Formal Methods and Blockchain Models: Open problems, challenges and opportunities (Talk Abstract)

Abstract

The goal of this presentation is not only to give an overview of the different approaches and future tool pertaining to applications of formal methods in blockchain but also to present several new formal-related and logic-based approaches and challenges.

1. The Central Question

The first two subsections consists of two basic questions:

- What are formal methods?
- What added value can be expected from the use of formal methods?

We will give some informal definitions about formal methods such as

- A formal method is a method which makes use of a formal language for specification or mathematical modeling.
- Formal methods are the application of a fairly broad variety of mathematical fundamentals like mathematical logic (formal languages), automata theory etc. in software and hardware design, specification and verification.

2. The Central Problem

The fundamental problem of the researcher in the field of formal methods is to be able to insurance that the behaviour of the system is following the basic specifications.
We can say that the specification is a set which consists of the description of the system's desired behaviour.

3. Formal Methods and Blockchain

3.1. An overview

3.1.1. Formal Logic and Blockchain. According to [1] there are so many blockchain models and three major topics for the community of formal methods:

- To construct logics of authorization
- To construct logics of concurrency
- To construct logics of incentives

In our presentation we will give some simple examples and we will verify that this problem is not a trivial problem.
The second example that will be in the presentation is the Blockchain Epistemic Logic based on [4].

3.1.2. Formal Verification and Smart Contracts. In [7] the writers describe a a framework to analyze and verify both the runtime safety and the functional correctness of Ethereum contracts guided by an attack on TheDAO contract that exploited subtle details of the EVM semantics to transfer roughly 50M worth of Ether into the control of an attacker.

3.1.3. Formal Methods, Privacy and blockchain. Formal methods can and should be applied to privacy on blockchain applications. The nature of privacy and the nature of blockchain technology offers several not trivial research opportunities for the formal methods community.It is well known that privacy is an important concern for public and private institutions such as hospitals, banks, academic institutions etc.
Designing blockchain applications which will preserve the privacy specifications should be a purpose for the blockchain community.

3.2. Agent-behavior in a blockchain system

In this sections we will give a first definition about **stable behavior of a miner** through topological approach, using coalgebraic tools and notions. Also we argue that it is important to develop syntax and semantics of modal logics for reasoning about multiple parties, creating a map of formal verification projects on Digital Currency field and templates and languages which are suitable for formal verification.

3.2.1. The Preliminaries . We will give the basic definitions

Definition 1. *Let $\mathscr{C}$ be category and $T : \mathscr{C} \to \mathscr{C}$ an endofunctor the a T-coalgebra is a pair (X, ξ) where X is an object in category $\mathscr{C}$ and ξ is an arrow in $\mathscr{C}$, i.e $\xi : X \to T(X)$*

Example 1 (Topology)**.** *It is well known that we can obtain concrete examples of colagebras from topological spaces [6]. If (X, τ) is a topological space we can see it as a $\mathscr{T}$-coalgebra using the operation which associates with every point $x \in X$ the filter U_x , i.e.*

Definition 2. *Let $T : \mathscr{C} \to \mathscr{C}$ be an endofunctor then a morphism between two T-coalgebras (X, ξ) and (Y, γ) is a morphism $f : X \to Y$ such that the following diagram commutes, i.e. $\gamma f = T(f)\xi$.*

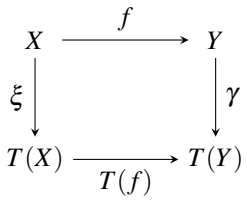

Figure 1. Morphism of $\mathscr{T}$-coalgebra

In computer science, coalgebra has emerged as a formal way of specifying the behaviour of systems and the behaviorally equivalent of two states.

Definition 3. *For two coalgebras $\xi : X \to T(X)$ and $\xi' : X' \to T(X')$, we say that two states $x \in X$ and $x' \in X'$ are **behaviourally equivalent** and we write $x \leftrightharpoons x'$ if there exists a coalgebra $\phi : U \to T(U)$ and two coalgebra homomorphisms $f : X \to U$ and $g : X' \to U$ such that $f(x) = g(x')$.*

It is obvious form the above definition that behaviour equivalence is a reflexive and symmetric relation, it is not difficult to show that in any category with pushouts the behaviour equivalence is also transitive relation. The initial step for our work is to introduce a definition about the behavior of agents using topological notion.

Definition 4 (Stable under Behavior - SuB). *Let X set, τ a topology over X and f a function $f : X \to X$, then a point is defined as Stable under Behavior of the open U_x and the orbit of function f if and only if for every $n \in \mathbb{N} : f^{(n)}(x) \in U_x$.*

Theorem 1. *Let (X, τ), (Y, ρ) be topological spaces, α a continuous function on X and $x \in X, y \in Y$ two behaviorally equivalent points, and x is Stable under Behavior of α and U_x then z - where $f(x) = g(y) = z \in (Z, \chi)$ - is Stable under Behavior of $f[U_x]$ and $g = f \circledcirc \alpha$, where $g : Z \to Z$ such that $g^{(n)}(z) = f\left(\alpha^{(n)}(x)\right)$*

4. CONCLUSIONS and FUTURE WORK

Based on the presented arguments, it is clear that we treat **states** as **miners**, also it becomes clear that it is important to develop syntax and semantics of modal logics for reasoning about multiple parties, creating a map of formal verification projects on Digital Currency field and templates and languages which are suitable for formal verification.
Furthermore, regarding the increasing models of blockchain systems, another goal of our team is to develop **a calculi for blockchain's logics**

APPENDIX

Appendixes could have the basic proofs of our work

References

[1] Herlihy, Maurice & Moir, Mark. (2016). Blockchains and the Logic of Accountability: Keynote Address. 27-30. 10.1145/2933575.2934579.

[2] Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cdric Fournet, Anitha Gollamudi, Georges Gonthier, Nadim Kobeissi, Natalia Kulatova, Aseem Rastogi, Thomas Sibut-Pinote, Nikhil Swamy, and Santiago Zanella-Bguelin. 2016. Formal Verification of Smart Contracts: Short Paper. In Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security (PLAS '16). ACM, New York, NY, USA, 91-96. DOI: https://doi.org/10.1145/2993600.2993611

[3] Halpern, J. Y., and Pass, R., A Knowledge-Based Analysis of the Blockchain Protocol, in Proceedings of the Sixteenth Conference on Theoretical Aspects of Ra-

tionality and Knowledge (TARK 2017), EPTCS 251 (2017), 324-335.

[4] Brnnler, Kai & Flumini, Dandolo & Studer, Thomas. (2017). A Logic of Blockchain Updates.

[5] Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., Rastogi, A., Sibut-Pinote, T., Swamy, N., Zanella-Beguelin, S.: Formal verification of smart contracts. In: PLAS (2016)

[6] Chung, K.O.: Weak homomorphisms of coalgebras. Doctoral dissertation. Iowa State University (2007)

[7] Patrick Blackburn, Johan F. A. K. van Benthem, and Frank Wolter. 2006. *Handbook of Modal Logic*, Volume 1 (Studies in Logic and Practical Reasoning). Elsevier Science Inc., New York, NY, USA.