

Psamathe: A DSL for Safe Blockchain Assets

Reed Oei
University of Illinois
reedoei2@illinois.edu

ABSTRACT

1 INTRODUCTION

[Seems like we should emphasize two things: why is this language declarative, and why are our programs easier to verify than Solidity programs (are they)?] [The other thing they seem to really care about is performance.]

[Should we put any effort into actually verifying things?]

Blockchains are increasingly used as platforms for applications called *smart contracts* [16], which automatically manage transactions in an unbiased, mutually agreed-upon way. Commonly proposed and implemented smart contracts include supply chain management [11], healthcare [10], *token contracts*, voting, crowdfunding, auctions, and more [9]. A *token contract* is a contract implementing a *token standard*, such as ERC-20 [1]. Smart contracts often manage *digital assets*, such as cryptocurrencies, or, depending on the application, bids in an auction, votes in an election, and so on. Token contracts are common on the Ethereum blockchain [17]—about 73% of high-activity contracts are token contracts [13]. Smart contracts cannot be patched after being deployed, even if a security vulnerability is discovered. Some estimates suggest that as much as 46% of smart contracts may have some vulnerability [12].

Psamathe (/səməθi/) is a new programming language we are designing around a new abstraction, a *flow*, representing an atomic transfer operation. Together with *modifiers* and *locators*, flows provide a **concise** way to write smart contracts that **safely** manage assets.

Solidity is the most commonly-used smart contract language on the Ethereum blockchain [2], and does not provide analogous support for managing assets. Typical smart contracts are more concise in Psamathe than in Solidity, because Psamathe handles common patterns and pitfalls automatically.

Other many newly-proposed blockchain languages include Flint, Move, Nomos, Obsidian, and Scilla [6–8, 14, 15]. Scilla and Move are intermediate-level languages, whereas Psamathe is a high-level language. Obsidian, Move, Nomos, and Flint use linear or affine types to manage assets; Psamathe uses *type quantities*, which provide the benefits of *linear types*, but give a more precise analysis of the flow of values in a program. None of these languages have flows, provide support for all the modifiers that Psamathe does, or have locators. In particular, the latter means that programs in those languages using linear or affine types must be more verbose to maintain linearity.

2 LANGUAGE

A Psamathe program is made of *transformers* and *types*. [TODO: Need to rewrite some of this to work with the new simpler flow language.] Figure 2 shows a simple contract declaring a type and a transformer, which implements the core of ERC-20’s transfer

```
1 contract ERC20 {
2   mapping (address => uint256) balances;
3   function transfer(address dst, uint256 amount)
4     public returns (bool) {
5     require(amount <= balances[msg.sender]);
6     balances[msg.sender] =
7       balances[msg.sender].sub(amount);
8     balances[dst] = balances[dst].add(amount);
9     return true;
10  }
11 }
```

Figure 1: An implementation of ERC-20’s transfer function in Solidity from one of the reference implementations [5]. 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.

```
1 type Token is fungible asset uint256
2 transformer transfer(balances : map address => Token,
3   dst : address, amount : uint256) {
4   balances[msg.sender] --[ amount ]-> balances[dst]
5 }
```

Figure 2: A Psamathe contract with a simple transfer function, which transfers amount tokens from the sender’s account to the destination account. It is implemented with a single flow, which automatically checks all the preconditions to ensure the transfer is valid.

function. ERC-20 is a standard for token contracts managing **fungible** tokens, and provides a bare-bones interface for this purpose.

Psamathe is built around the concept of a *flow*. [Why declarative] [Why easy to verify] [Why fast] Using the more declarative, *flow-based* approach provides the following advantages:

- **Invariant preservation:** Because of the design of the language, each flow is guaranteed to have certain safety properties, such as preserving the total amount of assets (except for when consumed or allocated). to preserve the amount of resources can do **[a lot]** to help preserve invariants, when compared to an imperative approach.
- **Precondition checking:** Psamathe automatically inserts dynamic checks of a flow’s validity; e.g., a flow of money would fail if there is not enough in the source, or if there is too much in the destination (e.g., due to overflow).
- **Data-flow tracking:** We hypothesize that flows provide a clearer way of specifying how resources flow in the code itself, which may be less apparent using other approaches, especially in complicated contracts. Additionally, developers must explicitly mark when assets are *consumed*, and only

assets marked as `consumable` may be consumed. [Because of venue, maybe we should emphasize that this might help code analysis tools, rather than people? It seems like that might be true: each flow can preserve the validity of the structure at every step, rather than needs to ensure that everything becomes valid again after doing multiple, smaller, changes.]

- **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.

