Choreographies Enactment Via Smart Contracts

Andrea Morichetta, Andrea Polini, Barbara Re, Francesco Tiezzi

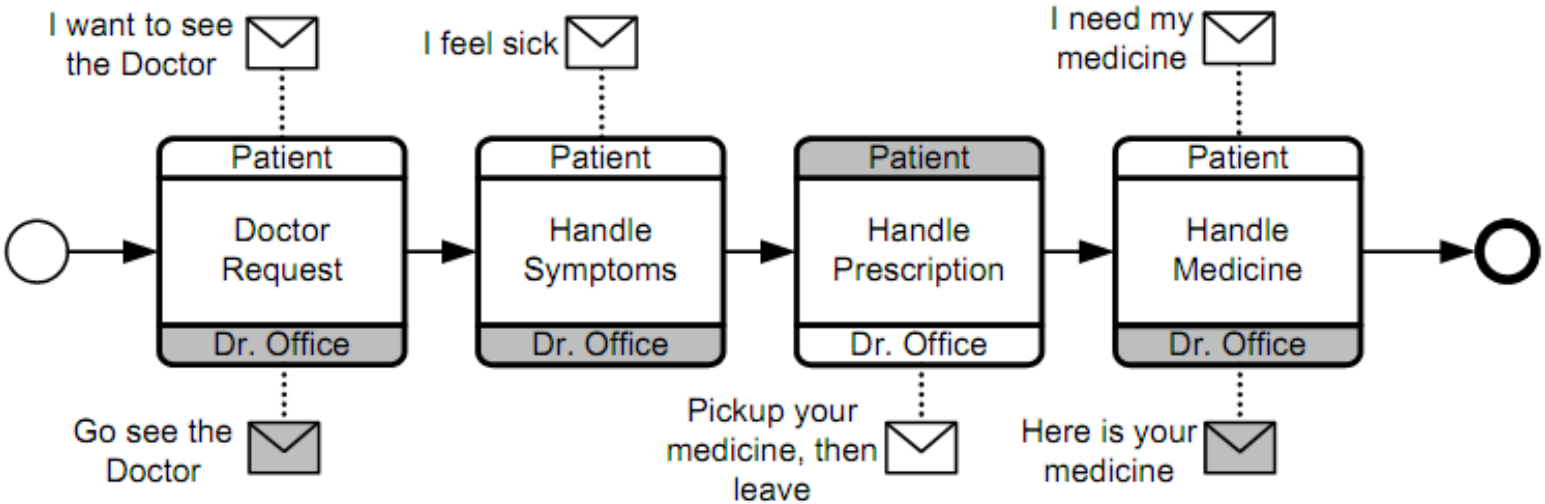
DLT 2019 - Pisa
Febbruary 12, 2019

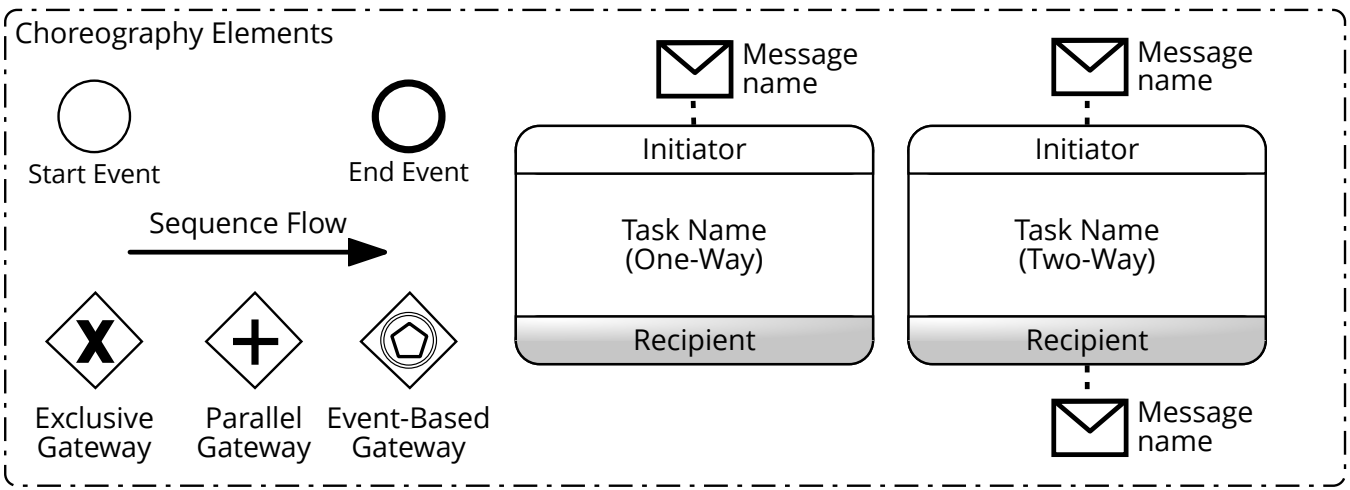
Modelling Choreographies

BPMN standard is the prominent modelling language to describe **decentralised inter-organisational systems** from the business perspective

- **Choreography models**, define the **sequence of exchanging messages** between two (or more) **independent participants or processes** by describing how they should **cooperate to reach a shared goal**
  - **Reusability**, the **same choreography** definition is usable by **different participants** operating in **different contexts** (industry, locale, etc) with different software (e.g. application software) and different message formats and standards
  - **Information Driven**, choreographies maintain their state by recording **mutations caused by exchanges of information** and their reactions between participants
  - **Heterogeneity**, choreographies can be used in different contexts and at different layers of abstraction

BPMN 2.0 Choreography





Main Objective

Problem:

Choreographies have **not been widely adopted** yet in the industry, mainly due to the **lack of a concrete implementation relying on a decentralized system that can guarantee trust between parties**

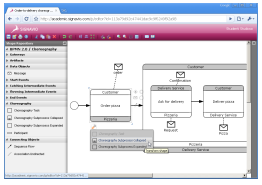
Solution:

The aim of our work is to **provide a framework** for the **deployment and enactment of BPMN choreographies using the blockchain technology and smart contracts**

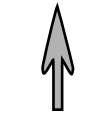
The main benefits of our solution are:

- to execute choreographies involving **untrusted parties in a decentralized and autonomous way**
- to **enforce the correct behaviour of each participant** in compliance with the choreography model
- **a completely transparent process for the final user, it is not required any blockchain knowledge** since both **the deployment and the execution are managed using the framework user interface**

