash t :: \sigma}{\Gamma \vdash \lambda x : \tau. t :: \tau \Rightarrow \sigma} \\
\\
\frac{\Gamma, \alpha : k \vdash t :: \tau}{\Gamma \vdash \Lambda \alpha : k. t :: \forall \alpha : \tau. \tau} \quad \frac{\Gamma \vdash t_1 :: \tau \Rightarrow \sigma \quad \Gamma \vdash t_2 :: \tau}{\Gamma \vdash t_1 t_2 :: \sigma} \\
\\
\frac{\Gamma \vdash \tau :: k \quad \Gamma \vdash t_1 :: \forall \alpha : k. \sigma}{\Gamma \vdash t_1 @ \tau :: \sigma[\alpha \mapsto \tau]}
\end{array}$$

Figure 2. Typing rules for System  $F_\omega$ 

[github.com/digital-asset/daml/blob/main/daml-lf/spec/daml-lf-1.rst](https://github.com/digital-asset/daml/blob/main/daml-lf/spec/daml-lf-1.rst). We discuss compilation later in Section 4.1.

### 3.1 System $F_\omega$ without Type-Level Lambdas

Daml-LF is based on System  $F_\omega$ , an extension of the simply-typed lambda calculus proposed by Girard [13]. Moreover, it is heavily inspired by GHC Core, the intermediate language used by GHC [27]. Similar to GHC Core, Daml-LF omits type-level lambdas from System  $F_\omega$ , and adds user-defined data types. So type expressions  $\tau, \sigma$  are built from type variables  $\alpha$ , the function arrow  $\Rightarrow$ , quantification  $\forall \alpha : k. \tau$ , type application  $\tau \sigma$ , and primitive type constructors  $T$ . Kinds  $k$  classify type expressions and rule out ill-formed type expressions, as formalized by the well-kinding judgement  $\Gamma \vdash \tau :: k$ .

$$\begin{array}{c}
\frac{\alpha : k \in \Gamma}{\Gamma \vdash \alpha :: k} \quad \frac{}{\Gamma \vdash \Rightarrow :: \star \rightarrow \star \rightarrow \star} \quad \frac{\Gamma, \alpha : k \vdash \tau :: k'}{\Gamma \vdash \forall \alpha : k. \tau :: k'} \\
\\
\frac{\Gamma \vdash \tau :: k_1 \rightarrow k_2 \quad \Gamma \vdash \sigma :: k_1}{\Gamma \vdash \tau \sigma :: k_2} \quad \frac{T_{\text{Prim}} \text{ has kind } k}{\Gamma \vdash T_{\text{Prim}} :: k}
\end{array}$$

The primitive type constructors  $T_{\text{Prim}}$  include the singleton type `Unit`, Booleans `Bool`, 64-bit integers `Int64`, fixed-point decimals `Decimal`, strings `Text`, dates `Date`, and timestamps `Timestamp`, all of kind  $\star$ , and the type constructor for lists `List` of kind  $\star \rightarrow \star$ . The primitive type constructors for smart contracts are below presented in Section 3.2.

Terms  $t$  are built from variables  $x$ , function abstraction  $\lambda x : \tau. t$ , function application  $t_1 t_2$ , type abstraction  $\Lambda \alpha : k. t$ , type application  $t @ \tau$ , and primitive constants  $C$ . All abstractions are annotated by the type or kind so that type checking is decidable. The typing rules for  $\Gamma \vdash t :: \tau$  are standard (Figure 2).

Well-kinding and well-typing is relative to a set of user-defined Daml-LF types and constants declared in Daml-LF modules. Daml-LF ensures that every package has a globally unique name (and so do the package's modules): The package identifier is a cryptographic hash of the Daml-LF code of the package, i.e., a form of content-based addressing. In this paper, we omit the package identifier and module name for readability and just use the unqualified Daml name. For example, the following Daml datatype declaration of binary trees with labelled leaves

```

data Tree a
= Leaf with leaf : a
| Node with
    left : Tree a
    right : Tree a

```

is represented by three Daml-LF type constructors, all of kind  $\star \rightarrow \star$ :

- A record type `Tree.Leaf` with a single field `leaf` for the argument of the `Leaf` constructor.
- The record type `Tree.Node` with fields `left` and `right` for the argument of the `Node` constructor.
- The variant type `Tree` with variants `Leaf` and `Node`.

Every record comes with a record constructor, field projections, and field update operations. Variant types come with constructors and pattern matching support. The typing rules enforce that these operations are fully applied; if necessary, the Daml compiler  $\eta$ -expands partially applied occurrences. This convention ensures that all constructors appear fully applied to their arguments, which simplifies the implementation of datatypes. Again, this is in line with GHC Core. For example, the typing rules for the record constructor `Tree.Node` and the variant constructor `Node` are the following:

$$\begin{array}{c}
\frac{\Gamma \vdash \tau :: \star \quad \Gamma \vdash e_1 :: \tau \quad \Gamma \vdash e_2 :: \tau}{\Gamma \vdash \text{Tree.Node } @ \tau e_1 e_2 :: \text{Tree.Node } @ \tau} \\
\\
\frac{\Gamma \vdash \tau :: \star \quad \Gamma \vdash e :: \text{Tree.Node } @ \tau}{\Gamma \vdash \text{Node } @ \tau e :: \text{Tree } @ \tau}
\end{array}$$

### 3.2 Primitives for Smart Contracts

Daml-LF has three type constructors for defining smart contracts:

- `Party :  $\star$`  for parties, i.e., a subset of strings
- `ContractId :  $\star \rightarrow \star$`  for contract identifiers (IDs)
- `Update :  $\star \rightarrow \star$`  for updates of the ledger state

Contract IDs are parametrized with a template type like in Daml; they uniquely identify contract instances of the template. Contract IDs are opaque to Daml programs so the semantics of Daml program is independent of how the Daml ledger allocates contract IDs. They can only be created via `create` commands within Daml-LF, but arbitrary values can be passed in as serialized arguments, as explained in Section 3.3. The primitive comparison operation  $\leq_{\text{ContractId}}$  allows for ordering contract IDs so that contract IDs can be used in functional data structures such as search trees.

