1 Specification

1.1 Syntax

$$C \in \text{ContractNames} \qquad m \in \text{TransactionNames}$$
$$t \in \text{TypeNames} \qquad x \in \text{Identifiers}$$
$$n \in \mathbb{Z}$$

q	::=	$! \mid \texttt{any} \mid \texttt{nonempty}$	(selector quantifiers)
$\mathcal{Q}$	::=	$q \mid \texttt{empty} \mid \texttt{every}$	(type quantities)
$\mathcal{C}$	::=	$\texttt{option} \mid \texttt{set} \mid \texttt{list}$	(collection type const
T	::=	$\texttt{void} \mid \texttt{bool} \mid \texttt{nat} \mid \mathcal{C}\ \tau \mid \tau \rightsquigarrow \tau \mid \{\overline{x : \tau}\} \mid t$	(base types)
τ	::=	$\mathcal{Q}\ T$	(types)
$\mathcal{V}$	::=	$n \mid \texttt{true} \mid \texttt{false} \mid \texttt{empty} \mid \lambda x : \tau.E$	(values)
$\mathcal{L}$	::=	$x \mid x[x] \mid x.x$	(locations)
E	::=	$\mathcal{V} \mid \mathcal{L} \mid x.m(\overline{x}) \mid \texttt{some}(x) \mid f \texttt{ in } x \mid \{\overline{x : \tau \mapsto x}\} \mid \texttt{let } x : \tau := E \texttt{ in } E \mid \texttt{if } x \texttt{ then } E \texttt{ else } E$	(expressions)
s	::=	$\mathcal{L} \mid \texttt{everything} \mid q\ x : \tau \texttt{ s.t. } E$	(selector)
$\mathcal{N}$	::=	$\mathcal{L} \mid \texttt{new } C(\overline{x}) \mid \texttt{consume}$	(nodes)
F	::=	$\mathcal{N} \xrightarrow{s} \mathcal{N}$	(flows)
Stmt	::=	$F \mid E \mid \texttt{revert}(E) \mid \texttt{try } S \texttt{ catch}(x : \tau)\ S \mid \texttt{if } x \texttt{ then } S \texttt{ else } S$	
		$\mid \texttt{var } x : \tau := E \mid S; S \mid \texttt{pack} \mid \texttt{unpack}(x)$	(statements)
M	::=	$\texttt{fungible} \mid \texttt{nonfungible} \mid \texttt{consumable} \mid \texttt{asset}$	(type declaration mo
$\mathcal{D}$	::=	$x : \tau$	(field)
		$\mid \texttt{type } t \texttt{ is } \overline{M}\ T$	(type declaration)
		$\mid \texttt{transaction } m(\overline{x : \tau}) \texttt{ returns } x : \tau \texttt{ do } S$	(transactions)
		$\mid \texttt{view } m(\overline{x : \tau}) \texttt{ returns } \tau := E$	(views)
Con	::=	$\texttt{contract } C\ \{\overline{\mathcal{D}}\}$	(contracts)
Prog	::=	$\overline{\texttt{Con}}\ ; S$	(programs)

Figure 1: Abstract syntax of LANGUAGE-NAME.

In the surface language, "collection types" (i.e., $\mathcal{Q}\ \mathcal{C}\ \tau$ or a transformer) are by default **any**, but all other types, like **nat**, are !.

[Some simplification ideas] [Could get rid of selecting by locations and only allowed selecting with quantifiers, and just optimize things like $! x : \tau$ **s.t.** $x = y$ into a lookup. Also, allowing any type quantity in a selector lets us do away with everything. Would actually be even nicer if we allowed any type quantity to appear in the quantifier, because then we wouldn't even need a special rule for everything.] [We could also get rid of "if" and instead do something like any $x : \tau$ **s.t.** if b then $x = y$ else $false$]

[Contract types should be consumable assets by default (consuming a contract is a self-destruct?)]

1.2 Statics

$$\Gamma \quad ::= \quad \emptyset \mid \Gamma, x : \tau \quad \text{(type environments)}$$

Definition 1. *Define* $\boldsymbol{Quant} = \{empty, any, !, nonempty, every\}$, *and call any* $\mathcal{Q} \in \boldsymbol{Quant}$ *a type quantity. Define* $empty < any < ! < nonempty < every$.

[Eliminate all the locations except for x and then use flows to extract and put stuff back?]

