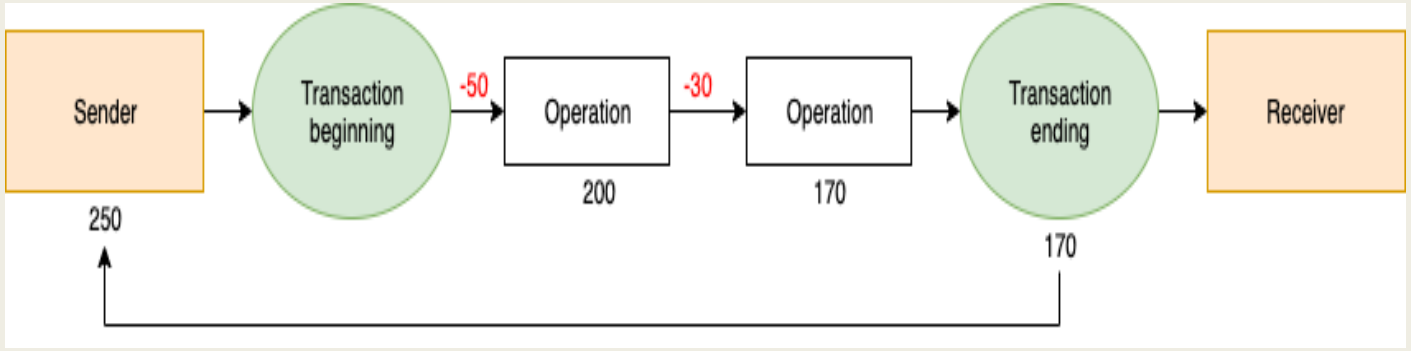
STATISTICAL MODEL CHECKING FOR BLOCKCHAIN-BASED APPLICATIONS

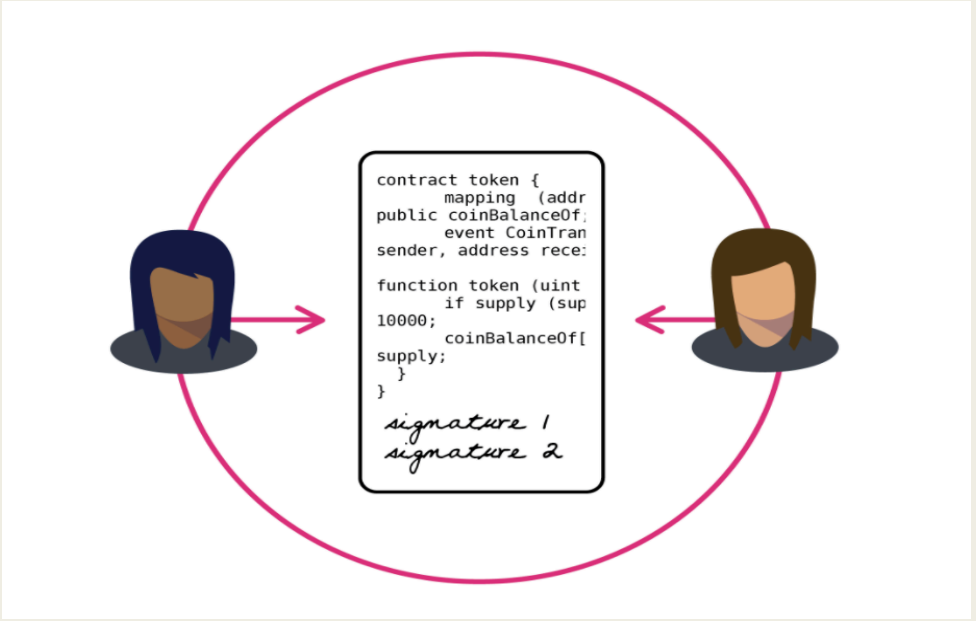
Blockchain

Blockchain technology protects users from cybercrimes through **decentralization**.

Each node of a blockchain network stores an entire history of *all the transactions* ever fulfilled making it really hard for attackers to mess with user assets.

A smart contract is a program that allows for the automatic closing of deals between two or more parties involved.



