CLOAK: Transitioning States on Legacy Blockchains Using Secure and Publicly Verifiable Off-Chain Multi-Party Computation

Qian Ren, Yingjun Wu, Han Liu, Anne Victor, Hong Lei, Lei Wang, Bangdao Chen

SSC

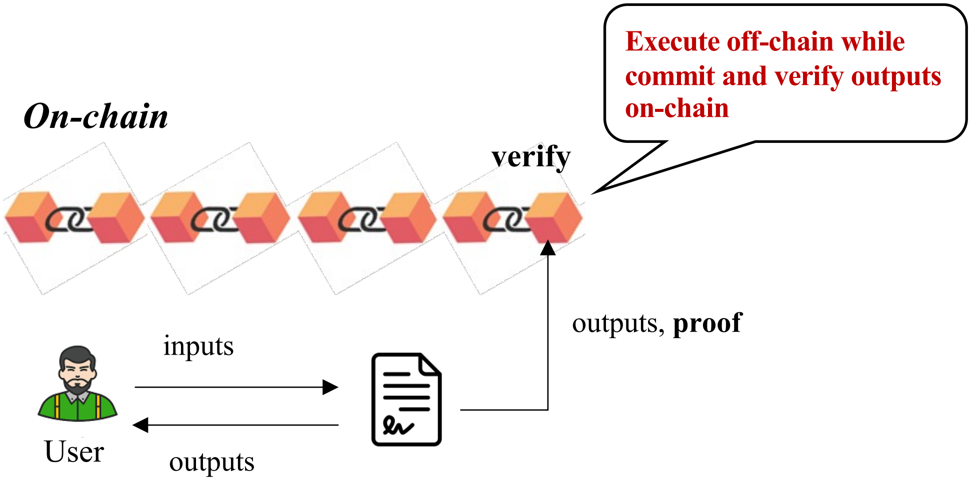
Oxford-Hainan Blockchain Research Institute

清華大學 Tsinghua University

海南大学 Hainan University

上海交通大學 Shanghai Jiao Tong University

Background: Confidential smart contract

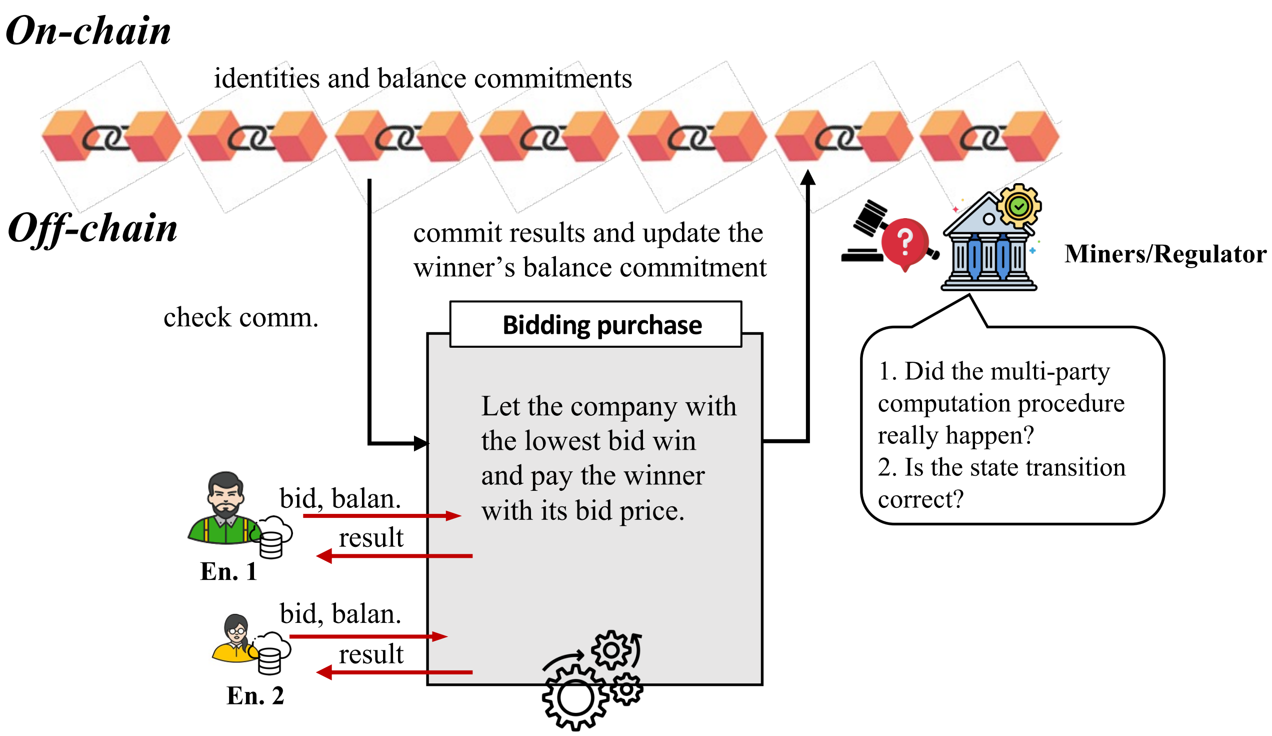


Confidential smart contract

Pros:

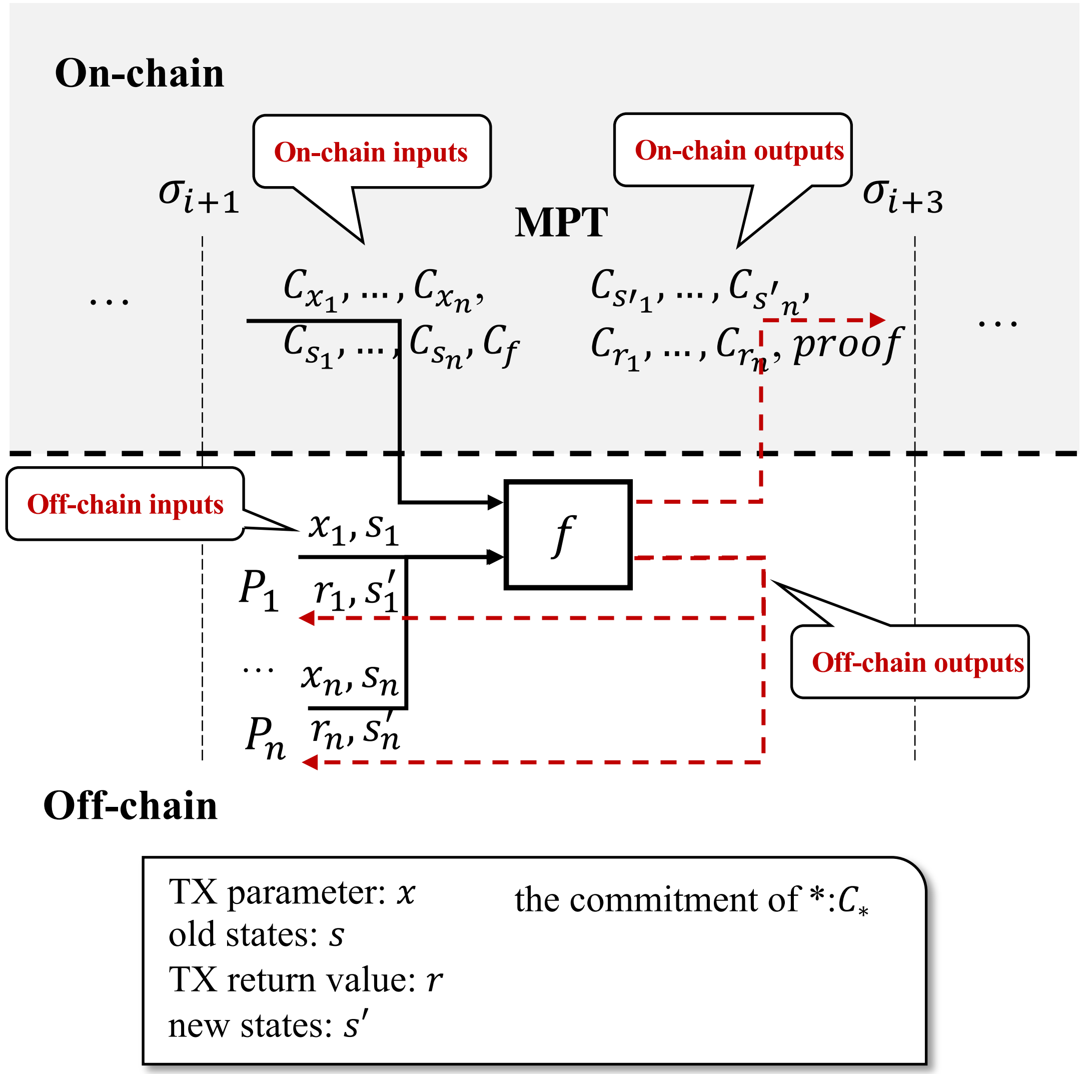
- **Better confidentiality:** Private inputs are handled off-chain and are not public to all nodes.
- **Better scalability:** With the proof, all nodes can validate the correctness of the transaction outputs without re-executing it

Motivating example: Blockchain + Supply chain finance



Transferring money on-chain by multi-party bidding purchase off-chain

Problem definition: Multi-party Transaction



Multi-party Transaction (MPT)

- **Confidentiality**: An MPT requires secret inputs and states owned by different parties. All secrets should keep private to their owners.
- **Public Verifiability**: All nodes can verify the result and new state

Limitations of current solutions

Cryptography-based solutions: [CCS’19, SP20, Security’22]

- Cannot support MPC
- Suffer on inefficiency, less public verifiability, or generality of MPC
- Suffer on poor toolchain and error-prone implementation of MPC+ZKP
- Require O(n) transactions to secure off-chain MPC
- …