$$\begin{array}{c}
\frac{\Gamma \vdash \tau :: \star \quad \Gamma \vdash e_1 :: \text{ContractId } \tau \quad \Gamma \vdash e_2 :: \text{ContractId } \tau}{\Gamma \vdash \leq_{\text{ContractId}} @ \tau e_1 e_2 :: \text{Bool}}
\end{array}$$

The type constructor `Update` of kind  $\star \rightarrow \star$  represents the monad of ledger updates. The monadic operations `pure` and `bind`  $x : \tau \leftarrow e$  in  $e'$  inject values into the monad and sequence dependent ledger updates. There are three primitive monad

operations:  $\text{create}@T\ e$ ,  $\text{fetch}@T\ e$ , and  $\text{exercise}@T\ Ch\ e_1\ e_2$ . They model (1) creating a contract instance of template  $T$  with argument  $e$ , (2) looking up the contract arguments of  $e$ , and (3) exercising the choice  $Ch$  on  $e_1$  with choice argument  $e_2$ . As for records and variants, we require those operations to be fully applied. In the typing rules below,  $T$  ranges over templates in the Daml-LF program.

$$\begin{array}{c}
\frac{\Gamma \vdash \tau :: \star \quad \Gamma \vdash e :: \tau}{\Gamma \vdash \text{pure } @\ \tau\ e :: \text{Update } \tau} \\
\\
\frac{\Gamma \vdash \tau_1 :: \star \quad \Gamma \vdash e_1 :: \text{Update } \tau_1 \quad \Gamma, x : \tau_1 \vdash e_2 :: \text{Update } \tau_2}{\Gamma \vdash \text{bind } x : \tau_1 \leftarrow e_1 \text{ in } e_2 :: \text{Update } \tau_2} \\
\\
\frac{\Gamma \vdash e :: T}{\Gamma \vdash \text{create } @\ T\ e :: \text{Update } (\text{ContractId } T)} \\
\\
\frac{\Gamma \vdash e :: \text{ContractId } T}{\Gamma \vdash \text{fetch } @\ T\ e :: \text{Update } T} \\
\\
\frac{\Gamma \vdash e_1 :: \text{ContractId } T \quad \Gamma \vdash e_2 :: \tau \quad \text{Choice } Ch \text{ has argument type } \tau \text{ and return type } \sigma}{\Gamma \vdash \text{exercise } @\ T\ Ch\ e_1\ e_2 :: \text{Update } \sigma}
\end{array}$$

### 3.3 Serializable Types

Daml-LF distinguishes between serializable and non-serializable types. Serializable types are first-order data, free of computation. In other words, a value of a serializable type is guaranteed to not contain any functions in it. Contract and choice arguments and choice results must be serializable. This ensures that all logic involved in a contract is encoded in its definition, and not by its arguments. While Daml-LF could in theory support higher-order contract arguments, this limitation is desirable for the following reasons:

- Humans can audit Daml-LF contracts and fully understand their implications without making assumptions about their arguments. This would be impossible if the arguments contained logic (i.e. functions). For example, if functions were allowed to appear in choice arguments, the controller could run arbitrary Daml code with the signatories' authorization.
- This decoupling between code and data also allows evolving the interpreter and the backing ledger more freely. For example, if we want to add optimization passes and just-in-time compilation before interpretation while storing data in contract arguments, such optimizations would have to retain enough data to reconstruct the unoptimized Daml-LF representation of the functions so that all parties involved can validate the stored data independent of their optimization settings. Similarly, it seems challenging to encode lambdas into arithmetic circuits if we were to support zero-knowledge proofs in the future.

- Isolating the set of types to a small universe of first-order types allows us to store contract data in a variety of databases, from centralized SQL servers to more traditional blockchains; and to establish a mapping with the existing data types for each platform. For instance, Daml-LF records can be turned into SQL columns, which in turn allow for efficient querying.

Type checking of template declarations enforces that template and choice parameter types are serializable. The primitive types are serializable and so are lists and contract IDs if their type argument is. For a Daml-LF record type  $R$  to be serializable, the type arguments and every field's type must be serializable. Similarly for a variant type  $V$ , the type arguments and each variant's argument type must be serializable.

For example, the Daml record `Cash` from [Section 2](#) is serializable because the two fields `currency` and `amount` have serializable types. For `Tree`, the polymorphic records `Tree.Leaf` and `Tree.Node` for the constructor arguments are serializable iff the type argument is serializable, and the same holds for the variant `Tree`. So `Tree Int64` is serializable.

As non-serializability propagates through type constructors, `Tree (Int64  $\Rightarrow$  Bool)` is not serializable either. Neither are ledger update types `Update  $\alpha$`  serializable; ledger updates can only be executed against the ledger as described below.

### 3.4 Semantics

Daml-LF has a call-by-value semantics defined by two big-step evaluation relations for closed terms. First, expression evaluation  $e \Downarrow r$  produces a result  $r$ , i.e., an expression value `Val  $v$`  or a fatal error `Err  $err$`  with an error message  $err$ . Expression values  $v$  include lambda abstractions and the literal values of built-in datatypes, contract IDs, parties, etc. Fully applied record and variant constructors form expression values iff all arguments are expression values. For example,

$$\text{Tree.Leaf } @\ (\text{Int64} \Rightarrow \text{Int64})\ (\lambda x : \text{Int64}. x + 1)$$

is a value because the lambda abstraction is a value and `Tree.Leaf` is fully applied. Expression evaluation may also return an `Update` expression  $u$ , which is considered an expression value too. Update expressions come in five forms:

- `create @  $T\ v$`  for creating a contract instance of template  $T$  with value  $v$  as contract argument
- `exercise @  $T\ Ch\ v_{\text{cid}}\ v_a$`  for exercising the choice  $Ch$  of template  $T$  on contract ID  $v_{\text{cid}}$  with choice argument  $v_a$
- `fetch @  $T\ v$`  for looking up the contract arguments of contract ID  $v$
- `pure @  $\tau\ v$`  for a pure value  $v$  of type  $\tau$
- `bind  $x : \sigma \leftarrow v$  in  $e$`  for a (blocked) computation of ledger changes

Second, the Update interpretation relation  $\langle u, s \rangle \Downarrow R$  interprets the above forms of ledger changes, using expression evaluation for the subterms. It depends on the current ledger state  $s$ , which is a map from contract IDs to the following information about the contract instance:

- The template identifier  $T$
- The contract arguments as an expression value  $v$  of a serializable type
- The signatories  $S$  and observers  $O$
- The contract state  $cs$  (Active or Archived)

A contract ID  $cid$  is fresh in  $s$  if  $s$  is undefined for  $cid$ . Update results  $R$  are either a value  $v$ , a transaction  $tx$  and an updated state  $s'$ , or a fatal error  $Err\ err$  with an error message  $err$ .

