Psamathe: A DSL for Safe Blockchain Assets

ACM Reference Format:
. 2020. Psamathe: A DSL for Safe Blockchain Assets. In *Proceedings of ACM Conference (Conference'17)*. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

[Authors/affiliations?]

1 INTRODUCTION

Blockchains are becoming more commonly used as platforms for applications, called *smart contracts*, which automatically manage transactions in an unbiased, mutually agreed-upon way. Commonly proposed and implemented applications for the blockchain often revolve around the management of *digital assets*. One of the most common forms of these are a variety of smart contracts that managed assets called *tokens*—about 73% of high-activity contracts, the 0.05% of contracts that handle 80% of all transactions, are token contracts [12], in addition to many more less-active token contracts. There are many token standards, especially on the Ethereum blockchain [14], including ERC-20, ERC-721, ERC-777, ERC-1155 [2] [5] [3] [4], with others in various stages of the standardization process. Other applications or proposed applications for smart contracts include supply chain management [10], healthcare [9], and other applications which require careful management of their respective assets such as voting, crowdfunding, or auctions [7].

However, smart contracts must be carefully reviewed before being deployed, as they cannot be patched if a security vulnerability is discovered. Despite this extra care, discoveries of vulnerabilities still occur regularly, often costing large amounts of money. The well-known DAO attack [13] caused the loss of over 40 million dollars, and was due to a reentrancy issue. The DAO attack is discussed in more depth in Section 3.4. Some estimates suggest that as much as 46% of smart contracts may be vulnerable [11].

Psamathe is a new programming language that we are designing, which is designed around a new abstraction, called a *flow*, representing an atomic transfer operation, which is widely applicable to smart contracts managing digital assets. It will also provide features to mark certain values as *assets*, with various *modifiers* to control their use, which combine with flows to make certain classes of bugs impossible. Solidity, the most commonly-used language for writing smart contracts on the Ethereum blockchain **[cite]**, being a general purpose language, does not provide analogous support for managing assets.

Contributions. We make the following contributions with Psamathe.

- **Flow abstraction**: Psamathe uses a new abstraction called a *flow* to encode semantic information about the flow of assets into the code.
- **Safety guarantees**: Psamathe ensures that assets are properly managed; eliminating reuse, asset-loss, and duplication bugs through the use of the flow abstraction and a type system tracking *type quantities*.
- **Conciseness**: Psamathe makes writing typical smart contract programs more concise by handling common patterns and pitfalls automatically.

2 LANGUAGE

A Psamathe program is made of *contracts*, each containing *declarations*, such as *fields*, *types*, and *functions*. A contract is the high-level grouping of functionality, just as in Solidity; each contract instance in Psamathe represents a contract on the blockchain. Fields function as the persistent storage of the contract, whose data is kept on the blockchain. Type declarations are the primary way to use the type system of Psamathe, providing a way of annotating values as assets (as well as other modifiers, discussed in Section 2.4). We distinguish between three types of function: *transactions*, *views*, and *transformers*. Transactions and views are both kinds of *method*, which may access the fields of a contract; a transaction can read **and** write fields, whereas a view may only read fields. A transformer is a **pure** function: it may contain flows and other statements, but it cannot mutate the state of any contract.

Figure 1 shows a simple contract declaring a type, a field, and a transaction, which implements the core functionality of ERC-20's transfer function (see Section 3.1 for more details on ERC-20).

```
contract ERC20 {
 type Token is fungible asset uint256
 balances : map address => Token
 transaction transfer(dst : address, amt : uint256):
  balances[msg.sender] --[ amt ]-> balances[dst]
}
```

Figure 1: A contract with a simple transfer function in Psamathe, which transfers amount tokens from the first to the second account. It is implemented with a single flow, which automatically checks all the preconditions to ensure the transfer is valid.

2.1 Syntax

Figure 2 shows a fragment of the syntax of the core calculus of Psamathe, which uses A-normal form and makes several other simplifications to the surface Psamathe language. These simplifications are performed automatically by the compiler. **[TODO: We have formalized this core calculus (in K???).]**

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

$$
\begin{array}{lll}
\mathfrak{q} & ::= ! \mid \mathtt{any} \mid \mathtt{nonempty} & \text{(selector quantifiers)} \\
\mathcal{Q} & ::= \mathfrak{q} \mid \mathtt{empty} \mid \mathtt{every} & \text{(type quantities)} \\
T & ::= \mathtt{bool} \mid \mathtt{nat} \mid \mathtt{map}\ \tau \ \Rightarrow\ \sigma \mid t \mid \ldots & \text{(base types)} \\
\tau & ::= \mathcal{Q}\ T & \text{(types)} \\
\mathcal{V} & ::= n \mid \mathtt{true} \mid \mathtt{false} \mid \mathtt{emptyval} \mid \ldots & \text{(values)} \\
\mathcal{L} & ::= x \mid x.x & \text{(locations)} \\
E & ::= \mathcal{V} \mid \mathcal{L} \mid \mathtt{total}\ t \mid \ldots & \text{(expressions)} \\
s & ::= \mathcal{L} \mid \mathtt{everything} \mid \mathfrak{q}\ x : \tau\ \textbf{s.t.}\ E & \text{(selector)} \\
\mathcal{S} & ::= \mathcal{L} \mid \mathtt{new}\ t & \text{(sources)} \\
\mathcal{D} & ::= \mathcal{L} \mid \mathtt{consume} & \text{(destinations)} \\
F & ::= \mathcal{S} \xrightarrow{s} \mathcal{D} & \text{(flows)} \\
\mathtt{Stmt} & ::= F \mid \mathtt{Stmt}; \mathtt{Stmt} \mid \ldots & \text{(statements)} \\
M & ::= \mathtt{fungible} \mid \mathtt{immutable} \mid \mathtt{unique} & \\
 & \quad \mid \mathtt{consumable} \mid \mathtt{asset} & \text{(type modifiers)} \\
\mathtt{Decl} & ::= \mathtt{type}\ t\ \mathtt{is}\ \overline{M}\ T & \text{(type declaration)} \\
 & \quad \mid \mathtt{transaction}\ m(\overline{x : \tau}) \longrightarrow x : \tau\ \mathtt{do}\ \mathtt{Stmt} & \text{(transactions)} \\
 & \quad \mid \ldots & \\
\mathtt{Con} & ::= \mathtt{contract}\ C\ \{\ \overline{\mathtt{Decl}}\ \} & \text{(contracts)}
\end{array}
$$

Figure 2: A fragment of the abstract syntax of the core calculus of Psamathe, a simplified form of the surface language.

2.2 Flows

Psamathe is built around the concept of a *flow*, an atomic, state-changing operation describing the transfer of a asset. Each flow has a *source* and a *destination*; they may optionally have a *selector* or a *transformer*, which default to **everything** and the identity transformer, respectively. The source of a flow *provides* values, the destination of the flow *accepts* these values, and the selector describes which subpart of the value(s) in the source should be transferred to the destination. Selectors act like filters from functional programming, or like a WHERE in SQL. Using a transformer in a flow is like mapping a function over the collection of values being flowed.