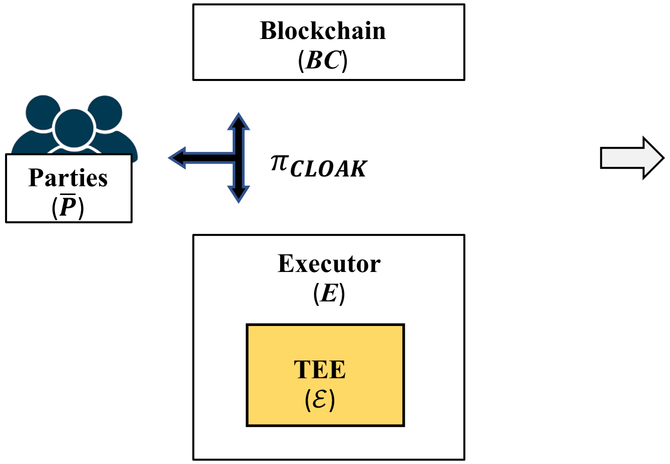
TEE-based solutions [SP16, EUROS&P19]

- Start with specified MPC settings, without considering the trusted negotiation needed by parties.
- Lack of security guarantees for off-chain interactions
- Require O(n) transactions to secure off-chain MPC
- …

Existing solutions for confidential smart contracts can hardly fit the need of MPT

System model and goals

System model



System goals

- **Confidentiality**: An MPT requires secret inputs and states owned by different parties. All secrets should keep private to their owners.
- **Public Verifiability**: All nodes could verify the result and new state
- **Executor balance security**: The honest executor will never lose its deposit.
- **Financial Fairness**: Honest parties should never lose their deposits.

Challenges and countermeasures

Challenges

Byzantine resistance with O(1) cost

Necessitate a low-cost punishment mechanism

Efficient nondeterministic negotiation

Parties negotiate without knowing each other a priori

Secure off-chain interactions

Identify and punish off-chain misbehaviors

Publicly verifiable proof

Non-participants (e.g., Miners) can verify MPTs

Countermeasures

Deposit once, transact multi-times

Nondeterministic negotiation subprotocol

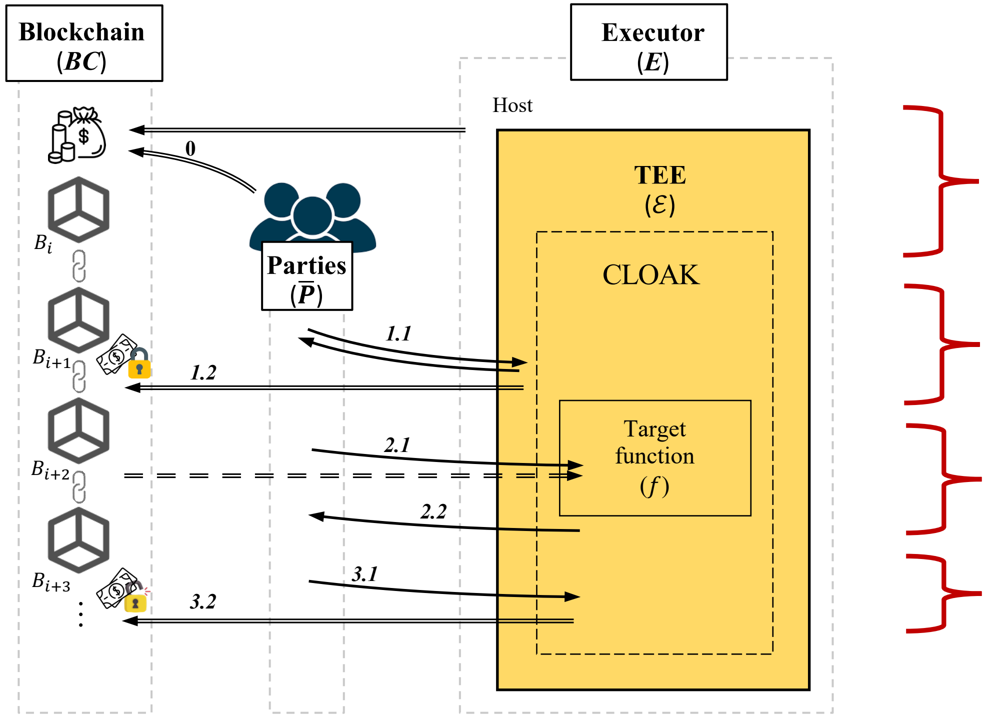
Negotiate off-chain, settle on-chain

Improved challenge-response mechanisms

Challenge-response submission (resp. delivery)

TEE-based universal succinct proof

Protocol overview



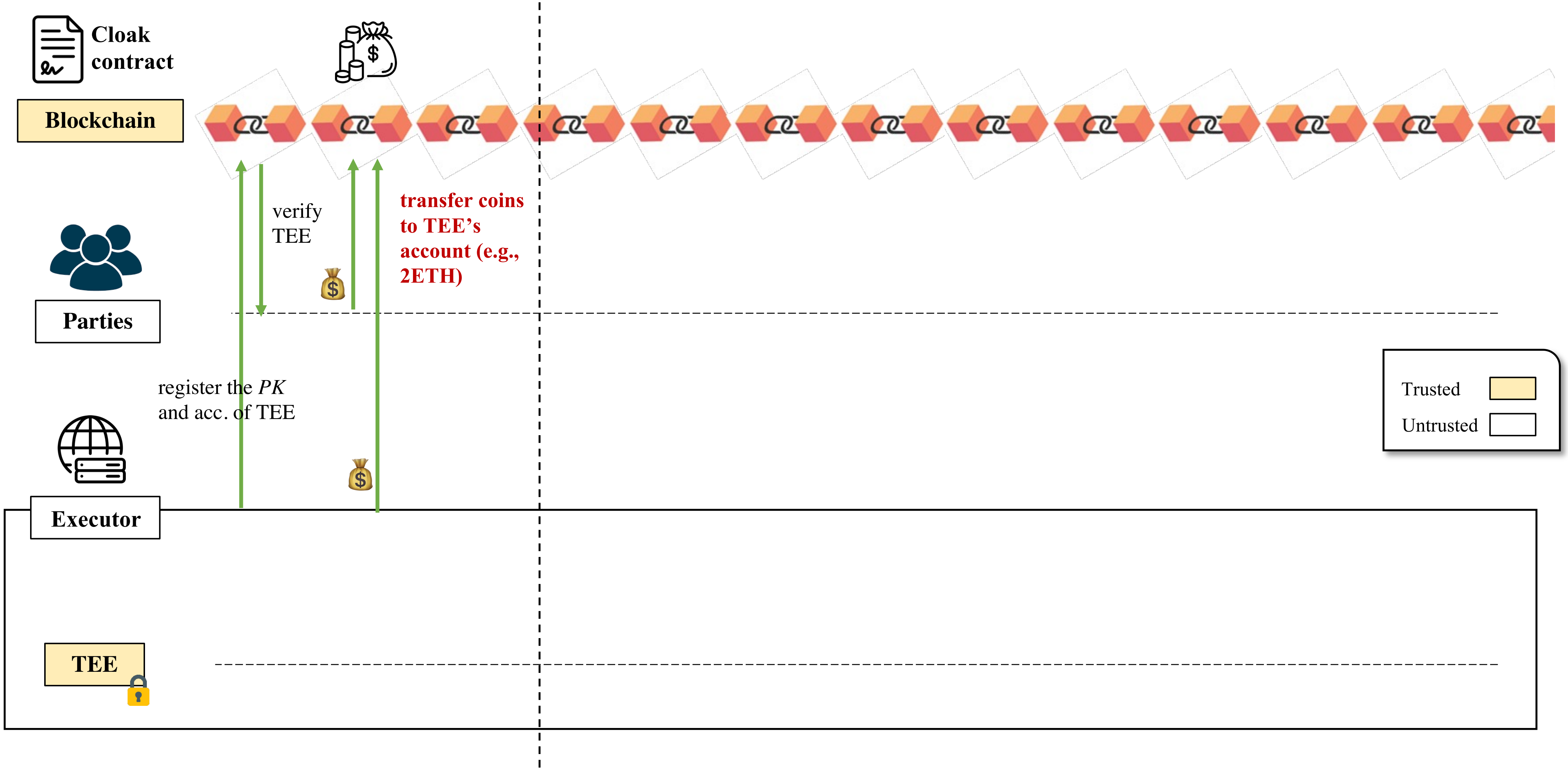
(Global) Setup phase: The executor and parties globally deposit coins to a TEE controlled account

(MPT) Negotiation phase: Parties interact with the TEE off-chain and commit the negotiation result on-chain

