Accurate Smart Contract Verification through Direct Modelling

Matteo Marescotti[1], **Rodrigo Otoni**[1], Leonardo Alt[2],
Patrick Eugster[1], Antti E. J. Hyvärinen[1], and Natasha Sharygina[1]

[1] Università della Svizzera italiana, Lugano, Switzerland
[2] Ethereum Foundation, Zug, Switzerland

2nd June 2021

Foreword

Industrial application of our work

- Component of the SMTChecker module of the Solidity compiler
  SMTChecker's constrained Horn clauses model checking engine

Availability of our tool

- `github.com/ethereum/solidity`
- Add `pragma experimental SMTChecker;` to the source file

Formal Verification of Smart Contracts

Essential for safety

Formal Verification of Smart Contracts

Essential for safety

Many works published

Formal Verification of Smart Contracts

Essential for safety

Many works published

- Symbolic execution, e.g.:
  - Oyente [Luu et al., CCS'16]
  - Maian [Nikolić et al., ACSAC'18]
  - Manticore [Mossberg et al., ASE'19]
  - VerX [Permenev et al., S&P'20]
- Model checking, e.g.:
  - Zeus [Kalra et al., NDSS'18]
  - SAFEVM [Albert et al., ISSTA'19]
  - VeriSol [Wang et al., VSTTE'20]
- Others, e.g.:
  - F* [Bhargavan et al., PLAS'16]
  - KEVM [Hildenbrandt et al., CSF'18]
  - Securify [Tsankov et al., CCS'18]
  - Why3 [Nehaï and Bobot, FM'19]
  - Solc-Verify [Hajdu and Jovanovic, VSTTE'19, ESOP'20]

Formal Verification of Smart Contracts

Essential for safety

Many works published

Limitations to be addressed

- Symbolic execution, e.g.:
  - Oyente [Luu et al., CCS'16]
  - Maian [Nikolić et al., ACSAC'18]
  - Manticore [Mossberg et al., ASE'19]
  - VerX [Permenev et al., S&P'20]
- Model checking, e.g.:
  - Zeus [Kalra et al., NDSS'18]
  - SAFEVM [Albert et al., ISSTA'19]
  - VeriSol [Wang et al., VSTTE'20]
- Others, e.g.:
  - F* [Bhargavan et al., PLAS'16]
  - KEVM [Hildenbrandt et al., CSF'18]
  - Securify [Tsankov et al., CCS'18]
  - Why3 [Nehaï and Bobot, FM'19]
  - Solc-Verify [Hajdu and Jovanovic, VSTTE'19, ESOP'20]

Common Feature: Domain Translation

Translation for reuse

- Established off-the-shelf frameworks, e.g.:
  - Boogie
  - LLVM
- Programming languages ecosystems, e.g.:
  - C/C++
  - WhyML

Common Feature: Domain Translation

Translation for reuse

- Established off-the-shelf frameworks, e.g.:
  - Boogie
  - LLVM
- Programming languages ecosystems, e.g.:
  - C/C++
  - WhyML

Translation layer drawbacks

- Error prone to develop
- Requires correctness proofs
- Adverse effect on precision and efficiency

Common Feature: Domain Translation

Translation for reuse

- Established off-the-shelf frameworks, e.g.:
  - Boogie
  - LLVM
- Programming languages ecosystems, e.g.:
  - C/C++
  - WhyML

Translation layer drawbacks

- Error prone to develop
- Requires correctness proofs
- Adverse effect on precision and efficiency

Our approach

- Direct modelling into the target formalism
  - Focus on Solidity contracts
  - Modelling in constrained Horn clauses (CHCs)

Smart Contracts Verification through Direct Modelling

- Rule-based encoding for assertion checking

Smart Contracts Verification through Direct Modelling

- Rule-based encoding for assertion checking, starting with the contracts' control-flow graphs

Smart Contracts Verification through Direct Modelling

- Rule-based encoding for assertion checking, starting with the contracts' control-flow graphs