Using a *flow-based* approach provides the following advantages over the typical *assignment-based* approach most languages use (e.g., incrementing, then decrementing):

- **Precondition checking**: For a flow to succeed, the source must have enough assets and the destination must be capable of receiving the assets flowed. For example, a flow of money would fail if there is not enough in the source, or if there is too much in the destination; the latter may occur because of overflow. Flows can also fail for other reasons: a developer may specify that a certain flow must send all assets matching a predicate, but in addition specify an expected *quantity* that must be selected: any number, exactly one, or at least one. The former will always succeed, but the latter two may cause the flow to fail.
- **Data-flow tracking**: It is clear where the resources are flowing from the code itself, which may not be apparent in complicated contracts, such as those involving transfer fees. Furthermore, developers must explicitly mark all times that assets are *consumed*, and only assets marked as **consumable** may be consumed. This restriction prevents assets, such as ether from being consumed.
- **Error messages**: When a flow fails, Psamathe provides automatic, descriptive error messages, such as "Cannot flow '<amount>' Token from account[<src>] to account[<dst>]: source only has <balance> Token.". By default, Solidity provides no error messages, forcing developers to write their own. Flows enable the generation of the messages by encoding the semantic information of a transfer into the program, instead of using low-level operations like increment and decrement or insert and delete.

2.3 Type Quantities

When a Psamathe program is type checked, each variable has an associated *type quantity* at every point in the program, which provides an approximation of the number of values the variable holds. The list of allowed type quantities is: **empty**, **any**, !, **nonempty**, **every** (note "!" means "exactly one"). Only **empty** asset variables may be dropped, ensuring that unused assets not dropped. Type quantities are **not** required in the surface language, and they will be added automatically; for example, `var toks : set Token := {}` is inferred to be an `empty set Token`, whereas `var C : Bank := new Bank()` is inferred to be `! Bank`.

Type quantities are primarily updated by flows. For example, after checking the flow `a --[ everything ]-> b`, we now know that `a` is empty, and depending on the type quantity that `a` used to have, we may now know that `b` is also empty (if `a` was empty), nonempty, or any other type quantity (other than **every**). Type quantities can also be updated by expressions, which can move values to other variables. For example, after checking `var x : (Token, Token) := (a, b)`, creating a new pair, both `a` and `b` are **empty**, as the assets they used to hold are now in `x`. **[Need to think more in depth about the differences between this and linear types. I personally find it more intuitive.]**

2.4 Modifiers

Modifiers can be used to place constraints on how values are managed: **asset**, **fungible**, **unique**, **immutable**, and **consumable**. A **asset** is a value that must not be reused or accidentally lost. A **fungible** value represents a quantity which can be **merged**, and it is **not** **unique**. A **unique** value can only exist in at most one storage; it must be **immutable**. A **immutable** value cannot be changed; in particular, it cannot be the source or destination of a flow, the only state-changing construct in Psamathe. A **consumable** value is an **asset** that it is sometimes appropriate to dispose of; however, this disposal must be done via the `consume` construct, a way of documenting that the disposal is intentional. All of these constraints, except for uniqueness, are enforced statically.

For example, ERC-20 tokens are **fungible**, while ERC-721 tokens are best modeled as being both **unique** and **immutable**. By default, neither is **consumable**, but one of the common extensions of both standards is to add a `burn` function, which allows tokens to be destroyed by users with the appropriate authentication. In this case, it would be appropriate to add the **consumable** modifier.

Psamathe also supports data structures that make working with assets easier, such as *linkings*, a bidirectional map between keys and collections of values to support modeling of an *account* holding a collection of assets. A `linking K <=> C V` is a `map K => C V` with additional operations, where `K` is the key type, `V` is the value type, and `C` is some collection type constructor, such as `list` or `set`. The additional operations supported are `L.hasOwner(v)` and `L.ownerOf(v)`, where `L : linking K <=> C V` and `v : V`. `L.hasOwner(v)` returns true if and only if there is some `k : K` such that `v in L[k]` is true. `L.ownerOf(v)` returns some `k : K` such that `v in L[k]`, if it exists. If it does not, it throws an error. **[Alternate implementation could be to return an `option`.] [I have some ideas about adding interfaces to the language, which I would love to do but it would complicate things.]** See Figure 4b for some example uses of this structure. Note that, though it is possible to partially implement linkings as a library in Solidity, in Psamathe, we can guarantee that looking up the owner of a value when the owner type is `unique` is a **well-defined** operation.

2.5 Error Handling

Computation on blockchains like the Ethereum blockchain is grouped into units called *transactions*. Transactions in the same *block* are executed in a nondeterministic, but sequential, order. Transactions either succeed or they fail and revert all changes. Psamathe also has transactional semantics: a sequence of flows will either all succeed, or, if a single flow fails, the rest will fail as well. If a sequence of flows fails, it “bubbles up”, like an exception, until it either: a) reaches the top level, at which point the entire transaction fails; or b) reaches a **`catch`**, in which case only the changes made inside the corresponding **`try`** block will be reverted, and the code inside the **`catch`** block will be executed.

2.6 Comparison with Solidity

The concept of contracts in Psamathe maps directly Solidity’s concept of contracts. Transactions, views, and transformers all map to the concept of **function** in Solidity: a transaction is a function that is public by default, a view is a function with the **view** modifier, and a transformer is a function with the **pure** modifier. A type declaration in Psamathe is best modeled by a **struct** in Solidity, although type declarations are more flexible: Solidity has does not support any of the modifiers that Psamathe does (note Solidity has its own concept of modifiers that is unrelated). **[Probably should put more effort into explanation for people who don’t know Solidity (at least, if we submit to a non-blockchain venue).]**

The Psamathe language provides all of the primitive types that Solidity does, with additional support for types such as linkings, explained above. Solidity also exhibits several atypical behaviors, such as acting as those all keys in a mapping exist, and providing the default value whenever a new key is used. This leads to ad-hoc workarounds, like those shown in Sections 3.2 and 3.3.

Before version 0.6.0, for the first four years since its release five years ago, Solidity did not have a try-catch construct [8]. The newly-added try-catch construct behaves similarly to that of Psamathe, as both will revert the changes made when an exception occurs. However, Solidity’s try-catch is structured in an atypical way, only allowing catching errors from a single expression, which must be an external call or a contract creation call.

3 EXAMPLES

In this section, we show several example smart contracts, with a Solidity version and a Psamathe version, and discuss the benefits of each version. In each example, we only show the fragment of the code that is necessary for space reasons, but both the fully Solidity and Psamathe implementations can be found in our repository. **[Do this] [Put online or in an appendix?]**

3.1 ERC-20

ERC-20 **[cite]** is a standard for smart contracts that manage **fungible** tokens, and provides a bare-bones interface for this purpose. Each ERC-20 contract manages the “bank accounts” for its own tokens, keeping track of which users, identified by addresses, have some number of tokens. We focus on one core function from ERC-20, the transfer function. ERC-20 is one of the commonly implemented standards on the Ethereum blockchain **[cite]**. **[Cite all Solidity code]** Figure 3 shows a Solidity implementation of the ERC-20 function transfer (cf. Figure 1). Note that event code has been omitted, because Psamathe handles events in the same way as Solidity. This example shows the advantages of the flow abstraction in precondition checking and error messages. **[rephrase, because you can’t see the error messages, but it’s still part of the advantages...]** In this case, the balance of the sender must be at least as large as the amount sent, and the balance of the destination must not overflow when it receives the tokens. Code checking these two conditions is automatically inserted, ensuring that the checks cannot be forgotten.

```
contract ERC20 {
 mapping (address => uint256) balances;
 function transfer(address dst, uint256 amt)
   public returns (bool) {
   require(amt <= balances[msg.sender]);
   balances[msg.sender] = balances[msg.sender].sub(amt);
   balances[dst] = balances[dst].add(amt);
   return true;
 }
}
```

Figure 3: An implementation of ERC-20’s transfer function in Solidity. All preconditions are checked manually. Note that we must include the SafeMath library (not shown), which checks for underflow/overflow, to use the add and sub functions.

