# Automating Security Analysis of Off-Chain Protocols

**Lea Salome Brugger, Laura Kovács, Anja Petković Komel, Sophie Rain, and Michael Rawson**
TU Wien

## Abstract

Game-theoretic approaches provide new ways to model and formally prove security properties of off-chain protocols. For complex protocols, carrying out such formal proofs is a cumbersome and error-prone task. We describe our ongoing efforts for automating the security analysis of off-chain protocols. We encode the game-theoretic protocol model, together with its security properties, as universally quantified formulas, and use SMT solving to enforce these properties.

**2012 ACM Subject Classification** Security and privacy → Logic and verification; Security and privacy → Formal security models

**Keywords and phrases** automated reasoning, secure blockchain, off-chain channels, game theory

**Digital Object Identifier** 10.4230/LIPIcs...

**Category** Lightning Paper

## 1 Introduction

Blockchain technology is becoming increasingly popular in cryptocurrency systems, such as Bitcoin [4], as it allows maintaining a decentralized and secure record of transactions. In order to scale the transaction throughput of a blockchain, off-chain solutions have been proposed which conduct only a few transactions on the blockchain [2]. An example of an off-chain solution is given by Bitcoin's Lightning Network [4], where (transaction) participants can open a shared channel in which they can deposit money. As long as the channel is open, the deposited money can be redistributed among participants in arbitrarily many off-the-blockchain transactions. Ultimately, the channel is closed, and the latest deposit distribution state is published on the blockchain [5].

In order to enhance trust in and increase the popularity of off-chain protocols, their security should be formally verified. In this regard, game-theoretical approaches have been proven to be quite useful [6, 5]. The advantages of employing game theory in the context of off-chain protocol security are manifold. Most importantly, by modeling a protocol as a game, the strategic interaction between different participants, also called players or agents, can be expressed. Therefore, not only *honest* behavior is considered — where all players act in the intended way in the blockchain — but *all* potential scenarios, including where a set of player behaves dishonestly. By assigning utility values for each player in the game to each possible outcome, one can formally establish whether a player or a set of players gains any benefit from deviating from the intended (honest) behavior.

Zappalà et al. have taken the first step towards establishing game-theoretic models for off-chain protocols [6]. By improving the results of [6], Rain et al. advocate the use of extensive form games (EFGs) for modeling closing and routing phases in off-chain protocols, among other uses [5]. The proposed game-theoretic models are analyzed manually, complemented with rigorous, but tedious, proofs ensuring that the respective models (do not) fulfill certain security properties. We note that a formal analysis of even seemingly simple protocols, like the closing phase of a Lightning channel in [5], requires a comparison of billions of different game strategies. While there is work on automating the analysis of games, such as [3], to the best of our knowledge, existing approaches are limited to fixed numeric utilities. However, to prove a protocol secure, all possible utility values must be considered, which imposes the challenge of using symbolic variables modeling utilities. In

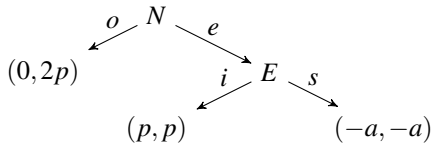


**Figure 1** Market Entry Game as EFG, with integer-valued $a, p > 0$.

this work, we address this challenge in an extension of [5]: we use symbolic utilities and propose *a fully automated framework to analyze game-theoretic security properties* of off-chain protocols (Section 3), by formalizing these properties as game-theoretic arguments (Section 2).

## 2 Formalization of Security Properties

▶ **Example 1** (Market Entry Game)**.** An EFG consists of players' finitely many subsequent choices, which lead to a utility for each player. To illustrate our work, consider the EFG in Figure 1 with two players: Player $N$, being a company thinking about entering a new market; and player $E$, who is established in this new market. Company $N$ first chooses if they want to enter the market (represented by action $e$), or stay out of it (action $o$). If $N$ picks action $o$, then $N$'s utility is 0, as they do not make any money in the market, but do not have any financial loss either; the other company $E$, however, gets all the profit $2p$ of this market. If $N$ chooses action $e$, then $E$ has to make a decision whether they ignore the new competitor (action $i$) and therefore share the profit (both getting utility $p$); or whether they fight them with an aggressive pricing strategy (action $s$), causing both companies a negative utility of $-a$.

In [5], Rain et al. established three game-theoretical security properties for off-chain protocols, as listed below. To this end, the intended behavior of the protocol, called the *honest behavior*, is analyzed, by defining *honest players* as the players who follow the honest behavior.

1. **Weak immunity**: No honest player can lose resources.
2. **Collusion resilience**: No strict subgroup of players benefits from deviating from the honest behavior.
3. **Practicality**: In each subgame of the game modeling the protocol, no player can benefit from unilaterally deviating from the honest behavior.

