1 Specification

1.1 Syntax

$C \in \textsc{ContractNames}$ $\quad$ $m \in \textsc{TransactionNames}$

$t \in \textsc{TypeNames}$ $\quad$ $x \in \textsc{IdentifierNames}$

$n \in \mathbb{Z}$

$\mathcal{Q}$	::=	$\texttt{unknown} \mid \texttt{empty} \mid \texttt{nonempty}$	(type quantities[Not sure what
τ	::=	$\texttt{void} \mid \texttt{bool} \mid \texttt{nat} \mid \mid \texttt{option}\ T \mid \texttt{list}\ T \mid \texttt{set}\ T \mid T \times T \mid T \rightsquigarrow T \mid \{\overline{x : T}\} \mid t$	(base types)
T	::=	$\mathcal{Q}\ \tau$	(types)
$\mathfrak{q}$	::=	$! \mid * \mid +$	(selector quantifiers)
C	::=	$n \mid \text{true} \mid \text{false}$	(constants)
$\mathcal{V}$	::=	$\text{C} \mid \lambda x : \tau . E$	(values)
$\mathcal{L}$	::=	$x \mid x[x] \mid x.x$	(locations)
$\mathcal{S}$	::=	$\mathcal{L} \mid \texttt{new}\ C(\overline{x}) \mid \texttt{consume}$	(storages)
E	::=	$\mathcal{V} \mid \mathcal{L} \mid \texttt{let}\ x : \tau\ \texttt{in}\ E$	(expressions)
f	::=	$E \mid \texttt{everything} \mid \mathfrak{q}\ x : \tau\ \textbf{s.t.}\ E$	(selector)
F	::=	$\mathcal{S} \xrightarrow{f} \mathcal{S}$	(flows)
S	::=	$F \mid \texttt{if}\ E\ \texttt{then}\ S \mid S ; S \mid \texttt{var}\ x : \tau$	(statements)
M	::=	$\texttt{fungible} \mid \texttt{nonfungible} \mid \texttt{consumable} \mid \texttt{asset}$	(type declaration modifiers)
$\mathcal{D}$	::=	$x : \tau \mid \texttt{type}\ t\ \texttt{is}\ \overline{M}\ \tau$	(declarations)
Con	::=	$\texttt{contract}\ C\ \{\ \overline{\mathcal{D}}\ \}$	(contracts)
Prog	::=	$\overline{\texttt{Con}}\ ;\ S$	(programs [Improve this, defin

Figure 1: Abstract syntax of LANGUAGE-NAME.

Consider τ an abbreviation for $\texttt{unknown}\ \tau$.

[What if we got rid of selecting by location and only allowed selecting with quantifiers, and just optimize things like $! \ x : \tau$ s.t. $x = y$ into a lookup.] [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?]

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

[Contract types should be (consumable?) assets by default, transformers are always assets, because they could be partially applied and holding assets.]

1.2 Statics

Γ ::= $\emptyset \mid \Gamma, x : \tau$ (type environments)

Define $* \leq ! \leq +$ (this is based on the amount of resources that every quantifier is *guaranteed* to

select). Define $|\mathcal{Q}|$ by

$$|\texttt{unknown}| = *$$
$$|\texttt{empty}| = *$$
$$|\texttt{nonempty}| = +$$

$\boxed{\Gamma \vdash e : \tau}$ **Typing**

$$\frac{}{\Gamma, x : \tau \vdash x : \text{demote}(\tau)}\ \textsc{Lookup} \qquad \frac{\Gamma, x : \tau \vdash e : \sigma \dashv \Gamma}{\Gamma \vdash (\lambda x : \tau . e) : \tau \rightsquigarrow \sigma}\ \textsc{Transformer}$$

$$\frac{\Gamma \vdash x : \texttt{empty}\ \tau}{\Gamma \vdash x : \tau}\ \textsc{Forget-Empty} \qquad \frac{\Gamma \vdash x : \texttt{nonempty}\ \tau}{\Gamma \vdash x : \tau}\ \textsc{Forget-Nonempty}$$

Definition 1. *Let τ be a type. The* canonical form of τ *is $[\![\tau]\!] = (\mathcal{Q}, \sigma)$ where $\tau = \mathcal{Q}\ \sigma$, such that if $\sigma = \mathcal{R}\ \pi$ for some quantity $\mathcal{R}$ and type π, then $\mathcal{R} = \textbf{one}$.*