3.2 ERC-721

ERC-721 **[cite]**, like ERC-20, is a token standard for the Ethereum blockchain. ERC-721 is a standard for tokens managing *nonfungible* tokens; that is, tokens that are unique. The ERC-721 standard requires many invariants hold, including: the tokens must be unique, the tokens must be owned by at most one account, at most one non-owning account can have *approval* for a token, and only if that token has been minted, we must be able to support *operators* who can manage all of the tokens of a user, among others.

Because Psamathe is designed to manage assets, it has features to help developers ensure that these correctness properties hold.

Figures 4a and 4b show implementations in Solidity and Psamathe, respectively, of the ERC-721 function transferFrom. The Solidity implementation is extracted from a reference implementation of ERC-721 given on the official Ethereum EIP page.

A Psamathe implementation has several benefits: because of the asset abstraction, we can be sure that token references will not be duplicated or lost; because Token has been declared as **unique**, we can be sure that we will not mint two of the same token. In addition to the invariants required by the specification, there are also internal invariants which the contract must maintain, such as the connection between idToOwner and ownerToNFTokenCount, which are handled automatically in the Psamathe version. This example demonstrates the benefits of having **unique** assets and the linking data structure built into the language itself.

3.3 Voting

One proposed use for the blockchain is smart contracts for managing voting **[cite]**. The voting scheme we implement here is a standard

Figures 5a and 5b show the core of an implementation of a simple voting contract in Solidity and Psamathe, respectively. This example shows that Psamathe is suited for a range of applications, as we can use the **unique** modifier to remove certain incorrect behaviors, shown in Figure 5. In this application, the use of **unique** ensures that each user, represented by an *address*, can be given permission to vote at most once, while the use of **asset** ensures that votes are not lost or double-counted. We also see that the Solidity implementation is more verbose than the Psamathe implementation because it must work around Solidity's limitations regarding mappings. In this example, the declaration of the weight and voted members of the Voter struct exist so that the contract can tell whether a voter has the default values or was actually authorized to vote/has already voted.

3.4 The DAO attack

One of the most financially impactful bugs in a smart contract on the Ethereum blockchain was the bug in the DAO contract which allowed a large quantity of ether, worth over 40 million dollars at the time, to be stolen [12]. The bug was caused by a reentrancy-unsafe function in the contract, illustrated below.

The Solidity function shown below allows a user to withdraw their balance of ether whenever they wish. It does this by first transferring the ether from the contract to the user's address, then decreasing the user's balance. However, in Ethereum, a transfer of ether also calls a special function on the receiving address, when it is a contract address, called a *fallback* function. In this function, arbitrary code may be executed, and because **call**.value() was used, this call has access to all of the remaining gas of the transaction. A malicious contract can use this to perform a *reentrant* call back into the withdrawBalance function, and withdraw their balance again—the user's balance has not been decreased yet. The fix in this case is a simple swap of the last two lines of the function, but reentrancy issues can be more complicated than this. **[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 Psamathe, this attack could not have occurred for several reasons. Consider the following implementation of the same function in Psamathe given below.

```
transaction withdrawBalance():
    userBalances[msg.sender] --> msg.sender.balance
```

Because of the additional information encoded in the flow construct, the compiler can output the safe version of the above code—reducing the balance before performing the external call—without any developer intervention. Additionally, Psamathe forbids any reentrant call from an external source, a similar approach to the Obsidian language [6], which would also prevent more complicated reentrancy attacks.

4 DISCUSSION

5 RELATED WORK

There have been many new blockchain languages proposed, such as Obsidian [6], Scilla **[cite]**, Move **[cite]**, Nomos **[cite]**, Flint **[cite]**.

Some of these languages, such as Scilla and Move, were proposed as intermediate-level languages, whereas Psamathe is intended to be a high-level language.

Several of these languages, such as Obsidian, Move, Nomos, and Flint use *linear types* to provide guarantees about assets, like those provided by the type quantities of Psamathe. However, none of these languages provide similar support for all the modifiers that Psamathe does.**[should check this to be sure...]** Furthermore, none of the languages have flows. **[Obsidian, Scilla, Move, Nomos, etc.?] [TODO: The safety guarantees provided by Psamathe differ from those provided by other languages because...Obsidian has similar concept of assets, but doesn't allow expressing immutability, uniqueness, or consumability (could do fungibility via an interface, I suppose); this is probably going to be similar to other languages built around linear type systems. Obsidian's reentrancy scheme is slightly different, Nomos has a similar global lock, it seems.]**

6 CONCLUSION AND FUTURE WORK

[Conclusion]

In the future, we plan to fully implement the Psamathe language, including proofs of all of its safety properties. We also hope to perform additional studies on the benefits of the language including conducting longer case studies and comparing the efficiency of the resulting programs. We would also like to perform a user study to evaluate the usability of the flow abstraction and the design of the language itself, as well as comparing it to Solidity.

```
contract NFToken {
 mapping (uint256 => address) idToOwner;
 mapping (uint256 => address) idToApproval;
 mapping (address => uint256) ownerToNFTokenCount;
 mapping (address => mapping (address => bool)) ownerToOperators;


 modifier canTransfer(uint256 tokId) {
  require(idToOwner[tokId] == msg.sender ||
       idToApproval[tokId] == msg.sender ||
       ownerToOperators[idToOwner[tokId]][msg.sender]);
  _;
 }
 function transferFrom(address src, address dst, uint256 tokId)
  external canTransfer(tokId) {
  require(idToOwner[tokId] != address(0));
  require(idToOwner[tokId] == src);
  require(dst != address(0));
  if (idToApproval[tokId] != address(0)) {
   delete idToApproval[tokId];
  }
  ownerToNFTokenCount[src] = ownerToNFTokenCount[src] - 1;
  delete idToOwner[tokId];
  idToOwner[tokId] = dst;
  ownerToNFTokenCount[dst] = ownerToNFTokenCount[dst].add(1);
 }
}
```

(a) A Solidity implementation of ERC-721's transferFrom. Note that some helper functions and modifiers have been unfolded, and some redundant checks have been removed for space reasons.

```
contract NFToken {
 type Token is unique immutable asset uint256
 type Approval is unique immutable consumable asset uint256
 balances : linking address <=> set Token
 approval : linking address <=> set Approval
 ownerToOperators : linking address <=> set address

 view canTransfer(tokId : uint256) returns bool :=
// `A in B` is true iff we can select `A` from `B`.
// It can be implemented efficiently if the LHS is hashable.
  tokId in balances[msg.sender] or
  tokId in approval[msg.sender] or
  msg.sender in ownerToOperators[balances.ownerOf(tokId)]
 transaction transferFrom(src : address, dst : address, tokId : uint256):
  only when _to != 0x0 and canTransfer(tokId)
  if approval.hasOwner(tokId) {
   approval[approval.ownerOf(tokId)] --[ tokId ]-> consume
  }
  balances[src] --[ tokId ]-> balances[dst]
}
```

(b) Psamathe implementation of ERC-721's transferFrom.

Figure 4: Implementation of ERC-721's transferFrom function, which sends a specific token from the src account to the dst account. It also must clear the approval of the token, if any.