CHC rule format

$$\forall V : \underbrace{H(x)}_{\text{head}} \leftarrow \underbrace{\exists y : P_1(y) \wedge \ldots \wedge P_n(y) \wedge (x; y)}_{\text{body}}$$

with V a set of variables over a background theory T, $x \; [\; y \quad V, n \quad 0$

Smart Contracts Verification through Direct Modelling

- Rule-based encoding for assertion checking, starting with the contracts' control-flow graphs

CHC rule format

$$\forall V : \underbrace{(H(x)}_{\textit{head}} \quad \underbrace{\exists y : P_1(y) \wedge \ldots \wedge P_n(y) \wedge \quad (x; y))}_{\textit{body}}$$

with V a set of variables over a background theory T, $x \; [\; y \quad V, n \quad 0$

Rule $\text{Jump}_{f;e}$

$$P_f^u(s; a; I^0) \qquad P_f^v(s; a; I) \wedge \text{SSA}_{\ v}(I; I^0) \wedge \text{SSA}_{\ e}(I^0)$$

Smart Contracts Verification through Direct Modelling

- Rule-based encoding for assertion checking, starting with the contracts' control-flow graphs

CHC rule format

$$\forall V : (\underbrace{H(x)}_{\text{head}} \quad \underbrace{\exists y : P_1(y) \wedge \ldots \wedge P_n(y) \wedge \quad (x; y)}_{\text{body}})$$

with V a set of variables over a background theory T, x [y V, n 0

Rule Jump$_{f;e}$

$$P^u_f(s; a; I^0) \qquad P^v_f(s; a; I) \wedge \text{SSA}_{\ v}(I; I^0) \wedge \text{SSA}_{\ e}(I^0)$$

Smart Contracts Verification through Direct Modelling

- Rule-based encoding for assertion checking, starting with the contracts' control-flow graphs

CHC rule format

$$\forall V : (\underbrace{H(x)}_{\text{head}} \leftarrow \underbrace{\exists y : P_1(y) \wedge \ldots \wedge P_n(y) \wedge (x; y)}_{\text{body}})$$

with V a set of variables over a background theory T, x [y V, n 0

Rule $\text{Jump}_{f;e}$

$$P^u_f(s; a; I^0) \qquad P^v_f(\underline{s}; a; I) \wedge \text{SSA}_{\ v}(I; I^0) \wedge \text{SSA}_{\ e}(I^0)$$

Smart Contracts Verification through Direct Modelling

- Rule-based encoding for assertion checking, starting with the contracts' control-flow graphs

CHC rule format

$$\forall V : \underbrace{(H(x)}_{\textit{head}} \quad \underbrace{\exists y : P_1(y) \wedge \ldots \wedge P_n(y) \wedge \quad (x; y))}_{\textit{body}}$$

with V a set of variables over a background theory T, $x \; [\; y \quad V, n \quad 0$

Rule $\text{Jump}_{f;e}$

$$P^u_f(s; a; I^0) \qquad P^v_f(s; \underline{a}; I) \wedge \text{SSA}_{\ v}(I; I^0) \wedge \text{SSA}_{\ e}(I^0)$$

Smart Contracts Verification through Direct Modelling

- Rule-based encoding for assertion checking, starting with the contracts' control-flow graphs

CHC rule format

$$\forall V : (\underbrace{H(x)}_{\text{head}} \leftarrow \underbrace{\exists y : P_1(y) \wedge \ldots \wedge P_n(y) \wedge (x; y)}_{\text{body}})$$

with V a set of variables over a background theory T, $x \; [\; y \quad V, n \quad 0$

Rule $\text{Jump}_{f;e}$

$$P_f^u(s; a; I^0) \qquad P_f^v(s; a; \underline{I}) \wedge \text{SSA}_{\ v}(I; I^0) \wedge \text{SSA}_{\ e}(I^0)$$