$\boxed{\texttt{select}(f, \mathfrak{q}, \tau)}$ $\boxed{\texttt{combine}(\mathfrak{q}, \tau)}$ $\boxed{\texttt{update}(\Gamma, \mathcal{S}, \tau)}$ **Storage modification** These auxiliary functions are used to update the statically known information about a storage after flowing in or out of it (see the Flow rule).

$$\texttt{select}(f, \mathfrak{q}, \tau) = \begin{cases} \texttt{empty}\ \tau & \text{if } f = \texttt{everything} \\ \texttt{empty}\ \tau & \text{if } \mathfrak{q} \geq ! \text{ and } [\![\tau]\!] = (\textbf{one}, \sigma) \\ \tau & \text{otherwise} \end{cases}$$

$$\texttt{combine}(\mathfrak{q}, \tau) = \begin{cases} \texttt{nonempty}\ \tau & \text{if } \mathfrak{q} \geq ! \\ \tau & \text{otherwise} \end{cases}$$

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

$\boxed{\Gamma \vdash \mathcal{S} :: \tau \Rrightarrow \sigma}$ **Storage Typing** The syntax $\tau \Rrightarrow \sigma$ 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.

$$\frac{}{\Gamma, S : \mathcal{Q}\ \tau \vdash S :: \tau \Rrightarrow \tau}\ \textsc{Flow-Storage} \qquad \frac{}{\Gamma, x : \tau \rightsquigarrow \sigma \vdash x :: \tau \Rrightarrow \sigma}\ \textsc{Flow-Transformer}$$

$$\frac{\tau\ \texttt{consumable}}{\Gamma \vdash \texttt{consume} :: \tau \Rrightarrow \texttt{void}}\ \textsc{Flow-Consume}$$

$$\frac{\texttt{contract}\ C\ \{\overline{\mathcal{F}}\ (\texttt{on create}(\overline{x : \tau})\ S)\ \overline{T}\} \qquad \Gamma \vdash \overline{y : \tau}}{\Gamma \vdash \texttt{new}\ C(\overline{y}) :: \texttt{void} \Rrightarrow C}\ \textsc{Flow-New}$$

$\boxed{\Gamma \vdash e\ \texttt{selects}_{\mathfrak{q}}\ \tau}$ **Selectors**

$$\frac{\Gamma \vdash e : \mathcal{Q}\ \tau}{\Gamma \vdash e\ \texttt{selects}_{|\mathcal{Q}|}\ \tau}\ \textsc{Select-Expr} \qquad \frac{s \in \{\texttt{everything}, \texttt{nothing}\}}{\Gamma \vdash s\ \texttt{selects}_{*}\ \tau}\ \textsc{Select-Special}$$

$$\frac{\Gamma, x : \tau \vdash p : \texttt{bool}}{\Gamma \vdash (\mathfrak{q}\ x : \tau\ \textbf{s.t.}\ p)\ \texttt{selects}_{\mathfrak{q}}\ \tau}\ \textsc{Select-Quant}$$

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

$$\frac{}{\Gamma, x : \tau \vdash x : \tau \dashv \Gamma}\ \textsc{Lin-Lookup} \qquad \frac{\Gamma \vdash x : \tau \qquad \neg(\tau\ \texttt{asset})}{\Gamma \vdash x : \tau \dashv \Gamma}\ \textsc{Lin-View}$$

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

$$\frac{\begin{array}{c}\Gamma \vdash S :: \tau \Rrightarrow \sigma \qquad \Gamma \vdash f\ \texttt{selects}_{\mathfrak{q}}\ \mathrm{demote}(\sigma) \\ \Delta = \texttt{update}(\Gamma, S, \texttt{select}(f, \mathfrak{q}, \Gamma(S))) \qquad \Delta \vdash D :: \sigma \Rrightarrow \pi\end{array}}{\Gamma \vdash (S \xrightarrow{f} D)\ \mathfrak{wf} \dashv \texttt{update}(\Delta, D, \texttt{combine}(\mathfrak{q}, \Delta(D)))}\ \textsc{Wf-Flow}$$

$$\frac{}{\Gamma \vdash (\texttt{var}\ x : \tau)\ \mathfrak{wf} \dashv \Gamma, x : \texttt{empty}\ \tau}\ \textsc{Wf-Var-Def} \qquad \frac{\Gamma \vdash x : \texttt{bool} \qquad \Gamma \vdash S\ \mathfrak{wf} \dashv \Delta}{\Gamma \vdash (\texttt{if}\ x\ \texttt{then}\ S)\ \mathfrak{wf} \dashv \Gamma \vee \Delta}\ \textsc{Wf-If}$$

$$\frac{\Gamma \vdash S_1\ \mathfrak{wf} \dashv \Delta \qquad \Delta \vdash S_2\ \mathfrak{wf} \dashv \Xi}{\Gamma \vdash (S_1; S_2)\ \mathfrak{wf} \dashv \Xi}\ \textsc{Wf-Seq}$$

