Projet de Recherche et d'Innovation Master – Telecom Paris

Supervisor: *Vadim MALVONE*

Contact: *vadim.malvone@telecom-paris.fr*

Keywords: *Formal verification, Model checking, Multi-agent systems, Game theory, Blockchain*

Students required: *1*

Towards the verification of smart contracts

The problem of assuring systems correctness is particularly felt in hardware and software design, especially in safety-critical scenarios. When we talk about a safety-critical system, we mean the one in which failure is not an option. To face this problem, several methodologies have been proposed. Amongst these, model checking [1] results to be very useful. This approach provides a formal-based methodology to model systems, to specify properties via temporal logics, and to verify that a system satisfies a given specification.

Notably, first applications of model checking just concerned closed systems, which are characterized by the fact that their behavior is completely determined by their internal states. Unfortunately, model checking techniques developed to handle closed systems turn out to be quite useless in practice, as most of the systems are open and are characterized by an ongoing interaction with other systems. To overcome this problem, model checking has been extended to multi-agent systems. In the latter context, temporal logics have been extended to temporal logics for the strategic reasoning such as Alternating-time Temporal Logic (ATL) [2], Strategy Logic (SL) [3], and their extensions.

Multi-agent systems can model various concrete scenarios, including smart contracts [4]. However, while smart contracts can be considered a type of multi-agent system, their verification presents different challenges. A current limitation of smart contract verification tools is their inefficacy in expressing and verifying liquidity properties [5] related to the exchange of crypto-assets. For example, current logics cannot specify properties such as: is it guaranteed that, in every reachable state, a user can execute a sequence of transactions to withdraw a specified amount of crypto-assets?

The aim of this project is divided in four macro steps:

1. Analyze the state of the art on formal verification for multi-agent systems and smart contracts.

2. Define a new logic for the strategic reasoning that can incorporate the liquidity property.

3. Provide a verification algorithm for the new proposed logic.

4. Develop a module in the VITAMIN tool [6] that can solve the verification problem for the new logic proposed.

Bibliography

[1] E. M. Clarke, O. Grumberg, and D. A. Peled. Model Checking. MIT Press, 1999.

[2] R. Alur, T.A. Henzinger, and O. Kupferman. Alternating-Time Temporal Logic. JACM, 49(5):672–713, 2002.

[3] F. Mogavero, A. Murano, G. Perelli, and M. Y. Vardi. Reasoning About Strategies: On the Model-Checking Problem. TOCL, 15(4):34:1--34:47, 2014.

[4] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, Muhammad Imran: An overview on smart contracts: Challenges, advances and platforms. Future Gener. Comput. Syst. 105: 475-491 (2020)

[5] Massimo Bartoletti, Angelo Ferrando, Enrico Lipparini, Vadim Malvone: Solvent: liquidity verification of smart contracts. CoRR abs/2404.17864 (2024)

[6] Angelo Ferrando, Vadim Malvone: VITAMIN: A Compositional Framework for Model Checking of Multi-Agent Systems. CoRR abs/2403.02170 (2024).