Robust and Efficient Sharding for Smart Contracts

- **Motivation**: Existing approaches to blockchain sharding require extensive coordination, and introduce livelocks for smart contracts.

- **Contribution**: a novel paradigm for sharding (or parallelizing) smart contract execution by separating execution from consensus; two ways of applying this paradigm to blockchains.

**Saber: sharding by separating execution from consensus**

- Consensus nodes (CNs):
  - Maintain and lock states
  - Check and order transactions
- Execution nodes (ENs):
  - Grouped into different "shards" (honest majority of each)
  - Execute the ordered transactions directly
- Advantages:
  - No intra-shard coordination or livelocks

**Execution sharding for Ethereum**

- Separation only in logic
  - CNs: original Ethereum miners collectively
  - order transactions via PoW
  - designate shards for parallel execution
  - ENs: miners registering to the ShardingManager contract
  - nodes execute transactions off-chain
  - submit the results by making a new transaction
- Sharding management
  - Ethereum miners can Register by deposit some Ether
  - They are periodically assigned to different shards via Shuffle
  - $r$ is an unbiased random number generated off-chain

**SaberLedger: public and permissionless blockchain**

- Batch processing by grouping transactions into blocks
- Proof-of-stake (PoS) for Sybil resistant identities
- A new BFT protocol for the underlying consensus
- A randomness beacon for epoch transitions
- A distributed storage (e.g., IPFS) for state sharding

<table>
<thead>
<tr>
<th> </th>
<th>Elastico</th>
<th>OmniLedger</th>
<th>Chainspace</th>
<th>Eris</th>
<th>SaberLedger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support blockchains</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Support cross-shard TXs</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Livelocks</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Intra-shard co-ordination transparent to clients</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Sybil-resistant identities</td>
<td></td>
<td> </td>
<td> </td>
<td> </td>
<td> </td>
</tr>
<tr>
<td>Distributed storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>