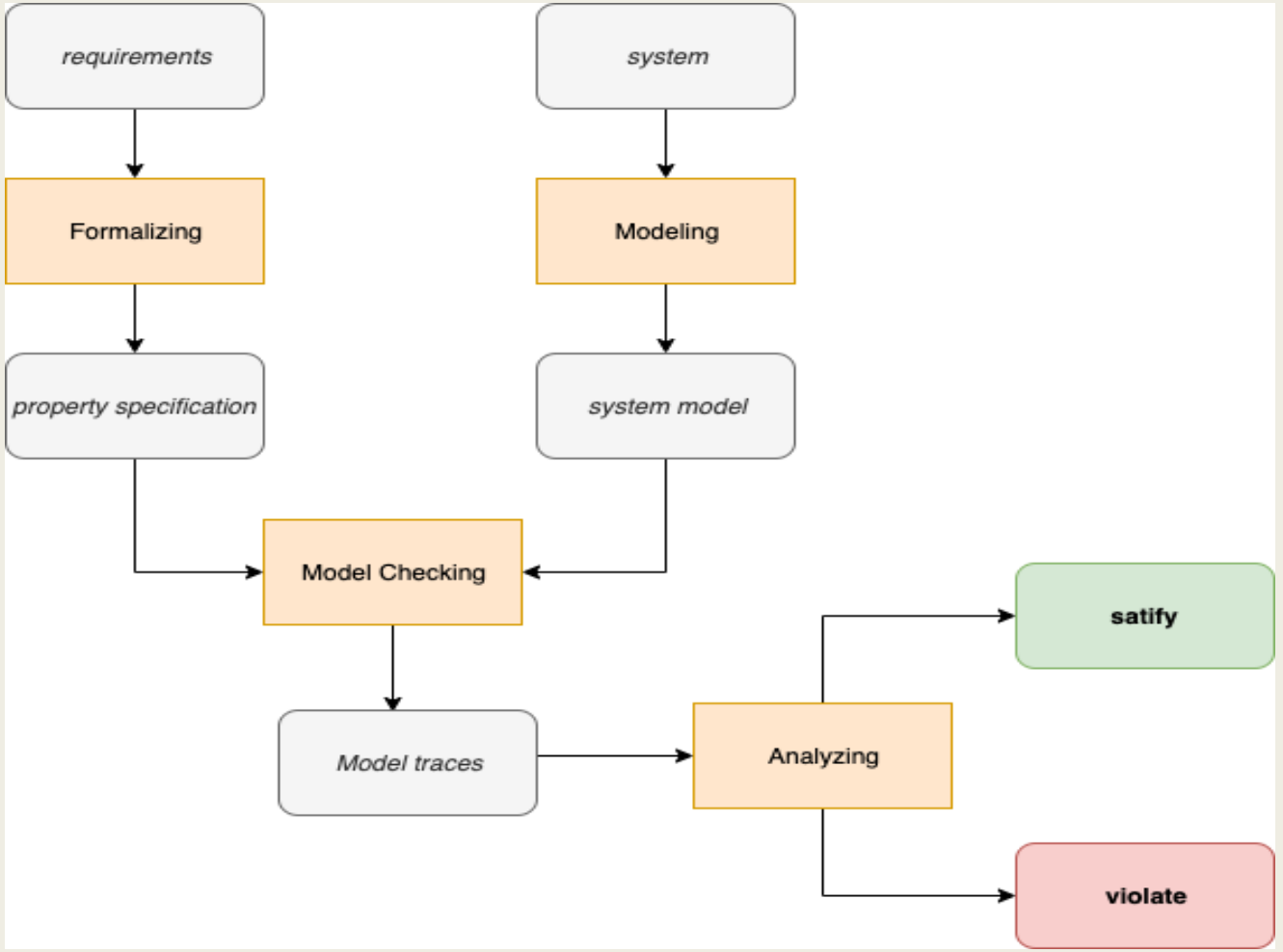


Model-checking

The main goal is to check
how much the program conforms
to a set of formal constraints
expressed in the language
of *linear temporal logic*

Model-checking is performed during
The following **3 stages**:

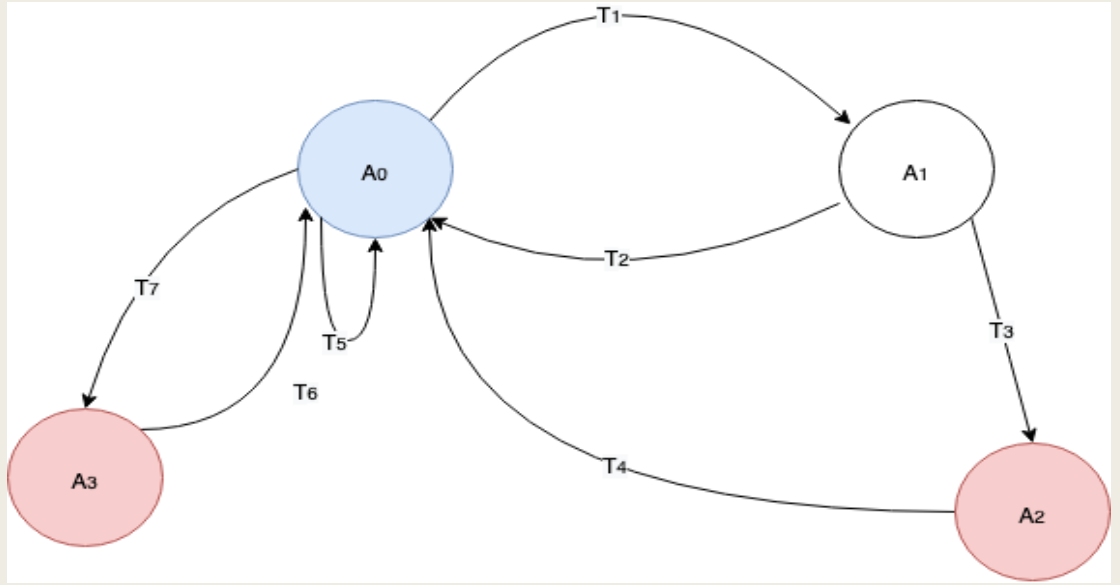
- The stage of modeling;
- The simulation stage;
- The stage of analysis.



Model and estimation

The diagram represents all the possible *states* and *transitions* of the simulated system as an oriented graph where:

a) **A0** - initial state;
b) **A1** - registration trial;
c) **A2** - successful registration;
d) **A3** - registration failure.

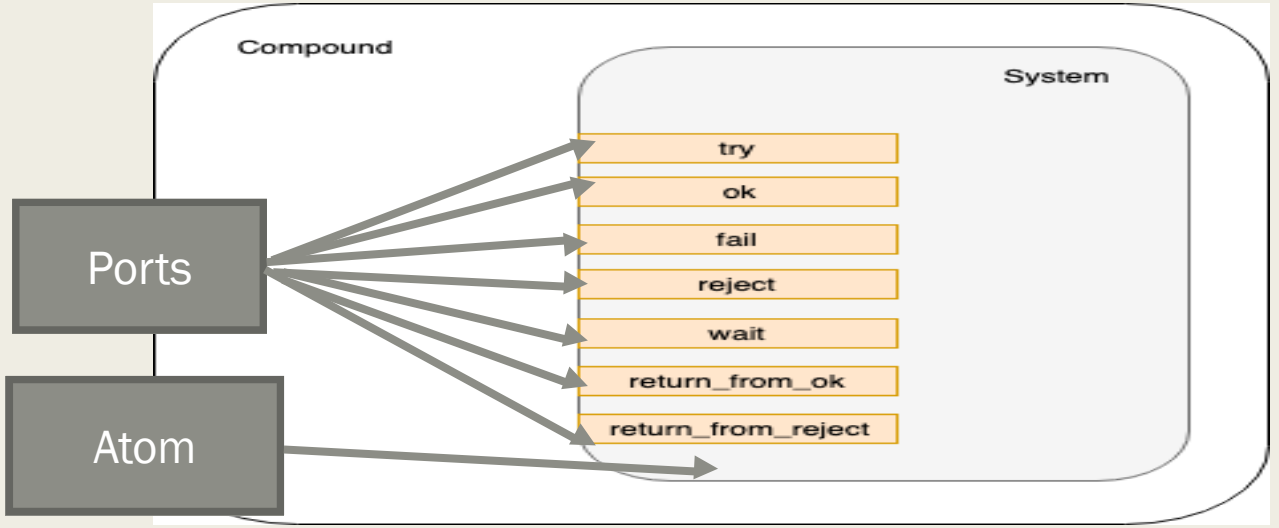


To evaluate the results of model checking a method of statistical analysis of stochastic systems was used, specifically the method of probability estimation - **PESTIM (Probability Estimation)**