$\boxed{\texttt{modifiers}(T) = \overline{M}}$ **Type Modifiers**

$$\texttt{modifiers}(T) = \begin{cases} \overline{M} & \text{if } (\texttt{type } T \texttt{ is } \overline{M} \ T) \\ \emptyset & \text{otherwise} \end{cases}$$

$\boxed{\tau \ \texttt{asset}}$ **Asset Types**

[The syntax for record "fields" and type environments is the same...could just use it]

$$
\begin{aligned}
(\mathcal{Q} \ T) \ \texttt{asset} \iff \ & \mathcal{Q} \neq \texttt{empty} \text{ and } (\texttt{asset} \in \texttt{modifiers}(T) \text{ or} \\
& (T = \tau \rightsquigarrow \sigma \text{ and } \sigma \ \texttt{asset}) \text{ or} \\
& (T = \mathcal{C} \ \tau \text{ and } \tau \ \texttt{asset}) \text{ or} \\
& (T = \{\overline{y : \sigma}\} \text{ and } \exists x : \tau \in \overline{y : \sigma}.(\tau \ \texttt{asset})))
\end{aligned}
$$

[It should be the case that a transformer can have an output of an asset type if and only if it has an input asset type (and it the case of curried transformers, that some input type is an asset).]

$\boxed{\tau \ \texttt{consumable}}$ **Consumable Types**

$$(\mathcal{Q} \ T) \ \texttt{consumable} \iff \texttt{consumable} \in \texttt{modifiers}(T) \text{ or } \neg((\mathcal{Q} \ T) \ \texttt{asset})$$

$\boxed{\text{demote}(\tau) = \sigma}$ $\boxed{\text{demote}_*(T_1) = T_2}$ **Type Demotion**

$$
\begin{aligned}
\text{demote}(\mathcal{Q} \ T) &= \mathcal{Q} \ \text{demote}_*(T) \\
\text{demote}_*(\textbf{void}) &= \textbf{void} \\
\text{demote}_*(\textbf{nat}) &= \textbf{nat} \\
\text{demote}_*(\textbf{bool}) &= \textbf{bool} \\
\text{demote}_*(t) &= \text{demote}_*(T) &&\text{where } \texttt{type } t \texttt{ is } \overline{M} \ T \text{ and } \texttt{asset} \in \overline{M} \\
\text{demote}_*(\mathcal{C} \ \tau) &= \mathcal{C} \ \text{demote}(\tau) \\
\text{demote}_*(\{\overline{x : \tau}\}) &= \left\{\overline{x : \text{demote}(\tau)}\right\} \\
\text{demote}_*(\tau \rightsquigarrow \sigma) &= \text{demote}(\tau) \rightsquigarrow \text{demote}(\sigma)
\end{aligned}
$$

$\boxed{\texttt{decls}(C) = \overline{\mathcal{D}}}$ **Contract Declarations**

$$\texttt{decls}(C) = \overline{\mathcal{D}} \text{ where } (\texttt{contract } C \ \{\overline{\mathcal{D}}\})$$

$\boxed{\texttt{fields}(C) = \Gamma}$ **Contract Fields**

$$\texttt{fields}(C) = \{\texttt{this}.f : \tau \mid f : \tau \in \texttt{decls}(C)\}$$

$\boxed{\Gamma \vdash E : \tau \dashv \Delta}$ **Expression Typing**

$$\frac{}{\Gamma \vdash \mathtt{empty} : \mathtt{empty}\ \mathcal{C}\ \tau \dashv \Gamma}\ \text{\sc Empty-Val} \qquad\qquad \frac{}{\Gamma, x : \tau \vdash x : \mathtt{demote}(\tau) \dashv \Gamma, x : \tau}\ \text{\sc Demote-Lookup}$$

$$\frac{}{\Gamma, x : \tau \vdash x : \tau \dashv \Gamma}\ \text{\sc Lin-Lookup} \qquad\qquad \frac{\Gamma \vdash x : \{\overline{y : \tau}\} \dashv \Gamma \qquad f : \sigma \in \overline{y : \tau}}{\Gamma \vdash x.f : \sigma \dashv \Gamma}\ \text{\sc Field-Lookup}$$

