Quality-Aware Transaction Validation in Blockchains

M.Sc. Thesis by:
Lorenzo Maria Bonelli
Matr. 876070

Context

Blockchains 2.0: with the introduction of the second generation of blockchains, this technology is no longer limited to managing cryptocurrencies.
Platforms such as Ethereum can execute code and run complex applications

bitcoin

«Payment system using peer-to-peer technology to operate with no central authority»

ethereum

«Global, open-source platform for decentralized applications"

Data Quality Assessment in Blockchains: Motivations

Data on the blockchain

are immutable and persistent after writing

are used to take decisions and drive business logic

Definition: «suitability of data for the respective data processing application»

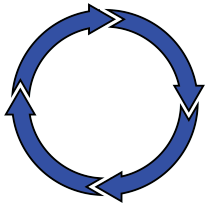
Klein and Lehner, 2009

There are many metrics that can be considered when dealing with data quality, but the literature agrees that some of them are relevant to almost every application:
accuracy, completeness, consistency, precision, timeliness

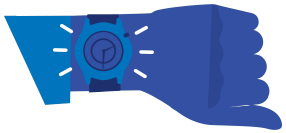
Goal

Objective: designing controls for assessing data quality in blockchain applications before storing data permanently

Data quality controls should be:



reusable



time-efficient

cost-efficient

State Of The Art

What has been discussed:

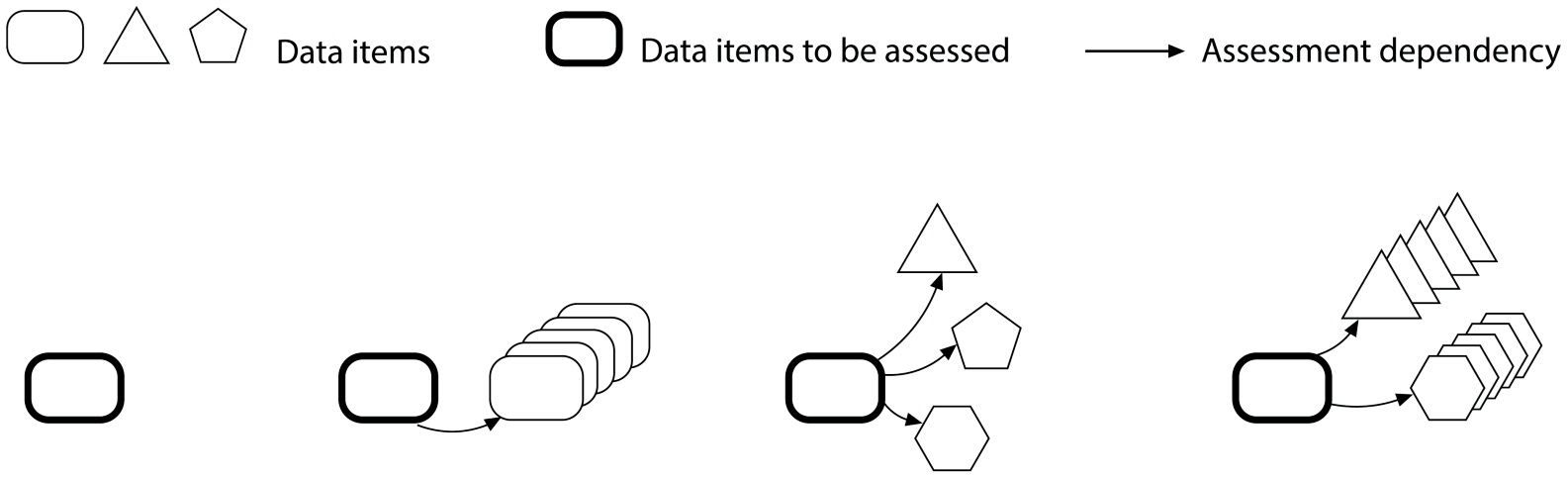
- Possible uses of the blockchain: IoT, financial transactions, access management, supply chain and others
- Limits of blockchain programming: costs, security, passive logic, impossibility to access off-chain data
- Necessity for smart contracts to implement data quality controls (theoretic approach)

What has not been discussed:

- How to concretely implement data quality controls inside smart contracts
- Limits of blockchain data quality controls
- Overhead, both in time and costs, brough by adding these controls

