

# Flint for Safer Smart Contracts

Franklin Schrans<sup>2</sup>, Daniel Hails<sup>1</sup>, Alexander Harkness<sup>1</sup>, Sophia Drossopoulou<sup>1</sup>,  
and Susan Eisenbach<sup>1</sup>

<sup>1</sup> Imperial College London, London SW7 2AZ, UK

{susan, sd}@ic.ac.uk

<sup>2</sup> Franklin Schrans's contributed while a student at Imperial College.

fr@nklinschrans.com

**Abstract.** The Ethereum blockchain platform supports the execution of decentralised applications or smart contracts. These typically hold and transfer digital currency to other parties on the platform; however, they have been subject to numerous attacks due to the unintentional introduction of bugs. Over a billion dollars worth of currency has been stolen since its release in July 2015. As smart contracts cannot be updated after deployment, it is imperative that the programming language supports the development of robust contracts.

We propose Flint, a new statically-typed programming language specifically designed for writing robust smart contracts. Flint's features enforce the writing of safe and predictable code. To encourage good practices, we introduce *protection blocks*. Protection blocks restrict who can run code and when (using *typestate*) it can be executed. To prevent vulnerabilities relating to the unintentional loss of currency, Flint *Asset* traits provide safe atomic operations, ensuring the state of contracts is always consistent. Writes to state are restricted, simplifying reasoning about smart contracts.

**Keywords:** smart contracts · Flint programming language design

## 1 Introduction

The Ethereum Virtual Machine[45,7] (EVM) is an open network supporting decentralised execution of programs, known as *smart contracts*. The EVM is similar to a stateful web service, but instead of being executed by computers controlled by an organisation it is deployed to its nodes (or *miners*). Smart contracts are held in an append-only data structure a *blockchain* composed of *blocks*, allowing miners to maintain a consistent view of the network's state. Cryptographic schemes ensure old blocks cannot be modified. Miners select which transaction to process from their transaction pool.

Users can interact with a smart contract by calling the functions it exposes. Function calls are executed by miners, which maintain the state of each smart contract and are paid for processing transactions. Ethereum users and smart contracts can exchange a digital currency known as *Ether* whose smallest denomination is the *Wei* ( $10^{-18}$  Ether). Users also use Ether to purchase *gas*, required to pay for computational costs when executing transactions.

Smart contracts implement self-managed agreements, enforced autonomously. The source code of a smart contract is available, and cannot be changed after deployment. Individuals who interact with smart contracts trust the correct execution of the code rather than reprogrammable machines controlled by a single authority. Smart contracts have been used to implement auctions, votes[19], and sub-currencies[33] for crowdfunding purposes. Voters do not have to place their trust in the integrity of an electoral organisation when the votes are counted using a smart contract.

Not being able to update a smart contract’s code after deployment requires it to be bug free. Attackers have found vulnerabilities in smart contracts allowing the redirection of Ether funds to their personal Ethereum account. Attacks against THEDAO[8] and the Multi-sig Wallet smart contracts[37,36] have accumulated losses of over a billion dollars worth of Ether.

The primary programming language used to write smart contracts, *Solidity*[19], is expressive and introduces features designed for smart contract programming. However, Solidity supports a variety of unsafe patterns[4] which makes it difficult for analysis tools[32,11] and programmers to find all vulnerabilities. Solidity has few built-in security mechanisms and even worse, vulnerabilities are easily introduced because of simple programming mistakes, such as forgetting a modifier. Others are harder to notice, such as implicit integer overflows, or discarding the return value of sensitive functions.

For traditional problems, languages such as Java[34], Haskell[30], Swift[3], Rust[40], and Pony[9] leverage years of research in programming languages to prevent the writing of unsafe code. In contrast, multiple programming languages[19,16,43,22,18] for writing smart contracts, including Solidity, have attempted to mimic languages such as JavaScript[25] and Python[39], without providing additional safety mechanisms for Ethereum’s unique programming model.

Smart contracts introduce new challenges, which we address in our statically-typed programming language Flint<sup>3</sup>, specifically designed for writing smart contracts. By identifying challenges and learning from past vulnerabilities, Flint’s features facilitate the development of robust code, and make it more difficult and unnatural to write vulnerable contracts. We highlight the features that should aid in the development of robust code:

1. **Protection Blocks:** Smart contracts often carry out sensitive operations which need to be protected from unauthorised calls. A call can be unauthorised because the caller shouldn’t be allowed to make the call or because (using *typestate*[14]) the contract isn’t a valid state to be executed (e.g. until you join a club you cannot participate in its activities). Flint requires programmers to systematically think about which Ethereum users are allowed to call a smart contract’s functions, and what state the contract has to be in, before defining it.
2. **Assets:** Flint supports special operations for handling Assets such as Wei in smart contracts. Transfer operations are performed atomically, and ensure

---

<sup>3</sup> Flint was made open source on GitHub[27] in April 2018 under the MIT license.

that the state of a contract is always consistent. In particular, Assets in Flint cannot be accidentally created, duplicated, or destroyed, but they can be atomically split, merged, and transferred to other Asset variables. Using Asset types avoids a class of vulnerabilities in which smart contracts' internal state does not accurately represent their true Wei balance.

3. **Wei is an asset:** In Solidity, Wei values are represented as integers rather than a dedicated type, allowing accidental conversions between numbers and currency. This can lead to inconsistent states, in which the actual balance of the smart contract is incorrect.
4. **Static typing:** Given that contracts cannot be corrected, type errors need to be found before contracts are released.
5. **Modifiers:** Flint's code is by default private and immutable. A programmer has to explicitly override either of these defaults. It is a compiler error to declare something mutable that isn't changed by the contract.
6. **Safe Arithmetic:** Integer overflow causes an exception and contract execution to terminate. There are also cyclic versions of the operators, but a programmer would have to use these special operators explicitly.
7. **Loops are finite:** The only loop construct is a for-in loop which is used to iterate over arrays, dictionaries and ranges.
8. **Initialisers:** Contracts and structs must define public initialisers, and all state properties will be initialised during their execution.
9. **Limited Fallback Functions:** Fallback functions cannot change any state. Default fallback functions rollback the contract.

As recommended by the Ethereum Foundation, we implemented a compiler for Flint which produces EVM bytecode via Solidity's intermediate representation Yul[17,20]. To fit into the existing Ethereum ecosystem, we use the Solidity Application Binary Interface (ABI) and leverage Ethereum's existing cryptographic schemes to use Ethereum user addresses to protect from rogue callers. Our novel protection system enables static checks on internal calls and runtime checks on external calls.

To evaluate Flint, we translated existing smart contracts and showed the resulting code to be more concise. To assess safety, we ran analysis tools on the bytecode produced and show that a certain class of vulnerabilities cannot be reproduced in Flint. We also assessed the performance of our main safety features.

## 2 Solidity: Current State of Play

Solidity [19] is statically-typed and imperative. With syntax inspired by JavaScript, Solidity provides a rich set of constructs and it is this expressivity that is visible in many of the bugs. Avoiding the vulnerabilities that have been exposed by the flawed contracts is critical in the design of Flint.

A Solidity contract is similar to an object-oriented class, which can inherit functionality from other classes. Solidity provides integers, addresses, fixed-size

arrays, dynamic arrays, and dictionaries (`mapping`). It is also possible for programmers to define their own types (`struct`) and their own *interfaces*. A contract contains storage fields, event declarations, and function declarations.

*Function modifiers* such as `require` can be used to check preconditions before entering a function’s body. If they fail, execution of the contract stops, and the sender receives an exception. Modifiers may mutate the contract’s state.

Functions return a specified number of values. A function’s signature can contain attributes to specify how they are allowed to access the contract’s state, and their visibility. Functions declared without visibility modifiers are implicitly `public`.

Contracts can define an unnamed *fallback function*. When an account calls a function of a contract which has not been defined, the fallback function is called. Calls can be delegated in which case mutation of state in the target function call is performed in the *caller’s* storage. So programmers who mistype a function’s name may unintentionally end up updating state in the wrong storage space.

## 2.1 Attacks Against Solidity Contracts

The design of the Solidity language itself has contributed to it being vulnerable to attack.[44] *“Solidity was introducing security flaws into contracts that were not only missed by the community, but missed by the designers of the language themselves.”*[8] One problem is unintuitive semantics [12] of the `call` method: *“you cannot assume anything about the state of your contract after the external call is executed.”* We highlight problems with example vulnerable contracts[4]:

1. **Call Re-entrancy:** *TheDAO Attack*. The attack on TheDAO was possible because Solidity does not have a way to make transfer of Ether and internal bookkeeping atomic, and because function calls are synchronous – thus a function which calls another contract may be re-entered before terminating. In its `refund` function, TheDAO contract sends Ether to a client, and then does the corresponding internal bookkeeping. A malicious client re-enters `refund` as soon as it receives the Ether, and thus Ether is repeatedly sent, the bookkeeping is not performed, and the process is repeated until `refund` runs out of gas or the contract runs out of Ether.
2. **Visibility Modifiers:** *the First Parity Multi-sig Wallet Hack*. At the time of the attack, Solidity initialisers could be called anywhere any number of times. The confusing semantics of delegation and fallback functions means that external contracts can update state not intended by the contract developer. Parity accounts control a common wallet. An attacker exploited the wallet to steal over \$80 million [37]. The library code Parity provided was written as a contract and users creating their own wallet contract, could delegate all the functions to the library instance. There is an initialising function to set the owner of a wallet that should only be called in the constructor that sets up a new wallet. Unfortunately, due to the semantics of delegation and fallback functions, the caller can call an initialiser at any time and set themselves as the owner of the entire Parity contract.