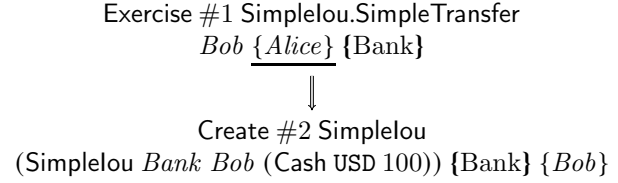
Transactions are Daml's hierarchical representation of ledger updates. A transaction  $tx$  is a list of actions, and an action  $a$  takes one of the following forms:

- Create  $cid\ T\ v\ S\ O$  represents the creation of a contract instance of template  $T$  with argument  $v$  under the contract ID  $cid$ , with signatories  $S$  and observers  $O$ .
- Exercise  $cid\ T.Ch\ v\ K\ C\ Q\ S\ tx$  represents the exercise of choice  $Ch$  in template  $T$  on contract with ID  $cid$  with choice argument  $v$ . The choice kind  $K$  is either consuming or nonconsuming. The set  $C$  captures the controllers,  $Q$  the choice observers, and  $S$  the signatories of the exercised contract. The Exercise action contains the result of executing the choice implementation as a subtransaction  $tx$ , which we refer to as its consequences.
- Fetch  $cid\ T\ S\ O$  represents that looking up the contract ID  $cid$  found a contract instance of template  $T$  with signatories  $S$  and observers  $O$ .

So actions are roots of trees and a transaction is a forest. For example, suppose that Alice submits a command to transfer her `SimpleIou` issued by the Bank over USD 100, with contract ID #1, to Bob. This command translates to executing the following Daml-LF expression, where we have omitted all the record clutter introduced by the Daml compiler:

```
exercise @ SimpleIou.SimpleTransfer #1 Bob
```

Interpreting this expression produces the transaction shown in Figure 3, with a single root whose consequence is shown as the child. Controller sets are underlined, signatory sets are in boldface, observer sets are not decorated, empty sets are omitted altogether, and all exercise actions are by default consuming. The exercise generates the consuming Exercise node at the root, and the `create` operation in the body of the `SimpleTransfer` choice leads to the Create child node.



**Figure 3.** Transaction tree for Alice transferring a `SimpleIou` of USD 100 to Bob

Update interpretation  $\langle u, s \rangle \Downarrow R$  works as follows. Here, we only discuss the successful case; if any check or sub-evaluation fails, interpretation generates an appropriate error and aborts.

For create @  $T\ v$ :

1. Find the template definition for  $T$ .
2. Evaluate the `ensure` predicate on  $v$  using  $\Downarrow$  and check that the result is `Val True`.
3. Evaluate the `signatory` and `observer` functions of  $T$  and convert the resulting Party lists into sets  $S$  and  $O$ .
4. Pick a contract ID  $cid$  that is fresh in  $s$ .
5. The interpretation result consists of the value  $cid$ , the transaction  $[Create\ cid\ T\ v\ S\ O]$ , and the updated state  $s[cid \mapsto (T, v, S, O, Active)]$ .

For exercise @  $T\ Ch\ v_{cid}\ v_{arg}$ :

1. Look up the contract data in the state  $s$ , say  $s(v_{cid}) = (T', v_c, S, O, cs)$ , and check that  $T' = T$  and  $cs = Active$ . Set  $K = consuming$  if  $Ch$  is consuming and  $K = nonconsuming$  otherwise.
2. Evaluate the `controller` and `observer` expression over the choice  $Ch$  on the contract argument  $v_c$  and the choice argument  $v_{arg}$  and convert the resulting Party lists into sets  $C$  and  $Q$ .
3. Substitute  $v_c$  and  $v_{arg}$  for the formal template and choice parameters in the choice body expression and evaluate it to an update expression  $u'$ .
4. Interpret  $u'$  in state  $s'$  where  $s' = s[v_{cid} \mapsto (T, v_c, S, O, Archived)]$  if  $Ch$  is consuming and  $s' = s$  otherwise. The result of interpreting  $u'$  consists of a value  $v_r$ , a transaction  $tx$ , and a new state  $s''$ .
5. The result of interpreting the Exercise then consists of  $v_r$ , the transaction  $Exercise\ v_{cid}\ T.Ch\ v_{arg}\ K\ C\ Q\ S\ tx$ , and the state  $s''$ .

For fetch @  $T\ v$ :

1. Look up the contract data in  $s$ , say  $s(v) = (T', v_c, S, O, cs)$ , and check that  $T = T'$  and  $cs = Active$ .
2. The result consists of the value  $v_c$ , the transaction  $[Fetch\ v_{cid}\ T\ S\ O]$ , and the unchanged state  $s$ .

For pure @  $\tau\ v$ , the result is  $(v, [], s)$ . Sequencing bind  $x : \sigma \leftarrow v$  in  $e$  composes the resulting transactions:

1. Interpret  $v$  in  $s$ , say  $\langle v, s \rangle \Downarrow (v_1, tx_1, s_1)$ .



2. Substitute  $v_1$  for  $x$  in  $e$  and evaluate it,  $e[x \mapsto v_1] \Downarrow u$ .
3. Interpret  $u$  in  $s_1$ , say  $\langle u, s_1 \rangle \Downarrow (v_2, tx_2, s_2)$ .
4. The result then is  $(v'', tx_1 ++ tx_2, s'')$ , where  $++$  concatenates two lists.

As can be seen, the ledger state of a contract ID is updated at most twice: Once when the contract ID is picked for a new contract instance and once when a consuming choice is exercised on it. Such immutable contract instances are reminiscent of Bitcoin’s UTXO model of transaction outputs, with the difference that Daml contract instances can store arbitrary data and not just an amount and a validation function. We compare Daml’s execution model in more detail to related work in [Section 5](#).

