Open issues in programming
Bitcoin contracts
(Oral Communication)

Roberto Zunino
University of Trento

Joint work with:
Massimo Bartoletti (Univ of Cagliari)
Stefano Lande (Univ of Cagliari)
Maurizio Murgia (Univ. of Trento)

DLT2020, 4 February 2020
init $\{ A : 1 \uparrow, \text{secret } a \}$

$B : 1 \uparrow, \text{secret } b \}$

(reveal $a$.

(reveal $b$. if $(a + b) \% 2 = 0$
then withdraw $A$
else withdraw $B$
+after $2 \cdot t : \text{withdraw } A$)
+after $t : \text{withdraw } B$

A fair lottery in Bitcoin (transactions)

CollectOrphan

Win($\pi, a$) with $\epsilon \neq \pi \subseteq a$
certifies that $a$ has won the lottery after $\pi$, but she can collect her winnings so far (see Theorem 5 for details)

in: Win($\pi, a$)
in-script: $\text{sig}_K(\text{WinTo}, \pi, a)$

out-script($T, \sigma$): $\text{ver}_K(\text{Collect}(T, \sigma))$
value($a$): $2^{L-|\pi|} + dB$

$\forall p$ with $a \neq p \subseteq \pi$:

out-script($p(T, \sigma)$: $\text{ver}_K(\text{Collect}(T, \sigma))$
value($p$): $dB$

lockTime: $\tau_1 + (L - |\pi|)\tau_{\text{Round}} + \tau_{\text{Ledger}}$

BitML compiler

Transition system semantics

Computational soundness

Toolchain (development & verification)
BitML implementation (oversimplification)

- Generate BitML transition system
- One Bitcoin transaction per state
- Redeem scripts check BitML transition semantics
- Everyone signs everything
BitML implementation (oversimplification)

Execution

- Put enabled transactions on the blockchain
- This forms an execution trace
Work in progress

Recursion
BitML recursion
- Currently NOT available in BitML
- In BitML state 2 is the same as state 5
- In Bitcoin, 5 is a different transaction from 2
Flavours of Recursion

- **Consensual recursion**
  - All participants must agree to recurse at **execution-time**
  - Compilation to Bitcoin still possible

- **Non-consensual recursion**
  - After stipulation, participants cannot prevent it
  - Requires some extensions of Bitcoin
Work in progress

"Layer 2" BitML
BitML as is

Tx fees paid at each step
Off-chain "long jumps"
Layer 2 BitML Guarantees

- As secure as regular BitML
- Smaller fees in the cooperating case
- Same fees in the adversarial case
- Rollback freedom
  - Last signed "long jump" wins
Thank you