3. **Contract as a Library:** *the Second Parity Multi-sig Wallet Hack*. At the time of the attack, Solidity libraries were just contracts so they could have updateable state. A second problem was that initialisers do not have to be called. The previous Parity Multi-sig contract was affected by another attack, which caused the loss of approximately \$260 million. The initialisation function now did have a modifier (`only_uninitialised`). The assumption from the developers was that their `WalletLibrary` would only be interacted with through delegate calls (mutating the caller's state rather than the library's state). However, `WalletLibrary`, which was just an ordinary contract, didn't actually call the initialisation function, so an attacker was able to call the initialiser, set the owner to itself and then terminate the contract. All of the other wallets delegating their calls to `WalletLibrary` were frozen: the instance of `WalletLibrary` they were delegating was destroyed. There were two problems: the first was that an initialiser did not have to be called at all, and the second was that a user was able to modify the state of a smart contract which was only meant to be used as a stateless library.
4. **Unchecked Calls:** *King of the Ether Throne*. Solidity does not require return values to be checked. This contract keeps track of a current king. An account needs to pay more than the king paid in order to dethrone him and when a king is dethroned, he gets sent his stake back. This will not happen if the contract runs out of gas and the boolean indicating whether the transaction was successful is not checked. When an out of gas exception occurs, the Ether is returned to the caller and as the king is not the caller he doesn't get his Ether back.
5. **Arithmetic Overflows:** *Proof of Weak Hands Coin*. Arithmetic operators have wrap-around semantics. This contract implements a currency. About \$476K was lost due to an arithmetic overflow following an addition.

The attacks can mostly be attributed to a mix of human error and unintuitive language semantics. Understanding the pitfalls that some Solidity programs have fallen into, was the starting point of the design of Flint. We now discuss how Flint makes the development of vulnerable contracts harder to write accidentally.

1. **Call Reentrancy:** *TheDAO Attack*. Flint uses an `@payable` function annotation, for currency transfer. `@payable` requires a Wei value rather than an integer. Wei is transferred atomically so there could not be a transfer before updating the contract's bookkeeping. Also there is limited re-entrancy, and our fallback functions cannot update state.
2. **Visibility Modifiers:** *the First Parity Multi-sig Wallet Hack*. Flint requires initialisers which have to initialise all state and which get called exactly once and that is before use. A caller could overwrite these values, if the contract developer made them visible, but the default is everything is private and immutable.
3. **Contract as a Library:** *the Second Parity Multi-sig Wallet Hack*. Libraries are stateless, Flint's default fallback functions just rollback, and Flint enforces the initialisation of contract state properties inside the `init` call which has to occur on the instantiation of contracts and structs.

4. **Unchecked Calls:** *King of the Ether Throne*. In Flint, the King of the Ether Throne vulnerability caused by discarding the result of `send` could not happen as it is a compile error to discard the result of a function call. There is also a possible denial of service attack[4] and the corresponding Flint program would only suffer from this problem, if the non re-entrancy of external calls were explicitly changed to allow re-entrancy.
5. **Arithmetic Overflows:** *Proof of Weak Hands Coin*. Flint’s default integers do not overflow. So a Flint programmer could cause an arithmetic overflow, but they have to do it explicitly by using the alternative integers operators.

The developers of Solidity apparently shared some of our concerns but have been proposing very different solutions to the problems. For example, having a modifier (`only_uninitialised`) although sufficient to prevent a constructor from being called twice, is not sufficient to get it called once, whereas Flint’s constructor is called exactly once and at the appropriate time. Solidity’s new inclusion of some SMT verification of arithmetic[1] should catch overflows, but Flint’s philosophy is to use safe arithmetic in the first place. We do not see how the Solidity developers are going to be able to alter their language to prevent the confusing semantics of fallbacks and delegation. Both languages have assertions. Solidity programmers need to insert them in their code in the places that Flint programmers will use safe arithmetic, protection blocks and Assets.

### 3 Flint by Example

We present Flint, influenced by Swift[3] syntax, for writing safe Ethereum smart contracts. Like in Solidity, a Flint smart contract’s state is represented by its fields, or *state properties*. Unlike in Solidity, state properties are declared in isolation from functions so that programmers can easily ensure that no unnecessary state properties are declared. Like in Solidity, they are stored in the smart contract’s persistent memory (*storage*), with high access costs.

Like in Solidity, a Flint contract’s behaviour is characterised by its functions. Unlike Solidity, they are declared within *protection blocks* rather than at the top level of the contract. This forces programmers to first think about what state the contract needs to be in and which parties should be able to make function calls before defining functions. Functions are by default non-mutating, but can explicitly mutate the contract’s state if declared as `mutating`. Functions are by default private, but those with a `public` modifier can be called by external Ethereum users. The standard library offers an `Asset trait`, which provides safe atomic operations to handle currency, ensuring the state of smart contracts is always consistent.

#### 3.1 Declaring Contracts

To introduce some features of Flint<sup>4</sup> we start the development of a `SimpleDAO` contract. When declaring the contract, we observe how Flint’s syntax requires programmers to write their smart contract in a specific sequence of steps.

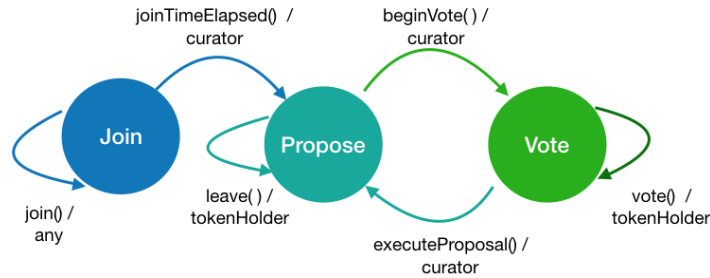


Fig. 1. DAO State Changes

- 1. Declaring the contract’s possible states.** The contract needs to enable users to join (`Join`), if they have joined to be able to propose transfers of `Wei` (`Propose`), and if a transfer has been proposed to vote (`Vote`). This *typestate* appears in the contract header. The `Address` type represents an Ethereum address (a user or another contract).

```

1 contract SimpleDAO (Join, Propose, Vote) {
2   var curator: Address // a very simple consensus mechanism
3   visible var proposal: Int = 0
4   var proposals: [Proposal] = [] // a list of all proposals to transfer Wei
5   var balances: [Address: Wei] = [:] // rmembers' Wei balances
6 }

```

- 2. Declaring the protection blocks.** Functions of a contract are declared within protection blocks, which restrict when the enclosed functions are allowed to be called. There are two elements to protection blocks: the caller protection and the optional typestate protection. A protection block declaration has to include the contract name (`SimpleDAO`) followed by `@(typestate)` (e.g., `Join`), followed by a `::` and admissible callers (e.g., `curator`). The first protection block for this contract is for setting up a new `SimpleDao` contract. Anyone (`any`) may do this and the caller’s address is bound to the caller local variable. This initialiser can only be called when the contract is created as all other contracts have a typestate parameter associated with them. The second protection block is for joining an existing contract. The third is for the curator to explicitly change the state from `Join` to `Propose`,

<sup>4</sup> For the full description of Flint see [41].

closing off the SimpleDAO from accepting new members. The final two protection blocks are for processing proposals and votes respectively. The bodies of the protection blocks are completed later.

```

7 SimpleDAO @(any) :: caller <- (any) { ... }
8 SimpleDAO @(Join) :: caller <- (any) { ... }
9 SimpleDAO @(Join) :: (curator) { ...}
10 SimpleDAO @(Propose) :: caller <- (tokenHolder) { ... }
11 SimpleDAO @(Propose) :: caller <- (curator) { ... }
12 SimpleDAO @(Vote) :: caller <- (tokenHolder) { ... }

```

**Declaring the global structs.** Struct values can be declared as state properties or local variables, and are initialised through their initialiser. When stored as a state property, the struct’s data resides in EVM storage. When stored as a local variable, it resides in EVM memory, and a pointer is allocated on the EVM stack. A struct’s functions are not explicitly protected by being in protection blocks, rather they will be protected by the contract functions that call them. Our contract only needs a `Proposal` struct:

```

13 struct Proposal {
14     var proposer: Address
15     var payout: Int
16     var recipient: Address
17     var yea: Int = 0
18     var nay: Int = 0
19     var finished: Bool = false
20     var success: Bool = false
21     var voted: [Address: Bool] = [:]
22 }
23 mutating init(proposer: Address, payout: Int, recipient: Address) { self.
24     proposer = proposer
25     self.payout = payout
26     self.recipient = recipient
27 }

```

**3. Declaring the functions.** Finally, functions are declared within the protection blocks. For example, the third protection block where the curator stops taking new members is only one function. The complete code appears in Appendix A.

```

1 SimpleDAO @(Join) :: (curator) {
2     public mutating func joinTimeElapsed() {
3         become Propose
4     }
5 }

```

### 3.2 Additional Language Features

**Initialisation** Each smart contract and struct must define exactly one public initialiser. All of the state properties must be initialised before the initialiser



returns. State properties can be declared with a default value and constants must be assigned exactly once.