REFERENCES

[1] [n.d.]. Solidity by Example. Retrieved 2020-07-28 from https://solidity.readthedocs.io/en/v0.7.0/solidity-by-example.html

[2] 2015. EIP 20: ERC-20 Token Standard. Retrieved 2020-07-28 from https://eips.ethereum.org/EIPS/eip-20

[3] 2017. EIP 777: ERC777 Token Standard. Retrieved 2020-07-28 from https://eips.ethereum.org/EIPS/eip-777

[4] 2018. EIP 1155: ERC-1155 Multi Token Standard. Retrieved 2020-07-28 from https://eips.ethereum.org/EIPS/eip-1155

[5] 2018. EIP 721: ERC-721 Non-Fungible Token Standard. Retrieved 2020-07-28 from https://eips.ethereum.org/EIPS/eip-721

[6] Michael Coblenz, Reed Oei, Tyler Etzel, Paulette Koronkevich, Miles Baker, Yannick Bloem, Brad A. Myers, Joshua Sunshine, and Jonathan Aldrich. 2019. Obsidian: Typestate and Assets for Safer Blockchain Programming. arXiv:cs.PL/1909.03523

[7] Chris Elsden, Arthi Manohar, Jo Briggs, Mike Harding, Chris Speed, and John Vines. 2018. Making Sense of Blockchain Applications: A Typology for HCI. In *CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. 1–14. https://doi.org/10.1145/3173574.3174032

[8] Elena Gesheva. 2020. Solidity 0.6.x features: try/catch statement. Retrieved 2020-07-29 from https://blog.ethereum.org/2020/01/29/solidity-0.6-try-catch/

[9] Harvard Business Review. 2017. The Potential for Blockchain to Transform Electronic Health Records. Retrieved February 18, 2020 from https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records

[10] IBM. 2019. Blockchain for supply chain. Retrieved March 31, 2019 from https://www.ibm.com/blockchain/supply-chain/

[11] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. 2016. Making Smart Contracts Smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (Vienna, Austria) *(CCS '16)*. Association for Computing Machinery, New York, NY, USA, 254–269. https://doi.org/10.1145/2976749.2978309

[12] Gustavo Oliva, Ahmed E. Hassan, and Zhen Jiang. 2019. An Exploratory Study of Smart Contracts in the Ethereum Blockchain Platform. *Empirical Software Engineering* (11 2019). https://doi.org/10.1007/s10664-019-09796-5

[13] Emin Gün Sirer. 2016. Thoughts on The DAO Hack. Retrieved July 29, 2020 from http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/

[14] Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151, 2014 (2014), 1–32.

A FORMALIZATION

A.1 Syntax

[Sets can only contain immutable types?] [Note that unique is not allowed if the type can contain a transformer.]

[We have public and private transactions...we could also have a public/private type? The difference being that public types can be transferred between contracts.] [Random note: We can optimize merge operations on unique types by dropping some checks.]

In the surface language, "collection types" (i.e., $Q\ C\ \tau$ 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

```
contract Ballot {
  struct Voter { uint weight; bool voted; uint vote; }
  struct Proposal { bytes32 name; uint voteCount; }

  address public chairperson;
  mapping(address => Voter) public voters;
  Proposal[] public proposals;

  function giveRightToVote(address voter) public {
    require(msg.sender == chairperson,
      "Only chairperson can give right to vote.");
    require(!voters[voter].voted, "The voter already voted.");
    voters[voter].weight = 1;
  }
  function vote(uint proposal) public {
    Voter storage sender = voters[msg.sender];
    require(sender.weight != 0, "Has no right to vote");
    require(!sender.voted, "Already voted.");
    sender.voted = true;
    sender.vote = proposal;
    proposals[proposal].voteCount += sender.weight;
  }
}
```

(a) Solidity implementation of the core voting functions [1].

```
contract Ballot {
  type Voter is unique immutable asset address
  type ProposalName is unique immutable asset string

  chairperson : address
  voters : set Voter
  proposals : linking ProposalName <=> set Voter

  transaction giveRightToVote(voter : address):
    only when msg.sender = chairperson
    new Voter(voter) −−> voters



  transaction vote(proposal : string):
    voters −−[ msg.sender ]−> proposals[proposal]
}
```

(b) Psamathe implementation of the core voting functions.

Figure 5: A voting contract with a set of proposals, for which each user must first be given permission to vote by the chairperson, assigned in the constructor of the contract (not shown). Each user can vote exactly once for exactly one proposal. The proposal with the most votes wins.

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 $\texttt{any}\ x : \tau$ s.t. $\texttt{if}\ b\ \texttt{then}\ x = y\ \texttt{else}\ \mathit{false}$]

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

A.2 Statics

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

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

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

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

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

$$\begin{aligned}(Q\ T)\ \texttt{consumable} \Leftrightarrow &\texttt{consumable} \in \texttt{modifiers}(T) \text{ or}\\ &\neg((Q\ T)\ \texttt{asset}) \text{ or}\\ &(T = C\ \tau \text{ and } \tau\ \texttt{consumable}) \text{ or}\\ &(T = \{\overline{y : \sigma}\} \text{ and } \forall x : \tau \in \overline{y : \sigma}.(\sigma\ \texttt{consumable}))\end{aligned}$$

$Q \oplus \mathcal{R}$ represents the quantity present when flowing $\mathcal{R}$ of something to a storage already containing Q. $Q \ominus \mathcal{R}$ represents the quantity left over after flowing $\mathcal{R}$ from a storage containing Q.

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

$$\begin{aligned}Q \oplus \texttt{empty} &= Q\\ Q \oplus \texttt{every} &= \texttt{every}\\ \texttt{nonempty} \oplus \mathcal{R} &= \texttt{nonempty} && \textit{if}\ \texttt{empty} < \mathcal{R} < \texttt{every}\\ !\oplus \mathcal{R} &= \texttt{nonempty} && \textit{if}\ \texttt{empty} < \mathcal{R} < \texttt{every}\\ \texttt{any} \oplus \texttt{any} &= \texttt{any}\end{aligned}$$

$$
\begin{array}{ll}
C \in \textsc{ContractNames} & m \in \textsc{TransactionNames} \\
t \in \textsc{TypeNames} & x, y, z \in \textsc{Identifiers} \\
n \in \mathbb{Z} &
\end{array}
$$