Smart Contracts Verification through Direct Modelling

- Rule-based encoding for assertion checking, starting with the contracts' control-flow graphs

CHC rule format

$$\forall V : (\underbrace{H(x)}_{\text{head}} \quad \underbrace{\exists y : P_1(y) \wedge \ldots \wedge P_n(y) \wedge \quad (x; y)}_{\text{body}})$$

with V a set of variables over a background theory T, $x \; [\; y \quad V, n \quad 0$

Rule $\text{Jump}_{f;e}$

$$P^u_f(s; a; l^0) \qquad P^v_f(s; a; l) \wedge \text{SSA}_{\ v}(l; l^0) \wedge \text{SSA}_{\ e}(l^0)$$

Smart Contracts Veri cation through Direct Modelling

Rule-based encoding for assertion checking, starting with the contracts' control- ow grap

CHC rule format

$$\forall V : (H(x) \land \{z\}) \rightarrow \exists y : P_1(y) \land \cdots \land P_n(y) \land \{z\} \land (x; y))$$

head body

with V a set of variables over a background theory x [y V , n 0

Rule Jump$_{f,e}$

$$P_f^u(s; a; I') \land P_f^v(s; a; I) \land SSA_v(I; I') \land SSA_e(I')$$

Smart Contracts Veri cation through Direct Modelling

Rule-based encoding for assertion checking, starting with the contracts' control- ow grap

CHC rule format

$$\forall V : (H(x) \quad 9 \quad y : P_1(y) \wedge \cdots \wedge P_n(y) \wedge \quad (x; y))$$

head | body

with V a set of variables over a background theory x [y V , n 0

Rule Jump$_{f,e}$

$$P_f^u(s; a; I^0) \quad P \quad {}^v_f(s; a; I) \wedge SSA_v(I; I^0) \wedge SSA_e(I^0)$$

Smart Contracts Veri cation through Direct Modelling

Rule-based encoding for assertion checking, starting with the contracts' control- ow grap

CHC rule format

$$\forall V : (\underbrace{H(x)}_{\text{head}} \leftarrow \underbrace{\exists y : P_1(y) \wedge \ldots \wedge P_n(y) \wedge \ldots (x; y))}_{\text{body}}$$

with V a set of variables over a background theory $x [y \quad V , n \quad 0$

Rule Jump$_{f;e}$

$$P^{u}_{f}(s; a; l') \quad P^{v}_{f}(s; a; l) \wedge SSA_{v}(l; l') \wedge SSA_{e}(l')$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             //assert(bid cash);
11             winner.transfer(bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer(bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer(bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s;a;l^0) \quad P \quad {}_f^v(s;a;l) \wedge SSA_v(l;l^0) \wedge SSA_e(l^0)$$

$$P_o^2 \quad P \quad {}_o^1$$

$$P_o^3 \quad P \quad {}_o^2 \wedge l_{nb} = l_v \quad 10^{15} \wedge l_b < l_{nb} \wedge l_w 6= 0$$

$$P_o^5 \quad P \quad {}_o^2 \wedge l_{nb} = l_v \quad 10^{15} \wedge l_b < l_{nb} \wedge : \ (l_w 6= 0)$$

$$P_o^4 \quad P \quad {}_o^3 \wedge l_b \quad l_c$$

$$P_o^6 \quad P \quad {}_o^3 \wedge : \ (l_b \quad l_c) \wedge l_r = 3$$

$$P_o^5 \quad P \quad {}_o^4 \wedge l_c^0 = l_c \quad l_b$$

$$P_o^6 \quad P \quad {}_o^5 \wedge l_b^0 = l_{nb} \wedge l_c^0 = l_c + l_v \wedge l_w^0 = l_s$$

$$P_o^n(b;c;w;s;v;l_b;l_c;l_w;l_s;l_v;l_{nb};l_r), \ n \ 2 \ f \ 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer(bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s;a;I^0) \quad P \; {}_f^v(s;a;I) \wedge SSA_v(I;I^0) \wedge SSA_e(I^0)$$

