Ledger Innovation Lab
03 rue Gretry, Paris
01/03/2022

Scope Statement:
Decentralized Test of Liveness

Calic Petar, Master ANDROIDE, Sorbonne Université
Supervised by: Nicolas Bacca, Co-Founder, VP Innovation Lab

SUMMARY

1/ Introduction

This project is to be realized by Petar Calic (me) under the supervision of Nicolas Bacca, VP of **Innovation lab at Ledger**, in the context of an internship of 6 months. I will be working mainly alone on the project with some assistance and guidance from Mr Bacca, the innovation team, the Data team, and many UPMC researchers that I will visit for consultations.
Know Your Customer (KYC) procedures are a critical function to assess customer risk and a legal requirement to comply with Anti-Money Laundering (AML) laws. Effective KYC involves knowing a customer's identity, their financial activities and the risk they pose.
Tests of liveness are a subgroup of tests designated to distinguish real and fake persons(bots). It consists of a set of technical features to counter biometric spoofing attacks where a replica imitates a person's biometrics or characteristics in order to deceive or bypass the identification and authentication steps given by the system. With the emergence of the internet with it, the daily increase of our everyday life dependence on its functionalities, increases the targets and vulnerabilities of third party malicious intentions. Here is one personal example: I made some nft's i wanted to give away freely to people that attended one online event i organized. The second I shared the link, a bot took all 100 of the tokens. A simple liveness check could prevent that. With AI capabilities to imitate humans rising every day, the task to discover bots that don't wish to be discovered, becomes more and more challenging.
However, there are still very successful tests like Google's CAPTCHA which relies on image recognition, mouse movements and a top secret server classifier. Our **goal** is to make an open source, completely decentralized Test of Liveness smart contract deployed on STARKNet, that would be accessible to anyone. There is also a more profound and general mission behind the project which is to make advances in the field of decentralized and open source technologies. We should start relying more on technologies that are verifiable than trustable.
An **important note** is that a test of liveness that relies purely on data collection and analysis, will never be 100% bot proof as the constant race of technologies between the two sides never stops. In order to be completely sure that we are dealing with a real person is to request a document verification for really critical systems. However we are confident that this test will repel more than 90% of most advanced bots. The cost of breach will hardly be profitable.

2/ Image analysis