Hello, researchers!

I am investigating ways of verifying temporal properties of smart contracts using Linear Temporal Logic.

Putting it simple, besides checking that a smart contract never violates some property P

(variables never overflow, balance is always positive, etc so called safety properties), I would like to

ensure that it behaves as expected over its lifetime: if event B fires, it must be the case, that,

before that, event A has fired; if event A fires then after some time, event B will fire; and so on.

As far as I know, most approaches concerning smart contract correctness are focused solely on safety

properties, while liveness properties stay out of reach for most modern tools/attempts.

My aim is to research this subject in several directions. Questions to be answered are:

1. To what extent Linear Temporal Logic (in its classic form) can be a good fit for specifying useful properties of smart contracts?

We have to do several specification attempts before the answer will emerge.

1. Do we need to extend LTL with modality of the past?

While doing some toy examples, I found,

that sometimes I need to express dependency between the current event and past events instead of

traditional “event A leads to event B” future-oriented style. I would like to make specification language as convenient as possible for a business user.

1. For bounded systems, temporal property can be model-checked. For unbounded systems, temporal model checking is undecidable; for that reason, I would like to build a reasoning framework inside Coq proof assistant

to be able to deduce properties using logical inference.

The research work is in its infancy, however, I made a prototype of the framework in Coq, and specified

one toy contract example.

What I would like to do is to specify some non-trivial contracts. There are many contracts source code

available online, but this is useless unless someone can answer questions regarding on how the contract

should

behave over time (having only the source code, you always have to guess about its intended

behavior)

For that reason, I need someone who can play a role of an expert on contract’s behavior under study.

This person can be someone who wants to check his contract for correctness, or more deeply understand

its properties.

Feel free to contact me if interested in any form

of research collaboration. We can discuss things.

Thanks!

P.S. For direct messaging, this site has “Messages” facility, look inside the profile.