$$P_o^2 \; P \; {}_o^1$$

$$P_o^3 \; P \; {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge I_w 6= 0$$

$$P_o^5 \; P \; {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge : \; (I_w 6= 0)$$

$$P_o^4 \; P \; {}_o^3 \wedge I_b \quad I_c$$

$$P_o^6 \; P \; {}_o^3 \wedge : \; (I_b \quad I_c) \wedge I_r = 3$$

$$P_o^5 \; P \; {}_o^4 \wedge I_c^0 = I_c \quad I_b$$

$$P_o^6 \; P \; {}_o^5 \wedge I_b^0 = I_{nb} \wedge I_c^0 = I_c + I_v \wedge I_w^0 = I_s$$

$$P_o^n(b;c;w;s;v;I_b;I_c;I_w;I_s;I_v;I_{nb};I_r), \; n \; 2 \; f \; 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s;a;I^0) \quad P \; {}_f^v(s;a;I) \wedge SSA_v(I;I^0) \wedge SSA_e(I^0)$$

$$P_o^2 \; P \; {}_o^1$$

$$P_o^3 \; P \; {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge I_w 6= 0$$

$$P_o^5 \; P \; {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge : \; (I_w 6= 0)$$

$$P_o^4 \; P \; {}_o^3 \wedge I_b \quad I_c$$

$$P_o^6 \; P \; {}_o^3 \wedge : \; (I_b \quad I_c) \wedge I_r = 3$$

$$P_o^5 \; P \; {}_o^4 \wedge I_c^0 = I_c \quad I_b$$

$$P_o^6 \; P \; {}_o^5 \wedge I_b^0 = I_{nb} \wedge I_c^0 = I_c + I_v \wedge I_w^0 = I_s$$

$$P_o^n(b;c;w;s;v;I_b;I_c;I_w;I_s;I_v;I_{nb};I_r), \; n \; 2 \; f \; 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s;a;I^0) \quad P \quad {}_f^v(s;a;I) \wedge SSA_v(I;I^0) \wedge SSA_e(I^0)$$

$$P_o^2 \quad P \quad {}_o^1$$

$$P_o^3 \quad P \quad {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge I_w 6= 0$$

$$P_o^5 \quad P \quad {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge : \ (I_w 6= 0)$$

$$P_o^4 \quad P \quad {}_o^3 \wedge I_b \quad I_c$$

$$P_o^6 \quad P \quad {}_o^3 \wedge : \ (I_b \quad I_c) \wedge I_r = 3$$

$$P_o^5 \quad P \quad {}_o^4 \wedge I_c^0 = I_c \quad I_b$$

$$P_o^6 \quad P \quad {}_o^5 \wedge I_b^0 = I_{nb} \wedge I_c^0 = I_c + I_v \wedge I_w^0 = I_s$$

$$P_o^n(b;c;w;s;v;I_b;I_c;I_w;I_s;I_v;I_{nb};I_r), \ n \ 2 \ f \ 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s; a; I^0) \quad P \quad {}_f^v(s; a; I) \wedge SSA_v(I; I^0) \wedge SSA_e(I^0)$$

$$P_o^2 \quad P \quad {}_o^1$$

$$P_o^3 \quad P \quad {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge I_w 6= 0$$

$$P_o^5 \quad P \quad {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge : \ (I_w 6= 0)$$

$$P_o^4 \quad P \quad {}_o^3 \wedge I_b \quad I_c$$

$$P_o^6 \quad P \quad {}_o^3 \wedge : \ (I_b \quad I_c) \wedge I_r = 3$$

$$P_o^5 \quad P \quad {}_o^4 \wedge I_c^0 = I_c \quad I_b$$

$$P_o^6 \quad P \quad {}_o^5 \wedge I_b^0 = I_{nb} \wedge I_c^0 = I_c + I_v \wedge I_w^0 = I_s$$