Parameters:

α = 0.1

β = 0.1

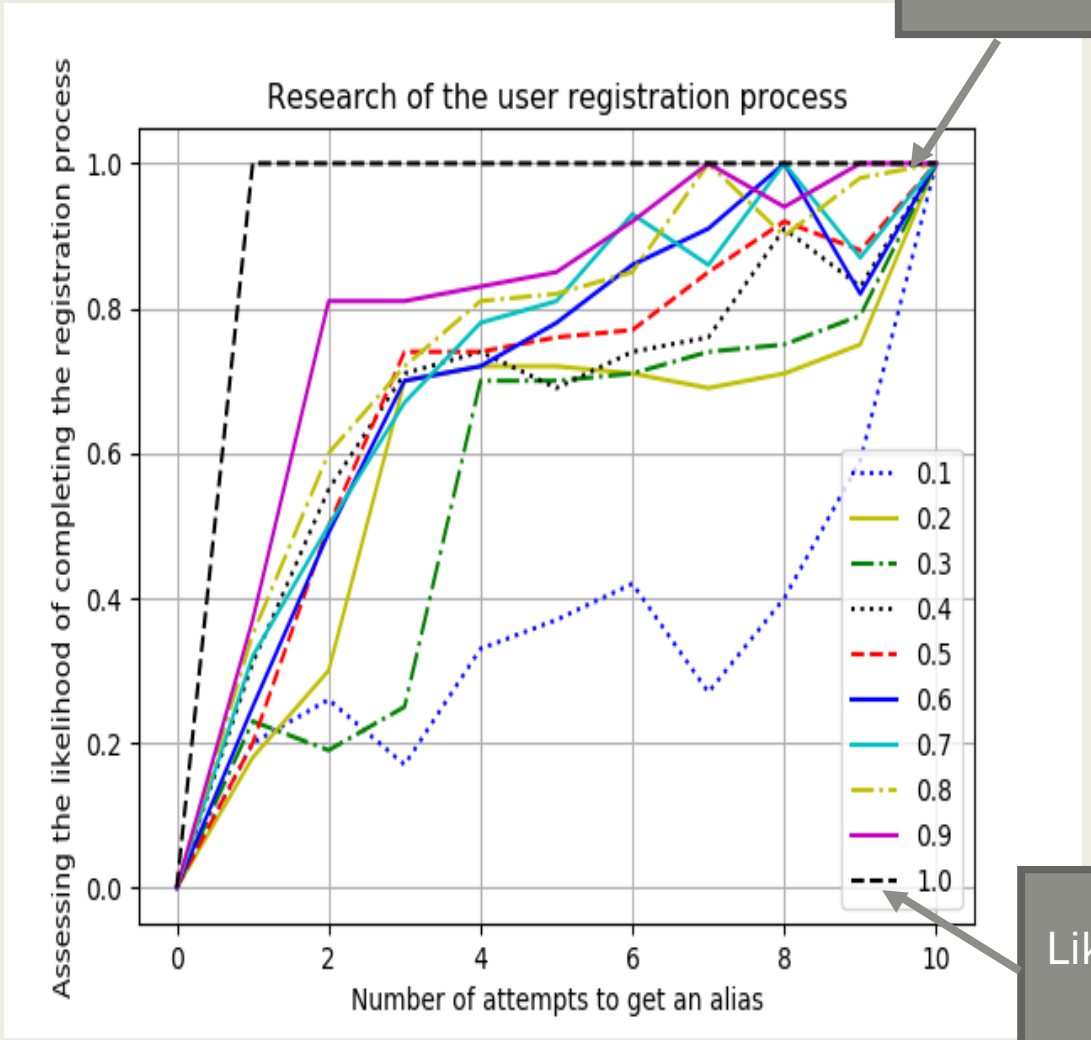


Results

$$\varphi(t) \equiv \Diamond_{[0,t]}[\neg(System.state = 0) \wedge (System.c \leq x)]$$

The results of the study :

1. the more the storage is filled up, the more time the user needs to go through the registration process;
2. after a certain number of attempts to obtain an alias defined by the N parameter, a user is guaranteed to be rejected in registration.



Max number of attempts

Likelihood of getting alias