**Type System** Flint is a statically-typed language, with no support for sub-typing. Flint supports basic types and dynamic types (Figure 2). Dynamic types can be passed by value or by reference (&).

Type	Description
Address	160-bit Ethereum address
Int	256-bit unsigned integer
Bool	Boolean value
String	String value
Void	Void value
Fixed-size Array	Fixed-size memory block containing elements of the same type. $T[n]$ refers to an array of size $n$ , of element type $T$ .
Array	Dynamically-sized array. $[T]$ refers to an array of element type $T$ .
Dictionary	Dynamically-size mappings from one key type to a value type. $[K: V]$ is a dictionary of key type $K$ and value type $V$ .
Structs	Struct values, including <code>Wei</code> , are considered to be of dynamic type.

**Fig. 2.** Flint Types

Flint has traits which are based on Rust[40] traits. There are both contract and struct traits and they describe the partial behaviour of the contracts and structs which conform to them. Contracts and structs can conform to multiple traits as long as there is at most one function body for any given function. An example struct trait with a conforming struct is given below. A contract trait would be similar with the keyword `contract` replacing `struct`.

```

1 struct trait Animal {
2     // Must have an empty and named initialiser
3     public init()
4     public init(name: String)
5     func isNamed() -> Bool
6     public func name() -> String
7     public func noise() -> String
8     public func speak() -> String {
9         if isNamed() {return name()} else {return noise()}
10    }
11 }
12
13 struct Person: Animal {
14     let name: String
15     public init() self.name = "John Doe"
16     public init(name: String) {self.name = name}
17     func isNamed() -> Bool {return true}
18     public func name() -> String {return self.name}

```

```

19 public func noise() -> String {return "Huh?"}
20 // Person can also have functions in addition to Animal
21 public func greet() -> String {return "Hi"}
22 }

```

Function	Description
send(address: Address, value: inout Wei)	Sends value Wei to the Ethereum address address, and clears the contents of value.
fatalError()	Terminates the transactions with an exception, and revert any state changes.
assert(condition: Bool)	Ensures condition holds, cause a fatalError().

**Fig. 3.** Flint Global Functions

**The Standard Library** We also define three global functions, shown in Figure 3. Global functions are defined in the special `Flint$Global` struct in `stdlib/Global.flint` and are imported globally by the compiler. There is an `Asset` trait defined in the standard library (see Appendix D) as well as `Wei` which conforms to it. Compiler checks ensure that contracts use `Wei` from the Standard Library.

#### Asset Traits

**No Unprivileged Creation** It is not possible to create an asset of non-zero quantity without transferring it from another asset.

**No Unprivileged Destruction** It is not possible to decrease the quantity of an asset without transferring it to another asset.

**Safe Internal Transfers** Transferring a quantity of an asset from one variable to another within the same smart contract does not change the smart contract's total quantity of the asset.

**Safe External Transfers** Transferring a quantity  $q$  of an asset  $A$  from a smart contract  $S$  to an external Ethereum address decreases  $S$ 's representation of the total quantity of  $A$  by  $q$ . Sending a quantity  $q'$  of an asset  $A$  to  $S$  increases  $S$ 's representation of the total quantity of  $A$  by  $q'$ .

**Safe Arithmetic Operators** The  $+$ ,  $-$ , and  $*$  operators throw an exception and abort execution of the smart contract when an overflow occurs. The  $/$  operator implements integer division. For the rare cases where the intended behaviour is cyclic, Flint also supports wrap-around operators,  $\&+$ ,  $\&-$ , and  $\&*$ .

**@payable Annotation** Similar to what Solidity does, when a user creates a transaction to call a function, Ether can be sent by using `@payable`. A single parameter marked `implicit` of type `Wei` must be declared; `implicit` parameters expose information from the Ethereum transaction to the developer of the smart contract, without using globally accessible variables, such as `msg.value` in Solidity.

```

1 @payable
2 public func receiveMoney(implicit value: Wei) {
3     doSomething(value)
4 }

```

**Events** JavaScript applications can listen to events emitted by an Ethereum smart contract. Flint provides the same functionality with slightly different syntax from that provided by Solidity.

```

1 contract Bank {
2     var balances: [Address: Int]
3     let didCompleteTransfer: Event<Address, Address, Int> // (origin, destination,
4         amount)
5 }
6 Bank :: caller <- (any) {
7     mutating func transfer(destination: Address, amount: Int) {
8         // Omitting the code which performs the transfer.
9         emit didCompleteTransfer(caller, destination, amount)
10    }
11 }

```

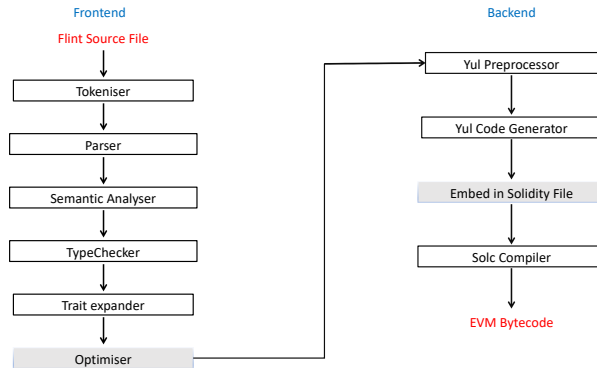
## 4 Implementation

We implemented `flintc`, a compiler for Flint which runs on Linux and macOS. The compiler’s source code (about 25,000 lines of Swift[3] code) is open source and available on GitHub[27].

The compiler stages are illustrated in Figure 4. Programs are analysed, compiled to the Yul intermediate representation, and finally to EVM bytecode. By embedding Yul in a Solidity file, tools built for Solidity work with Flint. We compile Yul code using the Solc[19] compiler. The tokeniser and parser are hand written as this has enabled us to provide better error messages.

The *Parser* has an additional step at the end which populates an environment. The environment contains information about the discovered types in the compilation step. Contract/Structure types contain information about the conforming traits, functions and fields. Contracts also contain additional information about any declared tpestates. This provides sufficient information to AST Passes for the checking of non-trivial program properties.

Our code architecture decouples AST traversal and node processing. The traditional visitor pattern[35] leverages dynamic method dispatch mechanisms to separate node processing logic from tree traversal logic. However, visited nodes invoke the visitor on their children nodes manually. Our nodes do not have references to visitors, rather we have an architecture which uses a single *AST Visitor*, and multiple *AST Passes*. Each AST Pass implements a process function for each type of AST node. The AST Visitor updates the tree using the nodes returned by the AST Pass, collects diagnostics, and propagates contextual information.



**Fig. 4.** Compiler Stages

The AST passes are Semantic Analyser, Type Checker, TraitResolver, and Yul Preprocessor.

The Semantic Analysis AST Pass verifies the correctness of the input program. This performs the static checks for caller and tpestate protection, traits, mutating functions, verifying whether there are uses of undefined variables, etc. Appendix E contains some examples of errors and warning diagnostics that are produced during this pass.

As there is no subtyping or polymorphism, the Type Checking pass is straightforward. Appendix E also contains examples of type error messages.

#### 4.1 Code Generation and Runtime

Before the code generation phase, like in most object oriented language compilers, we apply a preprocessing step which mangles function names (needed for disambiguating for overloading and for functions coming from different contracts or structs). For each parameter which can be passed by value or by reference an `isMem` parameter is added. At this stage traits are embedded in conforming structures and contracts.

We implement a code generating function per AST Node, which takes an AST node as a parameter, and returns its Yul representation. The `YulStruct` function generates code for a Flint struct. Similarly, we implement `YulFunction`, `YulAssignment`, `YulExpression`, etc.

#### 4.2 Functions and Application Binary Interface

Flint’s Application Binary Interface (ABI) specifies at the bytecode level how Ethereum users and other smart contracts can call the public functions of a Flint smart contract. Flint follows Solidity’s ABI, therefore Flint and Solidity contracts can interoperate. Users can call a smart contract’s function on Ethereum

by creating a transaction, and specifying which function to call with which arguments in the transaction payload. Transaction payloads are raw bytes, thus the data needs to be encoded. Specifying which function to call is done via encoding the function’s signature. Function arguments are appended to the function signature hash as a hexadecimal value. Calling *f* with arguments `100` and `true` would be encoded as `0x64` and `1`, padded with zeros to fill a 256-bit value. An Ethereum user or another smart contract can thus call *f* with arguments `100` and `true` by entering the following value in the transaction payload (without newline characters):

```
0x13d1aa2e
0000000000000000000000000000000000000000000000000000000000000064
0000000000000000000000000000000000000000000000000000000000000001
```

A struct value passed as an `inout` (reference) argument to a function is an implicit reference to either an EVM memory location or an EVM storage location. When accessing the memory location, the runtime needs to know whether it should read the value from memory or from storage. To support this, when a struct is passed by reference to a function, an extra boolean argument, specifying the location of the reference, is inserted in the argument list of the function call. The storage and memory of a Flint smart contract are organised similarly. The runtime functions `load` and `store` work for both variants. A contract’s state properties are stored in EVM storage sequentially, except for values in dynamic arrays and dictionaries. Local variables are stored in memory, and are allocated dynamically. The `allocateMemory` runtime function reserves a number of bytes in memory, and returns the start pointer of the block. The first 64 bytes of memory (8 words) are reserved as scratch space and can be used to perform temporary computation, or load values into memory to compute `sha3` hashes or emit Ethereum events. Memory location `0x40` (64th byte) holds a pointer to the next available memory location (initially `0x60`).