$$P_o^n(b; c; w; s; v; I_b; I_c; I_w; I_s; I_v; I_{nb}; I_r), \ n \ 2 \ f \ 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s; a; I_0^0) \quad P \;{}_f^v(s; a; I) \wedge SSA_v(I; I_0^0) \wedge SSA_e(I_0^0)$$

$$P_o^2 \quad P \;{}_o^1$$

$$P_o^3 \quad P \;{}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge I_w \text{ 6= } 0$$

$$P_o^5 \quad P \;{}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge : \; (I_w \text{ 6= } 0)$$

$$P_o^4 \quad P \;{}_o^3 \wedge I_b \quad I_c$$

$$P_o^6 \quad P \;{}_o^3 \wedge : \; (I_b \quad I_c) \wedge I_{r\text{-}} = 3$$

$$P_o^5 \quad P \;{}_o^4 \wedge I_c^0 = I_c \quad I_b$$

$$P_o^6 \quad P \;{}_o^5 \wedge I_b^0 = I_{nb} \wedge I_c^0 = I_c + I_v \wedge I_w^0 = I_s$$

$$P_o^n(b; c; w; s; v; I_b; I_c; I_w; I_s; I_v; I_{nb}; I_{r\text{-}}), \; n \; 2 \; f \; 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer(bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s;a;I^0) \quad P \quad {}_f^v(s;a;I) \wedge SSA_v(I;I^0) \wedge SSA_e(I^0)$$

$$P_o^2 \quad P \quad {}_o^1$$

$$P_o^3 \quad P \quad {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge I_w \not= 0$$

$$P_o^5 \quad P \quad {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge : \ (I_w \not= 0)$$

$$P_o^4 \quad P \quad {}_o^3 \wedge I_b \quad I_c$$

$$P_o^6 \quad P \quad {}_o^3 \wedge : \ (I_b \quad I_c) \wedge I_{r\text{-}} = 3$$

$$P_o^5 \quad P \quad {}_o^4 \wedge I_c^0 = I_c \quad I_b$$

$$P_o^6 \quad P \quad {}_o^5 \wedge I_b^0 = I_{nb} \wedge I_c^0 = I_c + I_v \wedge I_w^0 = I_s$$

$$P_o^n(b;c;w;s;v;I_b;I_c;I_w;I_s;I_v;I_{nb};I_{r\text{-}}), \ n \ 2 \ f \ 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer(bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s;a;I_0^0) \quad P \quad {}_f^v(s;a;I) \wedge SSA_v(I;I_0^0) \wedge SSA_e(I_0^0)$$

$$P_o^2 \quad P \quad {}_o^1$$

$$P_o^3 \quad P \quad {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge I_w 6= 0$$

$$P_o^5 \quad P \quad {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge : (I_w 6= 0)$$

$$P_o^4 \quad P \quad {}_o^3 \wedge I_b \quad I_c$$

$$P_o^6 \quad P \quad {}_o^3 \wedge : (I_b \quad I_c) \wedge I_r = 3$$

$$P_o^5 \quad P \quad {}_o^4 \wedge I_c^0 = I_c \quad I_b$$

$$P_o^6 \quad P \quad {}_o^5 \wedge I_b^0 = I_{nb} \wedge I_c^0 = I_c + I_v \wedge I_w^0 = I_s$$

$$P_o^n(b;c;w;s;v;I_b;I_c;I_w;I_s;I_v;I_{nb};I_r), \; n \; 2 \; f \; 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer(bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s;a;I^0) \quad P \quad {}_f^v(s;a;I) \wedge SSA_v(I;I^0) \wedge SSA_e(I^0)$$

$$P_o^2 \quad P \quad {}_o^1$$

$$P_o^3 \quad P \quad {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge I_w 6= 0$$

$$P_o^5 \quad P \quad {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge : \ (I_w 6= 0)$$