Note that $\Gamma(S)$ is the type that S currently has in Γ, or $\bot$ if it is not in Γ. **[Maybe there's a nicer way to do this, but since `update` will ignore anything that doesn't exists in the environment already, it works out.]**

[Not exactly sure how the merge $\Gamma \vee \Delta$ should work, but I imagine it should involve something like $\texttt{empty}\ \tau \vee \texttt{one}\ \tau = \texttt{option}\ \tau$. Then we define type compatibility and check type compatibility when we pack at the end of a transaction.]

Definition 2. *Let Γ and Δ be type environments. Then $\Gamma \leq \Delta$ if $\forall x \in \mathbf{dom}(\Gamma), \Gamma(x) \leq \Delta(x)$.*

Definition 3. *Let $\mathcal{Q}\ \tau$ and $\mathcal{R}\ \sigma$ be types. Then $\mathcal{Q}\ \tau \leq \mathcal{R}\ \sigma$ if $\mathcal{Q} \leq \mathcal{R}$.*

Definition 4. *A type quantity $\mathcal{Q}$ is* known *if $\mathcal{Q} = \mathbf{empty}\ \mathcal{S}$ or $\mathcal{Q} = \mathbf{nonempty}\ \mathcal{S}$ for some type quantity $\mathcal{S}$. Say that $\mathcal{Q}$ is* unknown *of it is known. Let $\mathcal{R}$ be a type quantity. Define*

$$\mathcal{Q} \leq \mathcal{R} \iff \mathcal{Q}\ \textit{is}$$

[TODO: Define τ `consumable`]

[Probably should only be possible to transfer resources via. "external" calls to calls to the same contract.]

[Selecting using a list from a set should yield a list (i.e., a deterministic order). This lets you do things that need a specific order without always storing things in lists. Probably a good idea? But how to make not confusng]

Demote definition **[TODO: Finish]**

$\boxed{\mathrm{demote}(\tau) = \sigma}$ **Type Demotion**

$$\begin{aligned}
\mathrm{demote}(\texttt{nat}) &= \texttt{nat} \\
\mathrm{demote}(\texttt{bool}) &= \texttt{bool} \\
\mathrm{demote}(t) &= \mathrm{demote}(\tau) && \text{where } t \text{ is } \texttt{asset}\ \tau \\
\mathrm{demote}(\mathcal{Q}\ \tau) &= \mathcal{Q}\ \mathrm{demote}(\tau) \\
\mathrm{demote}(\tau \times \sigma) &= \mathrm{demote}(\tau) \times \mathrm{demote}(\sigma) \\
\mathrm{demote}(\{\overline{x : \tau}\}) &= \left\{\overline{x : \mathrm{demote}(\tau)}\right\}
\end{aligned}$$

[Selecting from or with a list should yield a list, probably] [Asset retention theorem?] [Resource accessiblity?] [NOTE: Local transformers must be consumed, because they might be holding resources if partially applied. This is just like any asset local variable.]

[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.

```
F: voterSource --- newVoterAddress --> authorizedVoters
```

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

```
on fail F with Err:
    revert("This address is already authorized! Do not re-authorize it.")
on success F:
    emit AuthorizedVoter(newVoterAddress)
    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?]**

```
F1: A --- x ---> B
F2: C --- y ---> D
on fail {F1,F2}:
    // Stuff
on success {F1,F2}:
    // 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:

```
handle {
    A --- x --> B
    C --- y --> D
    E --- z --> F
} with {
    on fail :
        // Stuff
    on success:
        // Stuff
}
```

This can be mechanically rewritten to:

```
F1: A --- x --> B
F2: C --- y --> D
F3: E --- z --> F
on fail  {F1,F2,F3}:
    // Stuff
on success {F1,F2,F3}:
    // Stuff
```

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

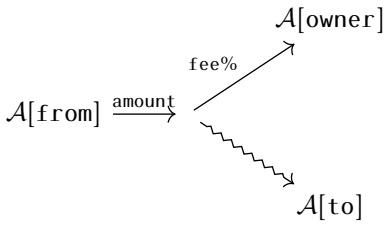
```
try
    A --- x --> B
    C --- y --> D
catch
    E --- z --> F
```

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.

`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/`):

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

In LANGUAGE-NAME, we would write this as:

```
transaction withdrawBalance():
    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):

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

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

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