Sponsored Fair Exchange

Serge Vaudenay

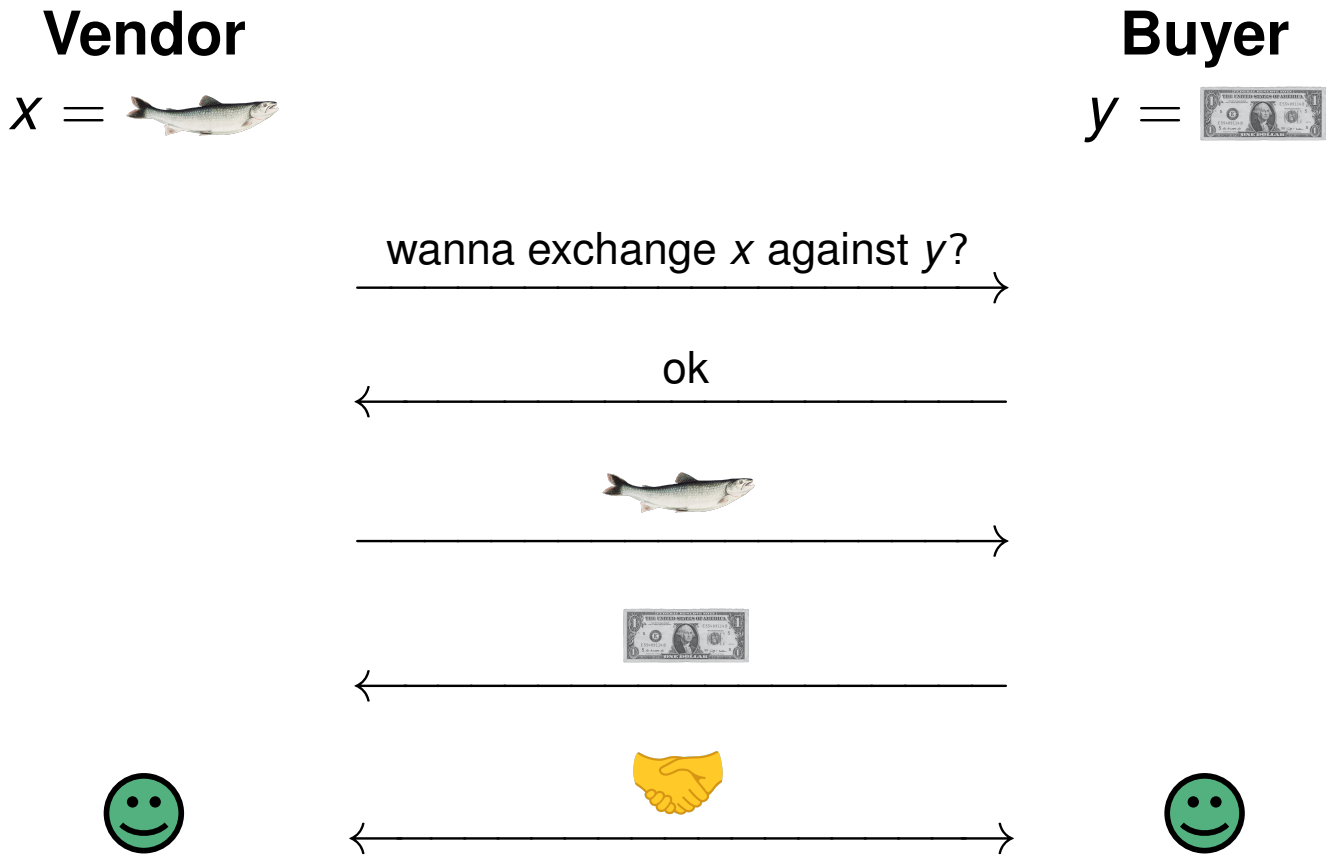
EPFL

in cooperation with

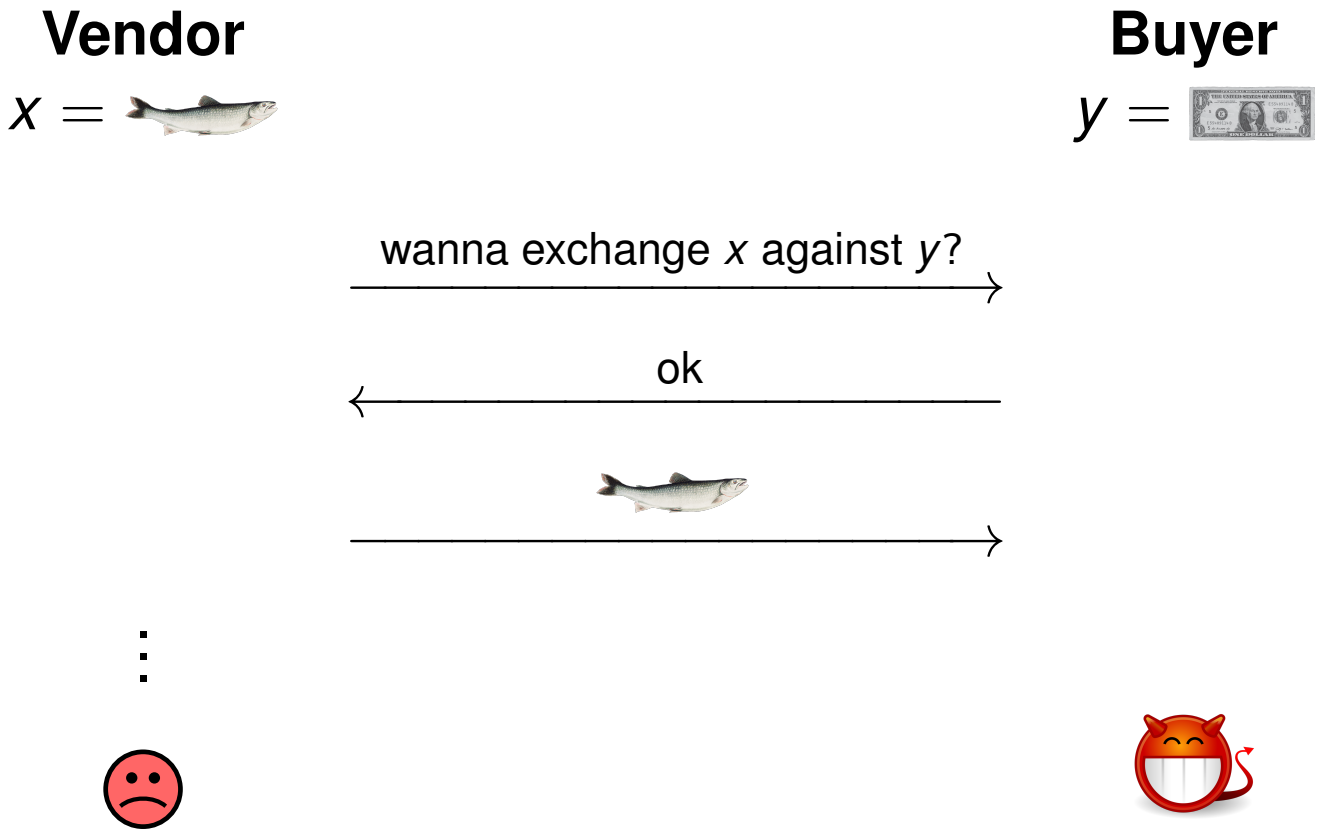
CIMA.SCIENCE
Powering The Edge

LASEC

The Problem of Fair Exchange



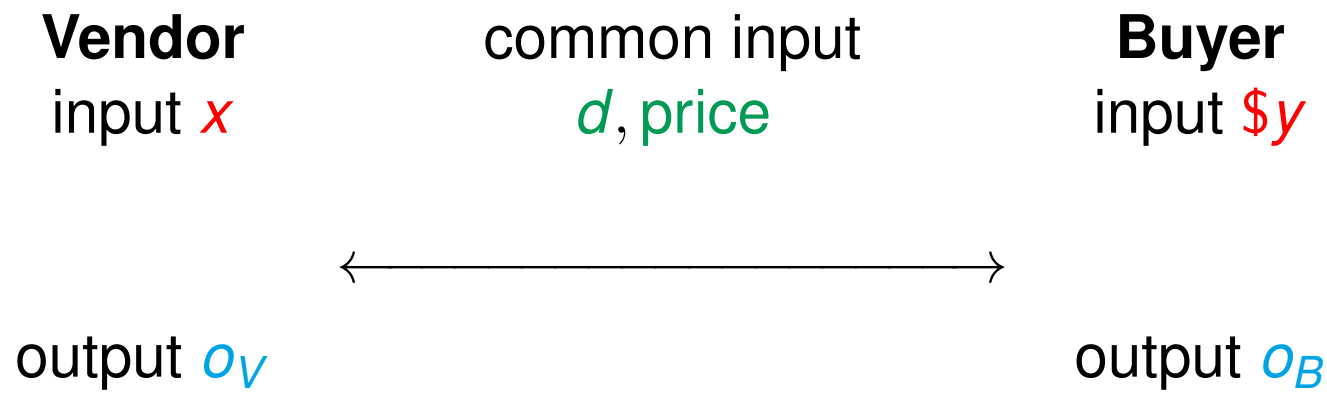
The Problem of Fair Exchange



Applications

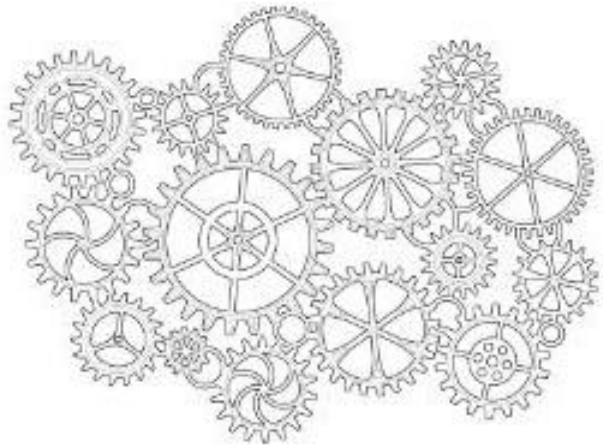
- **commerce** → good against payment
- **certified email** → mail against receipt
- **contract signing** → signature against signature
- . . .
- in this talk: **knowledge-coin fair exchange**

Knowledge-Coin Fair Exchange



- **timeliness**: every honest participant eventually terminates
- **effectiveness**: if V and B are honest, then
  $(d = \text{desc}(x) \wedge \text{price} = \text{num}(\$y)) \Rightarrow (o_V = \$y \wedge o_B = x)$
  and $(d \neq \text{desc}(x) \vee \text{price} \neq \text{num}(\$y)) \Rightarrow (o_V = o_B = \perp)$
- **fairness**:
  (honest V) either "no leakage" on x or $\text{num}(o_V) = \text{price}$
  (honest B) either "no loss" on $\$y$ or $\text{desc}(o_B) = d$
- \+ **privacy**: (honest V and B) "no leakage" on x