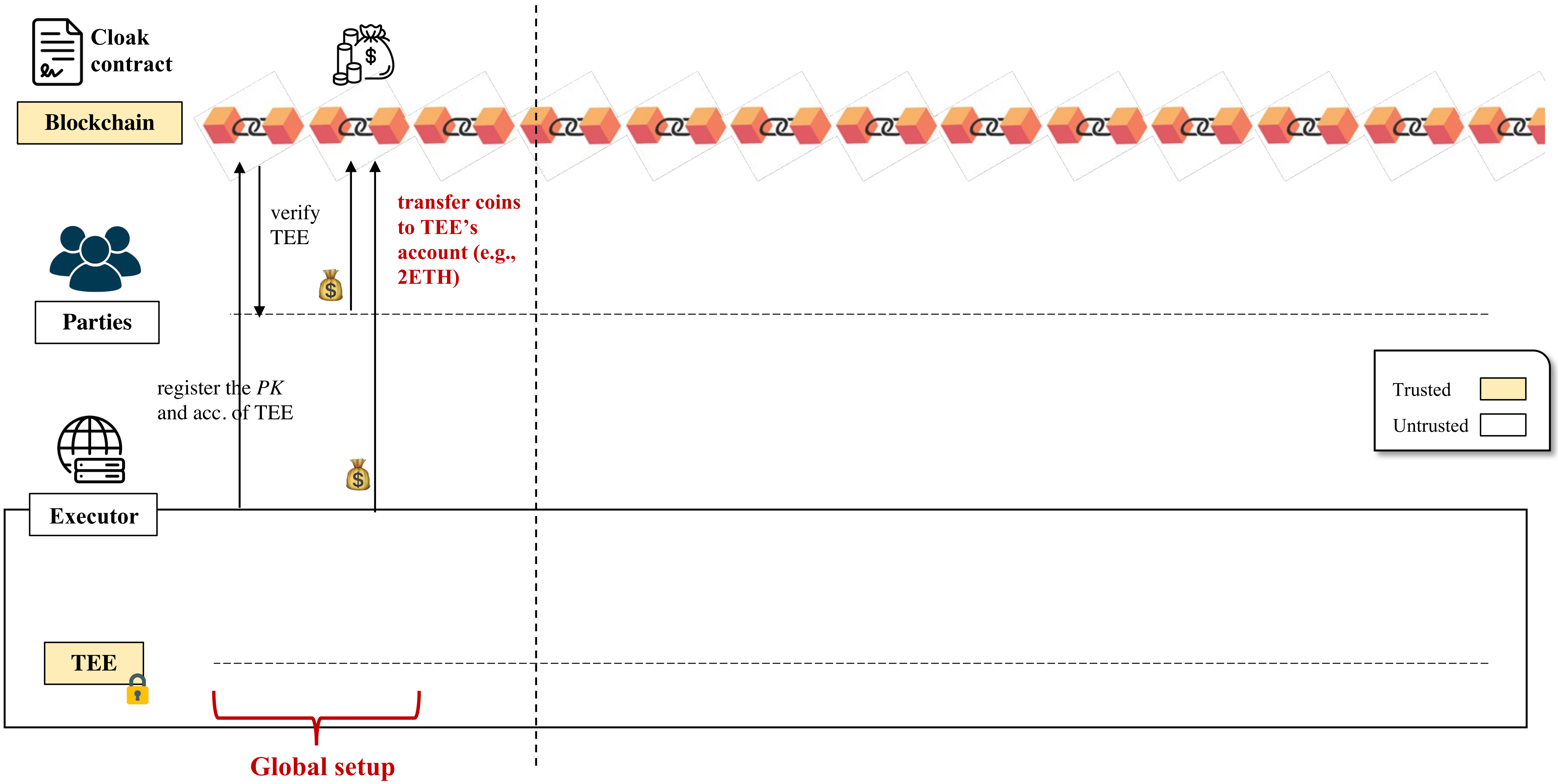
(MPT) Execution phase: The executor collects inputs from parties and blockchain to execute the MPT and get results

(MPT) Delivery phase: The executor delivers plaintext outputs, commit the MPT, and transition states on-chain

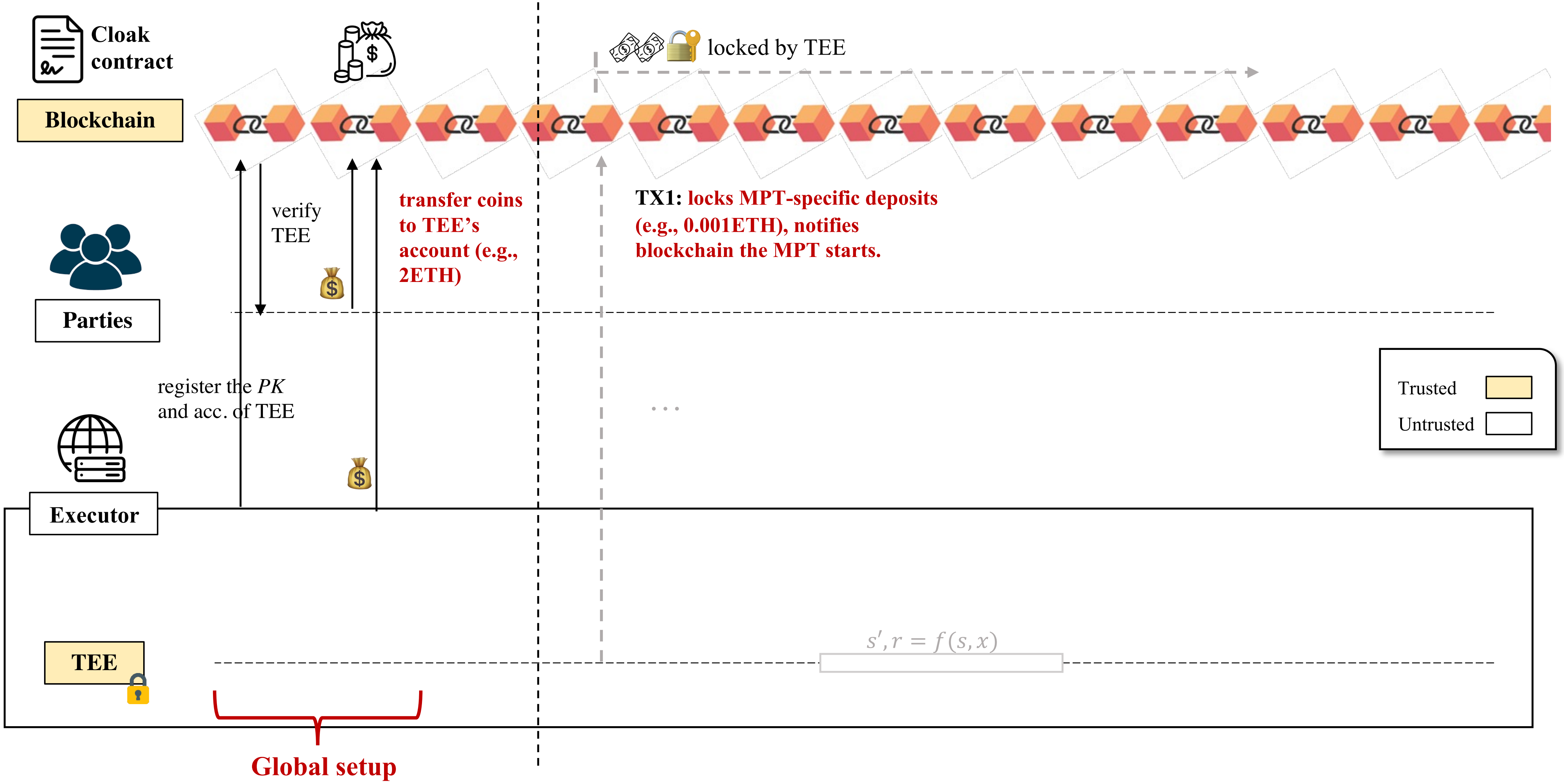
(Global) Setup phase: deposit once, transact multi-times



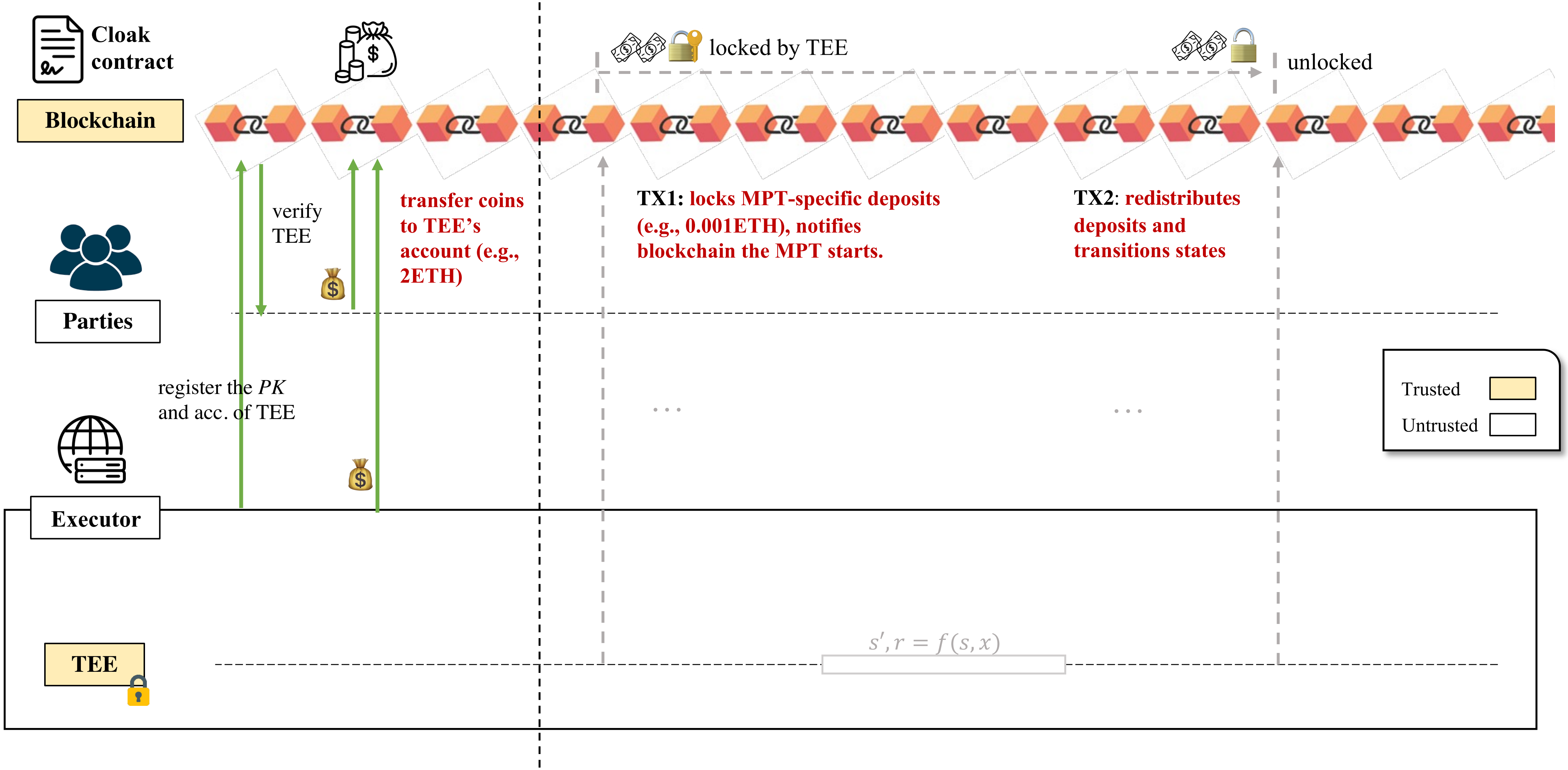
(Global) Setup phase: deposit once, transact multi-times