State properties of smart contracts are stored contiguously in storage, starting at location 0. Each state property occupies one word (32 bytes) in the case of basic types, or multiple words when storing structs or fixed-sized arrays. Structs can also be stored in memory. Dynamically-sized types, such as arrays and dictionaries, are not necessarily allocated contiguously. Storage accesses yield the same gas cost regardless of which location is accessed.

The Flint runtime contains 20 runtime functions to perform low-level operations. A runtime function *f* can be called from the Flint standard library using `flint$f`, but not from user-defined code.

Protection checks (both callers and `typestate`) are performed at compile-time for internal (same contract) function calls (except `try` code) while the protection of foreign contracts calling into Flint contracts, (and `try` code) are checked at runtime. To enable the verification, runtime checks are inserted immediately before running the function’s body. If the caller’s address is not in the set of caller protections required to call the function, an exception is thrown and the call is aborted (the `REVERT` opcode is executed).

Typestate protection checks are performed similarly to caller protection checks and are done at compile-time for internal functions and at runtime for foreign contracts calling into Flint contracts. At compile time an internal typestate enumeration is generated denoting all of the user defined states and the internal states. An internal contract state property is defined by the compiler with that type. When a runtime check needs to be performed the compiler will generate a comparison against the set of valid typestates, and if it is not valid, an exception is thrown and the call is aborted (the `REVERT` opcode is executed).

Typestate can only be changed in user-defined code through `become StateIdentifier` statements. The compiler will generate code to update the contract state property to the appropriate enumeration value.

### 4.3 Intermediate Representation Organisation

To generate the IR code it is done in the following order:

1. *Contract function definitions.* Code is generated for user-defined contract functions, one IR function for each Flint contract function. The Yul code does not include explicit declarations of state properties, as accesses to storage properties in functions are represented as static offsets into memory.
2. *Struct function definitions.* The function code for each user-defined and standard library struct is included next.
3. *Runtime functions.* Finally, we include the definition of any runtime functions.

## 5 Evaluation

In this section we compare Flint to Solidity. We were able to use the same analysers Oyente[32] and Mythril[11] by embedding Flint's IR code in a Solidity file. The Solidity and Flint gas costs have been retrieved from executing the calls on our simulated Ethereum network.

The most important features of Flint for writing robust code are protection blocks (with callers and typestate), `Assets`, and safe arithmetic so these are the features we examine in some detail. We provide small example programs for each construct in both languages so that we can compare code styles, potential for bugs as discovered by Solidity dynamic analysis tools, and gas usage. Solidity has run-time type checking which should add a performance overhead, whereas Flint currently has no optimisation and there is a performance overhead caused by embedding our Yul code in a Solidity file.

### 5.1 Caller Protections

To compare caller protections we define simple functions some of which can be called by any user, some by `owner`, and some by any customer in the `customers` array. In Solidity, we implement two modifiers, `onlyOwner` and `anyCustomer`, which check whether the caller is `owner` or is in the `customers` array, respectively.

SOLIDITY

```

1 modifier onlyOwner {
2     require(msg.sender == owner);
3     _;
4 }
5 modifier anyCustomer {
6     uint numCustomers = customers.length;
7     bool found = false;
8     for (uint i = 0; i < numCustomers; i++) {
9         if (customers[i] == msg.sender) { found = true; }
10    }
11    require(found);
12    _;
13 }
14 contract Callers {
15     address owner;
16     address[] customers;
17     uint256 counter;
18     modifier anyOwner {...}
19     modifier anyCustomer {...}
20     function anyUser() public constant returns(uint256) {...}
21     function ownerCall(uint counter) public constant onlyOwner returns(uint256)
22         {...}
23     function customerCall(uint counter) public constant anyCustomer returns(
24         uint256) {...}
25     function ownerInternalCalls() public onlyOwner {...}
26     function customerInternalCalls() public anyCustomer {...}
27 }

```

The organisation of the smart contracts presents notable differences. In the Solidity code (above), the state and the functions are all defined at the top level of the contract. Solidity does not enforce the inclusion of the user-defined modifiers we have specified in some of the function signatures. In the more concise Flint code (below) the contract itself and the protection blocks are at the top level.

FLINT

```

1 contract Callers {
2     var owner: Address
3     var customers: [Address]
4     var numCustomers: Int
5     var counter: Int
6 }
7 Callers :: owner <- (any) {
8     mutating public func addCustomer(customer: Address) {...}
9     public func anyUser() -> Int {...}
10 }
11 Callers :: (owner) {
12     public func ownerCall(counter: Int) -> Int {...}
13     public mutating func ownerInternalCalls() {...}
14 }
15 Callers :: (customers) {

```

```

16 public func customerCall(counter: Int) -> Int {...}
17 public mutating func customerInternalCalls() {...}
18 }

```

In Figure 5 we compare the gas costs of executing each function in the Solidity and Flint contracts. Flint is significantly faster when functions perform internal calls to functions which require the same caller protection. This is expected, as the caller protection check is only executed once.

The gas costs are similar for simple examples using a caller protection backed by a single address. When calling a function which calls multiple functions, requiring the same caller protection, Flint is up to 12 times faster than Solidity.

For caller protections backed by an array, the results aren't as good. Flint code is cheaper to run when the array is relatively small, but becomes more expensive when it is large. In the example which performs a large number of internal calls, the Flint code is up to two times faster as Flint performs a single runtime check, whereas Solidity performs one per function call.

Operation	Solidity	Flint	Difference (Solidity vs Flint)	Possible Explanation
Deploying	438121	514268	S: -14.8%	Flint does not optimise code.
Any call	268	283	S: -5% V: -32%	Determining which function was called is slightly faster in Flint.
Owner call	633	836	S: -24% V: -22%	
Owner many internal calls	32662	28673	S: +14% V: +496%	Only one dynamic caller protection check is performed in Flint.
Customer call (5 customers)	3791	1707	S: +122% V: +158%	Flint's array iteration algorithm is better suited for small arrays.
Customer call (20 customers)	13136	18047	S: -27% V: -37%	Solidity's array iteration algorithm suits larger arrays.
Customer call (50 customers)	31434	43847	S: -28% V: -43%	Same as above.
Customer many calls (5 customers)	168804	54426	S: +210% V: +1068%	Only one dynamic caller protection check is performed in Flint.
Customer many calls (20 customers)	510129	67326	S: +658% V: +2327%	Same as above.
Customer many calls (50 customers)	1192779	93126	S: +1181% V: +3792%	Same as above.

**Fig. 5.** Gas Costs for Callers.

We compare the result of the analyses performed by the dynamic Solidity analysis tools Oyente and Mythril. Both analysis tools detect if the customers



array has the potential to become too large. While in Solidity the array will silently overflow, in Flint it would throw an exception.

## 5.2 Typestate Protection

To examine typestate we define simple functions which can be called in only one of two states, as well as simple functions to transition between the two states. In Solidity, we implement a modifier, `atStage` which checks that the contract is in the correct State.

SOLIDITY

```

1 modifier atStage(Stages _stage) {
2     require(
3         stage == _stage,
4         "Function cannot be called at this time."
5     );
6     _;
7 }
8 contract StateMachine {
9     enum Stages {
10         Stage1,
11         Stage2
12     }
13     Stages public stage = Stages.Stage1;
14     modifier atStage(Stages _stage) { ... }
15     function nextStage() public { ... }
16     function Stage1Function() public atStage(Stages.Stage1) { ... }
17     function Stage1ComplexFunction() public atStage(Stages.Stage1) { ... }
18     function Stage2Function() public atStage(Stages.Stage2) { ... }
19 }

```

FLINT

```

1 contract States (State1, State2) { ... }
2 States @(any) :: (any) {
3     public init() {
4         become State1;
5     }
6 }
7 States @(State1) :: (any) {
8     public mutating func State2Transition() { ... }
9     public func State1Function() { ... }
10    public func State1ComplexFunction() { ... }
11 }
12 States @(State2) :: (any) {
13    public mutating func State1Transition() { ... }
14    public func State2Function() { ... }
15 }

```

We compare the gas costs of executing each function in the Solidity and Flint contracts in Figure 6. For simple external calls requiring a state check, the gas

consumption for both Flint and Solidity is low, although Flint has a slightly higher consumption, probably due to function selection not being optimised. State transition takes less gas in Flint as only a single memory store has to take place while the compiled Solidity code makes multiple changes.

For operations involving many internal calls, Flint has a much lower gas consumption, with the Flint code consuming only about half as much as the comparable Solidity code. This lower overhead is because Flint only has to perform a single runtime check at the start of the transaction rather than many checks for each function as the code progresses.