$$P_o^4 \quad P \quad {}_o^3 \wedge I_b \quad I_c$$

$$P_o^6 \quad P \quad {}_o^3 \wedge : \ (I_b \quad I_c) \wedge I_{r\text{-}} = 3$$

$$P_o^5 \quad P \quad {}_o^4 \wedge I_c^0 = I_c \quad I_b$$

$$P_o^6 \quad P \quad {}_o^5 \wedge I_b^0 = I_{nb} \wedge I_c^0 = I_c + I_v \wedge I_w^0 = I_s$$

$$P_o^n(b;c;w;s;v;I_b;I_c;I_w;I_s;I_v;I_{nb};I_{r\text{-}}), \ n \ 2 \ f \ 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer(bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s;a;I^0) \quad P \; {}_f^v(s;a;I) \wedge SSA_v(I;I^0) \wedge SSA_e(I^0)$$

$$P_o^2 \; P \; {}_o^1$$

$$P_o^3 \; P \; {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge I_w 6= 0$$

$$P_o^5 \; P \; {}_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge : \; (I_w 6= 0)$$

$$P_o^4 \; P \; {}_o^3 \wedge I_b \quad I_c$$

$$P_o^6 \; P \; {}_o^3 \wedge : \; (I_b \quad I_c) \wedge I_r = 3$$

$$P_o^5 \; P \; {}_o^4 \wedge I_c^0 = I_c \quad I_b$$

$$P_o^6 \; P \; {}_o^5 \wedge I_b^0 = I_{nb} \wedge I_c^0 = I_c + I_v \wedge I_w^0 = I_s$$

$$P_o^n(b;c;w;s;v;I_b;I_c;I_w;I_s;I_v;I_{nb};I_r), \; n \; 2 \; f \; 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer(bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function o er () public payable f
7          uint new_bid = msg.value = 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid cash);
11             winner.transfer (bid);
12             cash = cash = bid;
13         g
14         bid = new _bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s;a;l^0) \quad P \; {}_f^v(s;a;l) \wedge SSA_v(l;l^0) \wedge SSA_e(l^0)$$

$$P_o^2 \; P \; {}_o^1$$

$$P_o^3 \; P \; {}_o^2 \wedge l_{nb} = l_v \quad 10^{15} \wedge l_b < l_{nb} \wedge l_w 6= 0$$

$$P_o^5 \; P \; {}_o^2 \wedge l_{nb} = l_v \quad 10^{15} \wedge l_b < l_{nb} \wedge : \; (l_w 6= 0)$$

$$P_o^4 \; P \; {}_o^3 \wedge l_b \quad l_c$$

$$P_o^6 \; P \; {}_o^3 \wedge : \; (l_b \quad l_c) \wedge l_r = 3$$

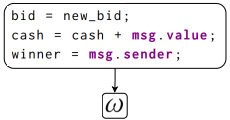
$$P_o^5 \; P \; {}_o^4 \wedge l_c^0 = l_c \quad l_b$$

$$P_o^6 \; P \; {}_o^5 \wedge l_b^0 = l_{nb} \wedge l_c^0 = l_c + l_v \wedge l_w^0 = l_s$$