(Global) Setup phase: deposit once, transact multi-times

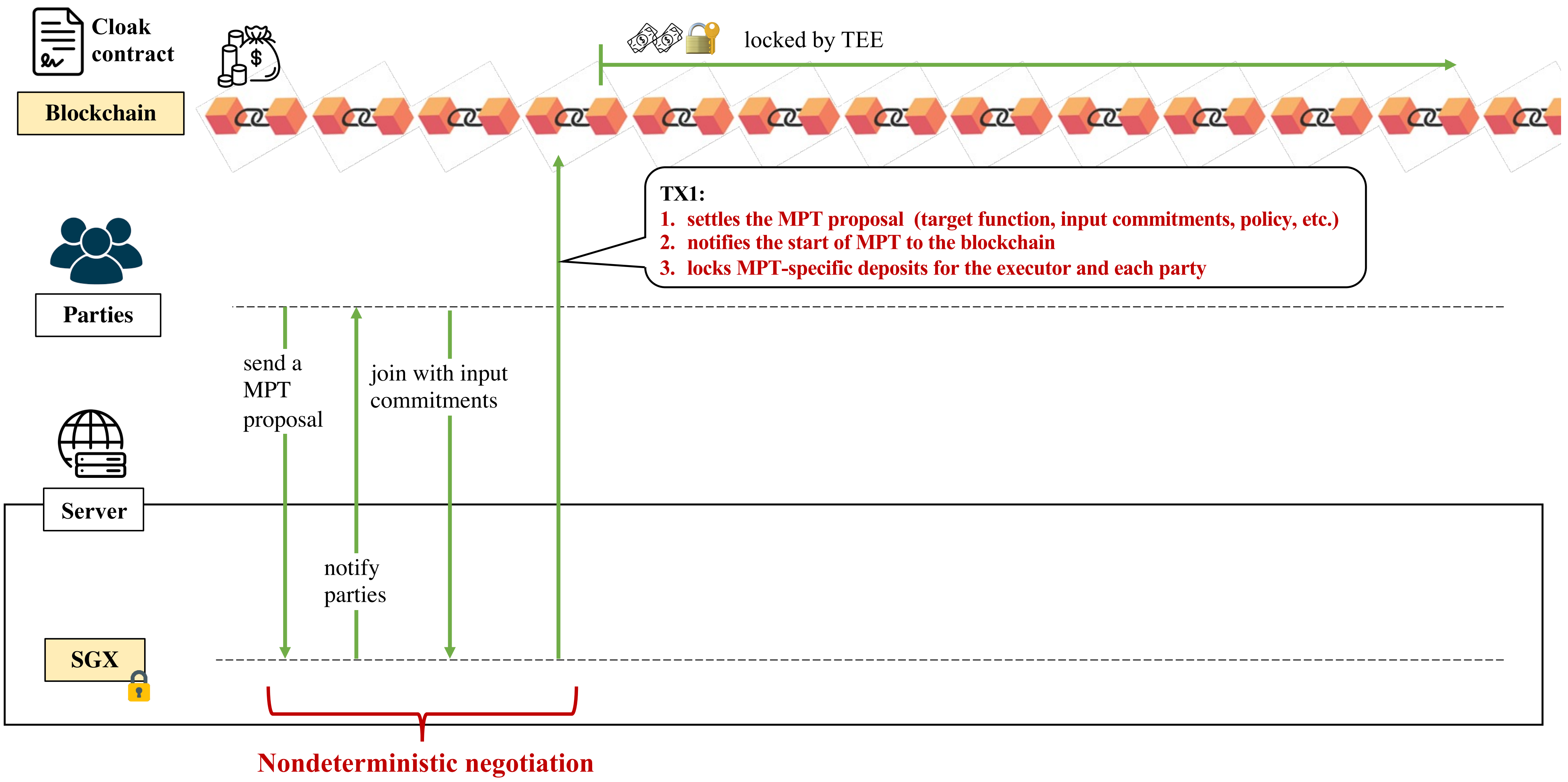


(Global) Setup phase: deposit once, transact multi-times



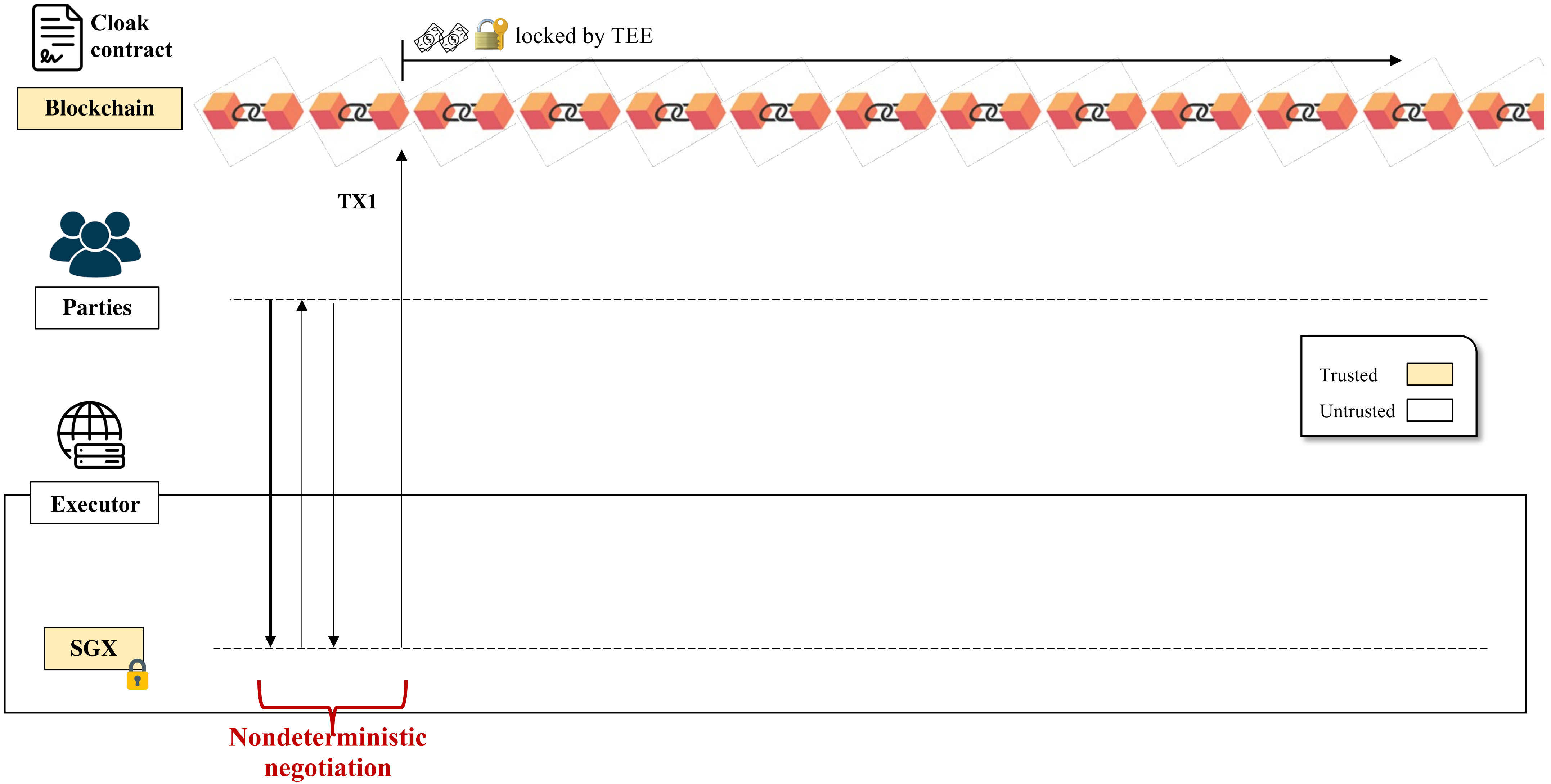
A party can concurrently join multiple MPTs as long as the sum of deposits required by joined MPTs does not exceed his coin balance in any time