Flint’s source code is more concise, whereas the compiled code is slightly larger and deployment therefore takes more gas.

Operation	Solidity	Flint	Difference (Solidity vs Flint)	Possible Explanation
Deploying	239350	282031	S: -15.1%	Flint does not optimise code.
External call	650	970	S: -33.0%	Flint function selector less optimised
Many internal calls (50)	18434	8729	S: +111%	Only one dynamic caller protection check is performed in Flint.
State transition (average)	20855	6696	S: +211%	Fewer state changes performed in Flint

**Fig. 6.** Gas Costs for Typestates.

### 5.3 Asset Types and Safe Arithmetic Operations

In this section we are interested in the security of Solidity and Flint contracts when handling Wei, and measure whether Flint **Assets** introduce performance penalties. We define the **Bank** smart contract where customers can send Wei to the contract, and **Bank** keeps track of how much each customer has sent. Customers can then withdraw their Wei, or transfer it to another **Bank** account. The complete Flint code for **Bank** is in Appendix B.

The `deposit` function of both smart contracts are similar, and record received Wei to state. Flint uses the Wei type, whereas as there is no built-in Wei type in Solidity, currency is held as an integer. It is easy to accidentally add currency to an account, or forget to do so. Using Flint’s Wei **Assets** allows safer and more concise code for transferring funds.

SOLIDITY

```

1 function deposit() anyCustomer public payable {
2     balances[msg.sender] += msg.value;
3 }

```

FLINT

```

1 @payable
2 public mutating func deposit(implicit value: Wei) {
3     balances[account].transfer(&value)
4 }

```

The comparison between `transfer` functions is similar. An additional advantage of the Flint `transfer` is the update of state when the currency is moved is atomic.

SOLIDITY

```

1 function transfer(uint amount, address destination) anyCustomer public {
2     require(balances[msg.sender] >= amount);
3     balances[destination] += amount;
4     balances[msg.sender] -= amount;
5 }

```

FLINT

```

1 public mutating func transfer(amount: Int, destination: Address) {
2     balances[destination].transfer(&balances[account], amount)
3 }

```

The `withdraw` function is one line shorter in Flint as we do not need to check whether the account holder has enough funds to perform an operation; an exception is thrown if the result of an arithmetic operation overflows. There are cleaner ways to say that a `withdraw` failed, but at least it is safe. However, if a Solidity programmer forgot and there wasn't enough in the account to make the withdrawal there would be a silent overflow and the value of the account's balance would be wrong.

SOLIDITY

```

1 function withdraw(uint amount) anyCustomer public {
2     require(balances[msg.sender] >= amount);
3     balances[msg.sender] -= amount;
4     msg.sender.transfer(amount);
5 }

```

FLINT

```

1 public mutating func withdraw(amount: Int) {
2     // Transfer some Wei from balances[account] into a local variable.
3     let w: Wei = Wei(&balances[account], amount)
4     // Send the amount back to the Ethereum user.
5     send(account, &w)
6 }

```

Figure 7 shows that the Flint version of the smart contract is marginally more expensive to run in terms of gas costs. However, the Oyente and Mythril analysers find 4 potential integer overflows on lines 30 (the array can become too large), and lines 34, 43, and 48 (the integer value in the `balances` mapping can become too large). They do not find any potential integer overflows in the Flint code.

Operation	Solidity	Flint	Difference	Possible Explanation
Deploying	422589	415901	+1.6%	Solidity and Flint produce similarly sized binaries.
Register	40741	61528	-34%	Solidity is more efficient at adding elements to an array.
Deposit 10 Wei	21460	24002	-11%	This is because of the overhead of Flint’s safe Asset operations, which prevent overflows and state inconsistencies.
Transfer 80 Wei	27200	30685	-11%	Same as above.
Withdraw 5 Wei	14301	17245	-17%	Same as above.
Mint 100 Wei	23098	20867	+10%	Similar results.

Fig. 7. Gas Costs for Bank

#### 5.4 The Solidity Attacks

In section 2.1 we described five attacks on four contracts. In section 3, we discussed how a Flint programmer would be unlikely to create the THEDAO’s vulnerability. When implementing a Multi-sig wallet, Flint’s initialisation can’t be omitted and fallback functions cannot update state. Flint libraries are stateless but a programmer doesn’t have to use them. When implementing a King of Ether contract, the Flint compiler would reject code that didn’t access the result of a function. In the Proof of Weak Hands Coin contract wrap-around semantics of Solidity integers used to hold the currency, caused an overflow. Its vulnerabilities could have been prevented using Flint’s `Assets`, in a similar way to our bank example in section 5.3. The same errors could be in a Flint contract by not using an `Asset` for the new `coin` and using our non-default wrap around integers `{balanceOf[caller] = balanceOf[caller] &- amount}`. At this stage in Flint’s development, only `Wei` is used with `@payable`. The plan is to extend `@payable` to work with any currency.

As the vulnerabilities in these contracts were the starting point for the design of Flint it isn’t surprising that the Flint code for them looks more robust. The Flint and Solidity code for the four (simplified) contracts is available at [28].

## 6 Related Work

**Languages** For traditional computer architectures, languages such as Java[34], Rust[40], and Pony[9] have been designed to prevent writing unsafe code. For instance, Java prevents direct access to memory, Rust uses *ownership types* to efficiently free memory, and Pony uses *reference capabilities* to prevent data races in concurrent programs. In contrast, even though the Ethereum platform requires smart contract programmers to ensure the correct behaviour of their program before deployment, Solidity lacks even a strong static type system to catch errors. Solidity provides both optional modifiers and assertions which programmers can use to decorate their contracts.

The Ethereum Foundation has created several other programming languages for writing smart contracts. Lisp Like Language[16] (LLL) was abandoned in favour of higher level languages. Serpent[22] is a high-level programming language with a syntax similar to Python’s that was deprecated due to numerous security issues, see [46]. Solidity, was an attempt to solve the issues these programming languages presented. Since Solidity, probably due to the vulnerabilities that have occurred, newer programming languages have been developed:

Vyper[18] inspired by Python, aims at providing developers with better security and more intuitive semantics than Solidity. Like Flint, it doesn’t have contract inheritance or infinite loops. However, its dynamically type system seems inappropriate for a language for robust contract development. Like in Solidity, assertions are provided to prevent vulnerabilities. Flint, too has assertions, but we don’t place as great an importance on the for vulnerability prevention as programmers can easily forget to include them.

Like Flint with its protection blocks, the Bamboo[29] programming language allows reasoning about smart contracts as state machines. Developers define which functions can be called in each state, and the language provides constructs to specify changes of state explicitly. Bamboo does not present any additional features geared towards the safety of programs.

There are several large organisations developing the Linux foundation’s Hyperledger Fabric[24] framework which can run on the EVM. Contracts in this framework can be written in a variety of languages including Javascript and Go. Currently the focus seems to be more focussed on building networks and applications.

There are substantial design activities for creating new languages for Smart Contracts that do not necessarily target the Ethereum platform. These designs all have correctness as part of their design goals. Closest to Flint is Obsidian[10], which includes typestate and linear types for resources. We haven’t gone to full linear types for assets because we believe they would be too restrictive. AxLang[31] is a Scala DSL that will compile to the JVM before being targeted at the EVM. The hope is that Scala verification tools will be useful on AxLang programs. The development of Plutus[38] is an effort to produce an eager Haskell-like language for a range of blockchains including Ethereum. Another functional language in the design stage, Formality[26], will target Ethereum’s web assembly language eWASM[23]. It isn’t obvious what eWASM will add to the safety of the compiler.

**Protections** Our protection blocks define both typestate[14,6] and caller protections. There have been many other techniques that protected code from being called by unwanted callers. Solidity modifiers allow checking for *any* type of assertion before the body of a function is entered. However, Solidity programmers are not required to use modifiers. As we believe protecting privileged functions in smart contracts is a basic requirement, Flint requires these to be coded before

writing functions,<sup>5</sup> Our implementation is also more efficient for internal calls, as shown in section 5.1. Flint users can use the `assert` function to perform other types of checks at runtime.

Ideas similar to our caller protections have arisen several times in the past. In the original definition of a capabilities by Jack Dennis et al.[13] they regard a capability as an unforgeable token (a number) which when possessed by a user, allows access to a resource. In Flint, a caller protection is linked with an Ethereum address, which can be regarded as an unforgeable token. An individual has the authority to call a function if it possesses the appropriate private key, and transferring authority is done by simply sharing the private key. In Pony[9], reference capabilities (similar to Flint’s protections) are associated with object references and are part of the object’s type. Flint’s caller protections are not encoded in the functions’ type. They are also similar to roles in role-oriented programming[15]. The underlying idea of role-oriented programming is to capture the human idea of roles and their interactions when writing code. Operating systems may use ACLs (access control lists)[2] to specify which users or system processes are granted access to which operations on objects.

**Analysis tools** In addition to designing the right language there is work aimed at finding vulnerabilities, focussing on early stages in the development cycle. Oyente[32] and Mythril[11] are both dynamic analysis tools. The Oyente symbolic execution tool analyses EVM bytecode. The authors of the tool claim they have found that 50% of smart contracts on Ethereum’s network has at least one vulnerability. Oyente finds issues such as timestamp dependencies, mishandled exceptions, and detects reentrancy calls. Mythril uses concolic analysis to determine execution paths. Mythril tries to find a variety of vulnerabilities, such as timestamp dependencies, integer overflows, and reentrancy issues. One of the concerns with both Oyente and Mythril is that they are not closely tied into contract development so vulnerabilities that they could catch may not be caught because the tool is not used.