$$\frac{\Gamma \vdash \overline{y : \tau} \dashv \Delta}{\Gamma \vdash \{\overline{x : \tau \mapsto y}\} \dashv \Delta}\ \text{\sc Build-Rec} \qquad\qquad \frac{\Gamma \vdash f\ \mathtt{selects}\ \mathtt{demote}(\sigma) \qquad \Gamma \vdash x :: \tau \Rrightarrow_{\mathcal{Q}} \sigma}{\Gamma \vdash (f\ \mathtt{in}\ x) : \mathtt{bool} \dashv \Gamma}\ \text{\sc Check-In}$$

$$\frac{(\mathtt{view}\ m(\overline{a : \tau})\ \mathtt{returns}\ \sigma := E) \in \mathtt{decls}(C) \qquad \Gamma, x : C \vdash \overline{y : \tau} \dashv \Gamma, x : C}{\Gamma, x : C \vdash x.m(\overline{y}) : \sigma \dashv \Gamma, x : C}\ \text{\sc View-Call}$$

$$\frac{\mathtt{dom}(\mathtt{fields}(C)) \cap \mathtt{dom}(\Gamma) = \emptyset}{(\mathtt{transaction}\ m(\overline{a : \tau})\ \mathtt{returns}\ \sigma\ \mathtt{do}\ S) \in \mathtt{decls}(C) \qquad \Gamma, \mathtt{this} : C \vdash \overline{y : \tau} \dashv \Delta, \mathtt{this} : C}{\Gamma, \mathtt{this} : C \vdash \mathtt{this}.m(\overline{y}) : \sigma \dashv \Delta, \mathtt{this} : C}\ \text{\sc Internal-Tx-Call}$$

$$\frac{\Gamma \vdash x : \mathtt{bool} \dashv \Gamma \qquad \Gamma \vdash y : \tau \dashv \Delta \qquad \Gamma \vdash z : \tau \dashv \Delta}{\Gamma \vdash (\mathtt{if}\ x\ \mathtt{then}\ y\ \mathtt{else}\ z) : \tau \dashv \Delta}\ \text{\sc If-Expr}$$

$$\frac{\Gamma \vdash E_1 : \tau \dashv \Delta \qquad \Delta, x : \tau \vdash E_2 : \sigma \dashv \Xi \qquad x \notin \mathtt{dom}(\Xi)}{\Gamma \vdash (\mathtt{let}\ x : \tau := E_1\ \mathtt{in}\ E_2) : \sigma \dashv \Xi}\ \text{\sc Let}$$

$$\frac{\Gamma, x : \tau \vdash E : \sigma \dashv \Gamma}{\Gamma \vdash (\lambda x : \tau.E) :: \mathtt{empty}\ (\tau \rightsquigarrow \sigma)}\ \text{\sc Transformer}$$

$\boxed{\Gamma \vdash \mathcal{S} :: \tau \Rrightarrow_{\mathcal{Q}} \sigma}$ **Storage Typing** The syntax $\tau \Rrightarrow_{\mathcal{Q}} \sigma$ means that the storage accepts τ and provides σ; that is, you can flow τ into it, and when you flow out of it, you get σ; moreover, you get at most $\mathcal{Q}$ of them.

$$\frac{}{\Gamma, S : \tau \vdash S :: \tau \Rrightarrow_! \tau}\ \text{\sc Store-One} \qquad\qquad \frac{}{\Gamma, S : \mathcal{Q}\ \mathcal{C}\ \tau \vdash S :: \tau \Rrightarrow_{\mathcal{Q}} \tau}\ \text{\sc Store-Col}$$

$$\frac{}{\Gamma, x : \mathcal{Q}\ (\tau \rightsquigarrow \sigma) \vdash x :: \tau \Rrightarrow_{\mathcal{Q}} \sigma}\ \text{\sc Store-Transformer} \qquad\qquad \frac{\tau\ \mathtt{consumable}}{\Gamma \vdash \mathtt{consume} :: \tau \Rrightarrow_{\mathtt{empty}} \mathtt{void}}\ \text{\sc Store-Consume}$$

$$\frac{\mathtt{fields}(C) = \overline{\mathtt{this}.f : \tau} \qquad \Gamma \vdash x : \{\overline{\mathtt{this}.f : \tau}\} \dashv \Gamma}{\Gamma \vdash \mathtt{new}\ C(x) :: \mathtt{void} \Rrightarrow_! C}\ \text{\sc Store-New}$$

$$\frac{(\mathtt{type}\ t\ \mathtt{is}\ \overline{M}\ T) \in \mathtt{decls}(C) \qquad \Gamma \vdash x : \mathtt{demote}(T) \dashv \Gamma}{\Gamma, \mathtt{this} : C \vdash \mathtt{new}\ t(x) :: \mathtt{void} \Rrightarrow_! t}\ \text{\sc Store-New-Ty}$$