(MPT) Negotiation phase: Nondeterministic negotiation subprotocol

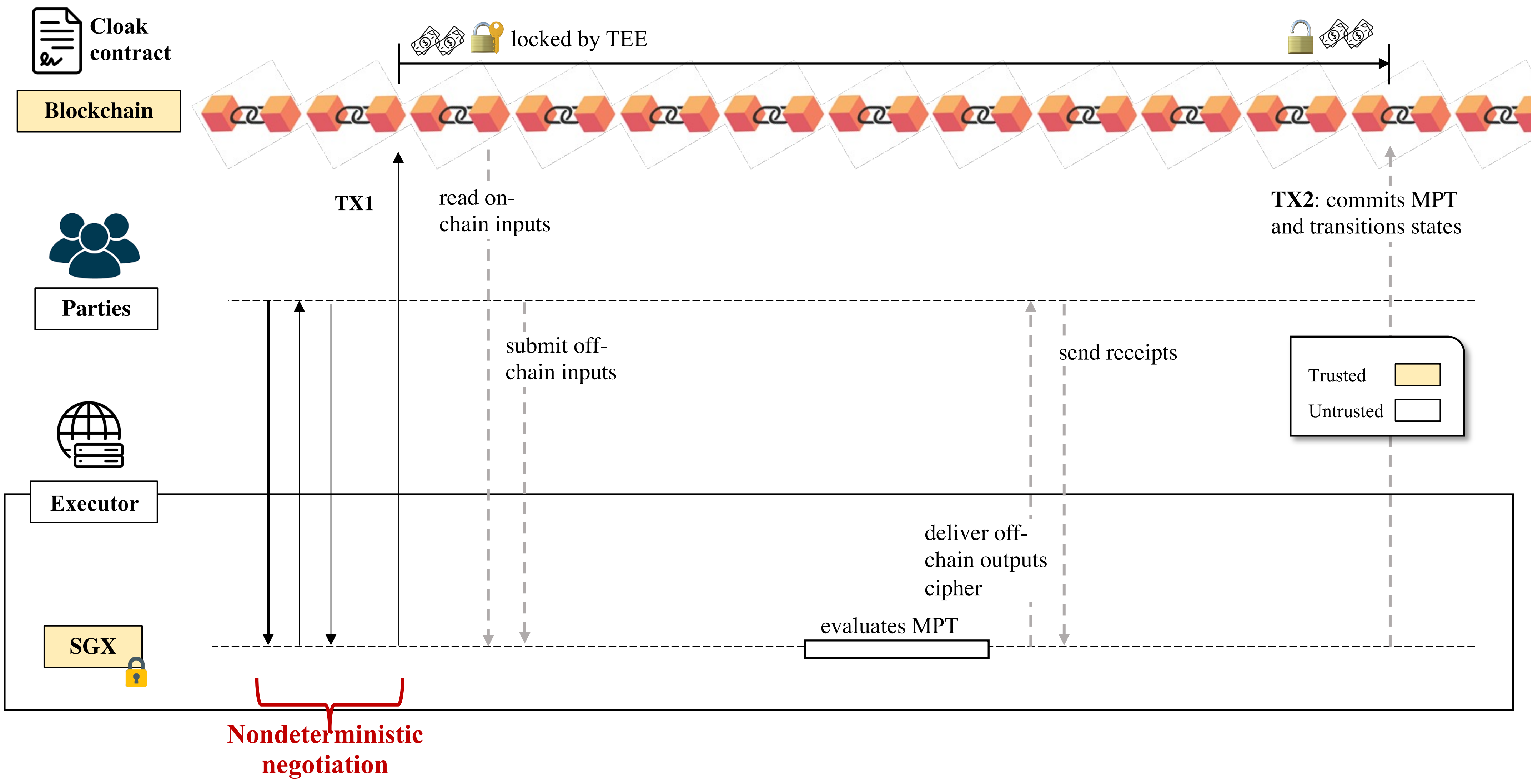


A party can negotiate to join an MPT without knowing other parties a priori

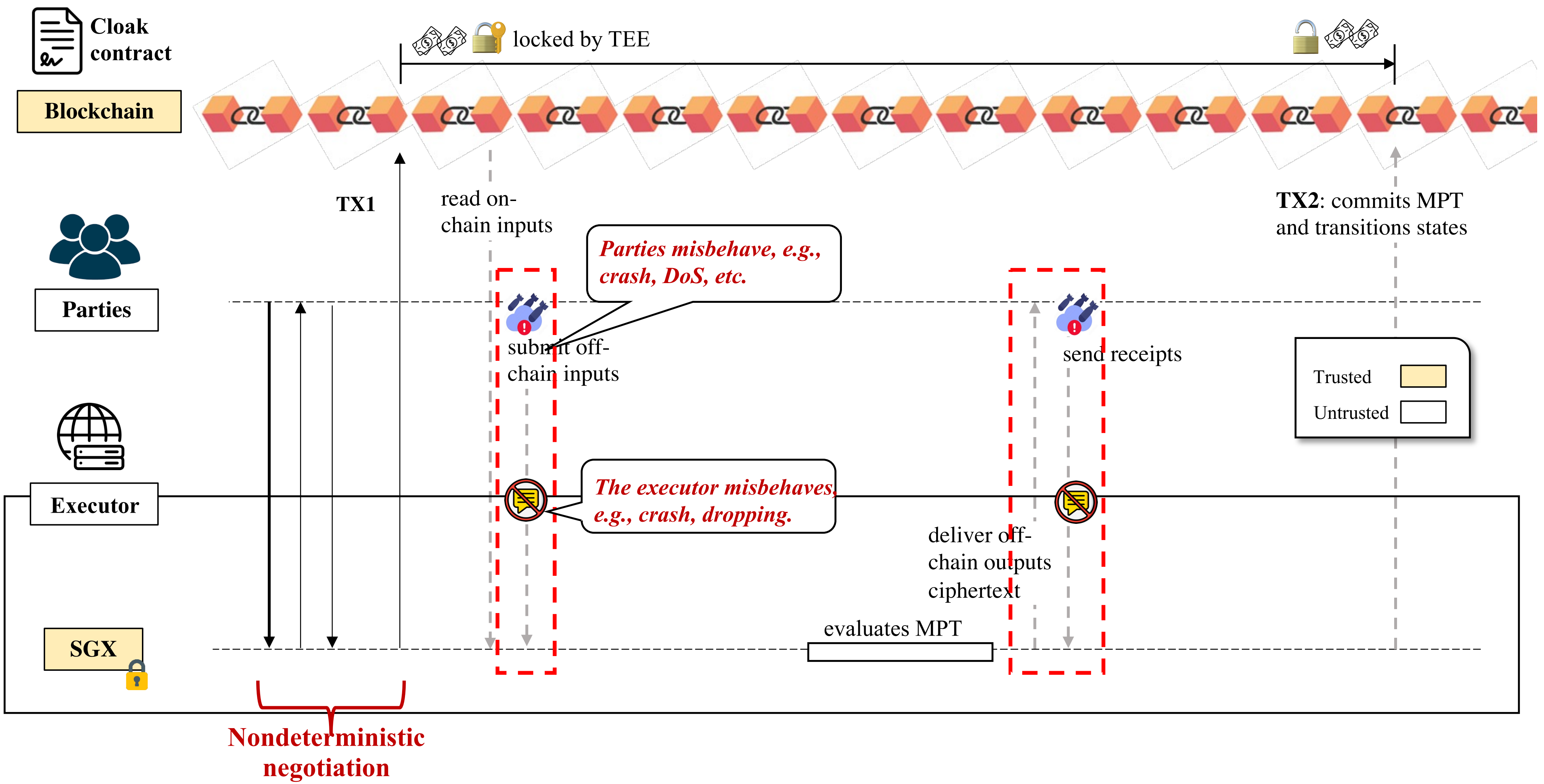
(MPT) Execution phase: Solving repudiation of misbehaved subjects during off-chain interactions



(MPT) Execution phase: Solving repudiation of misbehaved subjects during off-chain interactions

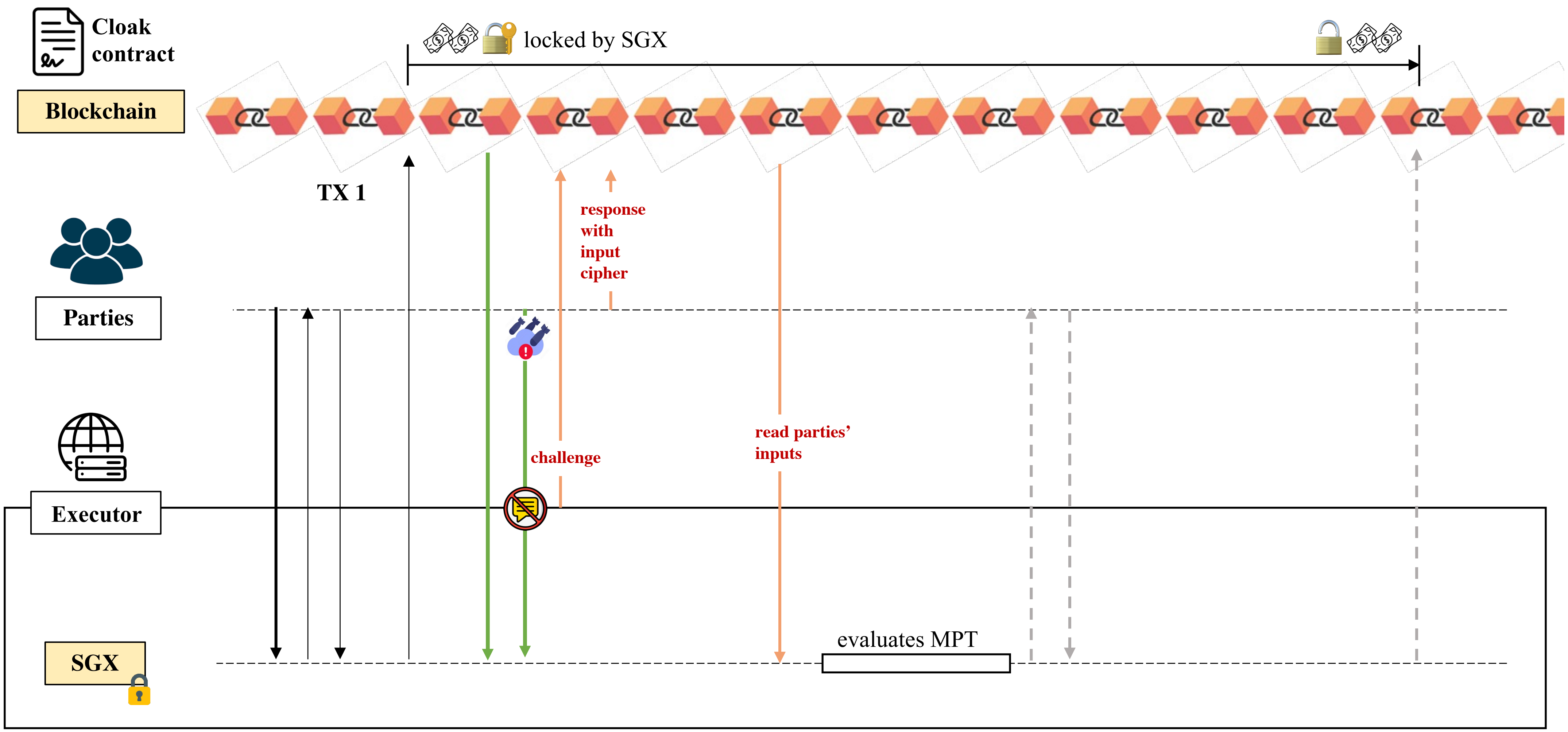


(MPT) Execution phase: Solving repudiation of misbehaved subjects during off-chain interactions