### 3.5 Turing Completeness

Daml-LF expressions do not contain a recursive binder such as Haskell’s `let` or OCaml’s `let rec`. Instead, a Daml-LF module can contain an arbitrary number of top-level *value definitions*, which bind a name to a Daml-LF expression, as opposed to defining a contract. Value definitions can be mutually recursive and therefore endow Daml-LF with unrestricted recursion and make it Turing complete.

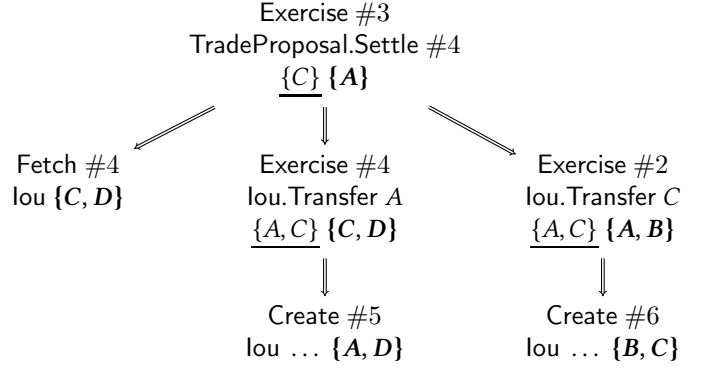
Moreover, Daml-LF admits non-monotonic datatypes, which can also be used to define fixpoint combinators without explicit recursion, as shown by the  $Z$  fixpoint combinator `fix`:

```
data Mu a = Mu with unroll : Mu a -> a
fix : ((a -> a) -> (a -> a)) -> a -> a
fix f =
  let x = Mu (\y -> f (\v -> (unroll y) y v))
  in f (\v -> (unroll x) x v)
```

Making Daml-LF total would not bear any practical advantages—in contrast to type-theory based theorem provers, where soundness relies on a total, non-turing complete language. What matters for DLT applications is the time it takes to compute a function; and total languages do not exclude writing functions that take thousands of years to compute. Instead, ledger implementations may assign a cost to each Daml-LF evaluation step and use this cost model for resource management, similar to Ethereum’s gas model [31].

### 3.6 Authorization Rules

In [Section 2](#), we sketched Daml’s authorization rules with signatories and controllers. Yet, authorization is not checked by the evaluation semantics from the previous section. Instead, we define the authorization rules on transactions. We write  $\mathcal{A} \vdash_a a$  and  $\mathcal{A} \vdash_a tx$  if the action  $a$  or the transaction  $tx$  is well-authorized in the authorization context  $\mathcal{A}$ , where  $\mathcal{A}$  a set of parties. When a party  $A$  submits a Daml command



**Figure 4.** Transaction for  $C$  exercising the `Settle` choice on a `TradeProposal` by  $A$  (contract ID #3) for swapping an `Iou` issued by  $B$  (#2) against one issued by  $D$  (#4)

to a ledger, the authorization context for the resulting transaction as a whole consists only of  $\{A\}$ . However, the authorization context can grow and change for sub(trans)actions of Exercise actions.

The formal authorization rules are given below. A `Create` action is well-authorized in the context  $\mathcal{A}$  iff  $\mathcal{A}$  contains all signatories. For a `Fetch`,  $\mathcal{A}$  must contain at least one signatory or observer of the fetched contract. The rule for Exercise is what enables delegation: First,  $\mathcal{A}$  must contain all controllers, as expected. Second, well-authorization of the consequences is checked in the context of the signatories and controllers. This encodes that a signatory has pre-authorized the consequences of the choices when the contract instance was created. Delegation is not transitive, though, as the authorization context  $\mathcal{A}$  of the Exercise action does not propagate to the consequences. Finally, a transaction is well-authorized if all its (top-level) actions are.

$$\begin{array}{c}
 \frac{S \subseteq \mathcal{A}}{\mathcal{A} \vdash_a \text{Create } cid \ T \ v \ S \ O} \quad \frac{\mathcal{A} \cap (S \cup O) \neq \{\}}{\mathcal{A} \vdash_a \text{Fetch } cid \ T \ S \ O} \\
 \\
 \frac{C \subseteq \mathcal{A} \quad S \cup C \vdash_a tx}{\mathcal{A} \vdash_a \text{Exercise } cid \ T.Ch \ v \ K \ C \ Q \ S \ tx} \\
 \\
 \frac{\forall a \in tx. \mathcal{A} \vdash_a a}{\mathcal{A} \vdash_a tx}
 \end{array}$$

Delegation not being transitive is a deliberate design choice in Daml. It simplifies reasoning about well-authorization of Daml programs because the authorization context for a choice implementation is determined solely by the template definition and thus independent of the calling context of the choice. On the one hand, this helps Daml programmers when they wonder whether sufficient authority is available in a choice implementation. On the other hand, it is also a security feature important for modularly composing workflows: When workflow building

blocks (i.e., choices) are composed into more complex ones as shown in the `Settle` choice, the authorization safety analysis for the building blocks remains unaffected. If the consequence of an `Exercise` action were instead checked in the augmented context  $\mathcal{A} \cup \mathcal{S} \cup \mathcal{C}$ , then the additional parties in  $\mathcal{A}$  could make a subaction well-authorized that in isolation would not be.

If transitive delegation is needed, the required signatories must be declared as explicit controllers of the `exercised` choices in the choice body. This pattern can be seen in the `Settle` choice where the initiator’s authority is passed through the `exercise` on `respId` via the `newOwner` controller of the `Transfer` choice to the creation of the new `IOU`. Figure 4 shows the transaction where *C* exercises the `Settle` choice on a `TradeProposal` (contract ID #3) where *A* offers *C* to trade the `IOU` with ID #2 issued by *B* for an `IOU` issued by *D* (#4). This transaction is well-authorized in the context  $\{C\}$ . Crucially, *A*’s authority from being a signatory on the `TradeProposal` contract #3 joins *C*’s authority from being the controller of the `Exercise` in the controllers  $\{A, C\}$  of the `Exercise` #4 so that *A*’s authority is available when creating #5.