$\boxed{\Gamma \vdash f\ \mathtt{selects}_{\mathcal{Q}}\ \tau}$ **Selectors**

$$\frac{\Gamma \vdash x : \tau \dashv \Gamma}{\Gamma \vdash x\ \mathtt{selects}_!\ \tau}\ \text{\sc Select-One} \qquad\qquad \frac{\Gamma \vdash x : \mathcal{Q}\ \mathcal{C}\ \tau \dashv \Gamma}{\Gamma \vdash x\ \mathtt{selects}_{\mathcal{Q}}\ \tau}\ \text{\sc Select-Col}$$

$$\frac{}{\Gamma \vdash \mathtt{everything}\ \mathtt{selects}_{\mathtt{every}}\ \tau}\ \text{\sc Select-Everything} \qquad\qquad \frac{\Gamma, x : \tau \vdash p : \mathtt{bool} \dashv \Gamma, x : \tau}{\Gamma \vdash (\mathtt{q}\ x : \tau\ \mathbf{s.t.}\ p)\ \mathtt{selects}_{\mathtt{q}}\ \tau}\ \text{\sc Select-Quant}$$

Definition 2. *Let* $\mathcal{Q}, \mathcal{R} \in \textbf{Quant}$. *Define the commutative operator* $\oplus$, *called* combine, *as the unique function* $\textbf{Quant}^2 \to \textbf{Quant}$ *satisfying*

$$every \oplus \mathcal{R} = every$$
$$empty \oplus \mathcal{R} = \mathcal{R}$$
$$nonempty \oplus \mathcal{R} = nonempty$$
$$! \oplus \mathcal{R} = nonempty \qquad if \, \mathcal{R} \neq empty$$
$$any \oplus any = any$$

Similarly, define the operator $\ominus$, *called* split, *as the unique function* $\textbf{Quant}^2 \to \textbf{Quant}$ *such that*

$$\mathcal{Q} \ominus empty = \mathcal{Q}$$
$$empty \ominus \mathcal{R} = empty$$
$$! \ominus \mathcal{R} = empty \qquad if \, \mathcal{R} \geq !$$
$$nonempty \ominus \mathcal{R} = any \qquad if \, \mathcal{R} \neq empty$$
$$\mathcal{Q} \ominus any = any$$
$$\mathcal{Q} \ominus every = empty$$
$$every \ominus \mathcal{Q} = every$$

Note that we write $(\mathcal{Q} \, T) \oplus \mathcal{R}$ to mean $(\mathcal{Q} \oplus \mathcal{R}) \, T$ and similarly $(\mathcal{Q} \, T) \ominus \mathcal{R}$ to mean $(\mathcal{Q} \ominus \mathcal{R}) \, T$. $\mathcal{Q} \oplus \mathcal{R}$ represents the quantity present when flowing $\mathcal{R}$ of something to a storage already containing $\mathcal{Q}$. $\mathcal{Q} \ominus \mathcal{R}$ represents the quantity left over after flowing $\mathcal{R}$ from a storage containing $\mathcal{Q}$.

$\boxed{\texttt{update}(\Gamma, \mathcal{S}, \tau)}$ **Type environment modification**

$$\texttt{update}(\Gamma, S, \tau) = \begin{cases} \Delta, S : \tau & if \, \Gamma = \Delta, S : \sigma \\ \Gamma & otherwise \end{cases}$$

Definition 3. *We can consider a type environment* Γ *as a function* IDENTIFIERS $\to$ TYPES $\cup \{\bot\}$ *as follows:*

$$\Gamma(x) = \begin{cases} \tau & if \, x : \tau \in \Gamma \\ \bot & otherwise \end{cases}$$

We write $\textbf{dom}(\Gamma)$ *to mean* $\{x \in$ IDENTIFIERS $\mid \Gamma(x) \neq \bot\}$.