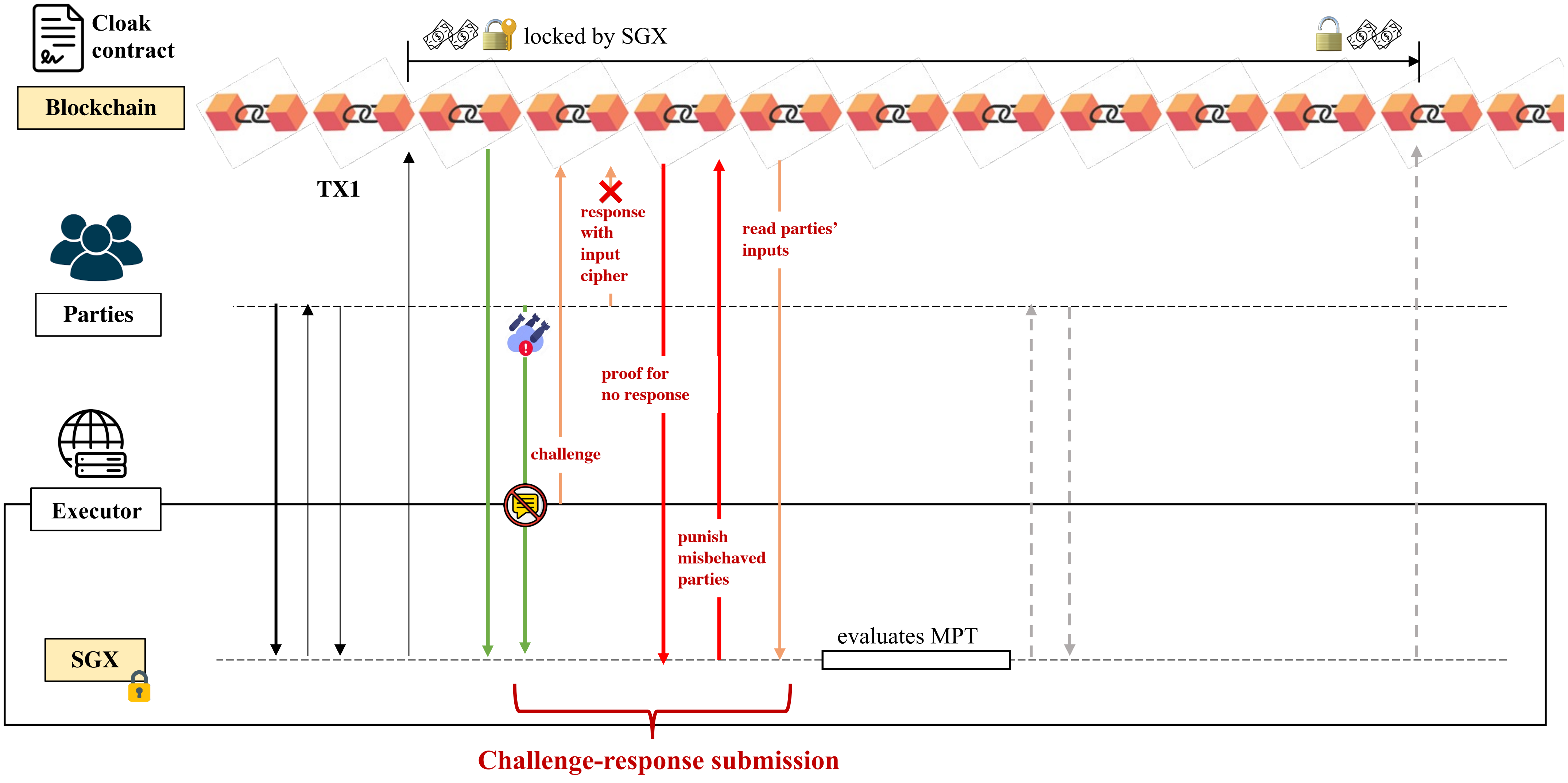


Blockchain/TEE cannot distinguish the executor dropping the off-chain inputs from parties not submitting the off-chain inputs