Smart Contracts as TTP



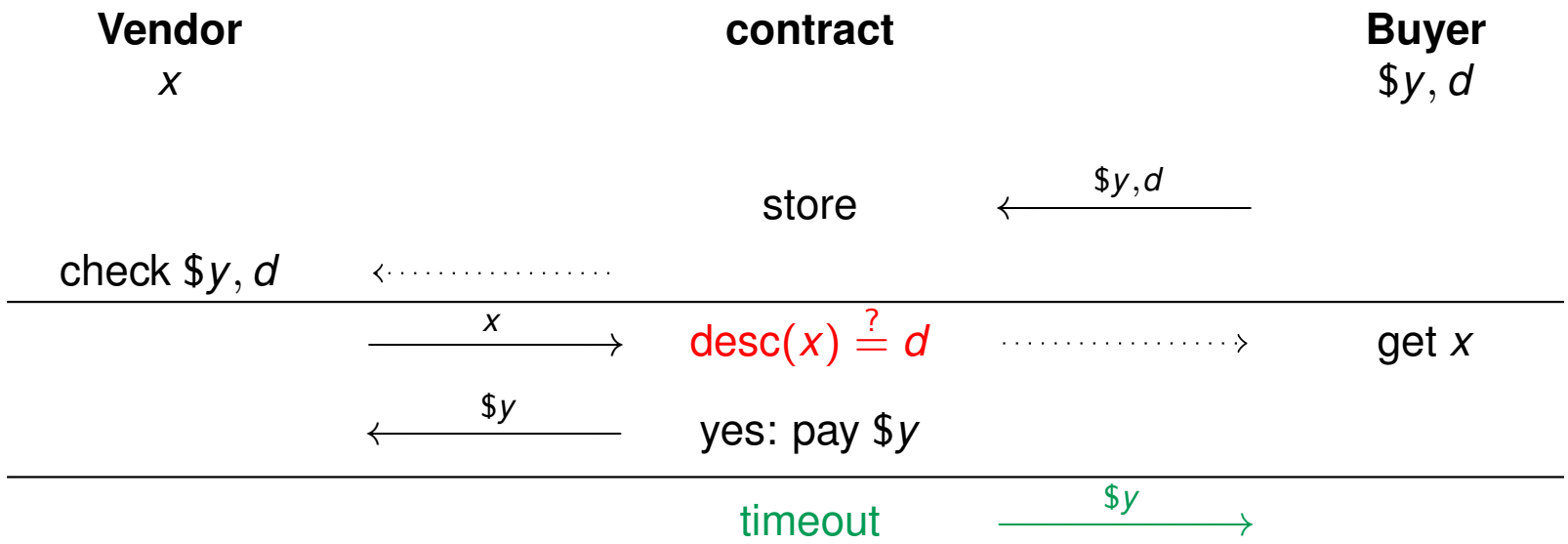
smart contracts:

- complexity measured in gas (slow + expensive platform)
- immutable (trusted)
- fully transparent