$$
\begin{array}{lcll}
\mathfrak{q} & ::= & ! \mid \texttt{any} \mid \texttt{nonempty} & \text{(selector quantifiers)} \\
\mathcal{Q}, \mathcal{R}, \mathcal{S} & ::= & \mathfrak{q} \mid \texttt{empty} \mid \texttt{every} & \text{(type quantities)} \\
C & ::= & \texttt{option} \mid \texttt{set} \mid \texttt{list} & \text{(collection type constructors)} \\
T & ::= & \texttt{bool} \mid \texttt{nat} \mid C\ \tau & \\
 & \mid & \texttt{map}\ \tau \Rightarrow \tau \mid \texttt{mapitem}\ \tau \Rightarrow \tau & \\
 & \mid & \texttt{linking}\ \tau \Leftrightarrow \tau \mid \texttt{link}\ \tau \Leftrightarrow \tau & \\
 & \mid & \tau \rightsquigarrow \tau \mid \{\overline{x : \tau}\} \mid t & \text{(base types)} \\
\tau, \sigma, \pi & ::= & \mathcal{Q}\ T & \text{(types)} \\
\mathcal{V} & ::= & n \mid \texttt{true} \mid \texttt{false} \mid \texttt{emptyval} \mid \lambda x : \tau.E & \text{(values)} \\
\mathcal{L}, \mathcal{M} & ::= & x \mid \mathcal{L}.x \mid \mathcal{L}[\mathcal{L}] & \text{(locations)} \\
E & ::= & \mathcal{V} \mid \mathcal{L} \mid x.m(\overline{x}) \mid \texttt{single}(x) \mid s\ \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 & \\
 & \mid & x = x \mid x \neq x \mid \texttt{total}\ x \mid \texttt{total}\ t & \text{(expressions)} \\
s & ::= & \mathcal{L} \mid \texttt{everything} \mid \mathfrak{q}\ x : \tau\ \textbf{s.t.}\ E & \text{(selector)} \\
\mathcal{S} & ::= & \mathcal{L} \mid \texttt{new}\ t & \text{(sources)} \\
\mathcal{D} & ::= & \mathcal{L} \mid \texttt{consume} & \text{(destinations)} \\
F & ::= & \mathcal{S} \xrightarrow{s} x \longrightarrow \mathcal{D} & \text{(flows)} \\
\texttt{Stmt} & ::= & F \mid E \mid \texttt{revert}(E) \mid \texttt{pack} \mid \texttt{unpack}(x) \mid \texttt{emit}\ E(\overline{x}) & \\
 & \mid & \texttt{try Stmt catch}(x : \tau)\ \texttt{Stmt} \mid \texttt{if}\ x\ \texttt{then Stmt else Stmt} & \\
 & \mid & \texttt{var}\ x : \tau := E\ \texttt{in Stmt} \mid \texttt{Stmt}; \texttt{Stmt} & \text{(statements)} \\
M & ::= & \texttt{fungible} \mid \texttt{unique} \mid \texttt{immutable} \mid \texttt{consumable} \mid \texttt{asset} & \text{(type declaration modifiers)} \\
\texttt{Decl} & ::= & x : \tau & \text{(field)} \\
 & \mid & \texttt{event}\ E(\overline{x : \tau}) & \text{(event declaration)} \\
 & \mid & \texttt{type}\ t\ \texttt{is}\ \overline{M}\ T & \text{(type declaration)} \\
 & \mid & [\texttt{private}]\ \texttt{transaction}\ m(\overline{x : \tau}) \longrightarrow x : \tau\ \texttt{do Stmt} & \text{(transactions)} \\
 & \mid & \texttt{view}\ m(\overline{x : \tau}) \longrightarrow \tau := E & \text{(views)} \\
 & \mid & \texttt{on create}(\overline{x : \tau})\ \texttt{do Stmt} & \text{(constructor)} \\
\texttt{Con} & ::= & \texttt{contract}\ C\ \{\ \overline{\texttt{Decl}}\ \} & \text{(contracts)} \\
\texttt{Prog} & ::= & \overline{\texttt{Con}}\ ;\ S & \text{(programs)}
\end{array}
$$

Figure 6: Abstract syntax of the core calculus of Psamathe.

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

Define the operator $\ominus$, *called* split, *as the unique function* $\boldsymbol{Quant}^2 \rightarrow \boldsymbol{Quant}$ *such that*

$$
\begin{array}{rcll}
\mathcal{Q} \ominus \texttt{empty} & = & \mathcal{Q} & \\
\texttt{empty} \ominus \mathcal{R} & = & \texttt{empty} & \\
\mathcal{Q} \ominus \texttt{every} & = & \texttt{empty} & \\
\texttt{every} \ominus \mathcal{R} & = & \texttt{every} & \textit{if}\ \mathcal{R} < \texttt{every} \\
\texttt{nonempty} - \mathcal{R} & = & \texttt{any} & \textit{if}\ \texttt{empty} < \mathcal{R} < \texttt{every} \\
! - \mathcal{R} & = & \texttt{empty} & \textit{if}\ ! \leq \mathcal{R} \\
! - \texttt{any} & = & \texttt{any} & \\
\texttt{any} - \mathcal{R} & = & \texttt{any} & \textit{if}\ \texttt{empty} < \mathcal{R} < \texttt{every}
\end{array}
$$

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 $(\mathcal{Q} \ominus \mathcal{R})\ T$.

Definition 3. *We can consider a type environment* Γ *as a function* $\textsc{Identifiers} \longrightarrow \textsc{Types} \cup \{\bot\}$ *as follows:*

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

We write $\textbf{dom}(\Gamma)$ *to mean* $\{x \in \textsc{Identifiers} \mid \Gamma(x) \neq \bot\}$, *and* $\Gamma|_X$ *to mean the environment* $\{x : \tau \in \Gamma \mid x \in X\}$ *(restricting the domain of* Γ*).*

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* $\sqsubseteq$ *as the reflexive closure of the strict partial order* $\sqsubset$ *given by*

$$\mathcal{Q} \sqsubset \mathcal{R} \Leftrightarrow (\mathcal{Q} \neq \texttt{any}\ \textit{and}\ \mathcal{R} = \texttt{any})\ \textit{or}\ (\mathcal{Q} \in \{!, \texttt{every}\}\ \textit{and}\ \mathcal{R} = \texttt{nonempty})$$

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

$$\mathcal{Q}\ T_{\mathcal{Q}} \leq \mathcal{R}\ T_{\mathcal{R}} \Leftrightarrow T_{\mathcal{Q}} = T_{\mathcal{R}}\ \textit{and}\ \mathcal{Q} \sqsubseteq \mathcal{R}$$

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

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

Denote the join of Γ and Δ by $\Gamma \sqcup \Delta$.

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

These rules are for ensuring that expressions are well-typed, and keeping track of which variables are used throughout the expression. Most rules do **not** change the context, with the notable exceptions of internal calls and record-building operations. We begin with the rules for typing the various literal forms of values. **[TODO: Single rule should work for any fungible (or mergeable??) type]**

$$\frac{}{\Gamma \vdash \mathbf{emptyval} : \mathbf{empty}\ C\ \tau \dashv \Gamma}\ \textsc{Empty-Val}$$

$$\frac{\Gamma \vdash x : \tau \dashv \Delta}{\Gamma \vdash \mathbf{single}(x) : !\ C\ \tau \dashv \Delta}\ \textsc{Single}$$

$$\frac{\Gamma, x : \tau \vdash E : \sigma \dashv \Gamma, x : \pi \qquad \neg(\pi\ \mathbf{asset})}{\Gamma \vdash (\lambda x : \tau.E) : !\ (\tau \rightsquigarrow \sigma) \dashv \Gamma}\ \textsc{Transformer}$$

$$\frac{\Gamma \vdash \overline{y : \tau} \dashv \Delta}{\Gamma \vdash \{\overline{x : \tau \mapsto y}\} \dashv \Delta}\ \textsc{Build-Rec}$$

Next, the lookup rules. Notably, the Demote-Lookup rule allows the use of variables of an asset type in an expression without consuming the variable as Lin-Lookup does. However, it is still safe, because it is treated as its demoted type, which is always guaranteed to be a non-asset **[probably should prove this to be sure]**.

$$\frac{}{\Gamma, x : \tau \vdash x : \mathrm{demote}(\tau) \dashv \Gamma, x : \tau}\ \textsc{Demote-Lookup}$$

$$\frac{\mathrm{demote}(\tau) \neq \tau}{\Gamma, x : Q\ T \vdash x : Q\ T \dashv \Gamma, x : \mathbf{empty}\ T}\ \textsc{Lin-Lookup}$$

$$\frac{f : \sigma \in \overline{y : \tau}}{\Gamma, x : \{\overline{y : \tau}\} \vdash x.f : \mathrm{demote}(\sigma) \vdash \Gamma, x : \{\overline{y : \tau}\}}\ \textsc{Record-Demote-Lookup}$$

$$\frac{\begin{array}{c} f : Q\ T \in \overline{y : \tau} \qquad \mathrm{demote}(\sigma) \neq \sigma \\ \overline{z : \sigma} = (\overline{y : \tau} \setminus \{f : Q\ T\}) \cup \{f : \mathbf{empty}\ T\} \end{array}}{\Gamma, x : \{\overline{y : \tau}\} \vdash x.f : Q\ T \vdash \Gamma, x : \{\overline{z : \sigma}\}}\ \textsc{Record-Lin-Lookup}$$

