Open issues in programming Bitcoin contracts

(Oral Communication)

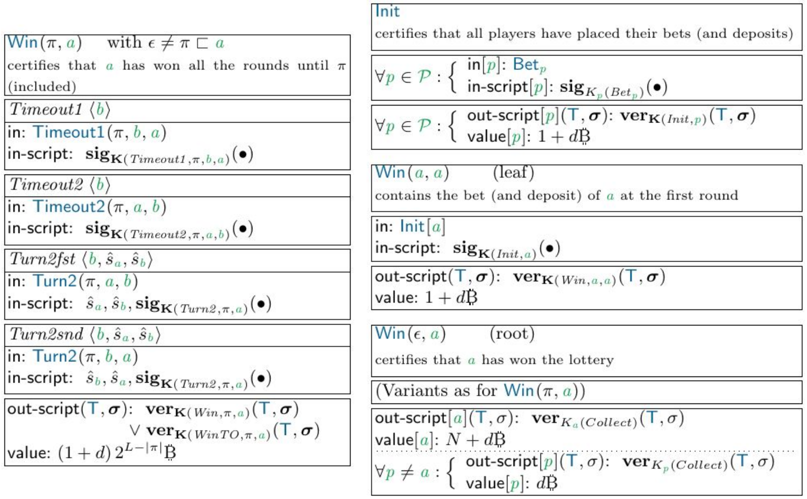
Roberto Zunino

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

A fair lottery in Bitcoin (transactions)



$\mathsf{Win}(\pi, a)$ with $\epsilon \neq \pi \sqsubset a$
certifies that a has won all the rounds until π (included)

Timeout1 $\langle b \rangle$
in: $\mathsf{Timeout1}(\pi, b, a)$
in-script: $\mathbf{sig}_{\mathbf{K}(\mathit{Timeout1}, \pi, b, a)}(\bullet)$

Timeout2 $\langle b \rangle$
in: $\mathsf{Timeout2}(\pi, a, b)$
in-script: $\mathbf{sig}_{\mathbf{K}(\mathit{Timeout2}, \pi, a, b)}(\bullet)$

Turn2fst $\langle b, \hat{s}_a, \hat{s}_b \rangle$
in: $\mathsf{Turn2}(\pi, a, b)$
in-script: $\hat{s}_a, \hat{s}_b, \mathbf{sig}_{\mathbf{K}(\mathit{Turn2}, \pi, a)}(\bullet)$

Turn2snd $\langle b, \hat{s}_a, \hat{s}_b \rangle$
in: $\mathsf{Turn2}(\pi, b, a)$
in-script: $\hat{s}_b, \hat{s}_a, \mathbf{sig}_{\mathbf{K}(\mathit{Turn2}, \pi, a)}(\bullet)$

out-script$(\mathsf{T}, \boldsymbol{\sigma})$: $\mathbf{ver}_{\mathbf{K}(\mathit{Win}, \pi, a)}(\mathsf{T}, \boldsymbol{\sigma})$
$\vee\, \mathbf{ver}_{\mathbf{K}(\mathit{WinTO}, \pi, a)}(\mathsf{T}, \boldsymbol{\sigma})$
value: $(1 + d)\, 2^{L - |\pi|}$₿

Init
certifies that all players have placed their bets (and deposits)

$\forall p \in \mathcal{P} : \begin{cases} \text{in}[p]\text{: } \mathsf{Bet}_p \\ \text{in-script}[p]\text{: } \mathbf{sig}_{K_p(\mathit{Bet}_p)}(\bullet) \end{cases}$

$\forall p \in \mathcal{P} : \begin{cases} \text{out-script}[p](\mathsf{T}, \boldsymbol{\sigma})\text{: } \mathbf{ver}_{\mathbf{K}(\mathit{Init}, p)}(\mathsf{T}, \boldsymbol{\sigma}) \\ \text{value}[p]\text{: } 1 + d\text{₿} \end{cases}$

$\mathsf{Win}(a, a)$ (leaf)
contains the bet (and deposit) of a at the first round

in: $\mathsf{Init}[a]$
in-script: $\mathbf{sig}_{\mathbf{K}(\mathit{Init}, a)}(\bullet)$

out-script$(\mathsf{T}, \boldsymbol{\sigma})$: $\mathbf{ver}_{\mathbf{K}(\mathit{Win}, a, a)}(\mathsf{T}, \boldsymbol{\sigma})$
value: $1 + d$₿