(MPT) Execution phase: Challenge-response submission subprotocol

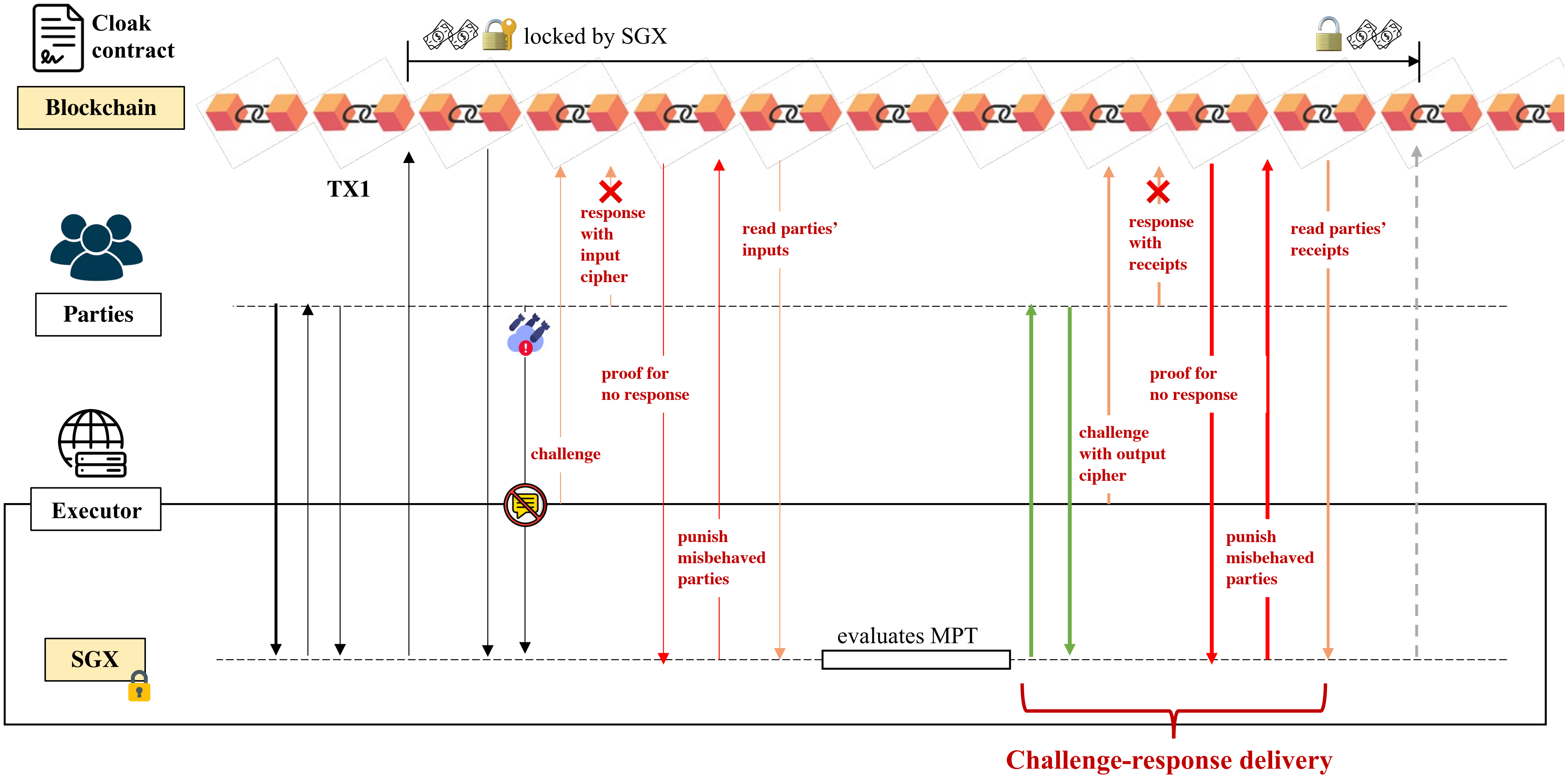


(MPT) Execution phase: Challenge-response submission subprotocol

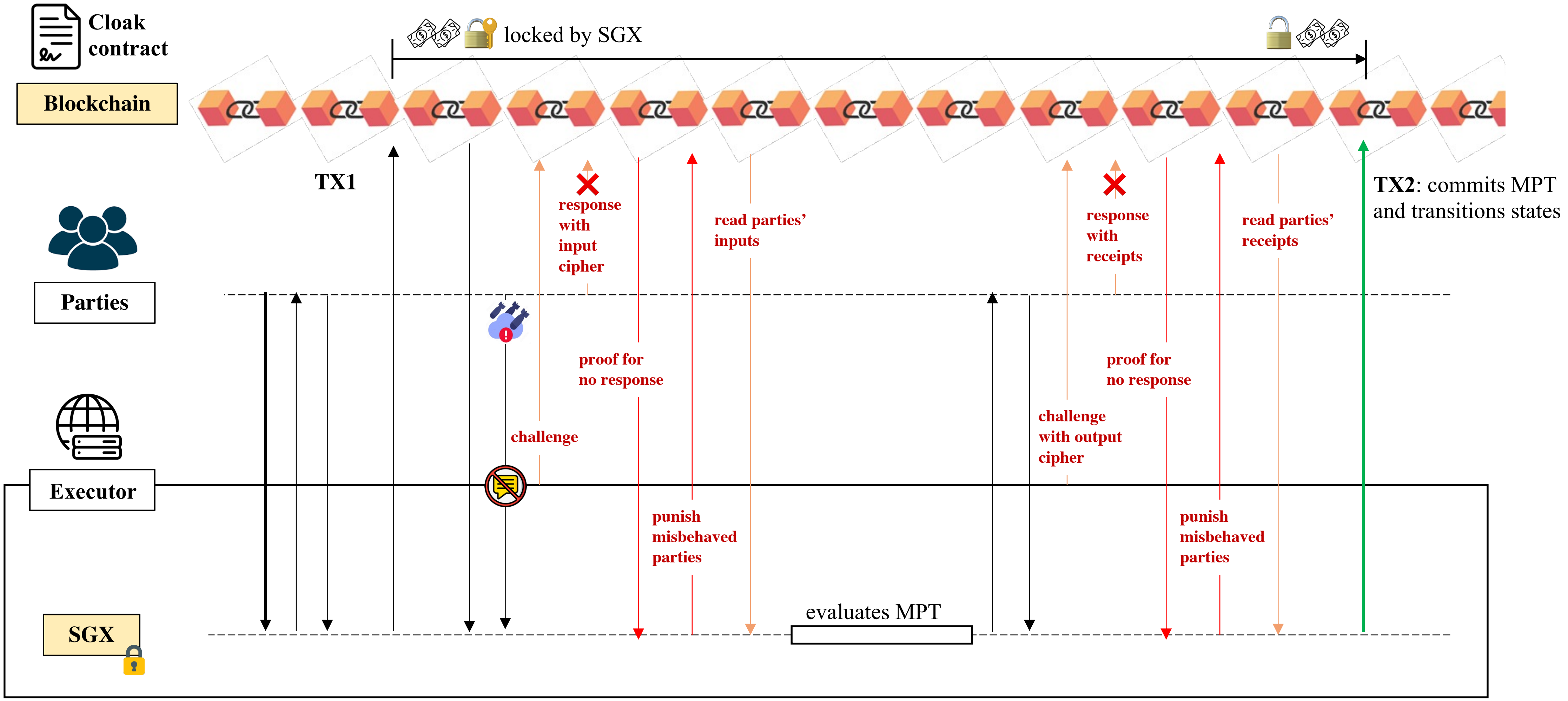


Blockchain/TEE can identify misbehaved subjects during off-chain input submission without repudiation

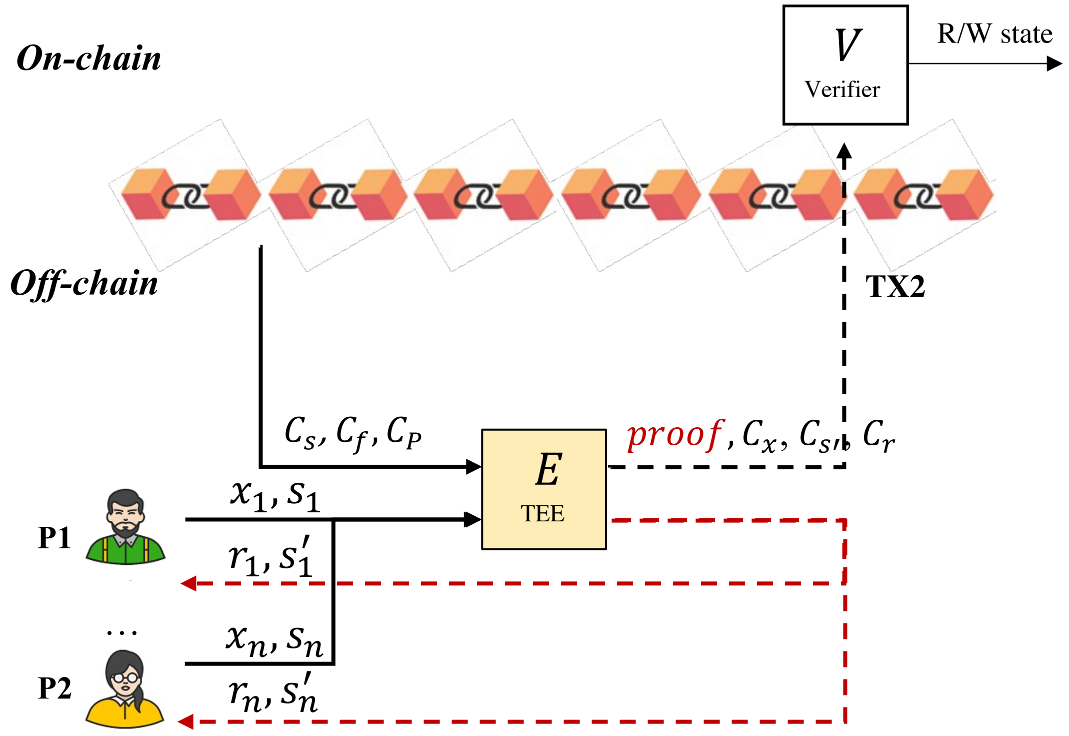
(MPT) Delivery phase: Challenge-response delivery subprotocol



(MPT) Delivery phase: Validating state transition caused by an MPT



(MPT) Delivery phase: TEE-based universal succinct proof



Verify:

$$\boldsymbol{verifySig}(proof, PK_{TEE}) = 1$$

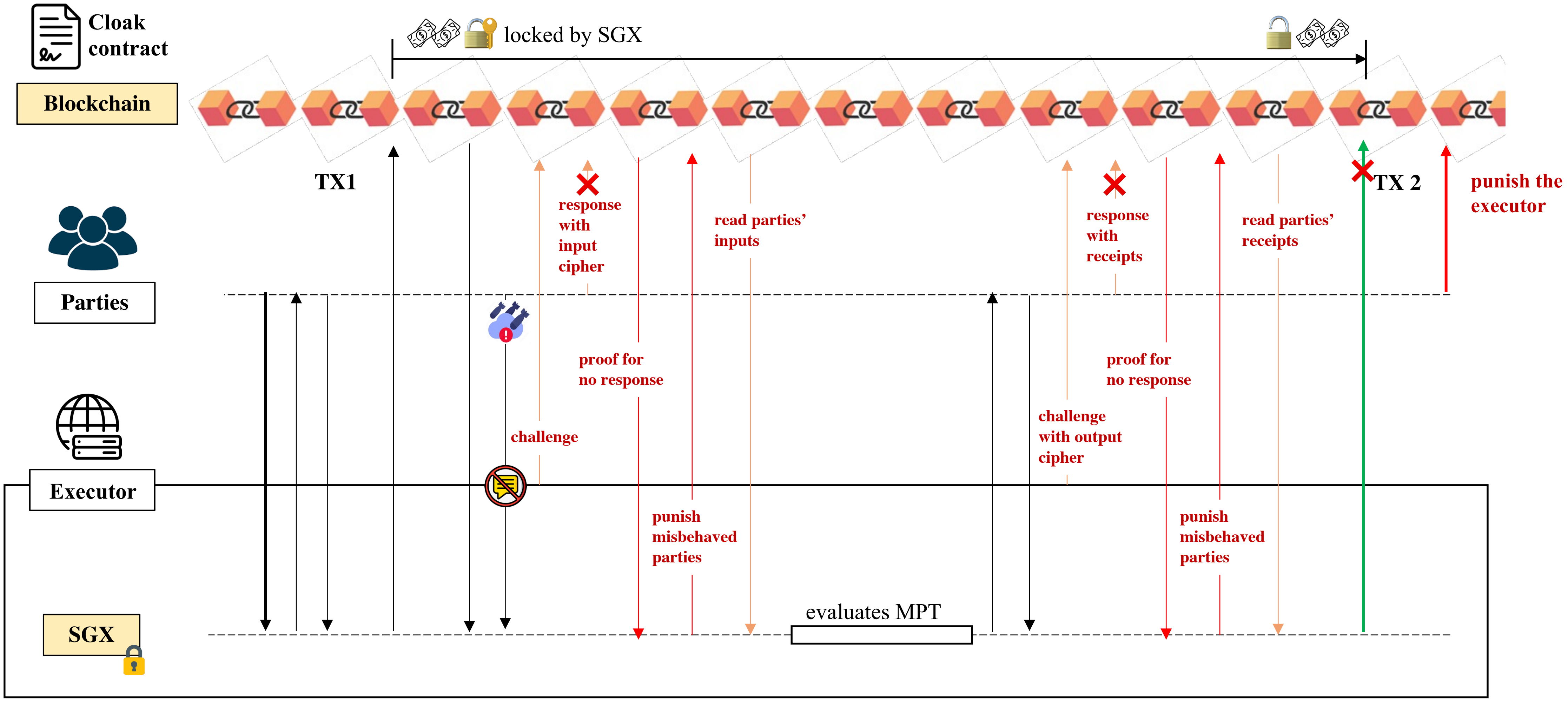
$$\boldsymbol{BC}.\{C_s, C_f, C_P\} = proof.\{C_s, C_f, C_P\}$$

Generate:

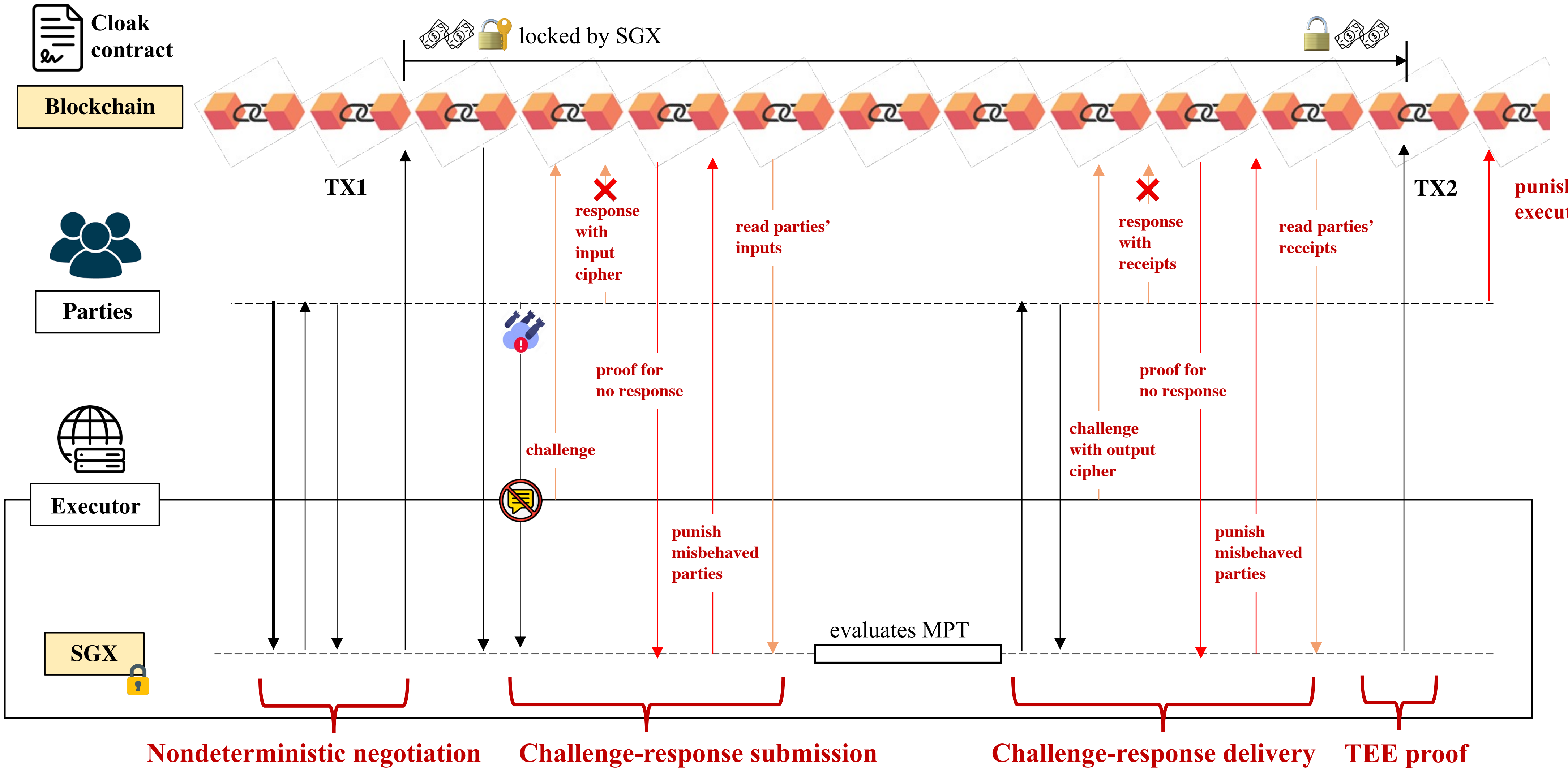
$$proof \leftarrow \boldsymbol{sign}_{TEE}(C_x, C_s, C_f, C_{s'}, C_r, C_P)$$

The validation just relies on the integrity of TEE, rather the trustworthiness of parties or the executor

(MPT) Delivery phase: Validating state transition caused by an MPT



(MPT) Cloak protocol



Cloak requires O(1) (i.e., 2 TXs) for evaluating an MPT without an adversary, while O(n) when an adversary presents

Compare CLOAK with related works

Table 1: Comparison of CLOAK with related works. Here, ●, ◗, ❍, ✕ denotes full, partial, not matched and not related, respectively. "Adversary Model" denotes how many entities' misbehavior are considered, where an executor denotes a server hosting TEE. "min(#TX)" denotes how many transactions are required by the approach. "Public Verifiability" denotes all elements are committed on-chain and state transition can be validated, where x denotes transaction parameter, s, s' denotes contract old and new states respectively, f denotes target function, r denotes return value, and $\mathcal{P}$ denotes privacy policy that includes party-input bindings, *etc.* "Financial Fairness" denotes that honest parties never lose their collateral without obtaining outputs.

Approach	Adversary Model		Chain Agnostic	min(#TX)	Confidentiality	Nondeterministic Negotiation	Public Verifiability						Financial Fairness
	#Parties	#Executors					x	s	f	r	s'	$\mathcal{P}$	
Ethereum [45]	1^*	✕	✕	$O(1)$	✕	✕	●	●	●	●	●	●	✕
Ekiden [13]	1^*	$m^* - 1^1$	●	$O(1)$	●	✕	❍[2]	●	●	❍[2]	●	●	✕
Confide [27]	1^*	$\lfloor m^*/3 \rfloor^3$	❍	$O(1)$	●	✕	●	●	●	●	●	●	✕
Hawk [25]	n^*	✕	●	$O(n)$	◗[4]	❍	●	❍	●	●	❍	❍	●
ZEXE [7]	n^*	1^*	❍	$O(1)$	◗	❍	●	●	●	●	●	❍	✕
Fastkitten [16]	$(n^* + 1^*) - 1$		❍	$O(n)$	◗	❍	❍	❍	❍	●	❍	❍	●
LucidiTEE [37]	n^*	$m^* - 1$	●	$O(n)$	●	●	●	◗[5]	●	●	◗[5]	◗[5]	✕
CLOAK	$(n^* + 1^*) - 1^6$		●	$O(1)$	●	●	●	●	●	●	●	●	●

Require at least one is honest

Only 2 TX in normal cases

Firstly

Most general

Adversary will be identified and punished

Evaluation

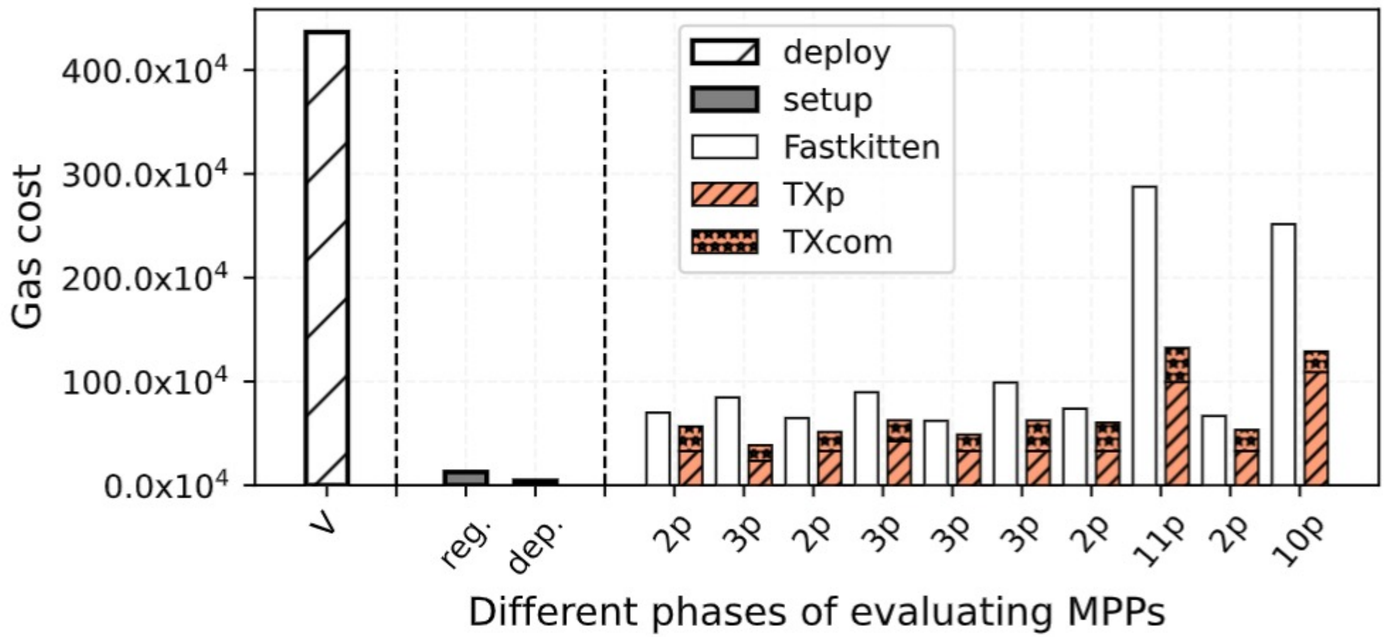


Figure 3: The gas cost of Cloak.

The gas cost of Cloak reduces by 32.4% on average.
As the number of parties grows, the efficiency of Cloak on gas cost stands out

CLOAK: Transitioning States on Legacy Blockchains Using Secure and Publicly Verifiable Off-Chain Multi-Party Computation

Qian Ren, Yingjun Wu, Han Liu, Anne Victor, Hong Lei, Lei Wang, Bangdao Chen

Questions?

SSC
Oxford-Hainan Blockchain Research Institute
清華大學 Tsinghua University
海南大学 HAINAN UNIVERSITY
上海交通大學 SHANGHAI JIAO TONG UNIVERSITY