Definition 4. *Let* $\mathcal{Q}$ *and* $\mathcal{R}$ *be type quantities,* $T_\mathcal{Q}$ *and* $T_\mathcal{R}$ *base types, and* Γ *and* Δ *type environments. Define the following orderings, which make types and type environments into join-semilattices. For type quantities, define the partial order* $\sqsubseteq$ *by*

$$\mathcal{Q} \sqsubseteq any; \quad every \sqsubseteq nonempty; \quad ! \sqsubseteq nonempty$$

For types, define the partial order $\leq$ *by*

$$\mathcal{Q} \, T_\mathcal{Q} \leq \mathcal{R} \, T_\mathcal{R} \iff T_\mathcal{Q} = T_\mathcal{R} \text{ and } \mathcal{Q} \sqsubseteq \mathcal{R}$$

For type environments, define the partial order $\leq$ *by*

$$\Gamma \leq \Delta \iff \forall x. \Gamma(x) \leq \Delta(x)$$

4

$\boxed{\Gamma \vdash S \text{ wf} \dashv \Delta}$ **Statement Well-formedness**

$$\frac{\begin{array}{cc} \Gamma \vdash S :: \tau \Rrightarrow_{\mathcal{Q}} \sigma & \Gamma \vdash f \text{ selects}_{\mathcal{R}} \text{ demote}(\sigma) \\ \Delta = \text{update}(\Gamma, S, \Gamma(S) \ominus \mathcal{R}) & \Delta \vdash D :: \sigma \Rrightarrow_{\mathcal{S}} \pi \end{array}}{\Gamma \vdash (S \xrightarrow{s} D) \text{ wf} \dashv \text{update}(\Delta, D, \Delta(D) \oplus \min(\mathcal{Q}, \mathcal{R}))} \text{ Wf-Flow}$$

$$\frac{\Gamma \vdash E : \tau \dashv \Delta \qquad \Delta, x : \tau \vdash S \text{ wf} \dashv \Xi, x : \sigma \qquad \neg(\sigma \text{ asset})}{\Gamma \vdash (\text{var } x : \tau := E \text{ in } S) \text{ wf} \dashv \Xi} \text{ Wf-Var-Def}$$

$$\frac{\Gamma \vdash x : \text{bool} \dashv \Gamma \qquad \Gamma \vdash S_1 \text{ wf} \dashv \Delta \qquad \Gamma \vdash S_2 \text{ wf} \dashv \Xi}{\Gamma \vdash (\text{if } x \text{ then } S_1 \text{ else } S_2) \text{ wf} \dashv \Delta \vee \Xi} \text{ Wf-If}$$

$$\frac{\Gamma \vdash S_1 \text{ wf} \dashv \Delta \qquad \Gamma, x : \tau \vdash S_2 \text{ wf} \dashv \Xi, x : \tau}{\Gamma \vdash (\text{try } S_1 \text{ catch } (x : \tau) \, S_2) \text{ wf} \dashv \Delta \vee \Xi} \text{ Wf-Try} \qquad\qquad \frac{\Gamma \vdash E : \tau \dashv \Gamma}{\Gamma \vdash \text{revert}(E) \text{ wf} \dashv \Gamma} \text{ Wf-Revert}$$

$$\frac{\Gamma \vdash E : \tau \dashv \Gamma}{\Gamma \vdash E \text{ wf} \dashv \Gamma} \text{ Wf-Expr} \qquad\qquad \frac{\Gamma \vdash S_1 \text{ wf} \dashv \Delta \qquad \Delta \vdash S_2 \text{ wf} \dashv \Xi}{\Gamma \vdash (S_1 ; S_2) \text{ wf} \dashv \Xi} \text{ Wf-Seq}$$

$$\frac{\text{this}.f : \tau \in \text{fields}(C)}{\Gamma, \text{this} : C \vdash \text{unpack}(f) \text{ wf} \dashv \Gamma, \text{this} : C, \text{this}.f : \tau} \text{ Wf-Unpack}$$

$$\frac{(\Gamma|_{\text{dom}(\text{fields}(C))}) \leq \text{fields}(C) \qquad \Delta = \{x : \tau \in \Gamma \mid x \notin \text{dom}(\text{fields}(C))\}}{\Gamma, \text{this} : C \vdash \text{pack} \text{ wf} \dashv \Delta, \text{this} : C} \text{ Wf-Pack}$$