The expression s **in** x allows checking whether a flow will succeed without the EAFP-style ("Easier to ask for forgiveness than permission"; e.g., Python). A flow $A \xrightarrow{s} B$ is guaranteed to succeed when "s **in** A" is true and "s **in** B" is false.

$$\frac{\Gamma \vdash x\ \mathbf{provides}_Q\ \tau \qquad \Gamma \vdash s\ \mathbf{selects}\ \mathrm{demote}(\tau)}{\Gamma \vdash (s\ \mathbf{in}\ x) : \mathbf{bool} \dashv \Gamma}\ \textsc{Check-In}$$

We distinguish between three kinds of calls: view, internal, and external. A view call is guaranteed to not change any state in the receiver, while both internal and external calls may do so. The difference between internal and external calls is that we may transfer assets to an internal call, but **not** to an external call, because we cannot be sure any external contract will properly manage the asset of our contract.

$$\frac{\begin{array}{c} \mathbf{dom}(\mathbf{fields}(C)) \cap \mathbf{dom}(\Gamma) = \emptyset \\ \mathbf{typeof}(C, m) = \{\overline{a : \tau}\} \rightsquigarrow \sigma \\ \Gamma, x : C \vdash \overline{y : \tau} \dashv \Gamma, x : C \end{array}}{\Gamma, x : C \vdash x.m(\overline{y}) : \sigma \dashv \Gamma, x : C}\ \textsc{View-Call}$$

$$\frac{\begin{array}{c} \mathbf{dom}(\mathbf{fields}(C)) \cap \mathbf{dom}(\Gamma) = \emptyset \\ \mathbf{typeof}(C, m) = \{\overline{a : \tau}\} \rightsquigarrow \sigma \\ \Gamma, \mathbf{this} : C \vdash \overline{y : \tau} \dashv \Delta, \mathbf{this} : C \end{array}}{\Gamma, \mathbf{this} : C \vdash \mathbf{this}.m(\overline{y}) : \sigma \dashv \Delta, \mathbf{this} : C}\ \textsc{Internal-Tx-Call}$$

$$\frac{\begin{array}{c} \mathbf{dom}(\mathbf{fields}(C)) \cap \mathbf{dom}(\Gamma) = \emptyset \\ (\mathbf{transaction}\ m(\overline{a : \tau}) \longrightarrow \sigma\ \mathbf{do}\ S) \in \mathbf{decls}(D) \\ \Gamma, \mathbf{this} : C, x : D \vdash \overline{y : \tau} \dashv \Gamma, \mathbf{this} : C, x : D \end{array}}{\Gamma, \mathbf{this} : C, x : D \vdash x.m(\overline{y}) : \sigma \dashv \Gamma, \mathbf{this} : C, x : D}\ \textsc{External-Tx-Call}$$

$$\frac{(\mathbf{on\ \ create}(\overline{x : \tau})\ \mathbf{do}\ S) \in \mathbf{decls}(C) \qquad \Gamma \vdash \overline{y : \tau} \dashv \Gamma}{\Gamma \vdash \mathbf{new}\ C(\overline{y}) : C}\ \textsc{New-Con}$$

Finally, the rules for If and Let expressions. In Let-Expr, we must ensure that the newly bound variable is either consumed or is not an asset after the body runs.

$$\frac{\Gamma \vdash x : \mathbf{bool} \dashv \Gamma \qquad \Gamma \vdash E_1 : \tau \dashv \Delta \qquad \Gamma \vdash E_2 : \tau \dashv \Xi}{\Gamma \vdash (\mathbf{if}\ x\ \mathbf{then}\ E_1\ \mathbf{else}\ E_2) : \tau \dashv \Delta \sqcup \Xi}\ \textsc{If-Expr}$$

$$\frac{\begin{array}{c} \Gamma \vdash E_1 : \tau \dashv \Delta \\ \Delta, x : \tau \vdash E_2 : \pi \dashv \Xi, x : \sigma \qquad \neg(\sigma\ \mathbf{asset}) \end{array}}{\Gamma \vdash (\mathbf{let}\ x : \tau := E_1\ \mathbf{in}\ E_2) : \pi \dashv \Xi}\ \textsc{Let-Expr}$$

$\boxed{\mathbf{elemtype}(T) = \sigma}$

$$\mathbf{elemtype}(T) = \begin{cases} \mathbf{elemtype}(S) & \text{if } \mathbf{type}\ T\ \mathbf{is}\ \overline{M}\ S \\ \sigma & \text{if } T = C\ \sigma \\ !\ T & \text{otherwise} \end{cases}$$

$\boxed{\Gamma \vdash \mathcal{L} : \tau}$ **Non-consuming location typing** This judgment is exclusively used for checking the types of the storages in a flow. It is safe to use because the flow rule handles updating the storages after the flow. **[Would be nice to combine the linking and map rules, and especially nice to avoid special casing them altogether. Could be done with a "keytype(T)" function. Maybe we could make it work on sets of mapitem or link, and then**

avoid even defining maps and linkings.]

$$\frac{(x\ \mathtt{immutable}) \notin \Gamma}{\Gamma, x : \tau \vdash x : \tau}\ \textsc{Loc-Var}$$

$$\frac{\begin{array}{c}\Gamma \vdash \mathcal{L} : \mathcal{Q}\ T \\ (f : \sigma) \in \mathtt{fields}(T) \qquad \neg(T\ \mathtt{immutable})\end{array}}{\Gamma \vdash \mathcal{L}.f : \sigma}\ \textsc{Loc-Member}$$

$$\frac{\Gamma \vdash \mathcal{L} : \mathcal{Q}\ (\mathtt{map}\ \tau\ \Rightarrow\ \sigma) \qquad \Gamma \vdash \mathcal{M} : \tau}{\Gamma \vdash \mathcal{L}[\mathcal{M}] : \sigma}\ \textsc{Loc-Map}$$

$$\frac{\Gamma \vdash \mathcal{L} : \mathcal{Q}\ (\mathtt{linking}\ \tau\ \Leftrightarrow\ \sigma) \qquad \Gamma \vdash \mathcal{M} : \tau}{\Gamma \vdash \mathcal{L}[\mathcal{M}] : \sigma}\ \textsc{Loc-Linking}$$

[How to handle immutable properly?] $\boxed{\Gamma \vdash \mathcal{S}\ \mathtt{provides}_{\mathcal{Q}}\ \tau}$ **Source Typing**

$$\frac{\Gamma \vdash S : \mathcal{Q}\ T}{\Gamma \vdash S\ \mathtt{provides}_{\mathcal{Q}}\ \mathtt{elemtype}(T)}\ \textsc{Provide-Var}$$

$$\frac{(\mathtt{type}\ t\ \mathtt{is}\ \overline{M}\ T) \in \mathtt{decls}(C)}{\Gamma, \mathtt{this} : C \vdash (\mathtt{new}\ t)\ \mathtt{provides}_{\mathtt{every}}\ !\ t}\ \textsc{Provide-Source}$$

$\boxed{\Gamma \vdash \mathcal{D}\ \mathtt{accepts}\ \tau}$ **Destination Typing** Note that the type quantities in Accept-One are different on the left and right of the turnstile. This is because, for example, when I have $D : \mathtt{nonempty\ set\ nat}$, it is reasonable to flow into it some $S : \mathtt{any\ set\ nat}$.

$$\frac{\Gamma \vdash D : \mathcal{Q}\ T}{\Gamma \vdash D\ \mathtt{accepts}\ \mathtt{elemtype}(T)}\ \textsc{Accept-Var}$$

$$\frac{\tau\ \mathtt{consumable}}{\Gamma \vdash \mathtt{consume}\ \mathtt{accepts}\ \tau}\ \textsc{Accept-Consume}$$