## 4 Implementation

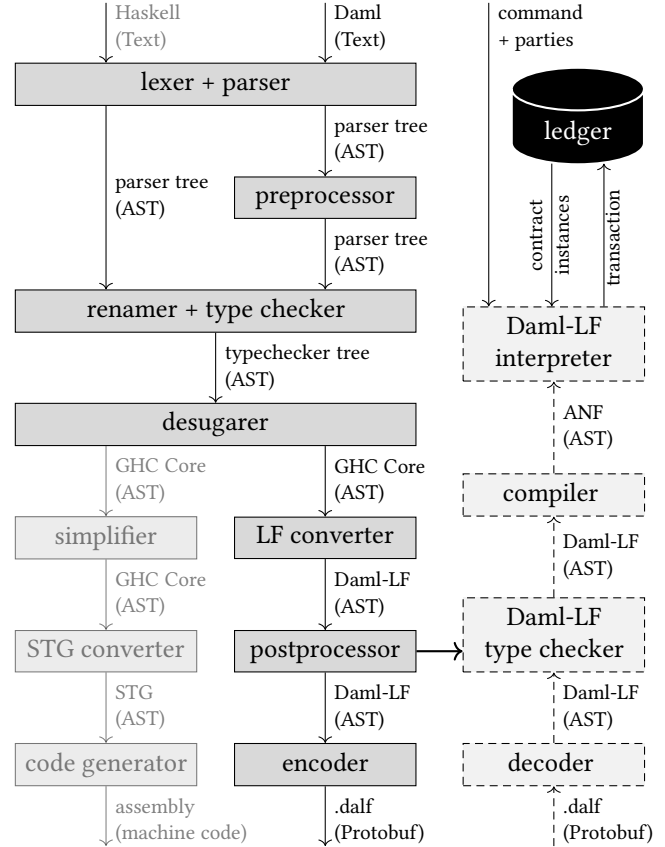
We now describe how we have implemented the Daml compiler from Daml to Daml-LF (Section 4.1) and the Daml-LF runtime (Section 4.2), and sketch how the Daml-LF runtime has been integrated into different ledgers (Section 4.3).

### 4.1 Daml Compiler

The Daml compiler compiles the Daml modules in a Daml package into a `.dalf` file, a Protobuf encoding of the generated Daml-LF code. The compiler uses the Glasgow Haskell Compiler (GHC) frontend to parse, type-check, and desugar the Daml code into GHC’s intermediate language GHC Core, a variant of System FC [30].

Initially, we implemented a Daml compiler from scratch, designing the language, writing parsers, type checkers and a desugarer. However, adding all the syntactic conveniences and language features was a daunting challenge. With every new feature, new bugs were introduced, especially around parsing and type checking. So we changed track and decided to reuse the frontend of GHC, a well-established compiler that has benefited from many decades of development. As a result, Daml now provides many of Haskell’s language features and syntactic conveniences that make developers productive, e.g., typeclasses and pattern matching with guards.

At the same time, we recognised there were weaknesses in Haskell that were very apparent when developing Daml. We thus set out to improve these aspects both for Daml users and for Haskell users. In particular, the Haskell record system has long been recognised as somewhat weak compared to other languages, so we started the work on the



**Figure 5.** Pipelines for GHC (left), the Daml compiler (middle), and the Daml-LF runtime (right)

`RecordDotSyntax` proposal, along with many other members of the open source Haskell community. It is now available in the most recent release of GHC (version 9.2) [12]. We also developed a Daml/Haskell IDE called `ghcide`. This project was later merged with another IDE project to produce the Haskell Language Server [21], which has become the standard Haskell IDE.

Figure 5 shows, from left to right, the pipelines of GHC, the Daml compiler, and the Daml-LF runtime, which we discuss later in Section 4.2. Pipeline stages are shown as rectangles and the arrows are labelled by the data that flows from one stage to the next. The wide rectangles are shared between GHC and the Daml compiler, i.e., the lexer, parser, renamer, type checker, and the desugarer. The renamer, type checker, and desugarer are exactly the same.

For Daml’s `template` and `choice` syntax, we have extended the GHC lexer and parser with appropriate parse rules. The modified parser desugars templates and choices into Haskell typeclasses so that the later stages can remain unchanged. Each template operation has their own Haskell typeclass so that upgrading is easy when we add more operations.

```
class HasEnsure t where ensure :: t -> Bool
class HasObserver t where observer :: t -> [Party]
```

```

class HasSignatory t where signatory :: t -> [Party]
class HasCreate t where
  create :: t -> Update (ContractId t)
class HasFetch t where fetch :: ContractId t -> Update t
class HasExercise t c r | t c -> r where
  exercise :: ContractId t -> c -> Update r

```

The `HasExercise` typeclass is parametrized by the template `t` and the choice argument `c` and the choice result `r`, where the combination of `t` and `c` uniquely determines `r`. This works because every choice generates a separate record type for the choice arguments. The parser also generates appropriate instance declarations for all declared templates and choices.

For example, the `SimpleIou` template becomes the Haskell datatype for the template arguments with typeclass instances for `HasEnsure`, `HasObserver`, etc. The primitive `Update` operations retained as type-level strings until the LF conversion phase replaces them with the appropriate Daml-LF primitives. The `SimpleTransfer` choice similarly yields a datatype for the choice argument with an `HasExercise` instance.

```

data SimpleIou = SimpleIou with
  issuer : Party
  owner  : Party
  cash   : Cash

instance HasEnsure SimpleIou where
  ensure this = (cash.amount this) > 0.0
instance HasObserver SimpleIou where
  observer this = [owner this]
instance HasSignatory SimpleIou where
  signatory this = [issuer this]
instance HasCreate SimpleIou where
  create = primitive @ "UCreate"
instance HasFetch SimpleIou where
  fetch = primitive @ "UFetch"

data SimpleTransfer = SimpleTransfer with
  newOwner : Party

instance HasExercise
  SimpleIou SimpleTransfer (ContractId SimpleIou)
  where exercise = primitive @ "UExercise"

```

The new preprocessor provides early warnings and errors of Haskell features that are not available in Daml, e.g., unsupported language extensions like GADTs. It also injects Daml-specific imports into the modules so that the later stages can handle the generated template code.