offloading necessary

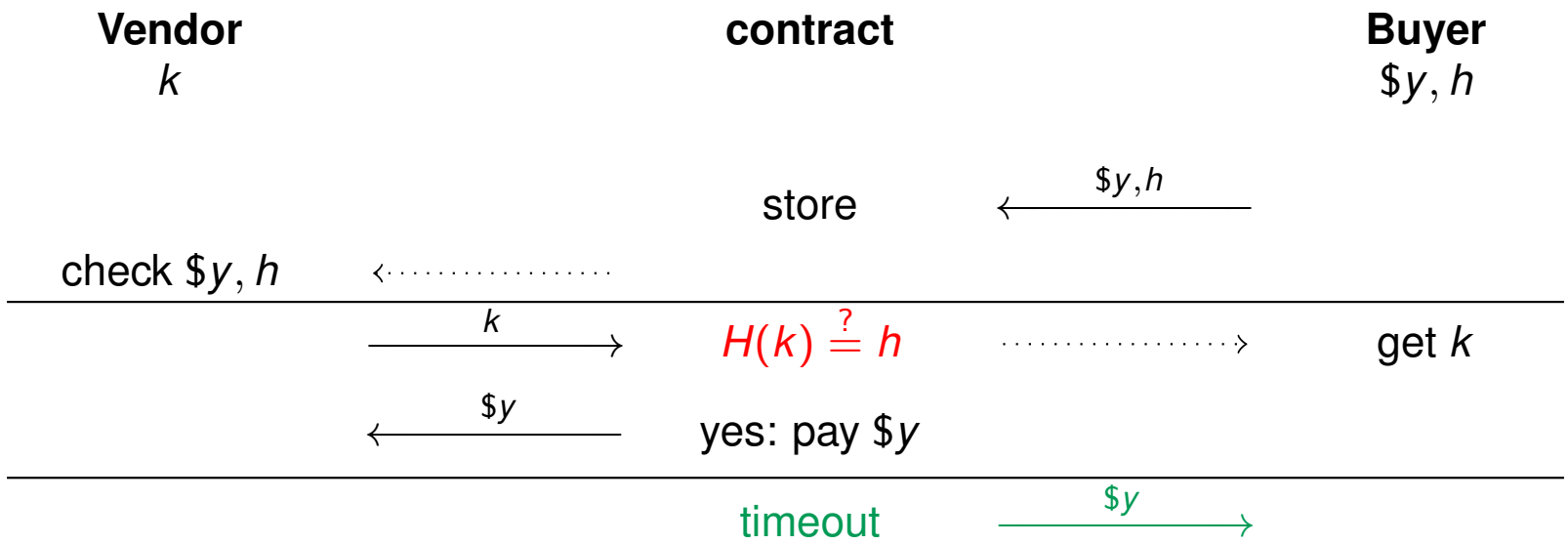
leaking

Fair Exchange based on Smart Contract



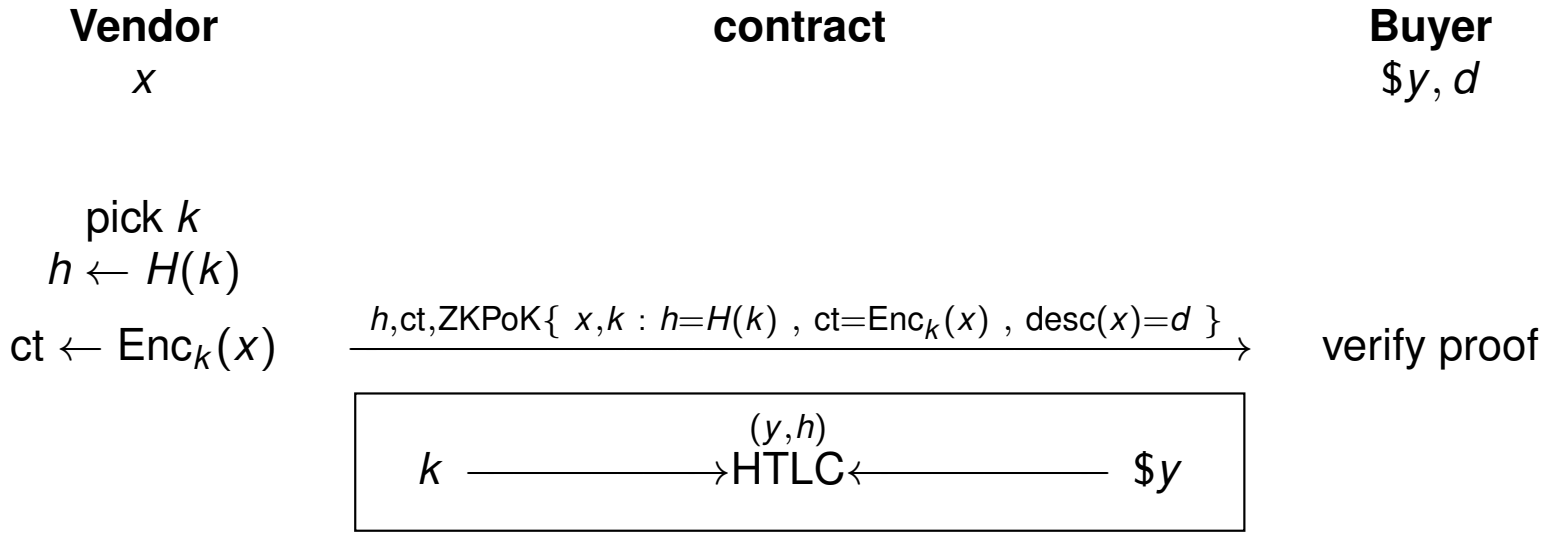
- ☺ **security**: it solves the problem!
- ☹ **complexity**: gas cost if x is large or desc is complicated
- ☹ **privacy**: everyone sees x

HTLC: Hash Time-Locked Contract



- ☺ **security**: it solves the problem (for desc $= H$)!
- ☺ **complexity**: low gas cost
- ☹ **privacy**: everyone sees k

ZKCP: Zero-Knowledge Contingent Payment



- ☺ **security**: it solves the problem!
- ☹ **complexity**: low gas cost but heavy ZK proof
- ☺ **privacy**: *x* remains private

Latest ZKCP Evolutions

- Atomic and Fair Data Exchange via Blockchain
  Tas-Seres-Zhang-Melczer-Kelkar-Bonneau-Nikolaenko [CCS 2024]
  `https://doi.org/10.1145/3658644.3690248`
  → specialized desc (KZG), for small x
- Decentralized Fair Exchange with Advertising
  Della Monica-Visconti-Vitaletti-Zecchini [CANS 2025]
  `https://doi.org/10.1007/978-981-95-4434-9_17`
  → specialized desc (img shrink), for small images
- Plaintext-Scale Fair Data Exchange
  Khabbazian [FC 2026] (to appear)
  arXiv: `https://doi.org/10.48550/arXiv.2506.14944`
  → specialized desc (KZG)