$\mathsf{Win}(\epsilon, a)$ (root)
certifies that a has won the lottery

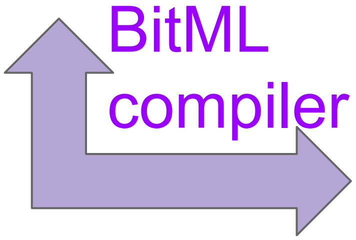
(Variants as for $\mathsf{Win}(\pi, a)$)

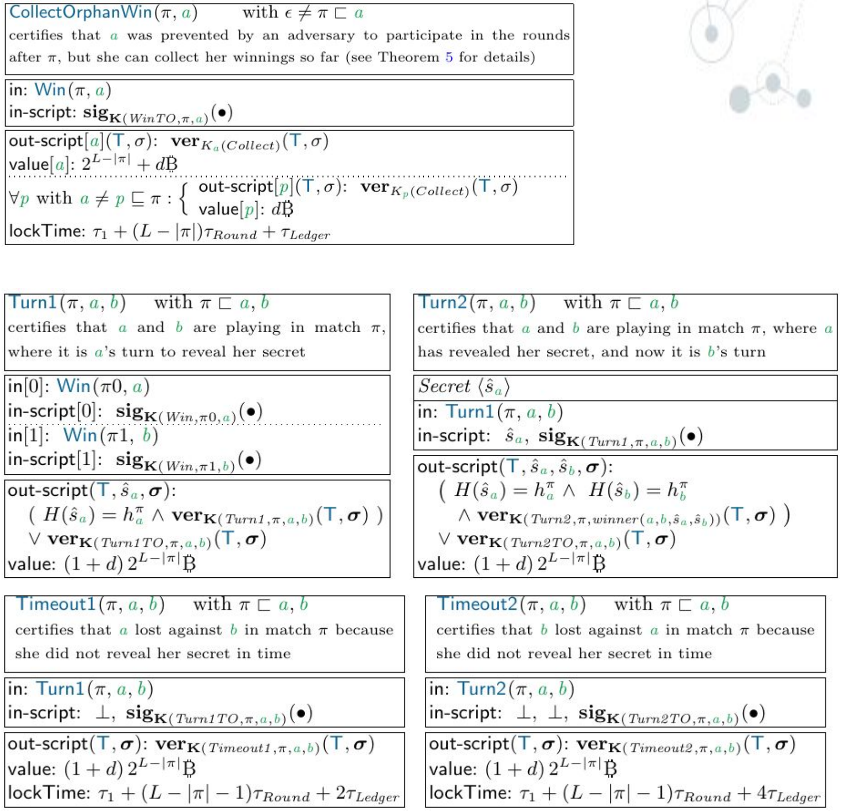
out-script$[a](\mathsf{T}, \sigma)$: $\mathbf{ver}_{K_a(\mathit{Collect})}(\mathsf{T}, \sigma)$
value$[a]$: $N + d$₿

$\forall p \neq a : \begin{cases} \text{out-script}[p](\mathsf{T}, \sigma)\text{: } \mathbf{ver}_{K_p(\mathit{Collect})}(\mathsf{T}, \sigma) \\ \text{value}[p]\text{: } d\text{₿} \end{cases}$

$$
\begin{aligned}
&\text{init } \{ A : 1\text{₿}, \text{secret } a \\
&\qquad B : 1\text{₿}, \text{secret } b \}
\end{aligned}
$$

$$
\begin{aligned}
&(\text{reveal } a. \\
&\quad (\text{ reveal } b.\ \text{if}(a + b)\%2 = 0 \\
&\qquad\qquad \text{then withdraw } A \\
&\qquad\qquad \text{else withdraw } B \\
&\quad + \text{after } 2 \cdot \mathrm{t} :\ \text{withdraw } A) \\
&+ \text{after } \mathrm{t} :\ \text{withdraw } B)
\end{aligned}
$$





$\mathsf{CollectOrphanWin}(\pi, a)$ with $\epsilon \neq \pi \sqsubset a$
certifies that a was prevented by an adversary to participate in the rounds after π, but she can collect her winnings so far (see Theorem 5 for details)

in: $\mathsf{Win}(\pi, a)$
in-script: $\mathbf{sig}_{\mathbf{K}(\mathit{WinTO}, \pi, a)}(\bullet)$

out-script$[a](\mathsf{T}, \sigma)$: $\mathbf{ver}_{K_a(\mathit{Collect})}(\mathsf{T}, \sigma)$
value$[a]$: $2^{L - |\pi|} + d$₿