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

$$\frac{\Gamma \vdash \mathcal{L} : \mathcal{Q}\ T \dashv \Gamma}{\Gamma \vdash \mathcal{L}\ \mathtt{selects}_{\mathcal{Q}}\ \mathtt{elemtype}(T)}\ \textsc{Select-Var}$$

$$\frac{}{\Gamma \vdash \mathtt{everything}\ \mathtt{selects}_{\mathtt{every}}\ \tau}\ \textsc{Select-Everything}$$

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

$\boxed{\mathtt{validSelect}(s, \mathcal{R}, \mathcal{Q})}$ We need to ensure that the resources to be selected are easily computable. In particular, we wish to enforce that we never select $\mathtt{everything}$ from a source containing $\mathtt{every}$ of something, nor do we use a selector like $\mathfrak{q}x : \tau$ s.t. E on a source contianing $\mathtt{every}$ of something. The following definition captures these restrictions.

$$\mathtt{validSelect}(s, \mathcal{R}, \mathcal{Q}) \Leftrightarrow \min(\mathcal{Q}, \mathcal{R}) < \mathtt{every} \text{ and } (\mathcal{Q} = \mathtt{every} \Rightarrow \exists \mathcal{L}.s = \mathcal{L})$$

$\boxed{\Gamma \vdash S\ \mathbf{ok} \dashv \Delta}$ **Statement Well-formedness**

Flows are the main construct for transferring resources. A flow has four parts: a source, a selector, a transformer, and a destination.

The selector acts as a function that "chooses" part of the source's resources to flow. These resources then get applied to the transformer, which is an applicative functor applied to a function type. **[Bringing back one would let us do all the collections the same way in all of these flow-related rules, which would be nice.]**

$$\frac{\begin{array}{c}\Gamma \vdash A\ \mathtt{provides}_{\mathcal{Q}}\ \tau \qquad \Gamma \vdash s\ \mathtt{selects}_{\mathcal{R}}\ \tau \\ \mathtt{validSelect}(s, \mathcal{R}, \mathcal{Q}) \qquad \Delta = \mathtt{update}(\Gamma, A, \Gamma(A) \ominus \mathcal{R}) \\ \Delta \vdash f : \tau \rightsquigarrow \sigma \dashv \Delta \qquad \Delta \vdash B\ \mathtt{accepts}\ \sigma\end{array}}{\Gamma \vdash (A \xrightarrow{s} f \longrightarrow B)\ \mathbf{ok} \dashv \mathtt{update}(\Delta, B, \Delta(B) \oplus \min(\mathcal{Q}, \mathcal{R}))}\ \textsc{Ok-Flow}$$

[TODO: Finish handling currying transformers.]

$$\frac{\begin{array}{c}\Gamma \vdash E : \tau \dashv \Delta \\ \Delta, x : \tau \vdash S\ \mathbf{ok} \dashv \Xi, x : \sigma \qquad \neg(\sigma\ \mathtt{asset})\end{array}}{\Gamma \vdash (\mathtt{var}\ x : \tau := E\ \mathtt{in}\ S)\ \mathbf{ok} \dashv \Xi}\ \textsc{Ok-Var-Def}$$

$$\frac{\Gamma \vdash x : \mathtt{bool} \dashv \Gamma \qquad \Gamma \vdash S_1\ \mathbf{ok} \dashv \Delta \qquad \Gamma \vdash S_2\ \mathbf{ok} \dashv \Xi}{\Gamma \vdash (\mathtt{if}\ x\ \mathtt{then}\ S_1\ \mathtt{else}\ S_2)\ \mathbf{ok} \dashv \Delta \sqcup \Xi}\ \textsc{Ok-If}$$

$$\frac{\begin{array}{c}\Gamma \vdash S_1\ \mathbf{ok} \dashv \Delta \\ \Gamma, x : \tau \vdash S_2\ \mathbf{ok} \dashv \Xi, x : \sigma \qquad \neg(\sigma\ \mathtt{asset})\end{array}}{\Gamma \vdash (\mathtt{try}\ S_1\ \mathtt{catch}\ (x : \tau)\ S_2)\ \mathbf{ok} \dashv \Delta \sqcup \Xi}\ \textsc{Ok-Try}$$

$$\frac{\Gamma \vdash E : \tau \dashv \Gamma \qquad \neg(\tau\ \mathtt{asset})}{\Gamma \vdash \mathtt{revert}(E)\ \mathbf{ok} \dashv \Gamma}\ \textsc{Ok-Revert}$$

$$\frac{\Gamma \vdash E : \tau \dashv \Delta \qquad \neg(\tau\ \mathtt{asset})}{\Gamma \vdash E\ \mathbf{ok} \dashv \Delta}\ \textsc{Ok-Expr}$$

$$\frac{\Gamma \vdash S_1\ \mathbf{ok} \dashv \Delta \qquad \Delta \vdash S_2\ \mathbf{ok} \dashv \Xi}{\Gamma \vdash (S_1; S_2)\ \mathbf{ok} \dashv \Xi}\ \textsc{Ok-Seq}$$

$$\frac{\mathtt{this}.f : \tau \in \mathtt{fields}(C)}{\Gamma, \mathtt{this} : C \vdash \mathtt{unpack}(f)\ \mathbf{ok} \dashv \Gamma, \mathtt{this} : C, \mathtt{this}.f : \tau}\ \textsc{Ok-Unpack}$$

$$\frac{\begin{array}{c}(\Gamma|_{\mathtt{dom}(\mathtt{fields}(C))}) \leq \mathtt{fields}(C) \\ \Delta = \{x : \tau \in \Gamma \mid x \notin \mathtt{dom}(\mathtt{fields}(C))\}\end{array}}{\Gamma, \mathtt{this} : C \vdash \mathtt{pack}\ \mathbf{ok} \dashv \Delta, \mathtt{this} : C}\ \textsc{Ok-Pack}$$

$\boxed{\vdash_C \mathtt{Decl}\ \mathbf{ok}}$ **Declaration Well-formedness**

$$\frac{\Gamma = \mathtt{this} : C, \mathtt{fields}(C), \overline{x : \tau} \qquad \Gamma \vdash E : \sigma \dashv \Gamma}{\vdash_C (\mathtt{view}\ m(\overline{x : \tau}) \longrightarrow \sigma := E)\ \mathbf{ok}}\ \textsc{Ok-View}$$

$$\frac{\begin{array}{c}\mathtt{this} : C, \overline{x : \tau}, y : \mathtt{empty}\ T \vdash S\ \mathbf{ok} \dashv \Delta, \mathtt{this} : C, y : \mathcal{Q}\ T \\ \mathtt{dom}(\mathtt{fields}(C)) \cap \mathtt{dom}(\Delta) = \emptyset \\ \forall x : \tau \in \Delta. \neg(\tau\ \mathtt{asset}) \qquad \neg(\mathcal{Q}\ T\ \mathtt{asset})\end{array}}{\vdash_C (\mathtt{transaction}\ m(\overline{x : \tau}) \longrightarrow y : \mathcal{Q}\ T\ \mathtt{do}\ S)\ \mathbf{ok}}\ \textsc{Ok-Tx-Public}$$

$$\frac{\begin{array}{c}\mathtt{this} : C, \overline{x : \tau}, y : \mathtt{empty}\ T \vdash S\ \mathbf{ok} \dashv \Delta, \mathtt{this} : C, y : \mathcal{Q}\ T \\ \mathtt{dom}(\mathtt{fields}(C)) \cap \mathtt{dom}(\Delta) = \emptyset \\ \forall x : \tau \in \Delta. \neg(\tau\ \mathtt{asset})\end{array}}{\vdash_C (\mathtt{private\ transaction}\ m(\overline{x : \tau}) \longrightarrow y : \mathcal{Q}\ T\ \mathtt{do}\ S)\ \mathbf{ok}}\ \textsc{Ok-Tx-Private}$$