Flows enable such messages by encoding all the necessary information into the program.

Each variable and function parameter has a *type quantity*, approximating the number of values in the variable, which is one of: **empty**, **any**, **!**, **nonempty**, **every** (“!” means “exactly one”). Type quantities are inferred if omitted. Only **empty** asset variables may be dropped.

Modifiers can be used to place constraints on how values are managed: **asset**, **fungible**, **unique**, **immutable**, and **consumable**. An **asset** is a value that must not be reused or accidentally lost. A **fungible** value represents a quantity that can be **merged**, and it is **not unique**. For example, ERC-20 tokens are **fungible**. A **immutable** value cannot be changed; in particular, it cannot be the source or destination of a flow. A **unique** value only exists in at most one variable; it must be **immutable** and an **asset** to ensure it is not duplicated. ERC-721 tokens are **unique** and **immutable**. A **consumable** value is an **asset** that it may be appropriate to dispose of, done via the `consume` construct, documenting that the disposal is intentional.

[TODO: Discuss locators] *Locators* are expressions that allow accessing or modifying parts of complex structures while maintaining linearity.

Psamathe 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, the error propagates, like an exception, until it either: a) reaches the top level, and the entire transaction fails; or b) reaches a **catch**, and then only the changes made in the corresponding **try** block will be reverted, and the code in the **catch** block will be executed.

3 EXAMPLES

The complete Solidity and Psamathe code is in our repository [3].

3.1 ERC-20

Figure 1 shows a Solidity implementation of the ERC-20 function transfer (cf. Figure 2). Each ERC-20 contract manages the “bank accounts” for its own tokens, keeping track of how many tokens each user has; users are represented by addresses. This example shows the advantages of flows in precondition checking, data-flow tracking, and error messages. In this case, the sender’s balance must be at least as large as amount, and the destination’s balance must not overflow when it receives the tokens. Psamathe automatically inserts code checking these two conditions, ensuring that the checks are not forgotten.

[Why declarative] [Why easy to verify] [Why just as fast]

```
1 contract Ballot {
2   struct Voter { uint weight; bool voted; uint vote; }
3   struct Proposal { bytes32 name; uint voteCount; }
4
5   address public chairperson;
6   mapping(address => Voter) public voters;
7   Proposal[] public proposals;
8
9   function giveRightToVote(address voter) public {
10    require(msg.sender == chairperson,
11           "Only chairperson can give right to vote.");
12    require(!voters[voter].voted,
13           "The voter already voted.");
14    voters[voter].weight = 1;
15  }
16  function vote(uint proposal) public {
17    Voter storage sender = voters[msg.sender];
18    require(sender.weight != 0, "No right to vote");
19    require(!sender.voted, "Already voted.");
20    sender.voted = true;
21    sender.vote = proposal;
22    proposals[proposal].voteCount += sender.weight;
23  }
24 }
```

Figure 3: A simple voting contract in Solidity.

```
1 type Voter is unique immutable asset address
2 type ProposalName is unique immutable asset string
3 type Election is asset {
4   chairperson : address
5   eligibleVoters : set Voter
6   proposals : map ProposalName => set Voter
7 }
8 transaction giveRightToVote(this : Election, voter : address) {
9   only when msg.sender = chairperson
10   new Voter(voter) --> this.eligibleVoters
11 }
12 transaction vote(this : Election, proposal : string) {
13   this.eligibleVoters --[ msg.sender ]-> this.proposals[proposal]
14 }
```

Figure 4: A simple voting contract in Psamathe.

3.2 Voting

One proposed use for blockchains is for voting [9]. Figures 3 and 4 show the core of an implementation of a voting contract in Solidity and Psamathe, respectively, based on the Solidity by Example tutorial [4]. Each contract instance has several proposals, and users must 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, and the proposal with the most votes wins.

This example shows Psamathe is suited for a range of applications. It also shows some uses of the **unique** modifier; in this contract, **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.

[Why declarative] [Why easy to verify] [Why just as fast]

3.3 Blind Auction

4 CONCLUSION AND FUTURE WORK

We have presented the Psamathe language for writing safer smart contracts. Psamathe uses the new flow abstraction, assets, and modifiers to provide safety guarantees for smart contracts. We showed two examples of smart contracts in both Solidity and Psamathe, showing that Psamathe is capable of expressing common smart contract functionality in a concise manner, while retaining key safety properties.

In the future, we plan to implement the Psamathe language, and prove its safety properties. We also hope to study the benefits of the language via case studies, performance evaluation, and the application of flows to other domains. Finally, we would also like to conduct a user study to evaluate the usability of the flow abstraction and the design of the language, and to compare it to Solidity, which we hypothesize will show that developers write contracts with fewer asset management errors in Psamathe than in Solidity.