1 The Optimistic Approach

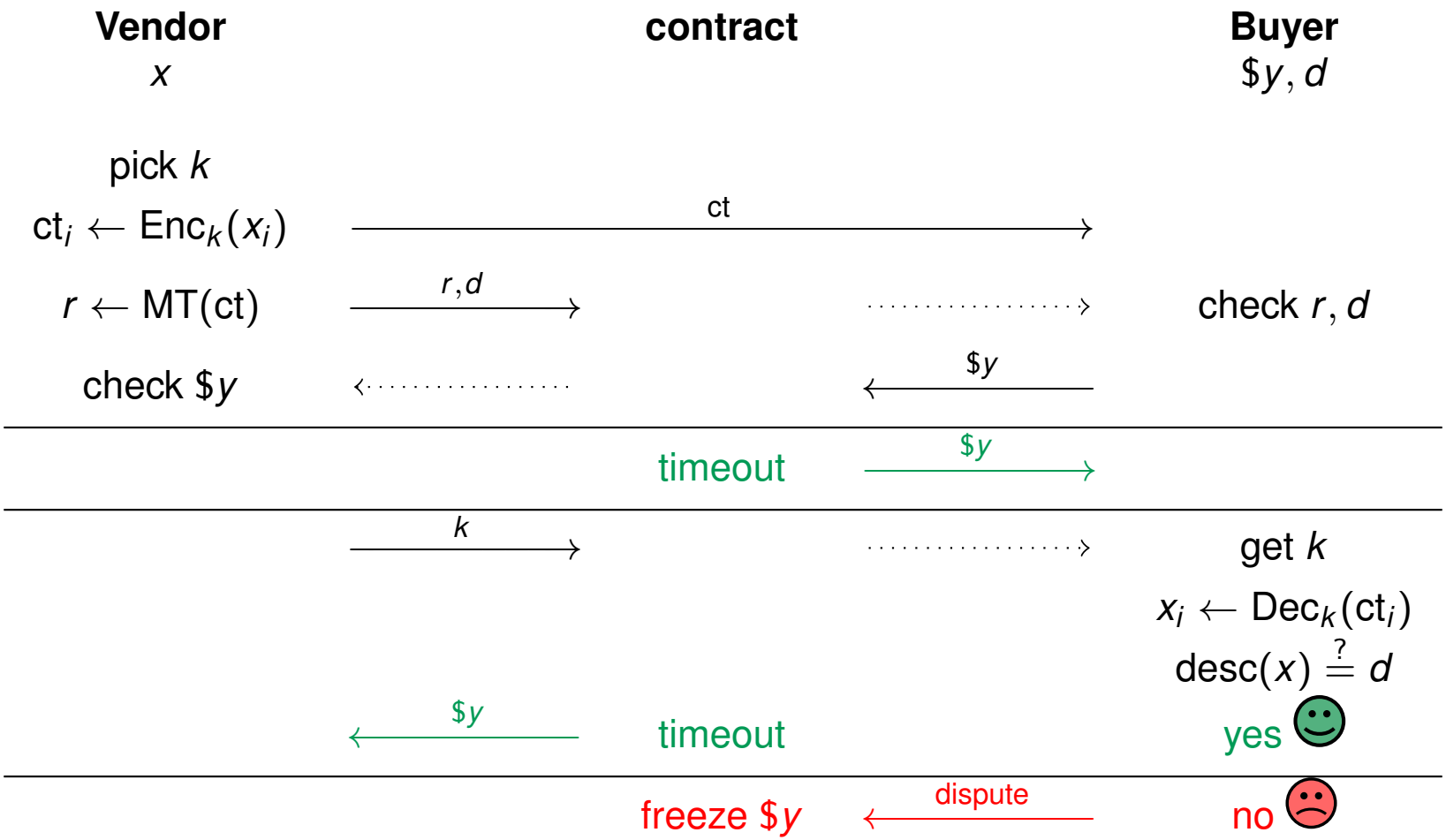
2 SOX Simplified

3 SOX: Sponsored Fair Exchange

OptiSwap

OptiSwap: Fast Optimistic Fair Exchange

Eckey-Faust-Schlosser [CCS 2020, https://doi.org/10.1145/3320269.3384749]

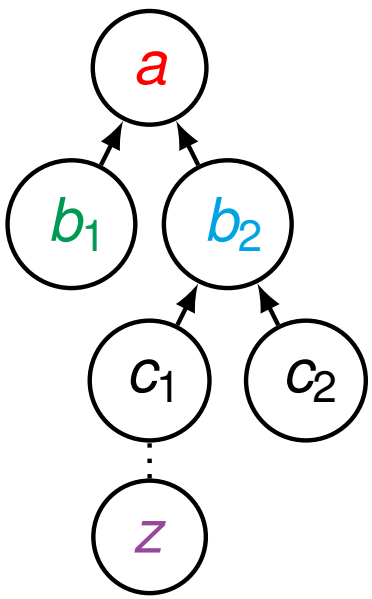


Interactive Dispute Resolution in OptiSwap

Vendor	**Smart Contract**	**Buyer**
(claim: $\text{val}(a) = d$)		(claim: $\text{val}(a) \neq d$)
$\xrightarrow{\text{claim:val}(b_1),\text{val}(b_2)}$	$\text{val}(a) \stackrel{?}{=} g_a(\text{val}(b_1), \text{val}(b_2))$	$\xleftarrow{\text{claim: val}(b_2)\text{ incorrect}}$

iterate until we reach a leaf of disagreement

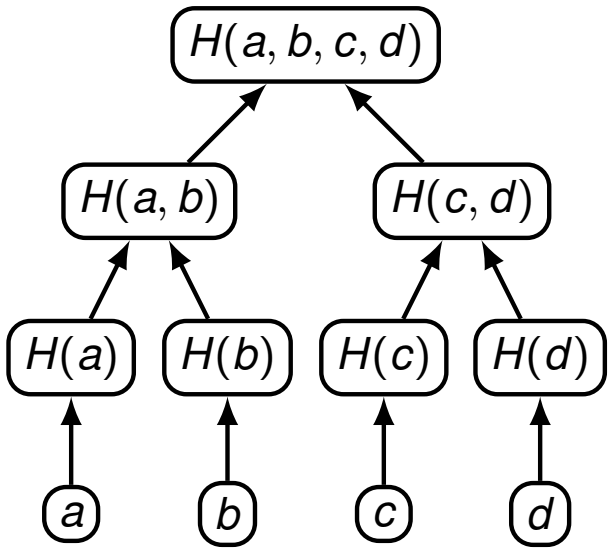
(claim: $\text{val}(z) = v$)		(claim: $\text{val}(z) \neq v$)
$\xrightarrow{\text{ct}_i + \text{proof}}$	verify proof	
	$v \stackrel{?}{=} \text{Dec}_k(\text{ct}_i)$	
	Vendor wins	