$$P_o^n(b;c;w;s;v;l_b;l_c;l_w;l_s;l_v;l_{nb};l_r), \; n \; 2 \; f \; 1::6g$$

Example: an Auction in Solidity

```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function offer() public payable f
7          uint new_bid = msg.value − 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid  cash);
11             winner.transfer(bid);
12             cash = cash − bid;
13         g
14         bid = new_bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```



Example: an Auction in Solidity

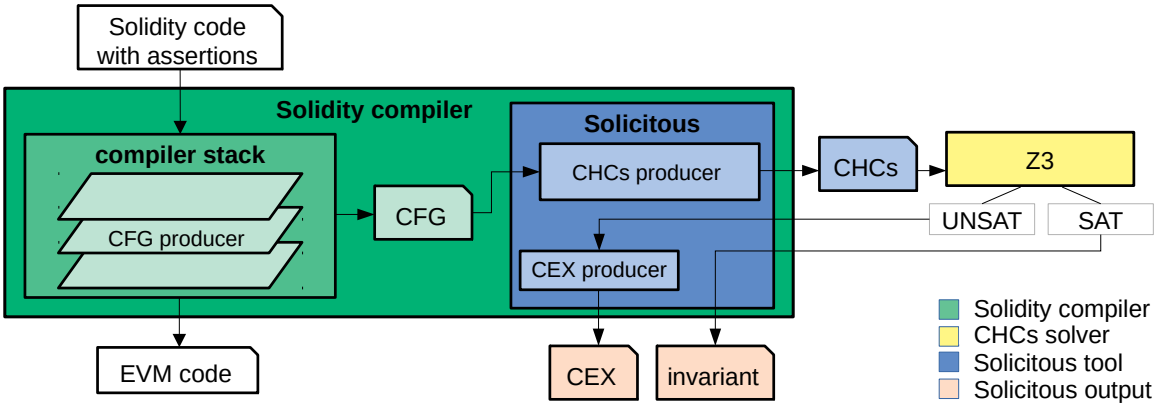
```
1  contract Auction f
2      uint bid = 0;
3      uint cash = 0;
4      address payable winner = address(0);
5
6      function offer() public payable f
7          uint new_bid = msg.value - 10^15 wei;
8          require(bid < new_bid);
9          if (winner 6= address(0)) f
10             assert(bid  cash);
11             winner.transfer(bid);
12             cash = cash - bid;
13         g
14         bid = new_bid;
15         cash = cash + msg.value;
16         winner = msg.sender;
17     g
18 g
```

$$P_f^u(s;a;I^0) \qquad P_f^v(s;a;I) \wedge \text{SSA}_{\ v}(I;I^0) \wedge \text{SSA}_{\ e}(I^0)$$

$$\begin{array}{ll}
P_o^2 & P_o^1 \\
P_o^3 & P_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge I_w \; 6= \; 0 \\
P_o^5 & P_o^2 \wedge I_{nb} = I_v \quad 10^{15} \wedge I_b < I_{nb} \wedge :(I_w \; 6= \; 0) \\
P_o^4 & P_o^3 \wedge I_b \quad I_c \\
P_o^6 & P_o^3 \wedge :(I_b \quad I_c) \wedge I_{r'} = 3 \\
P_o^5 & P_o^4 \wedge I_c^0 = I_c \quad I_b \\
P_o^6 & P_o^5 \wedge I_b^0 = I_{nb} \wedge I_c^0 = I_c + I_v \wedge I_w^0 = I_s
\end{array}$$

$$P_o^n(b;c;w;s;v;I_b;I_c;I_w;I_s;I_v;I_{nb};I_{r'}),\ n\ 2\ f1::6g$$

Modelling Framework



Solicitous (Solidity Contract verification using constrained Horn clauses)

- Assertion failures lead to reverts, which are modelled as error predicates
- Queries are made to the solver for the reachability of error predicates

Evaluation

- Evaluation with 22446 real-world contracts
  Solidity versions 0.5 to 0.8

	Solicitous	Solc-Verify	VeriSol	Mythril
Instances	**22446**	13310	12402	**22446**
Safe	**6651**	103	201	0
Unsafe	8	0	9	**21**
Unknown	2970	5601	230	728
Timeout	9058	3163	4032	19511
Error	3759	4443	7930	2186
Verified	**29%**	0.007%	0.01%	0.0009%

Evaluation

- Evaluation with 22446 real-world contracts
  Solidity versions 0.5 to 0.8

	Solicitous	Solc-Verify	VeriSol	Mythril
Instances	**22446**	13310	12402	**22446**
Safe	**6651**	103	201	0
Unsafe	8	0	9	**21**
Unknown	2970	5601	230	728
Timeout	9058	3163	4032	19511
Error	3759	4443	7930	2186
Verified	**29%**	0.007%	0.01%	0.0009%

Evaluation

- Evaluation with 22446 real-world contracts
  Solidity versions 0.5 to 0.8

	Solicitous	Solc-Verify	VeriSol	Mythril
Instances	**22446**	13310	12402	**22446**
Safe	**6651**	103	201	0
Unsafe	8	0	9	**21**
Unknown	2970	5601	230	728
Timeout	9058	3163	4032	19511
Error	3759	4443	7930	2186