Next, the abstract syntax tree (AST) is processed by the renamer, type checker, and desugarer. The desugarer in particular replaces typeclasses with dictionaries [15]. Thereafter, the AST is in GHC Core and the Daml compiler departs from GHC. The GHC simplifier, which optimizes GHC Core, is unfortunately unusable as Haskell's lazy evaluation is baked deeply into the optimization rules. Instead, the LF converter transforms GHC Core into Daml-LF. Thereby, it converts these typeclass instances back into Daml-LF templates and choices and it also replaces the `primitive` placeholder with

the appropriate primitive operations in Daml-LF. The conversion fails if GHC Core uses features from System FC that are not present in Daml-LF, e.g., GADTs.

The rest of the pipeline is mostly standard: The postprocessor first cleans up the generated Daml-LF code and applies Daml-LF-specific optimizations. Then, it typechecks the resulting Daml-LF code, as an extra safe-guard against bugs in the compiler stages. Finally, the encoder serializes the code as a binary Protobuf message, which is stored as a `.dalf` file.

We have made sure that builds with the Daml compiler are repeatable when run in single-threaded mode. That is, if the same Daml input program is compiled with the same version of the Daml compiler, then the same `.dalf` file will be generated. This is key for content-based addressing in Daml-LF, as every entity can simply recompile a Daml package if they do not want to trust the source of a shared `.dalf` file.

## 4.2 Daml-LF Runtime

The Daml-LF interpreter sits at the heart of the Daml-LF runtime. As illustrated in Figure 5 on the right, its input are commands of the form `create T v` or `exercise cid Ch v` for creating a contract of template `T` or exercising a choice `Ch` on contract ID `cid` with argument `v`. It also receives the list  $\mathcal{A}$  of parties submitting the commands. During interpretation, it queries the Daml ledger (or a cache thereof) for the needed contract instances. The output consists of a transaction in the happy case or an appropriate error. The transaction is then handed over to the Daml ledger for validation and state update.

The interpreter loads the referenced `.dalf` packages and their dependencies on demand via the package loader. The package loader first decodes the Protobuf-encoded Daml-LF code and typechecks it again. Then, another compilation step further transforms Daml-LF into a simpler non-serializable intermediate language in administrative normal form [11].

When all required packages have been loaded, the interpreter converts the commands into `Update` expressions and evaluates them according to the Daml-LF semantics  $\langle c, \_ \rangle \Downarrow \_$ , using an efficient CEK machine implementation [10]. If all evaluations succeed, the overall output consists of the concatenated transactions.

The authorization rules are also checked on the fly while the transaction is built up. If interpretation tries to exercise a choice, fetch a contract, or create a contract without the required authority, interpretation fails with an authorization error *before* it starts to evaluate the associated smart contract. This order matters because otherwise an interpretation error such as a failed `assert` or `ensure` clause could leak sensitive information via the error message to the submitter.

### 4.3 Ledger Integrations

Daml smart contracts run on a Daml ledger, as shown in Figure 1. dApps access the ledger via the Ledger API offered by the participants (as gRPC and HTTP JSON service): they can submit Daml commands and receive synchronous and asynchronous updates of the ledger state. This event-driven programming model over the uniform Ledger API makes Daml dApps portable across different technologies, as the same Daml smart contracts run on all integrations. To cater for different use cases, integrations with different ledger technologies are available, with different performance, security and confidentiality properties. We only list the available options for validating transactions and persisting the ledger; a meaningful comparison is beyond the scope of this paper.

- A SQL database such as Postgres and Oracle operated by a single trusted entity.
- A distributed node network run by possibly multiple entities using state machine replication for the deterministic Daml-LF interpreter, such as VMware Blockchain [29], Hyperledger Fabric, and Besu.
- As a second layer on top of a blockchain or consensus algorithm, where the contract instances are stored only locally on the participants and the data is encrypted end-to-end when in transit between participants. Here, the underlying ledger technology is used only for ordering the updates and coordinating the commits.

## 5 Related Work

Daml's ledger state is reminiscent of Bitcoin's UTXO model [22]: a contract creation corresponds to a "transaction output" identified by the contract ID, which can be "spent" by exercising a consuming choice. In between, a Daml contract may be used arbitrarily often via nonconsuming choices, to reduce contention.

Chakravarty et al. [7] proposed the extended UTXO (eUTXO) execution model, which is used by the Plutus [6] smart contract language running on the Cardano blockchain [5]. In eUTXO, the validation function for spending a transaction output takes an additional input parameter, the datum, which contains arbitrary contract-specific data. In Daml terminology, this datum corresponds to the contract arguments and the validator function is represented by the choices of the corresponding template. Daml contracts are more flexible in that they are not tied to a cryptocurrency value (the transaction output) and can be used consuming or nonconsuming. As eUTXO transactions are flat, the validators must manually figure out the relevant transaction parts. Daml transactions encode this in the tree structure and thus ensure composability.

Ethereum smart contracts are based on accounts with mutable state rather than UTXO. Accounts avoid the

problem that contract IDs become stale when an update archives the contract instance and re-creates an updated one. Conversely, accounts suffer from mutability in that the transaction submitter cannot pre-determine the precise effects, e.g., when the transaction depends on data that changes between submission and execution. Dangling contract IDs can be avoided in Daml by referencing contracts by parts of the stored data instead of by ID (not discussed in this paper).

Corda [24] is a DLT platform whose ledger state is a set of immutable contract instances as in Daml. Contract instances are defined using JVM classes that specify both an instance's data and how to validate transactions that create, reference, or consume such an instance. Corda requires programmers to specify validation as a boolean predicate on whole transactions, which leaves ample room for mistakes: too lenient checks lead to security vulnerabilities, while too stringent checks hamper workflow composability. Corda ships contract code as .jar files and executes them on the JVM. Contract execution on the JVM can be non-deterministic, which may lead to ledger participants getting out of sync; a problem avoided by Daml, as it is deterministic by construction.

In the remainder of this section, we compare Daml to closely related smart contract languages. Tolmach et al. [28] provide a good overview over the wider space.

Peyton Jones et al. [23] proposed a functional library of small building blocks and combinators to model bilateral financial contracts for valuation purposes. The contracts of Bahr et al. [4] have a similar focus of valuation and risk analysis, but add the ability to model complex portfolios of multiple parties. Daml picks up this idea of composing simple workflows into more complex ones: choices correspond to alternatives and choice bodies aggregate individual building blocks into larger atomic transactions.