The online Remix[21] IDE for Solidity has a built-in code analyser to find bug, such as reentrancy bugs and incorrect usage of low-level calls. In our testing, when running on the examples given in 2.1, the Remix Analyser warned when low-level calls’ return value was not checked, but was not able to find any reentrancy call issues that could be found by the dynamic analysis tools.

Converting to F\*[5] involves translating Solidity code to F\*, decompiling EVM bytecode to F\*, then checking equivalence between the two translations. Scilla[42] is a continuous passing style-based intermediate representation language for smart contracts that converts Scilla code to the Coq theorem prover where properties of the contract can be proven.

An SMT module has been added to the Solidity compiler[1]. Its current capabilities include catching infinite loops, arithmetic overflows, and re-entrancy,

---

<sup>5</sup> A programmer could decide, however, to write all functions in an any block with no `typestate`.

problems that by construction cannot exist in Flint code. The plans are to extend the subset of Solidity that it deals with and the problems it looks for.

## 7 Conclusions and Future Work

The goal of Flint is to make it easy to write smart contracts which are safe by construction. Although our current compiler targets the EVM, the language design was not much influenced by the choice of backend and could be retargeted. Flint needs to contain the constructs that programmers want in order to write easy to read smart contracts and no more. We haven't had difficulty translating existing smart contracts on the web into Flint. Omitting constructs that have been implicated many times such as sophisticated fallback functions, infinite loops, default integers with wrap-around semantics, functions that are public and mutable by default, will prevent previous errors re-appearing in new contracts.

We have provided many features such as protection blocks, restricting access with `typestate` and `callers`, non-wraparound integers, `Wei` implemented as an asset, and functions private and immutable by default. Our protection blocks shift the design pattern for developing smart contracts and we believe that should be a game changer. Flint programmers will have to think about who and when each piece of code can be accessed before starting to write any individual functions. Adding who can execute code after writing it by using modifiers is likely to be far more error prone than defining the gateway code first. Vyper has omitted Solidity's `new(ish)` modifiers because the designers are concerned about how error prone they are.

Our language design is certainly not frozen. `Wei` is checked by the compiler, but we need to ensure that all assets are treated as carefully as `Wei`. We also would like to be able to deal with collections of assets elegantly. We also have not investigated the problems caused by aliasing. Another area of interest is interacting with non-Flint contracts as we need to be confident that bad Solidity contracts do not pollute Flint contracts. Re-entrancy can be prevented by limiting the number of times (using `typestate`) a foreign and a Flint contract are allowed to interact. Our performance figures are in line with those of Solidity, and this is without an optimisation pass in our compiler. We do have plans to optimise, but only after the compiler provides the full functionality. We are currently working on a toolchain to provide the Flint programmer the toolset software engineers rely on.

Providing programmers a language with fewer ways they can make mistakes, is a first step towards ensuring contracts will be correct. But contracts have to implement the intentions of the people who request them and programming languages do not always encode intentions. Intentions need to be captured in specifications and existing specification techniques do not capture the long-term, open-world nature of smart contracts.

**Acknowledgements** We would like acknowledge Aurel Bily, Catalin Cracium, Calin Farcas, Yicheng Luo, Constantin Mueller, and Niklas Vangerow for their

work on Flint, both the language and the toolchain. We would like to thank Nobuko Yoshida and Alastair Donaldson for supporting some of this work. It has been partially supported by grant EPSRC EP/K011715/1 and a grant from the Ethereum Foundation.

## References

1. Alt, L., Reitwiessner, C.: Smt-based verification of solidity smart contracts. In: Proceedings, Part IV. vol. 11247, pp. 376–388. Springer Verlag, Limassol, Cyprus (11 2018)
2. Ancilotti, P., Boari, M., Lijtmaer, N.: Language features for access control. *IEEE Trans. Software Eng.* 9(1), 16–25 (1983), <https://doi.org/10.1109/TSE.1983.236166>
3. Apple: The Swift programming language. <https://swift.org>
4. Atzei, N., Bartoletti, M., Cimoli, T.: A Survey of Attacks on Ethereum Smart Contracts (SoK). In: International Conference on Principles of Security and Trust. pp. 164–186 (2017)
5. Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., Rastogi, A., Sibut-Pinote, T., Swamy, N., Zanella-Beguelin, S.: Formal verification of smart contracts. In: Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security-PLAS16. pp. 91–96 (2016)
6. Bierhoff, K., Aldrich, J.: Lightweight object specification with typestates. In: Proceedings of the 10th European Software Engineering Conference held jointly with 13th ACM SIGSOFT International Symposium on Foundations of Software Engineering, 2005, Lisbon, Portugal, September 5-9, 2005. pp. 217–226 (2005), <http://doi.acm.org/10.1145/1081706.1081741>
7. Buterin, V.: Ethereum: A next-generation smart contract and decentralised application platform. <https://github.com/ethereum/wiki/wiki/White-Paper> (2014)
8. CCN: Ethereum’s Solidity Flaw Exploited in DAO Attack Says Cornell Researcher. <https://www.ccn.com/ethereum-solidity-flaw-dao/>
9. Clebsch, S., Drossopoulou, S., Blessing, S., McNeil, A.: Deny capabilities for safe, fast actors. In: Proceedings of the 5th International Workshop on Programming Based on Actors, Agents, and Decentralized Control. pp. 1–12. ACM (2015)
10. Coblenz, M., Aldrich, J.: Obsidian: Language Development. <https://mcoblenz.github.io/Obsidian/> (2018)
11. ConsenSys: Mythril — Security analysis tool for Ethereum smart contracts. <https://github.com/ConsenSys/mythril/>
12. Daian, P.: Chasing the DAO Attacker’s Wake. <https://pdaian.com/blog/chasing-the-dao-attackers-wake/>
13. Dennis, J.B., Van Horn, E.C.: Programming semantics for multiprogrammed computations. *Communications of the ACM* 9(3), 143–155 (1966)
14. Drossopoulou, S., Damiani, F., Dezani-Ciancaglini, M., Giannini, P.: More dynamic object reclassification: Fickle&par;. *ACM Trans. Program. Lang. Syst.* 24(2), 153–191 (Mar 2002), <http://doi.acm.org/10.1145/514952.514955>
15. Edelweiss, N., Palazzo M. de Oliveira, J., de Castilho, J.M.V., Peressi, E., Montanari, A., Pernici, B.: T-ORM: temporal aspects in objects and roles. In: Halpin, T.A., Meersman, R. (eds.) Proceedings of the First International Conference on Object-Role Modelling, ORM-1, Magnetic Island, Australia, 4-6 July 1994. pp. 18–27 (1994)



16. Edgington, B.: LLL Programming Language. <http://lll-docs.readthedocs.io/en/latest/> (2017)
17. Ethereum: Joyfully Universal Language for (Inline) Assembly. <http://solidity.readthedocs.io/en/develop/julia.html>
18. Ethereum: The Vyper programming language. <https://github.com/ethereum/vyper>
19. Ethereum: Solidity Documentation. <http://solidity.readthedocs.io/en/latest/> (2014)
20. Ethereum: Yul. <https://solidity.readthedocs.io/en/latest/yul.html> (2016-2018)
21. Ethereum: Remix IDE for Solidity. <https://remix.ethereum.org> (2017)
22. Ethereum: Serpent. <https://github.com/ethereum/serpent> (2017)
23. Updates on Ethereum?s Moon Project. <https://github.com/ewasm> (2018)
24. Hyperledger Fabric. <https://www.hyperledger.org/projects/fabric> (2018)
25. Flanagan, D.: JavaScript: the definitive guide. " O'Reilly Media, Inc." (2006)
26. Updates on Ethereum?s Moon Project. <https://medium.com/@maiaivictor/updates-on-ethereums-moon-project-535f8c0497ef> (2018)
27. Franklin Schrans, Daniel Hails, A.H.: The Flint Programming Language GitHub Repository. <https://github.com/franklinsch/flint>
28. Franklin Schrans, Daniel Hails, A.H.: The Flint Programming Language GitHub Repository. <https://github.com/flintlang/flint/tree/master/examples/casestudies>
29. Hirai, Y.: The Bamboo programming language. <https://github.com/pirapira/bamboo>
30. Jones, S.P.: Haskell 98 language and libraries: the revised report. Cambridge University Press (2003)
31. Konstantinidis, A., Schultz, E.: AxLang: Compiling Scala to EVM Bytecode for Secure and Reliable Ethereum Smart Contracts. <https://guidebook.com/guide/117233/event/21956112/> (2018)
32. Luu, L., Chu, D.H., Olickel, H., Saxena, P., Hobor, A.: Making smart contracts smarter. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 254–269 (2016)
33. OpenZeppelin: StandardToken. <https://github.com/OpenZeppelin/openzeppelin-solidity/blob/master/contracts/token/ERC20/StandardToken.sol> (2018)
34. Oracle: The Java Language Specification. <https://docs.oracle.com/javase/specs/jls/se8/jls8.pdf> (2018)
35. Palsberg, J., Jay, C.B.: The essence of the visitor pattern. In: Computer Software and Applications Conference, 1998. COMPSAC'98. Proceedings. The Twenty-Second Annual International. pp. 9–15. IEEE (1998)
36. Parity: A Postmortem on the Parity Multi-Sig Library Self-Destruct. <http://paritytech.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/>
37. Parity: The Multi-sig Hack: A Postmortem. <http://paritytech.io/the-multi-sig-hack-a-postmortem/>
38. IOHK. <https://iohk.io/> (2018)
39. Python: Python. <https://www.python.org> (2018)
40. Rust: Rust Documentation. <https://doc.rust-lang.org> (2018)
41. Schrans, F., Hails, D.: Flint Programming Language Guide. <https://docs.flintlang.org/language-guide> (2018)
42. Sergey, I., Kumar, A., Hobor, A.: Scilla: a Smart Contract Intermediate-Level Language. arXiv preprint arXiv:1801.00687 (2018)
43. Wilcke, J.: Mutan Programming Language. <https://github.com/obscuren/mutan> (2017)