$\boxed{\vdash_C \mathcal{D} \text{ wf}}$ **Declaration Well-formedness**

$$\frac{\Gamma = \text{this} : C, \text{fields}(C), \overline{x : \tau} \qquad \Gamma \vdash E : \sigma \dashv \Gamma}{\vdash_C (\text{view } m(\overline{x : \tau}) \text{ returns } \sigma := E) \text{ wf}} \text{ Wf-View}$$

$$\frac{\begin{array}{c} \text{this} : C, \text{fields}(C), \overline{x : \tau}, y : \text{empty } T \vdash S \text{ wf} \dashv \Delta, \text{this} : C, y : \mathcal{Q} \, T \\ \text{dom}(\text{fields}(C)) \cap \text{dom}(\Delta) = \emptyset \qquad \forall x : \tau \in \Delta . \neg(\tau \text{ asset}) \end{array}}{\vdash_C (\text{transaction } m(\overline{x : \tau}) \text{ returns } y : \mathcal{Q} \, T \text{ do } S) \text{ wf}} \text{ Wf-Tx} \qquad \frac{}{\vdash_C (x : \tau) \text{ wf}} \text{ Wf-Field}$$

$$\frac{}{\vdash_C (\text{type } t \text{ is } \overline{M} \, T) \text{ wf}} \text{ Wf-Type}$$

$\boxed{\text{Con wf}}$ **Contract Well-formedness**

$$\frac{\forall d \in \overline{\mathcal{D}}.(\vdash_C d \text{ wf})}{(\text{contract } C \, \{\overline{\mathcal{D}}\}) \text{ wf}} \text{ Wf-Con}$$

$\boxed{\text{Prog wf}}$ **Program Well-formedness**

$$\frac{\forall C \in \overline{\text{Con}}.C \text{ wf} \qquad \emptyset \vdash S \dashv \emptyset}{(\overline{\text{Con}}; S) \text{ wf}} \text{ Wf-Con}$$

[Asset retention theorem?] [Resource accessiblity?]
[What guarantees should we provide (no errors except for flowing a resource that doesn't
exist in the source/already exists in the destination)?]

2 Introduction

LANGUAGE-NAME is a DSL for implementing programs which manage resources, targeted at writing smart contracts.

2.1 Contributions

We make the following main contributions:

- **Safety guarantees**: similar to [or maybe just exactly] linear types[or maybe uniqueness types? need to read more about this], preventing accidental resource loss or duplication. Additionally, provides some amount of reentrancy safety.

  - We can evaluate these by formalizing the language and proving them; the formalization is something that would be nice to do anyway.

- **Simplicity**: The language is quite simple—it makes writing typical smart contract programs easier and shorter, because many common pitfalls in Solidity are automatically handled by the language, such as overflow/underflow, checking of balances, short address attacks, etc.

  - We can evaluate these by comparing LOC, cyclomatic complexity, etc. Not sure what the right metric would be. [Or how cyclomatic complexity would work exactly in this language.]
  - We can also evaluate via a user study, but that will take a long(er) time.

- [Optimizations?] Some of the Solidity contracts are actually inefficient because:

  1. They use lots of modifiers which repeat checks (see reference implementation of ERC-721).
  2. They tend to use arrays to represent sets. Maybe this is more efficient for very small sets, but checking containment is going to be much faster with a `mapping (X => bool)` eventually.

  - We can evaluate this by profiling or a simple opcode count (which is not only a proxy for performance, but also means that deploying the contract will be cheaper).

3 Language Intro

The basic state-changing construct in the language is a *flow*. A flow describes a transfer of a *resource* from one *storage* to another. A *transaction* is a sequence of flows and *handlers*.

Each flow has a *source*, a *destination*, and a *selector*. The source and destination are two storages which hold a resource, and the selector describes which part of the resource in the source should be transferred to the destination. A flow may optionally have a *name*.

Note that all flows fail if they can't be performed. For example, a flow of fungible resources fails if there is enough of the resource, and a flow of a nonfungible resource fails if the selected value doesn't exist in the source location.

NOTE: If we wanted to be "super pure", we can implement preconditions with just flows by doing something like:

```
{ contractCreator = msg.sender } ––[ true ]–> consume
```

This works because { contractCreator = msg.sender } : set bool (specifically, a singleton), so if contractCreator = msg.sender doesn't evaluate to true, then we will fail to consume true from it. I don't think actually doing this is a good idea; at least, not in the surface language. Maybe it would simplify the compiler and/or formalization), but it's interesting/entertaining.