▶ **Example 2** (Security Properties for Market Entry Game)**.** We (randomly) fix the honest behavior of Example 1 to be: $N$ chooses $e$ and $E$ chooses $i$, which we notate as $(e,i)$, and check which security properties it satisfies. For weak immunity, we have to ensure that an honest player cannot get a negative utility, no matter what the other player does. Assume player $N$ is honest and chooses $e$. Then, player $E$ can deviate from the honest behavior and choose $s$, yielding the negative utility $-a$ for $N$. Hence, $(e,i)$ is not weak immune. Similarly, we conclude $(e,i)$ is collusion resilient and practical.

## 3 Automating Security Analysis

Our work automatically (dis)proves the three security properties from Section 2. Our approach, implemented in Python, takes as input an EFG and additionally an honest behavior with regard to the three security properties from Section 2. By applying game-based reasoning, our work outputs whether the considered security properties are valid for the input game and honest behavior. We also provide joint strategies (extending the honest behavior) witnessing the properties that hold.

Our framework encodes the game and security properties as formulas constructed from propositional variables, universally quantified integer variables, constant integer values and the usual

(interpreted) connectives, functions and predicates. These formulas are processed with the Z3 SMT solver [1]. For each of the three security properties from Section 2, we apply SMT solving to find a model representing a suitable joint strategy for the given honest behavior, satisfying the respective security property (as outlined in Example 3). Our approach also respects any constraints on the ordering of the utility variables that are provided by the user, and reports if they are infeasible. We have successfully applied our SMT-based framework to the analysis of closing/routing games [5], as well as to EFGs similar to Example 1, as also illustrated below.

▶ **Example 3.** We consider the weak immunity property of Example 2 for the honest history $(e,i)$. We would like to obtain a weak immune joint strategy, a choice of action for each player; hence, one action per internal node of the game tree. The formula asserting this property (in Z3) is:

```
1 ForAll([a, p], Implies(And(a > 0, p > 0),
2                        And(Or(->o, ->e), Or(Not(->o), Not(->e)),
3                            Or(e->i, e->s), Or(Not(e->i), Not(e->s))),
4                        And(->e, e->i),
5                        And(Implies(->o, 0 >= 0), Implies(->e, p >= 0),
6                        Implies(->e, -a >= 0), Implies(true, p + p >= 0),
7                        Implies(e->i, p >= 0), Implies(e->, -a >= 0)))))
```

where line 1 corresponds to the initial constraints on the utility variables $a$ and $p$. The assertions in lines 2–3 ensure we get a joint strategy: `->o`, `e->i`,..., `e->s` are Boolean variables corresponding to actions. If Z3 returns a model interpreting these variables as `true`, the corresponding actions are part of the joint strategy; otherwise they are not. The formula in line 4 fixes the desired honest history. It is followed by constraints for the weak immunity property, ensuring utilities of honest players are non-negative. As there is no model for the above formula, our work reports the EFG of Example 2 is not weak immune, as expected.

## 4 Conclusion

Our initial results in automating the security analysis of off-chain protocols use tailored SMT solving over game-theoretic security properties, with symbolic utilities. Deriving precise conditions on symbolic utilities under which a given protocol is secure, and scaling our work to more complex protocols are interesting tasks for further work.

## References


1 Leonardo De Moura and Nikolaj Bjørner. Z3: An efficient SMT solver. In *TACAS*, page 337–340, 2008.

2 Abdelatif Hafid, Abdelhakim Senhaji Hafid, and Mustapha Samih. Scaling blockchains: A comprehensive survey. *IEEE Access*, 8:125244–125262, 2020. doi:10.1109/ACCESS.2020.3007251.

3 Richard D. McKelvey, Andrew M. McLennan, and Theodore L. Turocy. Gambit: Software tools for game theory, version 16.0.0, 2014. URL: http://www.gambit-project.org.

4 Joseph Poon and Thaddeus Dryja. The Bitcoin Lightning network: Scalable off-chain instant payments, 2016. URL: https://lightning.network/lightning-network-paper.pdf.

5 Sophie Rain, Zeta Avarikioti, Laura Kovács, and Matteo Maffei. Towards a game-theoretic security analysis of off-chain protocols. 2021. doi:10.48550/ARXIV.2109.07429.

6 Paolo Zappalà, Marianna Belotti, Maria Potop-Butucaru, and Stefano Secci. Game Theoretical Framework for Analyzing Blockchains Robustness. In *DISC*, pages 42:1–42:18, 2021. doi:10.4230/LIPIcs.DISC.2021.42.