$\mathcal{O}$(depth of circuit) complexity

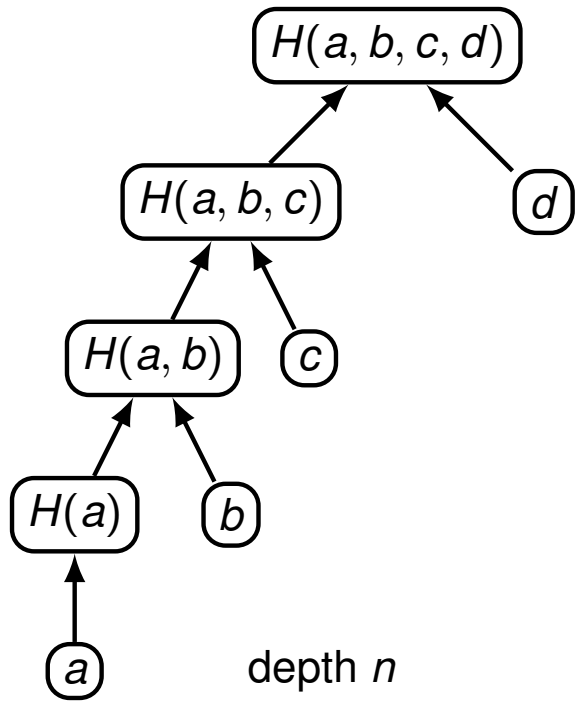
Some Typical Circuits

Merkle Hash



depth $1 + \log(n)$

SHA256



depth n

1 The Optimistic Approach

2 SOX Simplified

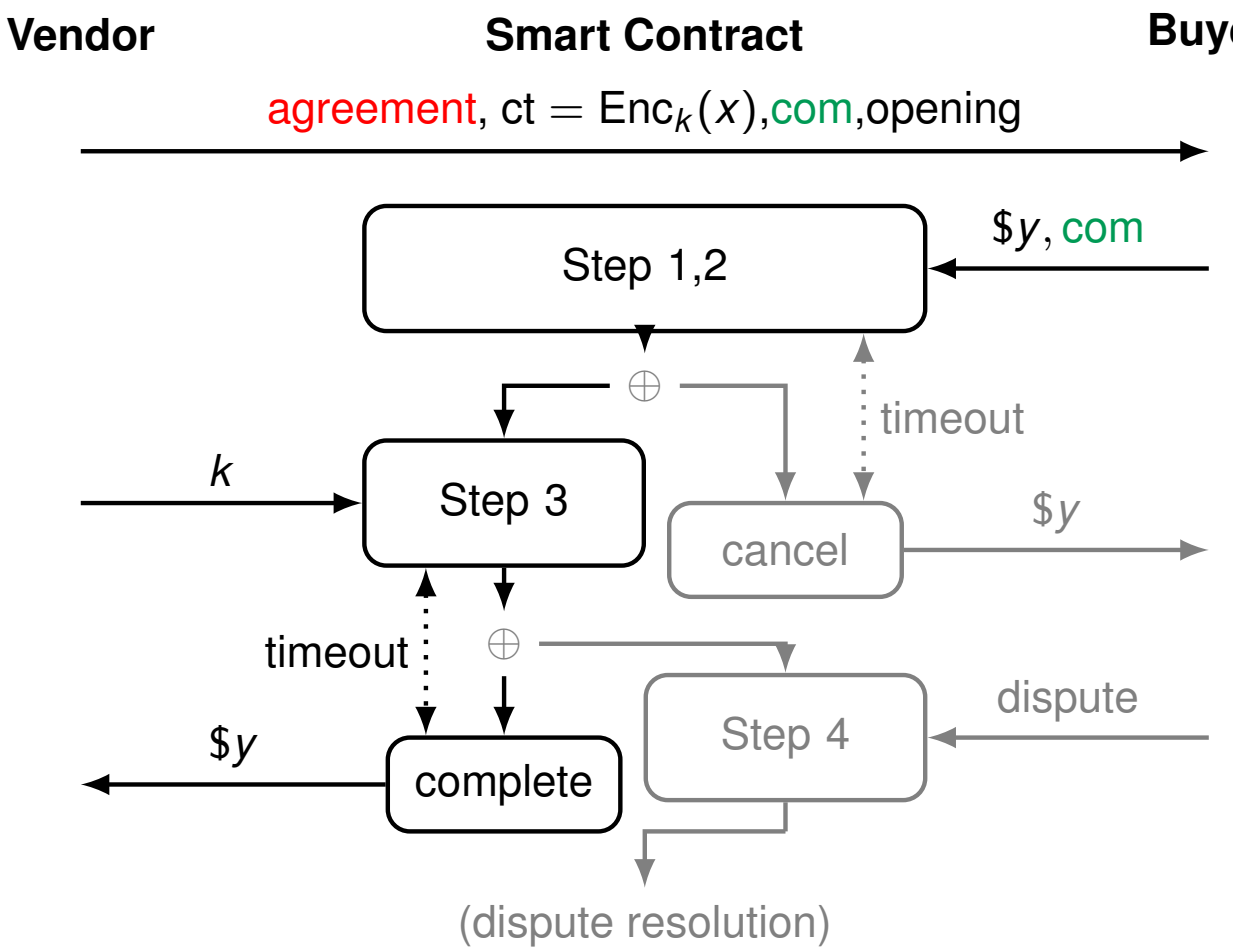
3 SOX: Sponsored Fair Exchange

What we Achieved

SOX = Sponsored Optimistic Xchange

- knowledge-coin fair exchange
- optimistic (better dispute: universal + logarithmic)
- with sponsors to favor economic inclusion