Actions A handler is a pair of a *trigger* and an *action*. Triggers specify when an action should be executed. An action can be:

1. An event

2. An external call

3. An error handler

[**For the moment, I think it is safe to allow constructors to act like a storage, and not like an external call. This is because when you call a constructor, you must have the full source code of the contract you're going to make, and therefore you can be sure that the code it runs is safe.**]
[**Can you do actions other than just providing an error message in on fail?**] [**Sending ether will also trigger an external call, which should be considered as being part of the** on success **block, probably**]

For example, below, we create a flow with a name F.

```
1 F: voterSource −−− newVoterAddress −−> authorizedVoters
```

We can then create handlers for this flow, such as the following:

```
1 on fail  F with Err:
2     revert("This address is  already authorized! Do not re−authorize it .")
3 on success F:
4     emit AuthorizedVoter(newVoterAddress)
5     call  newVoterAddress.receiveAuthorization() asserting resultCode = "SUCCESS"
```

It's possible to have triggers which only occur when some subset of actions occurs. Below, we create two flows. The trigger on fail {F1,F2} triggers when any one of the actions F1 or F2 fails. The trigger on success {F1,F2} triggers when **both** the actions F1 and F2 succeed. [**Is this confusing, or is this how you would expect it to work?**]

```
1 F1: A −−− x −−−> B
2 F2: C −−− y −−−> D
3 on fail  {F1,F2}:
4     // Stuff
5 on success {F1,F2}:
6     // Stuff
```

In fact, all handlers are internally translated into this form, so on fail F becomes on fail {F}, and on fail becomes on fail {F1,F2 ,..., Fn}, where F1, F2, ..., Fn are all the flows preceeding the handler. [**I think this is the right way to do it.**]

We can also allow the following syntax to be used, with minimal additional implementation troubles:

```
1 handle {
2     A −−− x −−> B
3     C −−− y −−> D
4     E −−− z −−> F
5 } with {
6     on fail :
7         // Stuff
8     on success:
9         // Stuff
10 }
```

This can be mechanically rewritten to:

```
1  F1: A --- x --> B
2  F2: C --- y --> D
3  F3: E --- z --> F
4  on fail {F1,F2,F3}:
5      // Stuff
6  on success {F1,F2,F3}:
7      // Stuff
```

[random note] The following pattern, while popular in Python [and probably some other languages], is not possible with this system.

```
1  try
2      A --- x --> B
3      C --- y --> D
4  catch
5      E --- z --> F
```

So that the second flow only happens if the first fails, you should instead just check whatever condition you're actually interested in. I don't think this will greatly impact usability, and in fact is probably easier to read because the condition has to be specified, and you won't get unexpected failures causing the flow. For example, say you want to do the third flow only when there isn't enough money in A and C for first two flows to occur. But the above implementation would also cause the money to be taken from C in the case that there's, for example, and overflow when you transfer to B, or if A has enough money, but not C, which may is desirable.

4   Examples

Transfer with fees   This is fairly common: for example, the contract with the most transactions does this, as do many gambling/auction contracts.

$$\mathtt{transfer(from, to, amount):}$$
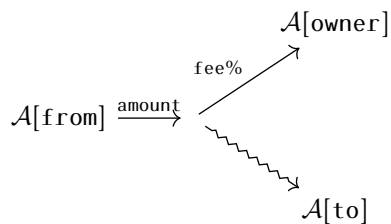
4.1   The DAO attack

We can prevent the DAO attack (the below is from https://consensys.github.io/smart-contract-best-practices/known_attacks/):

```
1  function withdrawBalance() public {
2      uint amountToWithdraw = userBalances[msg.sender];
3      // At this point, the caller's code is executed, and can call withdrawBalance again
4      require(msg.sender.call.value(amountToWithdraw)(""));
5      userBalances[msg.sender] = 0;
6  }
```

In LANGUAGE-NAME, we would write this as:

```
1  transaction withdrawBalance():
2      userBalances[msg.sender] −−> msg.sender.balance
```

Not only is this simpler, but the compiler can automatically place the actual call that does the transfer last, meaning that the mistake could simply never be made.

