Stage Henry Mont

iExec has developed and deployed the first decentralized marketplace for computing resources, enabling anyone to monetize computing power (servers, virtual machines, etc.), decentralized applications (DApps) and data sets [1]. This marketplace leverages mechanisms to prevent tampering and byzantine faults [2,3]. Moreover, it harnesses the Ethereum blockchain to facilitate secure and reliable matchmaking and transaction execution between providers and consumers, ensuring a high level of trustworthiness. In contrast to the classical cloud computing platforms such as Amazon or Google, the iExec marketplace operates without the need for a trusted third party and cannot be controlled or censored by any entity, including iExec.

In the iExec marketplace, applications, data, and resources are published as orders, issued by these entities. Each order includes crucial information such as pricing details, governance rules, and other relevant specifications. The matching between these orders is done on-chain and generates a deal, which in turns triggers the execution of the corresponding task off-chain. Indeed, a worker is selected out of the iExec network and executes the requested task within a Trusted Execution Environment (TEE) to ensure privacy and integrity of the processing. Finally, the result and an attestation confirming the secure execution within a TEE are provided to the client.

PoCo (Proof-of-Contribution) is a protocol created by iExec that acts as the decentralized trust party in the marketplace. Its duty is to ensure that a worker that contributes correctly to a computing task is rewarded and, at the same time, that a requester will not be charged unless a consensus is achieved on the result of the task. This is achieved by locking the requester’s funds for the duration of the consensus, and unlocking them depending on the outcome. The requester payment is composed of 3 parts, one for the worker pool, one for the application and one for the dataset. When a consensus is finalized, the payment is seized from the requester and the application and dataset owners are rewarded accordingly.

PoCo also uses a staking mechanism to prevent bad behavior and encourage good contributions from workers: when a deal is created on-chains, funds from the worker and the worker pool are locked in an escrow account and will only be reimbursed if a consensus is reached and if the result provided by the worker “won” the consensus. In case the worker returned a different result, its funds will be split among the workers who returned the correct result.

While this mechanism protects requesters against malicious actions from the workers and from the worker pool, it does not protect the requester from the other participants (i.e. the data provider and the application provider), nor does it protect these other participants from a malicious behavior from the requester (e.g. providing wrong input so that a consensus can never be reached).

Objective: This Master project focuses on incentivization of correct behavior in a decentralized computing marketplace. To that end, the goals are to assess threats posed by actors in the decentralized computing marketplace, study the state-of-the-art on incentivization (e.g., economic incentives, reputation [4]) in this context, then propose and evaluate mechanisms to mitigate these threats.

References:

[1] Gilles Fedak, Wassim Bendella, and Eduardo Alves. iExec : Blockchain-Based Decentralized Cloud Computing. Technical report, http://iex.ec/wp-content/uploads/pdf/iExec-WPv3, 2018.

[2] Luis FG Sarmenta. Sabotage-tolerance mechanisms for volunteer computing systems. In Proceedings First IEEE/ACM International Symposium on Cluster Computing and the Grid, pages 337–346. IEEE, 2001.

[3] Gilles Fedak, Cécile Germain, Vincent Neri, and Franck Cappello. Xtremweb : A generic global computing system. In Proceedings First IEEE/ACM International Symposium on Cluster Computing and the Grid, pages 582–587. IEEE, 2001.

[4] Omar Hasan, Lionel Brunie, and Elisa Bertino. Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey. ACM Computing Surveys (CSUR) 55.2 (2022): 1-37.