Proposed Framework

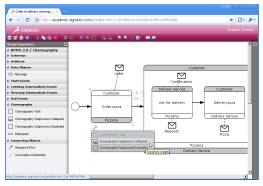


Modeling Tool



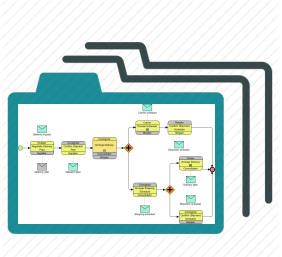
Modeler

Proposed Framework

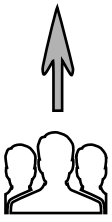


Modeling Tool

Publishing

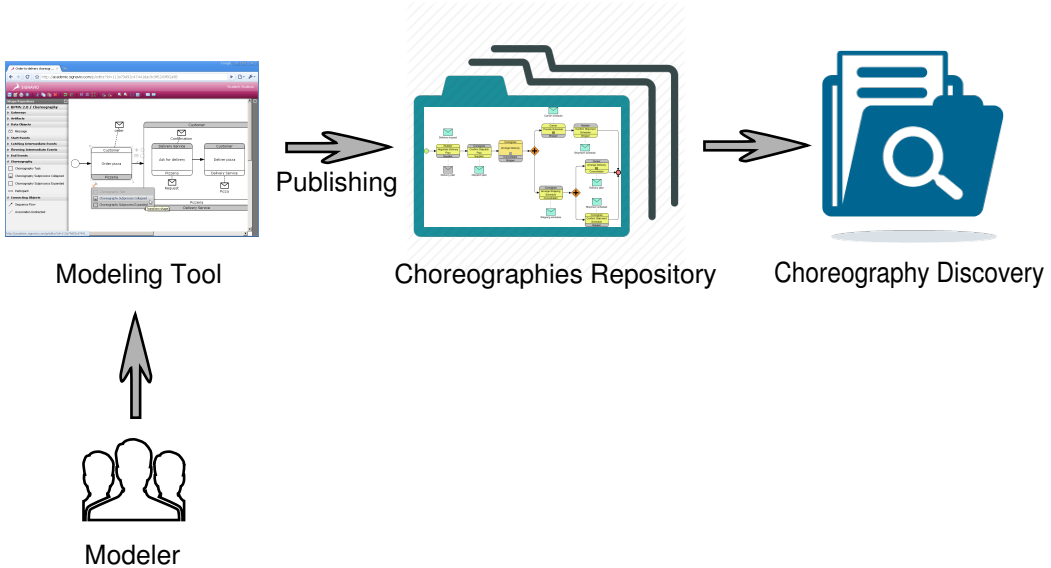


Choreographies Repository

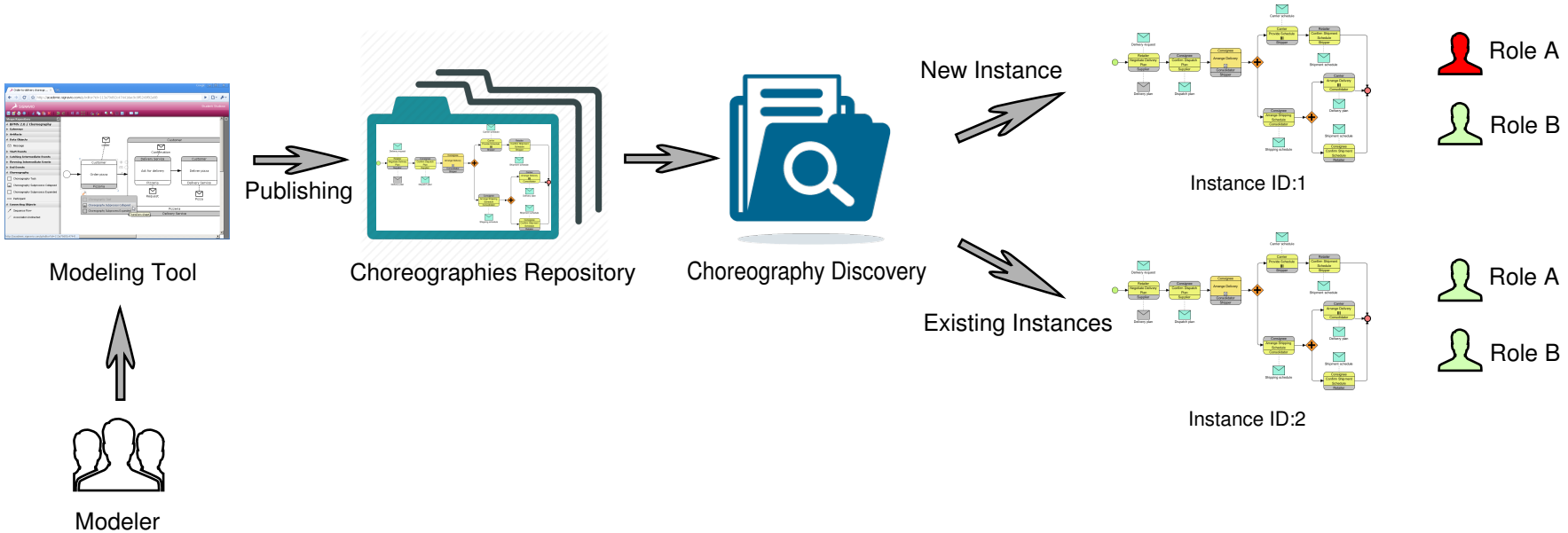


Modeler

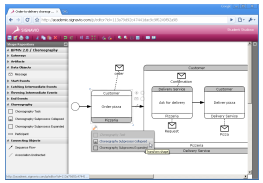
Proposed Framework



Proposed Framework

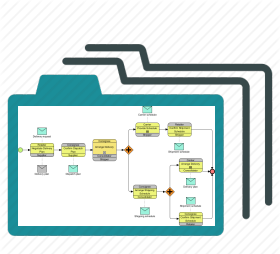


Proposed Framework



Modeling Tool

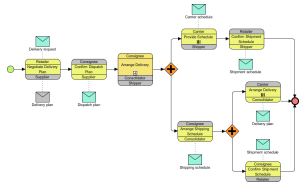
Publishing



Choreographies Repository

Choreography Discovery

New Instance

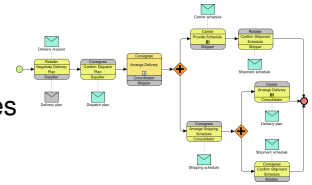


Instance ID:1

Role A

Role B

Existing Instances



Instance ID:2

Role A

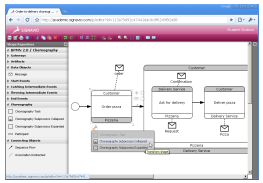
Role B

Modeler

Contract Generation

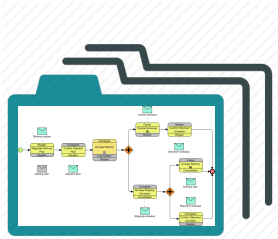
Solidity Contract

Proposed Framework



Modeling Tool

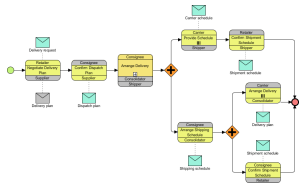
Publishing



Choreographies Repository

Choreography Discovery

New Instance

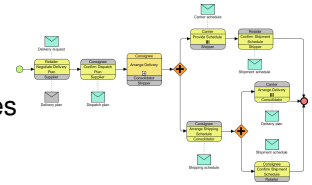


Instance ID:1

Role A

Role B

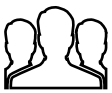
Existing Instances