Verified	**29%**	0.007%	0.01%	0.0009%

Evaluation

- Evaluation with 22446 real-world contracts
  Solidity versions 0.5 to 0.8

	Solicitous	Solc-Verify	VeriSol	Mythril
Instances	**22446**	13310	12402	**22446**
Safe	**6651**	103	201	0
Unsafe	8	0	9	**21**
Unknown	2970	5601	230	728
Timeout	9058	3163	4032	19511
Error	3759	4443	7930	2186
Verified	**29%**	0.007%	0.01%	0.0009%

Evaluation

- Evaluation with 22446 real-world contracts
  Solidity versions 0.5 to 0.8

	Solicitous	Solc-Verify	VeriSol	Mythril
Instances	**22446**	13310	12402	**22446**
Safe	**6651**	103	201	0
Unsafe	8	0	9	**21**
Unknown	2970	5601	230	728
Timeout	9058	3163	4032	19511
Error	3759	4443	7930	2186
Verified	**29%**	0.007%	0.01%	0.0009%

Evaluation

- Evaluation with 22446 real-world contracts
  Solidity versions 0.5 to 0.8

	Solicitous	Solc-Verify	VeriSol	Mythril
Instances	**22446**	13310	12402	**22446**
Safe	**6651**	103	201	0
Unsafe	8	0	9	**21**
Unknown	2970	5601	230	728
Timeout	9058	3163	4032	19511
Error	3759	4443	7930	2186
Verified	**29%**	0.007%	0.01%	0.0009%

Evaluation

- Evaluation with 22446 real-world contracts
  Solidity versions 0.5 to 0.8

	Solicitous	Solc-Verify	VeriSol	Mythril
Instances	**22446**	13310	12402	**22446**
Safe	**6651**	103	201	0
Unsafe	8	0	9	**21**
Unknown	2970	5601	230	728
Timeout	9058	3163	4032	19511
Error	3759	4443	7930	2186
Verified	**29%**	0.007%	0.01%	0.0009%

Evaluation

- Evaluation with 22446 real-world contracts
  Solidity versions 0.5 to 0.8

- Verified $= \dfrac{\text{safe} + \text{unsafe}}{\text{num. of instances}}$

	Solicitous	Solc-Verify	VeriSol	Mythril
Instances	**22446**	13310	12402	**22446**
Safe	**6651**	103	201	0
Unsafe	8	0	9	**21**
Unknown	2970	5601	230	728
Timeout	9058	3163	4032	19511
Error	3759	4443	7930	2186
Verified	**29%**	0.007%	0.01%	0.0009%

Summary

- Direct modelling of smart contracts into CHCs
- Solicitous implemented inside the Solidity compiler

Summary

- Direct modelling of smart contracts into CHCs
- Solicitous implemented inside the Solidity compiler

Future Work

- Smart contract verification
  - Enhancement of the modelling to account for gas consumption
  - Instantiation of the approach to languages other than Solidity
  - Production of correctness certificates as witnesses of safe results
- Tool improvements
  - Support for additional Solidity features
  - Integration with different back-end solvers

Summary

- Direct modelling of smart contracts into CHCs
- Solicitous implemented inside the Solidity compiler

Future Work

- Smart contract verification
  - Enhancement of the modelling to account for gas consumption
  - Instantiation of the approach to languages other than Solidity
  - Production of correctness certificates as witnesses of safe results
- Tool improvements
  - Support for additional Solidity features
  - Integration with different back-end solvers

`verify.inf.usi.ch/research/fvsc`