4.2 approveAndCall

Many token contracts include the concept of approveAndCall, typically similarly to the following (taken from: 0x174bfa6600bf90c885c7c01c7031389ed1461ab9, one of the most popular contracts on the blockchain by transaction count):

```
1  function approveAndCall(address _spender, uint256 _value, bytes memory _extraData) public returns (bool success) {
2      tokenRecipient spender = tokenRecipient(_spender);
3      if (approve(_spender, _value)) {
4          spender.receiveApproval(msg.sender, _value, address(this), _extraData);
5          return true;
6      }
7  }
```

In LANGUAGE-NAME, we can do the same thing by associating a call with a flow.

```
1  transaction approveAndCall(_spender : address, _value : uint256, _extraData : bytes):
2      consume everything from allowance[msg.sender, _spender]
3      approvalSource −−[ _value ]−> allowance[msg.sender, _spender],
4      on success: call  receiveApproval(msg.sender, _value, address(this), _extraData)
```

5 Random Thoughts

[Ignore this for now, just some stuff for fun that may or may not end up being useful.] [At some point, maybe for antoher language, would like to figure out the more general type quantity thing where you can freely combine set and list and nonempty and one, etc.] [We could also add sum types and "sum type quantities" so you can say x : Left (a + b). Something like {ℓ, r} where ℓ and r are state specifiers. Probably would work best with labeled sum types.] [Add at "at most one" quantity, which makes the type quantities into a group?] [Free group of quantities list set and option makes teh type quantities we care about? What are the inverses?]

$$\texttt{nonempty} = \texttt{option}^{-1}$$

Definition 5. *[Don't think this really has a good name]* A resource $\mathcal{R}$ is a tuple $(R, +, 0, \leq, -)$ where

  (i) $(R, +, 0)$ is a monoid.

 (ii) $(R, \leq)$ is a partial order that is compatible with $(R, +, 0)$. That is, for any $x, y \in R$ such that $x \leq y$, and for any $z \in R$, we have $x + z \leq y + z$.

(iii) $- : R \times R \to R$ is a function so that for any $x, y \in R$ such that $y \leq x$, we have $(x - y) + y = x$.

Examples

  1. The natural numbers with the standard operations is a resource $(\mathbb{N}, +, 0, \leq, -)$, where $-$ is *saturating subtraction*: $n - m = 0$ if $m > n$.

2. For any set A, we can build the resource $(\mathcal{P}(A), \cup, \emptyset, \subseteq, \setminus)$, where $X \setminus Y$ is the set difference operation.

3. Similarly, given any set A, we can build the resource $(\mathcal{P}_{\text{fin}}(A), \cup, \emptyset, \subseteq, \setminus)$; this resource is called the *nonfungible resource on A*, written $\text{nf}(A)$.

4. [I have no idea if this is useful, but it's fun] The set of strings on an alphabet Σ can be made into the *prefix resource* $(\Sigma^*, \varepsilon, \cdot, \leq_p, -_p)$ or the *suffix resource* $(\Sigma^*, \varepsilon, \cdot, \leq_s, -_s)$, where $\cdot$ is concatenation, $x \leq_p y$ if x is a prefix of y and similarly $x \leq_s y$ if x is a suffix of y. The functions $-_p$ and $-_s$ are defined as follows:
$$(x \cdot y) -_p x = y$$
and
$$(x \cdot y) -_s y = x$$

Definition 6. *For any two resources $\mathcal{R}$ and $\mathcal{S}$, their* direct product, $\mathcal{R} \oplus \mathcal{S}$ *is* $(R \times S, +_{RS}, (0_R, 0_S), \leq_{RS}, -_{RS})$, *where*

$$(r_1, s_1) +_{RS} (r_2, s_2) := (r_1 +_R r_2, s_1 +_S s_2)$$
$$(r_1, s_1) -_{RS} (r_2, s_2) := (r_1 -_R r_2, s_1 -_S s_2)$$
$$(r_1, s_1) \leq_{RS} (r_2, s_2) : \Longleftrightarrow r_1 \leq_R r_2 \wedge s_1 \leq_S s_2$$

Definition 7. *Let $\mathcal{R}$ be a resource and let A be a set. The exponential resource $\mathcal{R}^A$* [I suspect this would be an exponential, anyway] *is defined so*

$$\mathcal{R}^A := (R^A, +, \mathbf{0}, \leq, -)$$

where for $f, g \in R^A$, we define

$$\mathbf{0}(x) := 0$$
$$(f + g)(x) := f(x) + g(x)$$
$$f \leq g :\Leftrightarrow \forall x \in A. f(x) \leq g(x)$$
$$(f - g)(x) := f(x) - g(x)$$

Note that $f - g$ is only defined when $g \leq f$.