$\forall p \text{ with } a \neq p \sqsubseteq \pi : \begin{cases} \text{out-script}[p](\mathsf{T}, \sigma)\text{: } \mathbf{ver}_{K_p(\mathit{Collect})}(\mathsf{T}, \sigma) \\ \text{value}[p]\text{: } d\text{₿} \end{cases}$

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

$\mathsf{Turn1}(\pi, a, b)$ with $\pi \sqsubset a, b$
certifies that a and b are playing in match π, where it is a's turn to reveal her secret

in[0]: $\mathsf{Win}(\pi 0, a)$
in-script[0]: $\mathbf{sig}_{\mathbf{K}(\mathit{Win}, \pi 0, a)}(\bullet)$
in[1]: $\mathsf{Win}(\pi 1, b)$
in-script[1]: $\mathbf{sig}_{\mathbf{K}(\mathit{Win}, \pi 1, b)}(\bullet)$

out-script$(\mathsf{T}, \hat{s}_a, \boldsymbol{\sigma})$:
$(\ H(\hat{s}_a) = h_a^\pi \wedge \mathbf{ver}_{\mathbf{K}(\mathit{Turn1}, \pi, a, b)}(\mathsf{T}, \boldsymbol{\sigma})\ )$
$\vee\, \mathbf{ver}_{\mathbf{K}(\mathit{Turn1TO}, \pi, a, b)}(\mathsf{T}, \boldsymbol{\sigma})$
value: $(1 + d)\, 2^{L - |\pi|}$₿

$\mathsf{Turn2}(\pi, a, b)$ with $\pi \sqsubset a, b$
certifies that a and b are playing in match π, where a has revealed her secret, and now it is b's turn

Secret $\langle \hat{s}_a \rangle$
in: $\mathsf{Turn1}(\pi, a, b)$
in-script: $\hat{s}_a$, $\mathbf{sig}_{\mathbf{K}(\mathit{Turn1}, \pi, a, b)}(\bullet)$

out-script$(\mathsf{T}, \hat{s}_a, \hat{s}_b, \boldsymbol{\sigma})$:
$(\ H(\hat{s}_a) = h_a^\pi \wedge\ H(\hat{s}_b) = h_b^\pi$
$\wedge\, \mathbf{ver}_{\mathbf{K}(\mathit{Turn2}, \pi, \mathit{winner}(a, b, \hat{s}_a, \hat{s}_b))}(\mathsf{T}, \boldsymbol{\sigma})\ )$
$\vee\, \mathbf{ver}_{\mathbf{K}(\mathit{Turn2TO}, \pi, a, b)}(\mathsf{T}, \boldsymbol{\sigma})$
value: $(1 + d)\, 2^{L - |\pi|}$₿

$\mathsf{Timeout1}(\pi, a, b)$ with $\pi \sqsubset a, b$
certifies that a lost against b in match π because she did not reveal her secret in time

in: $\mathsf{Turn1}(\pi, a, b)$
in-script: $\perp$, $\mathbf{sig}_{\mathbf{K}(\mathit{Turn1TO}, \pi, a, b)}(\bullet)$

out-script$(\mathsf{T}, \boldsymbol{\sigma})$: $\mathbf{ver}_{\mathbf{K}(\mathit{Timeout1}, \pi, a, b)}(\mathsf{T}, \boldsymbol{\sigma})$
value: $(1 + d)\, 2^{L - |\pi|}$₿
lockTime: $\tau_1 + (L - |\pi| - 1)\tau_{\mathit{Round}} + 2\tau_{\mathit{Ledger}}$