A field definition is always okay, as long as the type doesn't have the **every** modifier. **[Add this restriction to the rest of the places where we write types.] [Maybe we should always restrict variable definitions so that you can only write named types that appear in the current contract. This isn't strictly necessary, because everything will still work, but you'll simply never be able to get a value of an asset type not created in the current contract.]**

$$\frac{Q \neq \texttt{every}}{\vdash_C (x : Q\ T)\ \textbf{ok}}\ \textsc{Ok-Field}$$

A type declaration is okay when it's modifiers are all compatible with each other, and it has the **asset** modifier if its base type is an asset. The latter restriction isn't strictly necessary, but is intended to help developers realize which types are assets without unfolding the entire type definition. **[TODO: What if the base type is a non-consumable asset, and we write consumable. Is that okay? Probably not.]**

$$\frac{\begin{array}{c} T\ \texttt{asset} \implies \texttt{asset} \in \overline{M} \\ \texttt{unique} \in \overline{M} \implies \texttt{immutable} \in \overline{M} \\ \texttt{fungible} \in \overline{M} \implies \texttt{unique} \notin \overline{M} \end{array}}{\vdash_C (\texttt{type}\ t\ \texttt{is}\ \overline{M}\ T)\ \textbf{ok}}\ \textsc{Ok-Type}$$

Note that we need to have constructors, because only the contract that defines a named type is allowed to create values of that type, and so it is not always possible to externally initialize all contract fields.

$$\frac{\begin{array}{c} \texttt{fields}(C) = \overline{\texttt{this}.f : Q\ T} \\ \texttt{this} : C, \overline{x : \tau}, \overline{\texttt{this}.f : \texttt{empty}\ T} \vdash S\ \textbf{ok} \dashv \Delta \\ \forall y : \sigma \in \Delta.\neg(\sigma\ \texttt{asset}) \end{array}}{\vdash_C (\texttt{on create}(\overline{x : \tau})\ \texttt{do}\ S)\ \textbf{ok}}\ \textsc{Ok-Constructor}$$

$\boxed{\texttt{Con ok}}$ **Contract Well-formedness**

$$\frac{\begin{array}{c} \forall d \in \overline{\texttt{Decl}}.(\vdash_C d\ \textbf{ok}) \\ \exists! d \in \overline{\texttt{Decl}}.\exists \overline{x : \tau}, S.d = \texttt{on create}(\overline{x : \tau})\ \texttt{do}\ S \end{array}}{(\texttt{contract}\ C\ \{\overline{\texttt{Decl}}\})\ \textbf{ok}}\ \textsc{Ok-Con}$$

$\boxed{\texttt{Prog ok}}$ **Program Well-formedness**

$$\frac{\forall C \in \overline{\texttt{Con}}.C\ \textbf{ok} \qquad \emptyset \vdash S \dashv \emptyset}{(\overline{\texttt{Con}}; S)\ \textbf{ok}}\ \textsc{Ok-Prog}$$

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

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

$\boxed{\text{demote}(\tau) = \sigma}$ $\boxed{\text{demote}_*(T_1) = T_2}$ **Type Demotion** demote and demote$_*$ take a type and "strip" all the asset modifiers from it, as well as unfolding named type definitions. This process is useful, because it allows selecting asset types without actually having a value of the desired asset type. Note that demoting a transformer type changes nothing. This is because a transformer is **never** an asset, regardless of the types that it operators on, because it has no storage.

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

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

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

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

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

$\boxed{\texttt{typeof}(C, m) = \tau \rightsquigarrow \sigma}$ **Method Type Lookup**

$$\texttt{typeof}(C, m) = \begin{cases} \{\overline{x : \tau}\} \rightsquigarrow \sigma & \text{if } (\texttt{private transaction}\ m(\overline{x : \tau})\ \texttt{returns}\ y : \\ \{\overline{x : \tau}\} \rightsquigarrow \sigma & \text{if } (\texttt{transaction}\ m(\overline{x : \tau})\ \texttt{returns}\ y : \sigma\ \texttt{do}\ S) \in \\ \{\overline{x : \tau}\} \rightsquigarrow \sigma & \text{if } (\texttt{view}\ m(\overline{x : \tau})\ \texttt{returns}\ \sigma := E) \in \texttt{decls}(C) \end{cases}$$

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

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

A.3 WIP ideas

Definition 5. *Let* $\texttt{mgu}(\tau, \sigma)$ *denote the most general unifier of* τ *and* σ *such that if* $\texttt{mgu}(\tau, \sigma) = \theta$, *then* $\theta(\tau) = \sigma$; *if there is no unifier, then* $\texttt{mgu}(\tau, \sigma) = \bot$.

$$\frac{\emptyset \vdash S\ \textbf{ok} \dashv \Gamma \qquad \Gamma \vdash E : \tau \dashv \Delta \qquad \forall y.\neg(\Delta(y)\ \texttt{asset})}{(x : \tau := S\ \texttt{return}\ E)\ \textbf{ok}}\ \textsc{Init-Ok}$$

$$\frac{\begin{array}{c} \texttt{interface}\ I(\pi)\ \texttt{where}\ \overline{t\ \texttt{is}\ \overline{M}}\ \{\overline{\texttt{type}\ s}\ \overline{x : \tau}\} \\ \texttt{implementation}\ x\ \texttt{of}\ I(\sigma)\ \{\ldots\} \\ \texttt{mgu}(\pi, \sigma) \circ \texttt{mgu}(\sigma, \tau) = \theta \qquad \theta \neq \bot \\ \forall i.\forall N \in \overline{M_i}.\theta^{-1}(t_i)\ \texttt{is}\ \theta(N) \end{array}}{I(\tau)\ \texttt{resolvable}_x}\ \textsc{Resolvable-Impl}$$

$$\frac{\begin{array}{c} \overline{t} \subseteq \texttt{vars}(\tau) \\ \forall z : \pi \in \overline{y : \sigma}.\texttt{vars}(\pi) \subseteq \texttt{vars}(\tau) \cup \overline{s} \end{array}}{(\texttt{interface}\ I(\tau)\ \texttt{where}\ \overline{t\ \texttt{is}\ \overline{M}}\ \{\overline{\texttt{type}\ s}\ \overline{y : \sigma}\})\ \textbf{ok}}\ \textsc{Interface-Ok}$$

$$\frac{\begin{array}{c} \texttt{interface}\ I(\tau)\ \texttt{where}\ \overline{t\ \texttt{is}\ \overline{M}}\ \{\overline{\texttt{type}\ s}\ \overline{x : \tau}\} \\ \overline{x : \pi} = \overline{x : \tau}[\overline{\tau}/\overline{t}][\overline{\sigma}/\overline{s}] \\ \forall F \in \overline{x : \rho := S\ \texttt{return}\ E}.F\ \textbf{ok} \end{array}}{(\texttt{implementation}\ x\ \texttt{of}\ I(\sigma)\ \{\overline{\texttt{type}\ s\ \texttt{is}\ \pi}\ \overline{x : \rho := S\ \texttt{return}\ E}\})\ \textbf{ok}}\ \textsc{Impl-Ok}$$

[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)?]

NOTE: We can implement preconditions (i.e., "only when") 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.