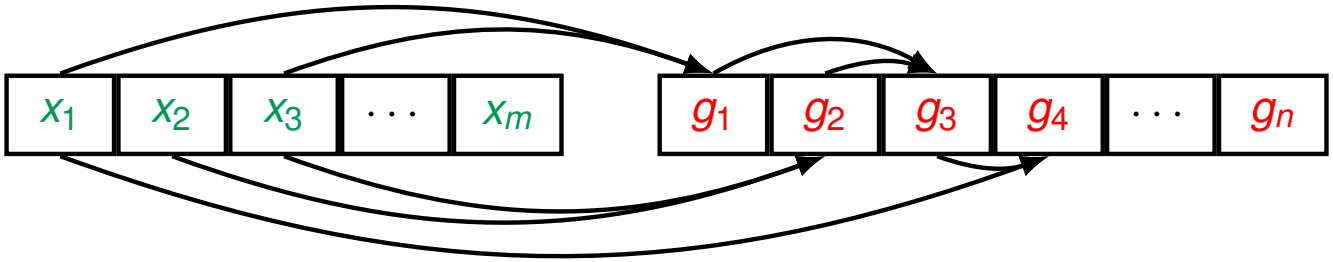
SOX Simplified



agreement: includes the circuit for $\mathsf{desc}(\cdot) \stackrel{?}{=} d$, the value of $y

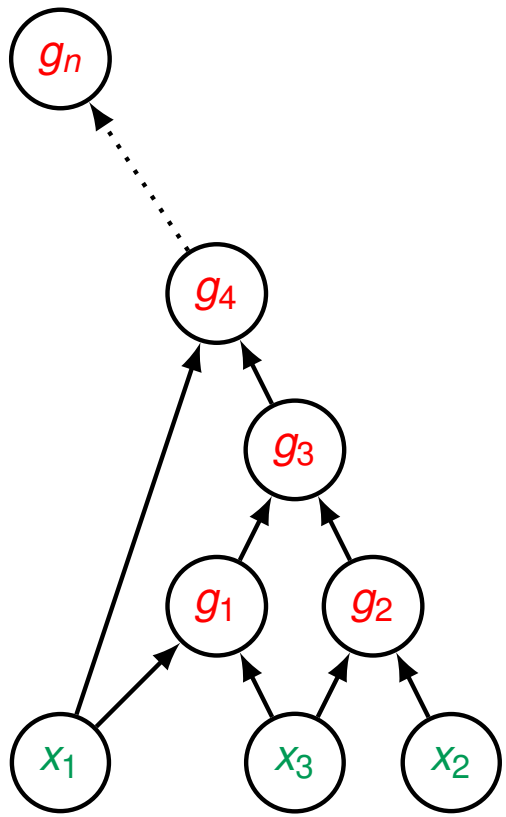
com: binds to h_{circuit} and h_{ct} (Merkle hash)

SOX Dispute



$w_i = \mathrm{IncAcc}(\mathrm{val}(g_1), \ldots, \mathrm{val}(g_i))$

Vendor	**Smart Contract**	**Buyer**
	(agree on w_0, disagree on w_n)	
		claim:$w_{n/2}$ ←
disagree →		
		claim:$w_{n/4}$ ←
agree →		
	⋮	claim:$w_{3n/8}$ ←
	(agree on w_{i-1}, disagree on w_i)	
proof →	verify proof	



$\mathcal{O}(\log n)$ complexity

SOX: Performance

protocol	desc	large x	onchain comp	offchain comp
FDE	KZG	☹	☺	☹
DVVZ	shrink	☹	☺	☹
K-FDE	KZG	☺	☺	☺
OptiSwap	balanced	☺	☺	☺
SOX	any	☺	☺	☺