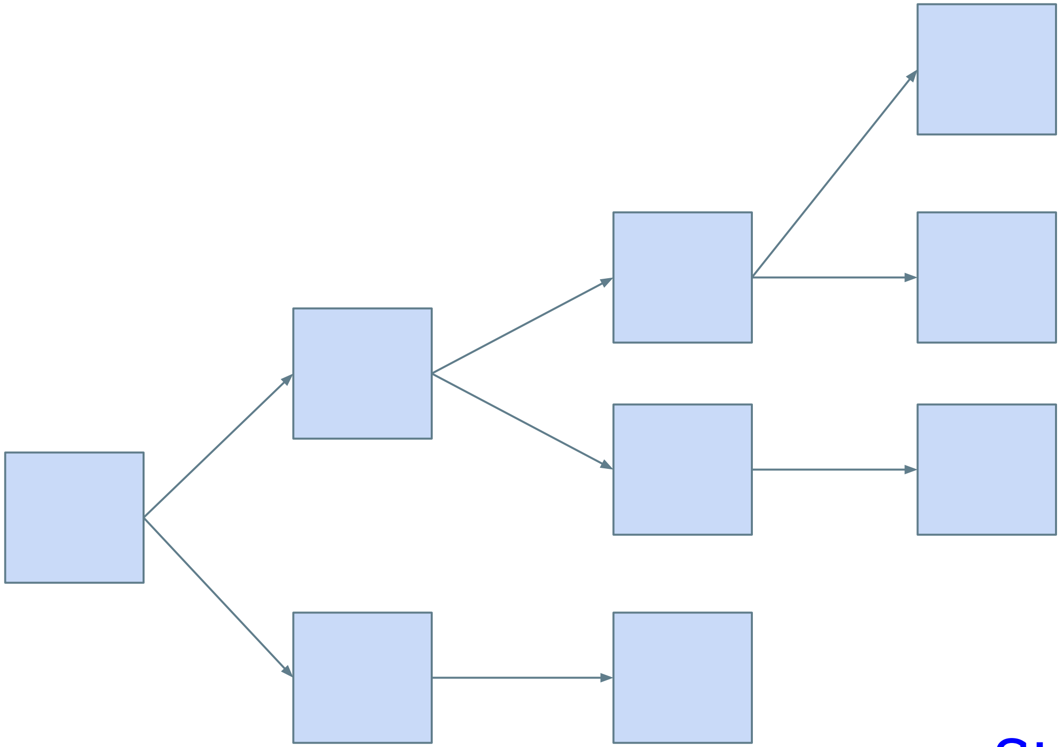
$\mathsf{Timeout2}(\pi, a, b)$ with $\pi \sqsubset a, b$
certifies that b lost against a in match π because she did not reveal her secret in time

in: $\mathsf{Turn2}(\pi, a, b)$
in-script: $\perp$, $\perp$, $\mathbf{sig}_{\mathbf{K}(\mathit{Turn2TO}, \pi, a, b)}(\bullet)$

out-script$(\mathsf{T}, \boldsymbol{\sigma})$: $\mathbf{ver}_{\mathbf{K}(\mathit{Timeout2}, \pi, a, b)}(\mathsf{T}, \boldsymbol{\sigma})$
value: $(1 + d)\, 2^{L - |\pi|}$₿
lockTime: $\tau_1 + (L - |\pi| - 1)\tau_{\mathit{Round}} + 4\tau_{\mathit{Ledger}}$

- Transition system semantics
- Computational soundness
- Toolchain (development & verification)