REFERENCES

- [1] 2015. EIP 20: ERC-20 Token Standard. Retrieved 2020-07-28 from <https://eips.ethereum.org/EIPS/eip-20>
- [2] 2020. Ethereum for Developers. Retrieved 2020-07-31 from <https://ethereum.org/en/developers/>
- [3] 2020. Psamathe. <https://github.com/ReedOei/Psamathe>
- [4] 2020. Solidity by Example. Retrieved 2020-07-28 from <https://solidity.readthedocs.io/en/v0.7.0/solidity-by-example.html>
- [5] 2020. Tokens. Retrieved 2020-08-03 from <https://github.com/ConsenSys/Tokens>
- [6] Sam Blackshear, Evan Cheng, David L Dill, Victor Gao, Ben Maurer, Todd Nowacki, Alistair Pott, Shaz Qadeer, Dario Russi Rain, Stephane Sezer, et al. 2019. Move: A language with programmable resources.
- [7] 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*
- [8] Ankush Das, Stephanie Balzer, Jan Hoffmann, Frank Pfenning, and Ishani Santurkar. 2019. Resource-aware session types for digital contracts. *arXiv preprint arXiv:1902.06056* (2019).
- [9] Chris Elsdén, 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>
- [10] 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>
- [11] IBM. 2019. Blockchain for supply chain. Retrieved March 31, 2019 from <https://www.ibm.com/blockchain/supply-chain/>
- [12] 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>
- [13] 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>
- [14] Franklin Schrans, Susan Eisenbach, and Sophia Drossopoulou. 2018. Writing safe smart contracts in Flint. In *Conference Companion of the 2nd International Conference on Art, Science, and Engineering of Programming*. 218–219.
- [15] Ilya Sergey, Vaivaswatha Nagaraj, Jacob Johannsen, Amrit Kumar, Anton Trunov, and Ken Chan Guan Hao. 2019. Safer Smart Contract Programming with Scilla. *Proc. ACM Program. Lang.* 3, OOPSLA, Article 185 (Oct. 2019), 30 pages. <https://doi.org/10.1145/3360611>
- [16] Nick Szabo. 1997. Formalizing and Securing Relationships on Public Networks. *First Monday* 2, 9 (1997). <https://doi.org/10.5210/fm.v2i9.548>

```

1 type Bid is consumable asset {
2   sender : address,
3   blindedBid : bytes,
4   deposit : ether
5 }
6 type Reveal is { value : nat, fake : bool, secret : bytes }
7 type BlindAuction is asset {
8   beneficiary : address,
9   biddingEnd : nat,
10  revealEnd : nat,
11  ended : bool,
12  bids : map address => list Bid,
13  highestBidder : address,
14  highestBid : ether,
15  pendingReturns : map address => ether
16 }
17
18 transformer bid(this : BlindAuction, bid : bytes) {
19   only when now <= this.biddingEnd
20   [ new Bid(msg.sender, big, msg.value) ] --> this.bids[msg.sender]
21 }
22 transformer reveal(this : BlindAuction, reveals : list Reveal) {
23   only when biddingEnd <= now and now <= revealEnd
24   zip(this.bids[msg.sender], reveals)
25     --[ any such that _.fst.blindedBid = keccak256(_.snd) ]
26     --> revealBid(this, _)
27     --> placeBid(this, _)
28 }
29 transformer revealBid(this : BlindAuction, bid : Bid, reveal : Reveal) {
30   --> toPlace : list { sender : address, value : ether } {
31     try {
32       only when not reveal.fake
33         and reveal.value >= this.highestBid
34         bid.deposit --[ reveal.value ]-> var value : ether
35         [ { sender -> bid.sender, value -> value } ] --> toPlace
36     } catch {}
37     bid.deposit --> bid.sender.balance
38     bid --> consume
39   }
40 transformer placeBid(this : BlindAuction, toPlace : { sender : address, value : ether }) {
41   try {
42     only when highestBidder != 0x0
43     this.highestBid --> this.pendingReturns[highestBidder]
44   } catch {}
45   toPlace.sender --> highestBidder
46   toPlace.value --> highestBid
47 }
48 transformer withdraw(this : BlindAuction) {
49   this.pendingReturns[msg.sender] --> msg.sender.balance
50 }
51 transformer auctionEnd(this : BlindAuction) {
52   only when now >= this.revealEnd and not this.ended
53   true --> this.ended
54   highestBid --> beneficiary.balance
55 }

```

Figure 5: [TODO]

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