1 The Optimistic Approach

2 SOX Simplified

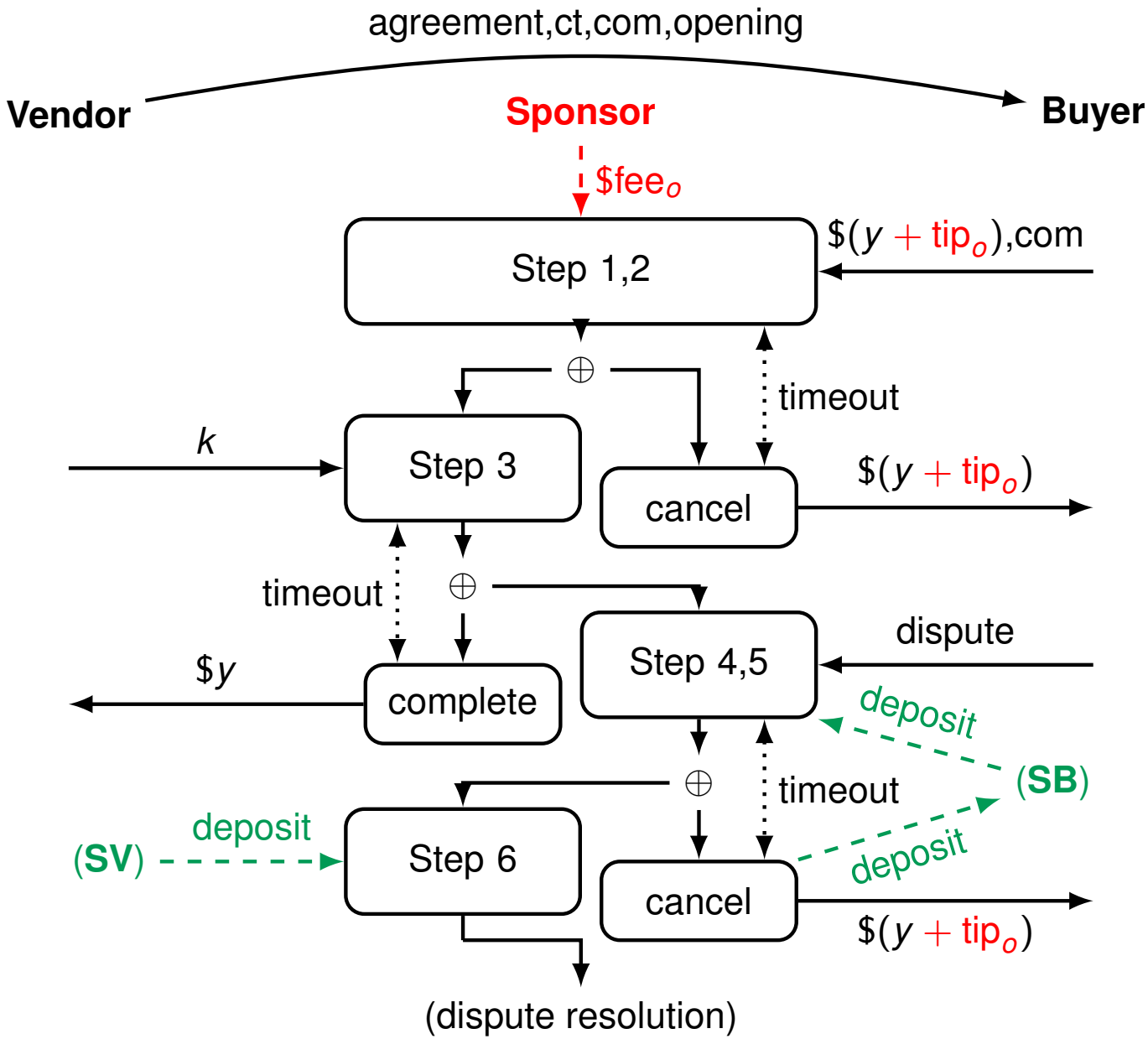
3 **SOX: Sponsored Fair Exchange**

Sponsors

V should not pay any fees
B should pay fees only if the transaction succeeds

- **optimistic sponsor** (taking risks):
  pays for blockchain fees during the optimistic transaction
  gets a reward when the exchange completes
- **dispute sponsor** for V/B (riskless):
  pays for blockchain fees during dispute
  gets a reward when V/B wins (winner-takes-all)
- 5 participants: V, B, S, SV, SB
  SV and SB appointed only if B triggers the dispute

Adding Sponsors



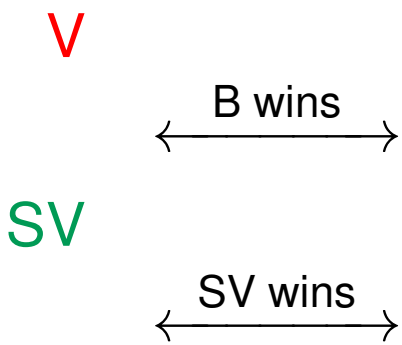
(show argument to find dispute sponsors)

Dispute Theaters

Theorem

A honest participant never loses in a dispute resolution.

- what if dispute is run by two malicious participants?
- malicious V, B
- honest SV (V with good argument)

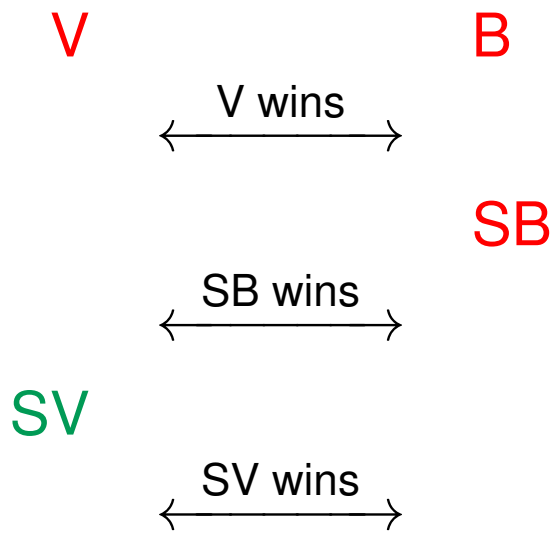


☹ SV loses money

- if a sponsor loses, they can restart a dispute by taking the role of their participant

Double Challenge

- malicious V, B, SB
- honest SV (V with good argument)



☹ SV loses money

- if a sponsor loses after a first challenge flipped the outcome, they can restart a dispute by taking the role of their participant
- note: a honest participant cannot be replaced in a challenge
- fairness for all after running the dispute up to 3 times

Conclusion

- knowledge-coin fair Xchange is solved with smart contracts
- SOX works for any description function
- sponsors for economic inclusion

`https://eprint.iacr.org/2026/904`