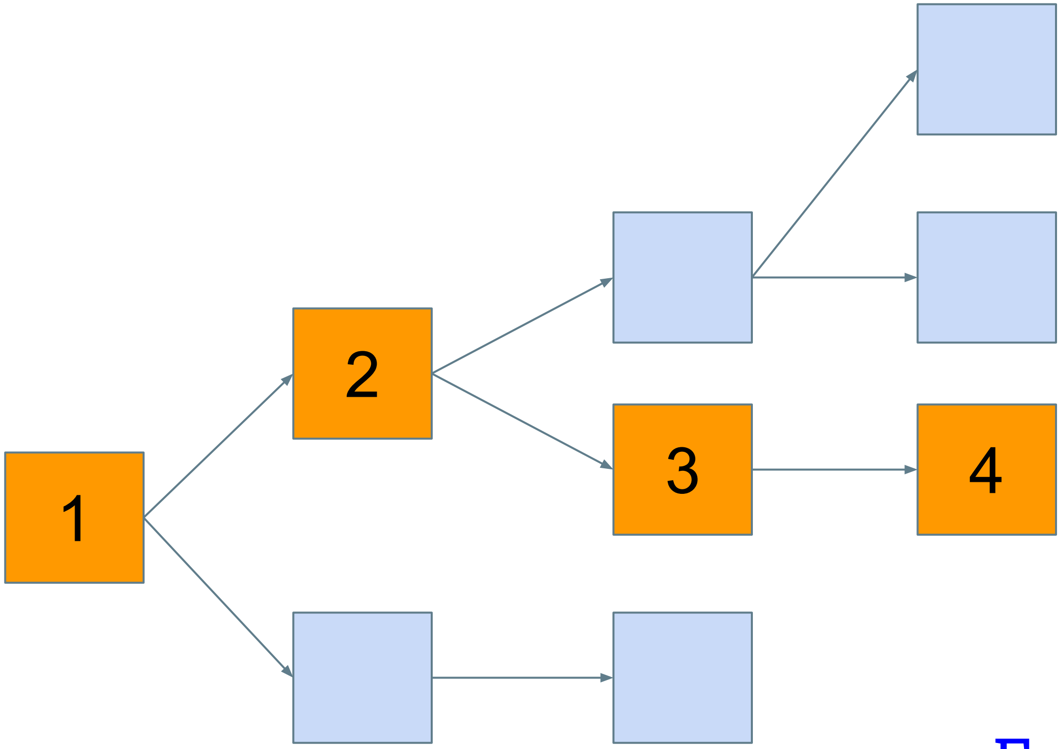
BitML implementation (oversimplification)



Stipulation

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

BitML implementation (oversimplification)