44. Wired: A \$50 million hack just showed that the dao was all too human. <https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/>
45. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151 (2014)
46. Zeppelin: Serpent Compiler Audit. <https://blog.zeppelin.solutions/serpent-compiler-audit-3095d1257929> (2017)

## Appendices

### A The SimpleDAO

```

1 // A condensed smart contract for a Decentralized Autonomous Organization (DAO)
2 // to automate organizational governance and decision-making.
3
4 // Removed features:
5 // - Splitting DAO
6 // - Grace/Quorum Periods
7 // Moved consensus features to curator to simplify contract
8
9 struct Proposal {
10     var proposer: Address
11     var payout: Int
12     var recipient: Address
13     var yea: Int = 0
14     var nay: Int = 0
15     var finished: Bool = false
16     var success: Bool = false
17     var voted: [Address: Bool] = [:]
18
19     mutating init(proposer: Address, payout: Int, recipient: Address) {
20         self.proposer = proposer
21         self.payout = payout
22         self.recipient = recipient
23     }
24 }
25
26 contract SimpleDAO (Join, Propose, Vote) {
27     var curator: Address
28     visible var proposal: Int = 0
29     var proposals: [Proposal] = []
30     var balances: [Address: Wei] = [:]
31 }
32
33 SimpleDAO @(any) :: caller <- (any) {
34     public init(curator: Address){
35         self.curator = curator
36         become Join
37     }
38
39     public mutating fallback() {
40         fatalError()
41     }
42
43     public func tokenHolder(addr: Address) -> Bool {
44         return balances[addr].getRawValue() != 0

```

```

45     }
46
47     public func getTotalStake() -> Int {
48         var sum: Int = 0
49         for let balance: Wei in balances {
50             sum += balance.getRawValue()
51         }
52         return sum
53     }
54 }
55
56 SimpleDAO @Join :: caller <- (any) {
57
58     @payable
59     public mutating func join(implicit value: inout Wei) {
60         balances[caller].transfer(&value)
61     }
62 }
63
64 SimpleDAO @Join :: (curator) {
65     public mutating func joinTimeElapsed() {
66         become Propose
67     }
68 }
69
70 SimpleDAO @Propose :: caller <- (tokenHolder) {
71     public mutating func newProposal(value: Int, recipient: Address) -> Int {
72         // Sanity checks omitted to be concise
73         let pID: Int = proposals.size + 1;
74         proposals[pID] = Proposal(caller, value, recipient)
75         return pID
76     }
77
78     public mutating func leave() {
79         send(caller, &balances[caller])
80     }
81 }
82
83 SimpleDAO @Propose :: (curator) {
84     public mutating func beginVote(proposal: Int) {
85         self.proposal = proposal
86         become Vote
87     }
88 }
89
90 SimpleDAO @Vote :: caller <- (tokenHolder) {
91     public mutating func vote(approve: Bool) {
92         if proposals[proposal].voted[caller] {
93             fatalError()
94         }

```

```

95
96     if approve {
97         proposals[proposal].yea += balances[caller].getRawValue()
98     } else {
99         proposals[proposal].nay += balances[caller].getRawValue()
100     }
101
102     proposals[proposal].voted[caller] = true
103 }
104
105 public mutating func executeProposal() {
106     if(caller != proposals[proposal].proposer || proposals[proposal].finished)
107     {
108         fatalError()
109     }
110
111     proposals[proposal].finished = true
112     // Quorum check omitted for brevity.
113     if proposals[proposal].yea > proposals[proposal].nay {
114         proposals[proposal].success = true
115         let transfervalue: Wei = Wei(0)
116         let totalstake: Int = getTotalStake()
117         for let value: Wei in balances {
118             let rawvalue: Int = (proposals[proposal].payout * value.getRawValue())
119                 / totalstake
120             transfervalue.transfer(&value, rawvalue)
121         }
122         send(proposals[proposal].recipient, &transfervalue)
123     }
124 }
125 }

```

## B The Bank Contract

```

1
2 // Contract declarations contain only their state properties.
3 contract Bank {
4     var manager: Address
5     var balances: [Address: Wei] = [:]
6     var accounts: [Address] = []
7     var lastIndex: Int = 0
8
9     var totalDonations: Wei = Wei(0)
10
11     event didCompleteTransfer {
12         let from: Address
13         let to: Address
14         let value: Int

```

```

15     }
16 }
17
18 // The functions in this block can be called by any user.
19 Bank :: account <- (any) {
20     public init(manager: Address) {
21         self.manager = manager
22     }
23
24     // Returns the manager's address.
25     public mutating func register() {
26         accounts[lastIndex] = account
27         lastIndex += 1
28     }
29
30     public func getManager() -> Address {
31         return manager
32     }
33
34     @payable
35     public mutating func donate(implicit value: Wei) {
36         // This will transfer the funds into totalDonations.
37         totalDonations.transfer(&value)
38     }
39 }
40
41 // Only the manager can call these functions.
42 Bank :: (manager) {
43
44     // This function needs to be declared "mutating" as its body mutates
45     // the contract's state.
46     public mutating func freeDeposit(account: Address, amount: Int) {
47         var w: Wei = Wei(amount)
48         balances[account].transfer(&w)
49     }
50
51     public mutating func clear(account: Int) {
52         balances[account] = Wei(0)
53     }
54
55     // This function is non-mutating.
56     public func getDonations() -> Int {
57         return totalDonations.getRawValue()
58     }
59 }
60
61 // Any user in accounts can call these functions.
62 // The matching user's address is bound to the variable account.
63 Bank :: account <- (accounts) {
64     public func getBalance() -> Int {

```

```

65     return balances[account].getRawValue()
66 }
67
68 public mutating func transfer(amount: Int, destination: Address) {
69     // Transfer Wei from one account to another. The balances of the
70     // originator and the destination are updated atomically.
71     // Crashes if balances[account] doesn't have enough Wei.
72     balances[destination].transfer(&balances[account], amount)
73
74     // Emit the Ethereum event.
75     emit didCompleteTransfer(from: account, to: destination, value: amount)
76 }
77
78 @payable
79 public mutating func deposit(implicit value: Wei) {
80     balances[account].transfer(&value)
81 }
82
83 public mutating func withdraw(amount: Int) {
84     // Transfer some Wei from balances[account] into a local variable.
85     let w: Wei = Wei(&balances[account], amount)
86
87     // Send the amount back to the Ethereum user.
88     send(account, &w)
89 }
90 }

```

## C The Flint Grammar

The grammar is specified in Backus-Naur form. Elements in square brackets are tokens, and elements in parentheses are optional.

```
; FLINT GRAMMAR (RFC 7405)
```

```
; TOP LEVEL
topLevelModule = 1*(topLevelDeclaration CRLF);
```

```
topLevelDeclaration = contractDeclaration
                    / contractBehaviourDeclaration
                    / structDeclaration
                    / enumDeclaration
                    / traitDeclaration;
```

```
; CONTRACTS
contractDeclaration = %s"contract" SP identifier SP [identifierGroup] SP "{" *(WSP variableDeclaration CRLF) "}"
```

```
; VARIABLES
variableDeclaration = [*(modifier SP)] WSP (%s"var" / %s"let") SP identifier typeAnnotation [WSP "=" WSP expression]
```

```
; TYPES
```

```

typeAnnotation = ":" WSP type;

type = identifier ["<" type *(", " WSP type) ">"]
      / basicType
      / arrayType
      / fixedArrayType
      / dictType;

basicType = %s"Bool"
           / %s"Int"
           / %s"String"
           / %s"Address";

arrayType      = "[" type "]";
fixedArrayType = type "[" numericLiteral "]";
dictType       = "[" type ":" WSP type "]";

; ENUMS
enumDeclaration = %s"enum" SP identifier SP [typeAnnotation] SP "{" *(WSP enumCase CRLF) "}";
enumCase        = %s"case" SP identifier
                / %s"case" SP identifier WSP "=" WSP expression;

; TRAITS
traitDeclaration = %s"struct" SP %s"trait" SP identifier SP "{" *(WSP traitMember CRLF) "}"
                 / %s"contract" SP %s"trait" SP identifier SP "{" *(WSP traitMember CRLF) "}"
                 / %s"external" SP %s"trait" SP identifier SP "{" *(WSP traitMember CRLF) "}";

traitMember = functionDeclaration
             / functionSignatureDeclaration
             / initializerDeclaration
             / initializerSignatureDeclaration
             / contractBehaviourDeclaration
             / eventDeclaration;

; EVENTS
eventDeclaration = %s"event" identifier parameterList

; STRUCTS
structDeclaration = %s"struct" SP identifier [":" WSP identifierList ] SP "{" *(WSP structMember CRLF) "}";

structMember = variableDeclaration
             / functionDeclaration
             / initializerDeclaration;

; BEHAVIOUR
contractBehaviourDeclaration = identifier WSP [stateGroup] SP "::" WSP [callerBinding] callerProtectionGroup WSP

contractBehaviourMember = functionDeclaration
                        / initializerDeclaration
                        / fallbackDeclaration