Hvitved et al. [1, 16, 17] developed Peyton Jones et al.'s ideas further into the Contract Specification Language CSL, a process calculus for event-driven transaction systems, which has been implemented by Deon Digital [9]. CSL stores contract instances as a process term on the ledger, including lambda expressions. Upon an event, the process term reduces to another term according to the process calculus rules. This format gives a lot flexibility for combining workflows before instantiation. In contrast, Daml requires the programmer to encode the composition in a new template and produce and deploy the .dalf package. In return, Daml contract instances on the ledger are always bound to a template, which helps with understanding the ledger state. For CSL, it is much harder to figure out what a partially evaluated contract instance represents, as one has to study the raw process term.

While both CSL and Daml claim composability, CSL's notion is more restricted: The CSL composition operators can only be applied before the contract instance is deployed;



building workflows on top of existing contract instances on the ledger is impossible. So one has to envision all further possible use cases of a contract at the very beginning. For example, an `Iou` can be used in a `TradeProposal` workflow only if this was decided when the `Iou` contract was created for the first time; and similarly any follow-up usages. In contrast, Daml allows to compose workflows of deployed contract instances; the `TradeProposal` can work with already deployed `Ious`. In fact, the `Iou` workflows need not even know that they are part of a larger workflow, thanks to Daml’s hierarchical transactions.

In Rainfall [20], the ledger stores a multiset of tagged facts (template ID and contract arguments in Daml) and separately the rules for transforming facts. Facts are annotated with by-authority and obs-authority, which correspond to Daml’s signatories and observers on templates. A rule pattern-matches on input facts, possibly consuming them, and produces new output facts; to that end, the rule can acquire by-authority from input facts, similar to how signatories pre-authorize choice consequences in Daml. The use-set stored with each fact determines the rules that may use the fact. This use-set effectively introduces a dynamic notion of a template: all facts with the same tag and use-set are instances of the same template. The main difference between Rainfall and Daml is the execution model: Daml references data via unique contract IDs whereas Rainfall finds facts by the content. So all `Ious` with the same owner, issuer and cash amount are interchangeable in Rainfall.

The Plutus language is based on System  $F_{\omega}$  like Daml. The Plutus compiler from Plutus to Plutus Core uses GHC, too, but with a different setup: Transaction code is embedded into plain Haskell programs via Template Haskell; before the GHC backend, a new stage translates these embedded fragments into Plutus Core to be run on-ledger. The surrounding program is supposed to be run off-ledger. For Daml, we strictly separate the on-ledger code written in Daml from the off-ledger code. To this end, the Daml SDK generates bindings for the Java and Typescript, which are used more widely for building off-ledger applications.

## 6 Conclusion

We have presented the smart contract language Daml where **templates** define the data model for shared on-ledger data together with the **choices** governing how this data may be changed. The programmer annotates all data and choices with the required authorizers (**signatory** and **controller**) and the **observer**s that get notified about data creation and modification. These policies not only govern access control, they also partition the data by ownership, which can be exploited for parallel processing.

The Daml ecosystem includes more than just the Daml language, which this paper focuses on. The Daml SDK includes a VS Code IDE with syntax highlighting, type inference, go-to-definition, etc. Daml Script allows programmers to script scenarios of ledger interactions, as unit tests or for debugging. Daml Triggers provide a simple way to react to ledger updates by sending new commands. More complex off-ledger logic, including the user interface for the dApp, is typically written in a mainstream programming language and not in Daml. dApps commonly interface with Daml code using custom bindings for Daml templates and choices, which currently can be auto-generated for Java and TypeScript.

In the future, we plan to extend Daml with more flexible ways than explicit `DiscloseIou` choices to disclose contract instances to other parties, so that they can exercise their delegated choices. To improve Damls modularity, we are also working on template interfaces that specify available choices without implementation. For the Daml ledger implementations, we plan to expose some functionality of the underlying blockchain or DLT to the Daml code. In particular, we plan to enable Daml smart contracts to directly interact with the native blockchain assets, which is currently only possible via trusted third parties.

**Acknowledgements.** We thank everyone at Digital Asset who contributed to Daml and Daml-LF, in particular, Jost Berthold, Shayne Fletcher, Rafael Guglielmetti, Rohan Jacob-Rao, Shaul Kfir, Ben Lippmeier, Ognjen Marić, David Millar-Durrant, and Sofus Mortensen.

## References

- [1] Jesper Andersen, Patrick Bahr, Fritz Henglein, and Tom Hvitved. 2014. Domain-Specific Languages for Enterprise Systems. In *Leveraging Applications of Formal Methods, Verification and Validation. Technologies for Mastering Change (LNCS)*, Tiziana Margaria and Bernhard Steffen (Eds.), Vol. 8802. Springer, 73–95. [https://doi.org/10.1007/978-3-662-45234-9\\_6](https://doi.org/10.1007/978-3-662-45234-9_6)
- [2] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muradharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolic, Sharon Weed Cocco, and Jason Yellick. 2018. Hyperledger Fabric: a distributed operating system for permissioned blockchains. In *EuroSys 2018*, Rui Oliveira, Pascal Felber, and Y. Charlie Hu (Eds.). ACM, 30:1–30:15. <https://doi.org/10.1145/3190508.3190538>
- [3] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. 2017. A Survey of Attacks on Ethereum Smart Contracts (SoK). In *Principles of Security and Trust (POST 2017) (LNCS)*, Matteo Maffei and Mark Ryan (Eds.), Vol. 10204. Springer, 164–186. [https://doi.org/10.1007/978-3-662-54455-6\\_8](https://doi.org/10.1007/978-3-662-54455-6_8)
- [4] Patrick Bahr, Jost Berthold, and Martin Elsmann. 2015. Certified Symbolic Management of Financial Multi-Party Contracts. In *International Conference on Functional Programming (ICFP 2015)*. ACM, 315–327. <https://doi.org/10.1145/2784731.2784747>
- [5] Cardano. 2021. <https://cardano.org/>.