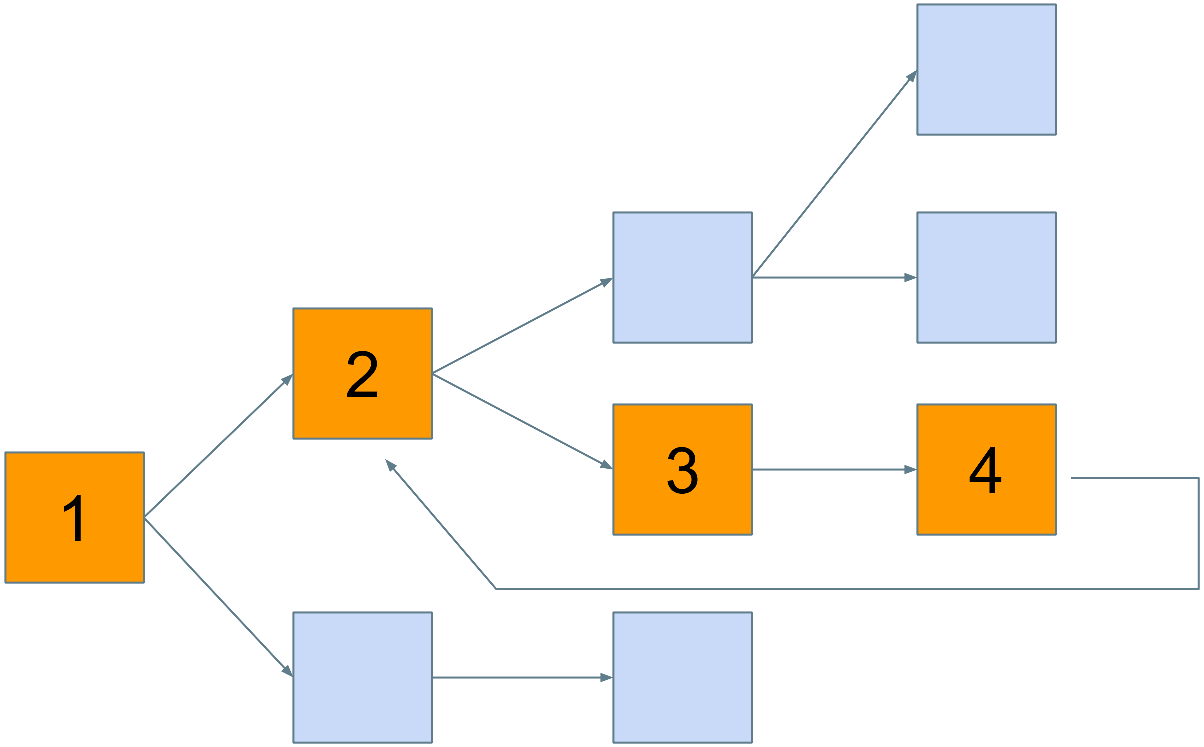
Execution

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

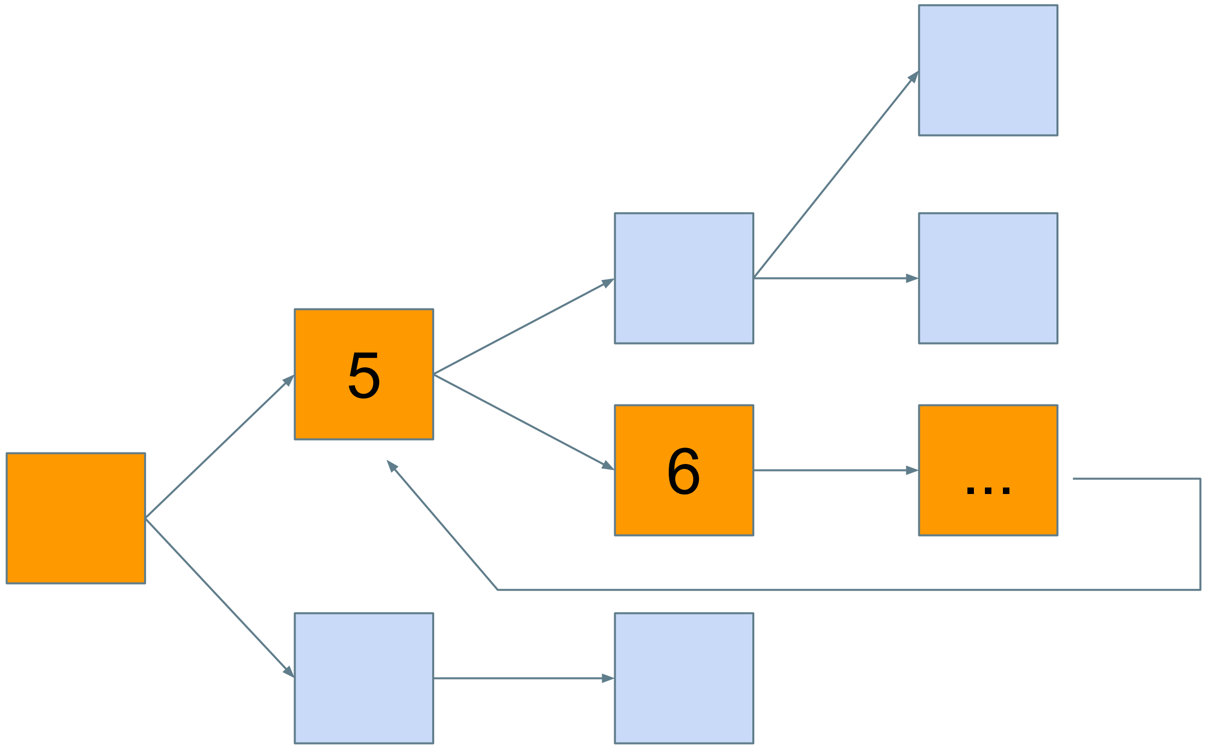
Work in progress

Recursion

BitML recursion



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

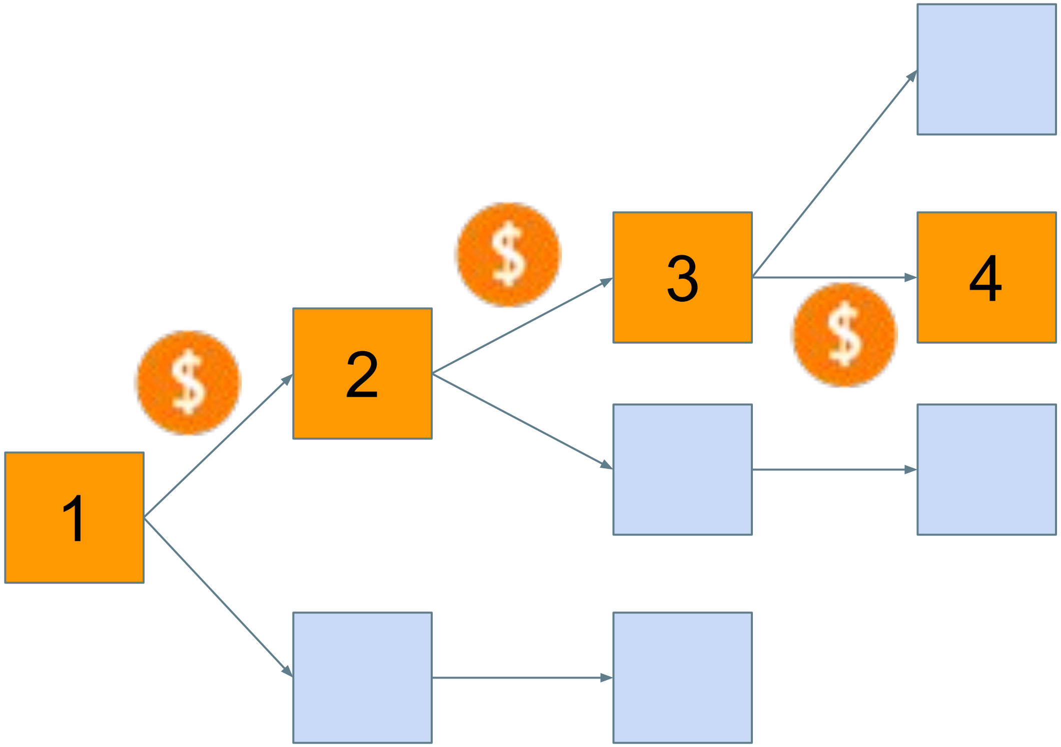
Flavours of Recursion

- Consensual recursion
  - All participants must agree to recurse at execution-time
  - Compilation to Bitcoin still possible
