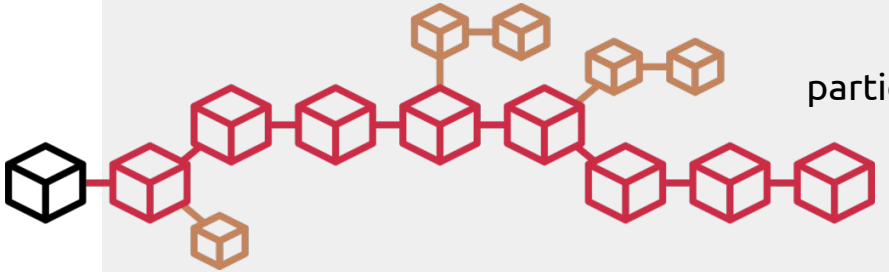
Trustable Oracles Towards Trustable Blockchains

Pedro Duarte da Costa
pedro.duartecosta@fe.up.pt

Supervisors
Filipe Figueiredo Correia -
Hugo Sereno Ferreira -
Proponent
Mário Ribeiro Alves -

Context



Blockchain

A distributed ledger, shared by untrusted participants, with strong guarantees about accuracy and consistency.

Smart Contracts

Applications that run on the blockchain.

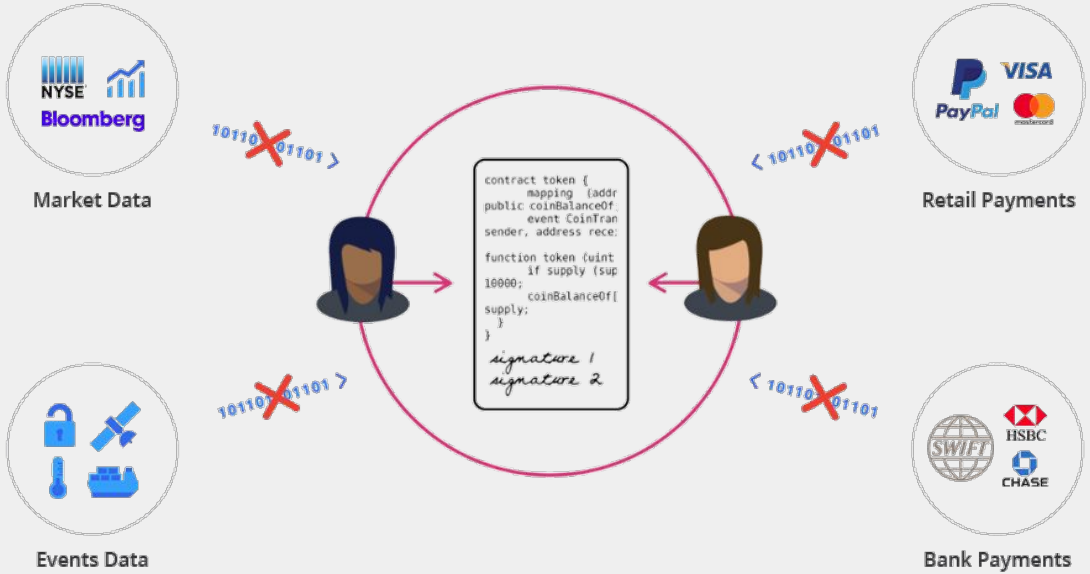
Are self-verifying, self-executing and immutable.

The terms are directly written in lines of code which persist on the blockchain

The Smart Contract Connectivity Problem

The blockchain is deterministic. Meaning that verified in different points in time it always has the same state.

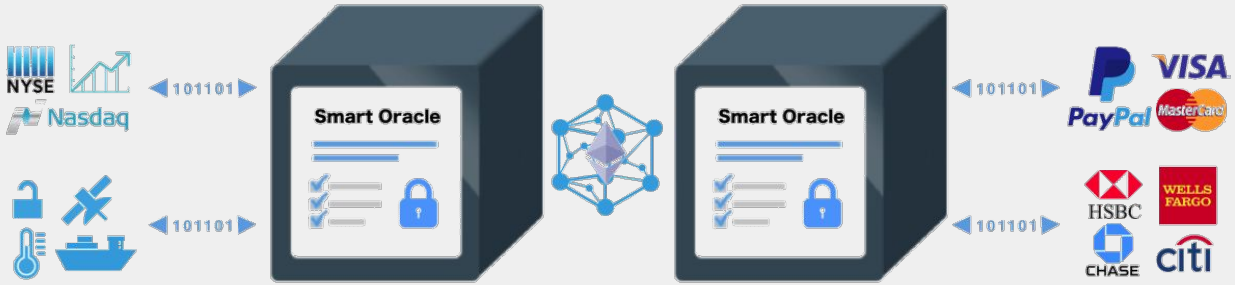
But the internet is non-deterministic, thus contracts cannot directly query the internet.



Oracles

Oracles run the smart contracts queries and input the answer in the blockchain.

The problem? We must trust oracles to be reliable and honest.



Motivation

Some on-chain operations can be very expensive and time consuming, creating a need to perform these operations outside of the blockchain while guaranteeing the trustworthiness of the results.

State of Art

Hardware Oracles

The **Town Crier** system leverages trusted hardware (Intel SGX) to provide a strong guarantee that data comes from an existing, trustworthy source.

Software Oracles

Oraclize.it provides Authenticity Proofs for the data it fetches guaranteeing that the original data-source is genuine and untampered. **ChainLink** uses decentralized oracle network provides the same security guarantees as smart contracts themselves.

Consensus-based Oracles

Hivemind (previously Truthcoin), **Augur**, **Gnosis** and **Astraea** base their data feed on ”Wisdom of the Crowd” and incentives to report results.

Objective & Expected Results

Investigate and design a solution to perform off-chain operations while keeping the user trust in the results.

Two scenarios for oracle investigation and implementation:

- The correct validation of off-chain data with it’s on-chain proof.
- Untampered relaying of a vote count result to the smart contract.

Thanks

pedrocosta.eu/thesis-abstract

Faculty of Engineering, University of Porto
BRPX - Bright Development Studio, S.A.