- [6] Cardano. 2021. Plutus. <https://developers.cardano.org/docs/smart-contracts/>
- [7] Manuel M. T. Chakravarty, James Chapman, Kenneth MacKenzie, Orestis Melkonian, Michael Peyton Jones, and Philip Wadler. 2020. The Extended UTXO Model. In *Financial Cryptography and Data Security (FC 2020) (LNCS)*, Matthew Bernhard, Andrea Bracciali, L. Jean Camp, Shin'ichiro Matsuo, Alana Maurushat, Peter B. Rønne, and Massimiliano Sala (Eds.), Vol. 12063. Springer, 525–539. [https://doi.org/10.1007/978-3-030-54455-3\\_37](https://doi.org/10.1007/978-3-030-54455-3_37)
- [8] Decentralized Application Security Project. 2019. TOP 10. <https://dasp.co/>
- [9] Deon Digital. 2021. <https://www.deondigital.com/>.
- [10] Mattias Felleisen and D. P. Friedman. 1987. A Calculus for Assignments in Higher-Order Languages. In *Principles of Programming Languages (POPL 1987)*. ACM, 314–325. <https://doi.org/10.1145/41625.41654>
- [11] Cormac Flanagan, Amr Sabry, Bruce F. Duba, and Matthias Felleisen. 1993. The Essence of Compiling with Continuations. In *Programming Language Design and Implementation (PLDI 1993)*. ACM, 237–247. <https://doi.org/10.1145/155090.155113>
- [12] GHC proposal 0282. 2021. Record Dot Syntax. <https://github.com/ghc-proposals/ghc-proposals/blob/master/proposals/0282-Record-Dot-Syntax.md>
- [13] Jean-Yves Girard. 1972. *Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre supérieur*. Ph.D. Dissertation. Université Paris Diderot.
- [14] Guy Golan-Gueta, Ittai Abraham, Shelly Grossman, Dahlia Malkhi, Benny Pinkas, Michael K. Reiter, Dragos-Adrian Seredinschi, Orr Tamir, and Alin Tomescu. 2019. SBFT: A Scalable and Decentralized Trust Infrastructure. In *Dependable Systems and Networks (DSN 2019)*. IEEE, 568–580. <https://doi.org/10.1109/DSN.2019.00063>
- [15] Cordelia Hall, Kevin Hammond, Simon Peyton Jones, and Philip Wadler. 1994. Type classes in Haskell. In *Programming Languages and Systems (ESOP 1994) (LNCS)*, Donald Sannella (Ed.), Vol. 788. Springer, 241–256. [https://doi.org/10.1007/3-540-57880-3\\_16](https://doi.org/10.1007/3-540-57880-3_16)
- [16] Tom Hvitved. 2011. *Contract formalisation and modular implementation of domain-specific languages*. Ph.D. Dissertation. Department of Computer Science, University of Copenhagen.
- [17] Tom Hvitved, Felix Klaedtke, and Eugen Zălinescu. 2012. A trace-based model for multiparty contracts. *Journal of Logic and Algebraic Programming* 81, 2 (2012), 72–98. <https://doi.org/10.1016/j.jlap.2011.04.010>
- [18] Hyperledger Besu 2021. An enterprise-grade Java-based, Apache 2.0 licensed Ethereum client. <https://github.com/hyperledger/besu>.
- [19] Lawrence Lessig. 2006. *Code: And Other Laws of Cyberspace, Version 2.0*. Basic Books.
- [20] Ben Lippmeier, Amos Robinson, and Andrae Muys. 2019. Smart Contracts as Authorized Production Rules. In *Principles and Practice of Programming Languages (PPDP 2019)*, Ekaterina Komendantskaya (Ed.). ACM, 14:1–14:14. <https://doi.org/10.1145/3354166.3354179>
- [21] Neil Mitchell, Moritz Kiefer, Pepe Iborra, Luke Lau, Zubin Duggal, Hannes Siebenhandl, Javier Neira Sanchez, Matthew Pickering, and Alan Zimmerman. 2020. Building an Integrated Development Environment (IDE) on top of a Build System. In *Implementation and Application of Functional Languages (IFL 2020)* (University of Kent, UK), Olaf Chitil (Ed.). ACM, 1–10. <https://doi.org/10.1145/3462172.3462180>
- [22] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>.
- [23] Simon Peyton Jones, Jean-Marc Eber, and Julian Seward. 2000. Composing Contracts: An Adventure in Financial Engineering (Functional Pearl). In *International Conference on Functional Programming (ICFP 2000)*. ACM, 280–292. <https://doi.org/10.1145/351240.351267>
- [24] R3. 2021. Corda. <https://www.corda.net/>.
- [25] Carol M. Rose. 1987–1988. Crystals and Mud in Property Law. *Stanford Law Review* 40, 3 (1987–1988), 577–610.
- [26] Roberto Saltini and David Hyland-Wood. 2019. IBFT 2.0: A Safe and Live Variation of the IBFT Blockchain Consensus Protocol for Eventually Synchronous Networks. arXiv:1909.10194
- [27] Martin Sulzmann, Manuel M. T. Chakravarty, Simon Peyton Jones, and Kevin Donnelly. 2007. System F with type equality coercions. In *Types in Languages Design and Implementation (TLDI 2007)*. ACM Press, 53–66. <https://doi.org/10.1145/1190315.1190324>
- [28] Palina Tolmach, Yi Li, Shang-Wei Lin, Yang Liu, and Zengxiang Li. 2021. A Survey of Smart Contract Formal Specification and Verification. *ACM Comput. Surv.* 54, 7, Article 148 (2021), 38 pages. <https://doi.org/10.1145/3464421>
- [29] VMware. 2021. VMware Blockchain. <https://www.vmware.com/products/blockchain.html>.
- [30] Stephanie Weirich, Justin Hsu, and Richard A. Eisenberg. 2013. System FC with Explicit Kind Equality. In *International Conference on Functional Programming (ICFP 2013) (SIGPLAN Not.)*, Vol. 48, 9. ACM, 275–286. <https://doi.org/10.1145/2500365.2500599>
- [31] Gavin Wood. 2014. Ethereum: A secure decentralised generalised transaction ledger. <https://github.com/ethereum/yellowpaper>.
- [32] Max Young. 2008. *Understanding Contract Law*. Routledge.