- Non-consensual recursion
  - After stipulation, participants can not prevent it
  - Requires some extensions of Bitcoin

Work in progress

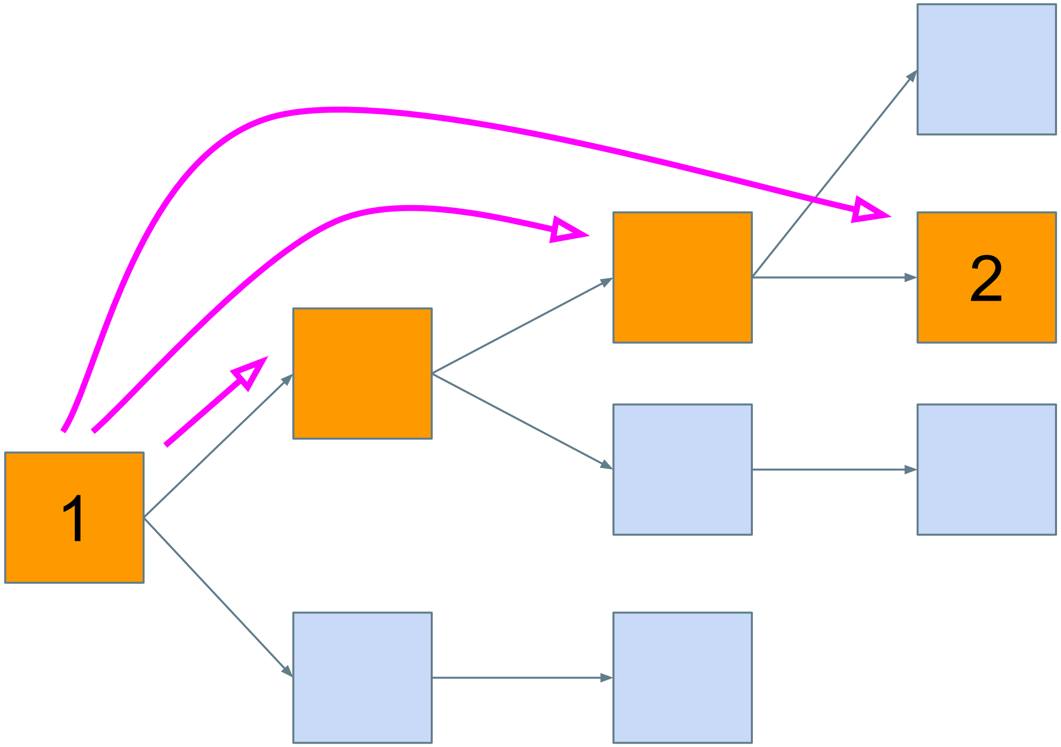
"Layer 2” BitML

BitML as is



Tx fees paid at each step

Off-chain "long jumps"



Executing BitML off-chain?

- Optimize for cooperating agents
- Protect from malicious ones
- Off-chain "long jump" signatures save fees

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