Approach (1)

Data need



Approach (2)

Data provision patterns

The data required for assessment can be made available through four blockchain-specific patterns:

A single transaction bringing all the values needed inside its payload	Multiple ordered transactions bringing different pieces of information	Multiple interleaved transactions bringing different pieces of information	*Off-chain* data stored on a network node or web-accessible information are needed

Approach (2)

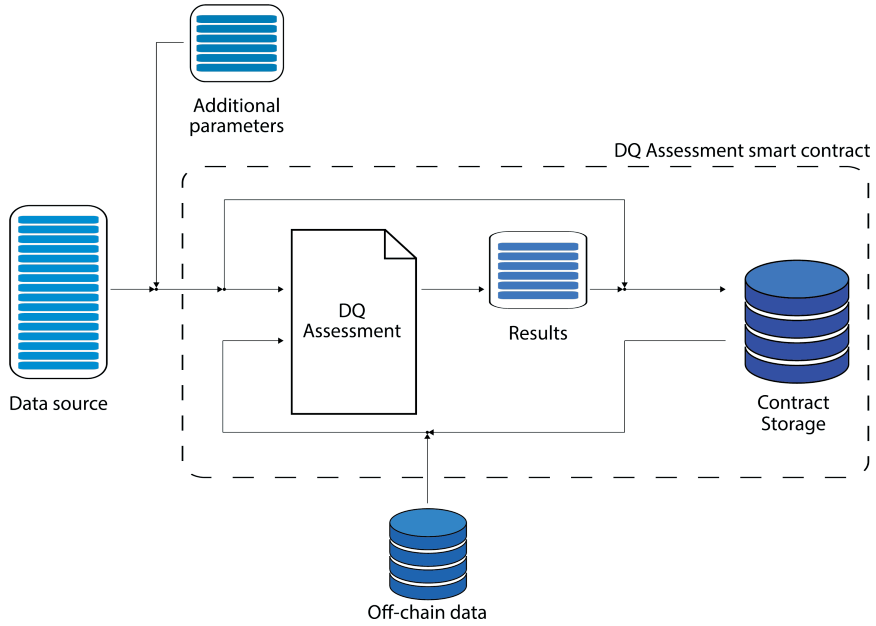
Data provision patterns

The data required for assessment can be made available through four blockchain-specific patterns:

A single transaction bringing all the values needed inside its payload	Multiple ordered transactions bringing different pieces of information	Multiple interleaved transactions bringing different pieces of information	*Off-chain* data stored on a network node or web-accessible information are needed
Stateless Smart contract	*Stateful smart contract*	*Stateful smart contract with correlation*	*Smart contract with oracle*

Approach (3)

Architecture



Scenarios

- Drug transportation
- Drug prescription

Technologies

Blockchain

ethereum

Language

solidity

Environment

remix

Implementation

Scenario 1: drug transportation

Goal: monitor temperature inside trucks for drug transportation
Implementation choices: stateful smart contract
Challenges: array management

Scenario 2: drug prescription

Goal: check new prescriptions against ongoing ones
Implementation choices: stateful smart contract with oracle
Challenges: oracle management

Evaluation

Design of evaluation:
- Deploy the same contract with and without data quality controls
- Test different gas prices to find the optimal one
- Measure overhead with the chosen gas price

Metrics:
- Gas amount
- Time

Results:
- Impact on contract creation
- Impact on contract interaction

Gas price = 1 Gwei		% Increase by adding DQ controls		
		Time	Gas Units	Cost (Gwei)
Transport	Creation	**100%**	**132%**	**132%**
	New record stored	**40%**	**3%**	**3%**
Prescription	Creation	**156%**	**50%**	**50%**
	Drug accepted	**150%**	**231%**	**642%**
	Drug refused	**280%**	**135%**	**316%**

Conclusions and Future Work

Conclusions:

- As the number of applications running on the blockchain is constantly growing, it is vital to enable smart contracts to perform data quality controls
- Writing smart contracts is a complex and error-prone activity
- DQ controls have an high impact on costs

Future work:

- Expand the number of scenarios
- Test blockchains other than Ethereum

POLITECNICO
MILANO 1863

Thank you for your attention