```



```

        / initializerSignatureDeclaration
        / functionSignatureDeclaration;

; ACCESS GROUPS
stateGroup      = "@" identifierGroup;
callerBinding   = identifier WSP "<-";
callerProtectionGroup = identifierGroup;
identifierGroup = "(" identifierList ")";
identifierList  = identifier *("," WSP identifier)

; FUNCTIONS + INITIALIZER + FALLBACK
functionSignatureDeclaration = functionHead SP identifier parameterList [returnType]
functionDeclaration         = functionSignatureDeclaration codeBlock;
initializerSignatureDeclaration = initializerHead parameterList
initializerDeclaration      = initializerSignatureDeclaration codeBlock;
fallbackDeclaration         = fallbackHead parameterList codeBlock;

functionHead   = [*(attribute SP)] [*(modifier SP)] %s"func";
initializerHead = [*(attribute SP)] [*(modifier SP)] %s"init";
fallbackHead   = [*(modifier SP)] %s"fallback";

attribute = "@" identifier;
modifier  = %s"public"
           / %s"mutating"
           / %s"visible";

returnType = "->" type;

parameterList = "()"
              / "(" parameter *("," parameter) ")";

parameter      = *(parameterModifiers SP) identifier typeAnnotation [WSP "=" WSP expression];
parameterModifiers = %s"inout" / %s"implicit"

; STATEMENTS
codeBlock = "{" [CRLF] *(WSP statement CRLF) WSP statement [CRLF]"}";
statement = expression
          / returnStatement
          / becomeStatement
          / emitStatement
          / forStatement
          / ifStatement;

returnStatement = %s"return" SP expression
becomeStatement = %s"become" SP expression
emitStatement   = %s"emit" SP functionCall
forStatement    = %s"for" SP variableDeclaration SP %s"in" SP expression SP codeBlock

; EXPRESSIONS
expression = identifier

```

```

        / inOutExpression
        / binaryExpression
        / functionCall
        / literal
        / arrayLiteral
        / dictionaryLiteral
        / self
        / variableDeclaration
        / bracketedExpression
        / subscriptExpression
        / rangeExpression
        / attemptExpression;

inOutExpression = "&" expression;

binaryOp = "+" / "-" / "*" / "/" / "**"
          / "&+" / "&- " / "&*"
          / "="
          / "==" / "!="
          / "+=" / "-=" / "*=" / "/="
          / "||" / "&&"
          / ">" / "<" / "<=" / ">="
          / ".";

binaryExpression = expression WSP binaryOp WSP expression;

self = %s"self"

rangeExpression = "(" expression ( "..<" / "... " ) expression ")"

bracketedExpression = "(" expression ")";

subscriptExpression = subscriptExpression "[" expression "];
                    / identifier "[" expression "];

attemptExpression = try expression
try = %s"try" ( "!" / "?" )

; FUNCTION CALLS
functionCall = identifier "(" [expression] *( "," WSP expression ) ")";

; CONDITIONALS
ifStatement = %s"if" SP expression SP codeBlock [elseClause];
elseClause = %s"else" SP codeBlock;

; LITERALS
identifier = ( ALPHA / "_" ) *( ALPHA / DIGIT / "$" / "_" );
literal = numericLiteral
        / stringLiteral
        / booleanLiteral

```

```

        / addressLiteral;

number          = 1*DIGIT;
numericLiteral = decimalLiteral;
decimalLiteral = number
               / number "." number;

addressLiteral = %s"0x" 40HEXDIG;

arrayLiteral    = "[";
dictionaryLiteral = "[:]";

booleanLiteral = %s"true" / %s"false";
stringLiteral  = "" identifier "";

```

## D Assets

```

1 // Any currency should implement this trait to be able to use the currency
2 // fully. The default implementations should be left intact, only
3 // 'getRawValue' and 'setRawValue' need to be implemented.
4
5 struct trait Asset {
6 // Initialises the asset "unsafely", i.e. from 'amount' given as an integer.
7   init(unsafeRawValue: Int)
8
9 // Initialises the asset by transferring 'amount' from an existing asset.
10 // Should check if 'source' has sufficient funds, and cause a fatal error
11 // if not.
12   init(source: inout Self, amount: Int)
13
14 // Initialises the asset by transferring all funds from 'source'.
15 // 'source' should be left empty.
16   init(source: inout Self)
17
18 // Moves 'amount' from 'source' into 'this' asset.
19   mutating func transfer(source: inout Self, amount: Int) {
20     if source.getRawValue() < amount {
21       fatalError()
22     }
23
24     // TODO: support let _: Int = ...
25     let unused1: Int = source.setRawValue(value: source.getRawValue() - amount)
26     let unused2: Int = setRawValue(value: getRawValue() + amount)
27   }
28
29   mutating func transfer(source: inout Self) {
30     transfer(source: &source, amount: source.getRawValue())
31   }

```

```

32
33 // Returns the funds contained in this asset, as an integer.
34 mutating func setRawValue(value: Int) -> Int
35
36 // Returns the funds contained in this asset, as an integer.
37 func getRawValue() -> Int
38 }
39
40 struct Wei: Asset {
41     var rawValue: Int = 0
42
43     init(unsafeRawValue: Int) {
44         self.rawValue = unsafeRawValue
45     }
46
47     init(source: inout Wei, amount: Int) {
48         transfer(source: &source, amount: amount)
49     }
50
51     init(source: inout Wei) {
52         let amount: Int = source.getRawValue()
53         transfer(source: &source, amount: amount)
54     }
55
56     mutating func setRawValue(value: Int) -> Int {
57         rawValue = value
58         return rawValue
59     }
60
61     func getRawValue() -> Int {
62         return rawValue
63     }
64 }

```

## E Compiler Diagnostics

### Caller Protections

Use of undeclared caller protection.

Caller protection 'admin' is undefined in 'Bank', or has incompatible type.

No matching function for function call.

Function 'setManager' is not in scope or cannot be called using caller protection '(any)'. Note: Perhaps you meant this function, which requires caller protection '(manager)'.

### Mutation

Mutating statement in nonmutating function.

Use of mutating statement in a nonmutating function.

No mutating statements in mutating function (Warning).

Function does not have to be declared mutating: none of its statements are mutating.

Reassignment to constant.

Cannot reassign to value: 'manager' is a let-constant. Note: 'manager' is declared on line 18, column 12.

### Initialisation

State property is not assigned a value.

State property 'manager' needs to be assigned a value, as no initialiser was declared.

Return from initialiser without initialising all properties.

Return from initialiser without initialising all properties. Note: 'manager' is uninitialised.

Contract does not have a public initialiser.

Contract 'Bank' needs a public initialiser accessible using caller capability 'any'.

Contract has multiple public initialisers.

A public initialiser has already been defined. Note: A public initialiser is defined on line 5, column 6.

Public contract initialiser is not accessible using caller capability any.

Public contract initialiser should be callable using caller capability 'any'.

### Invalid Declarations

Invalid redeclaration of an identifier.

Invalid redeclaration of 'setManager'. Note: Previous declaration on line 12, column 4.

Use of invalid character. The \$ character is reserved for use in the standard library.

Use of invalid character '\$' in 'my\$Func'.

Contract Behaviour Declaration has no matching Contract Declaration.

Contract behaviour declaration for 'Bank' has no associated contract declaration.

Invalid contract behaviour declaration.

Contract behaviour declaration for Bank has no associated contract declaration.

Invalid @payable function.

receive is declared @payable but doesn't have an implicit parameter of a currency type.

Ambiguous @payable value parameter.

Ambiguous implicit payable value parameter. Only one parameter can be declared 'implicit' with a currency type.

Public function has a parameter of dynamic type, such as struct, array, or dictionary.

Function 'isSeatFree' cannot have dynamic parameters. Note: 'seat' cannot be used as a parameter.

Use of undeclared identifier.

Use of undeclared identifier 'manager'.

Missing return in non-void function.

Missing return in function expected to return 'Int'.

Code after return (Warning).

Code after return will never be executed.

### Type Checking

Incompatible return type.

Cannot convert expression of type 'Int' to expected return type 'Address'.

Incompatible assignment.

Incompatible assignment between values of type Int and Wei.

Incompatible argument type.

Cannot convert expression of type Int to expected argument type Wei