Instance ID:2

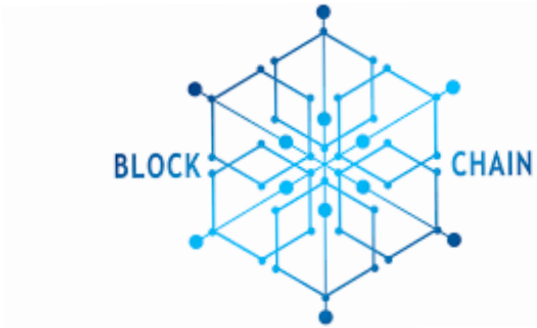
Role A

Role B



Modeler

Contract Generation

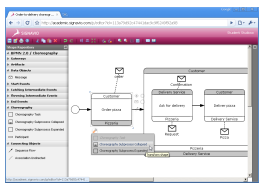


0xca35b7d915458ef54e2f44e8fa733c

Deploy

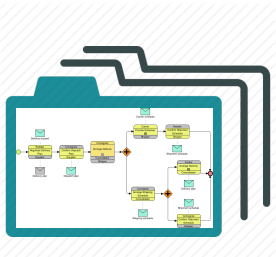
Solidity Contract

Proposed Framework



Modeling Tool

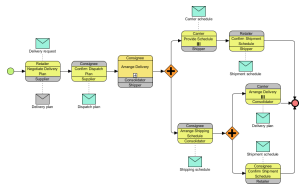
Publishing



Choreographies Repository

Choreography Discovery

New Instance

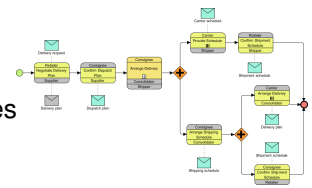


Instance ID:1

Role A

Role B

Existing Instances

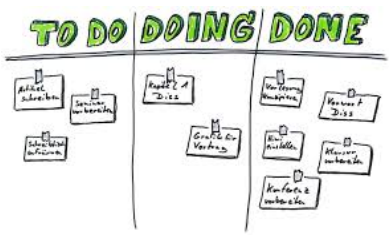


Instance ID:2

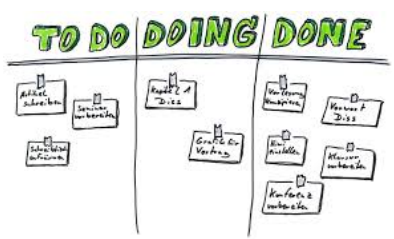
Role A

Role B

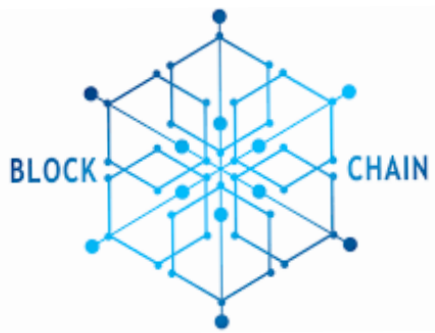
Modeler



Role A



Role B



0xca35b7d915458ef54e2f44e8fa733c

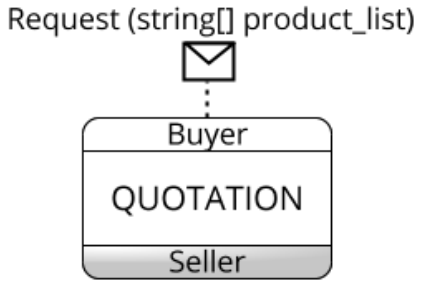
Contract Generation

Deploy

Solidity Contract

Feasibility of the Approach

```
1  contract Choreography{
2    enum State {DISABLED, ENABLED, DONE} State s;
3    struct Element{string ID; State status;}
4    struct StateMemory{string[] product_list}
5
6    Element[]    chorElements;
7    StateMemory currentMemory;
8
9    mapping (string=>uint) position;
10   string[] elementsID=["sid-b014d0d4", ..."sid-ECEB8C20"];
11
12   mapping(string=>address) roles;
13   string[] roleList = [ "Seller", "Buyer"];
14 }
```




```
1  function QUOTATION_Request(string[] product_list)
2                                                  public checkRole(roleList[1]) {
3    require(chorElements[position["sid-b014d0d4"]].status==State.ENABLED);
4    currentMemory.product_list=product_list;
5    ...
6    done("sid-b014d0d4");
7    enable("sid-ECEB8C20");
8    next_parallelGateway ();
9  }
```

Concluding Remarks

The proposed framework aims at:

- **facilitating the enactment of choreographies** in a secure and trustable environment
- **eliminating third parties governing authorities** for ensuring the respect of the agreements/laws
- guaranteeing the **integrity and the immutability of data**
- bringing together **supply and demand** between unknown parties
- **facilitating to non-domain experts** the deployment and execution of choreographies into a complex platform like blockchain

Thank you!

Andrea Morichetta

andrea.morichetta@unicam.it

PROS Lab - http://pros.unicam.it

Computer Science Department - https://computerscience.unicam.it

University of Camerino - http://www.unicam.it