netidee

STIPENDIEN

Automated Verification of Game-Theoretic Security Properties for Decentralized Protocols

Endbericht | Call 17 | Stipendium ID 6321

Inhalt

1 Einleitung 3

2 Allgemeines 5

3 Ergebnisse 6

4 Geplante weiterführende Aktivitäten 7

5 Anregungen für Weiterführung durch Dritte 8

1 Einleitung

Anwendungen der Blockchain-Technologie wie Kryptowährungen und decentralized Finance werden immer beliebter. Die Sicherstellung der Sicherheit solcher Anwendungen erfolgt momentan hauptsächlich durch die formale Analyse der zugrundeliegenden kryptografischen Protokolle. Obwohl diese Bemühungen effektiv sind, können sie böswillige Aktionen, die trotz formaler kryptografischer Garantien möglich sind, nicht erfassen. Eine relevante Gruppe von Protokollen, die sogenannten Off-Chain Protokolle, beherbergen aufgrund ihrer Struktur vieler solcher trotz Kryptographie möglichen bösartigen Aktionen.

Off-Chain Protokolle erreichen eine scheinbar widersprüchliche Eigenschaft: Sie ermöglichen, dass der Großteil der Transaktionen einer Kryptowährung Off-Chain (also ohne der Blockchain) durchgeführt, und die Transaktionen dennoch sicher sein können. Die Idee besteht darin, die Blockchain nur im Streitfall zu nutzen und ansonsten auf Off-Chain Transaktionen zwischen Teilnehmenden zurückzugreifen. Das Lightning Network von Bitcoin ist die am weitesten verbreitete Off-Chain Implementierung und beherbergt zum Zeitpunkt des Schreibens Bitcoins im Wert von mehr als 170 Millionen USD. Im Wesentlichen hinterlegen Parteien Geld in einer gemeinsamen Adresse, dem sogenannten Channel, und können später beliebig viele Off-Chain Transaktionen miteinander durchführen, indem sie das Guthaben im Channel umverteilen. Am Ende kann der Kanal geschlossen und der letzte Zustand (d.h. die Verteilung des Guthabens) On-Chain (also auf der Blockchain) gepostet werden. Off-Chain Transaktionen sind nicht auf das Ende des Channels beschränkt, sondern können über Channels hinweg weitergeleitet werden (sogenannte Multi Hop Zahlungen). Neben solchen Payment Channel Netzwerken wird zur Zeit ein ganzes Ökosystem von Off-Chain Protokollen für unterschiedlichste Kryptowährungen entwickelt.

Die kryptografischen Protokolle, die diesen Off-ChainKonstruktionen zugrunde liegen, sind recht komplex und beruhen vor allem auf spieltheoretischen Argumenten, um böswilliges Verhalten zu verhindern. Zum Beispiel verwendet das Lightning Network einen Bestrafungsmechanismus, um Parteien davon abzuhalten, alte Zustände On-Chain zu veröffentlichen, und einen Entsperrmechanismus, bei dem Parteien zunächst einen Nachbarn bezahlen und dann den gezahlten Betrag vom anderen abrufen, um Multi Hop Zahlungen sicherzustellen (d.h. entweder werden alle Kanäle konsistent aktualisiert oder keiner).

Off-Chain Protokolle unterliegen typischerweise strengen Sicherheitsanalysen, die sich jedoch auf kryptografische Eigenschaften konzentrieren und die spieltheoretischen nicht erfassen. Die spieltheoretische Sicherheit solcher Protokolle ist davon abhängig, ob es jemandem einen Vorteil bringt eine solche böswillige Aktion zu wählen. Diese Überlegung ist von spieltheoretischer Natur, daher sprechen

wir von spieltheoretischer Sicherheit. Es ist essentiell eine solche Analyse zu etablieren, um Bestrafungsmechanismen, die negative Konsequenzen für jedes böswillige Verhalten garantieren, in die Blockchain Protokolle einzubetten.

Kurz gesagt, ermöglicht die spieltheoretische Sicherheitsanalyse das Nachvollziehen der Anreizkompatibilität (Incentive Compatibility): Das heißt, ob böswilliges, aber kryptografisch mögliches Verhalten durch Bestrafungsmechanismen entmutigt wird. Sie ermöglicht auch das Erkennen und sogar Verhindern von Szenarien, die direkt zu Angriffen führen könnten. Der Mehrwert von spieltheoretischen Modellen zur Untersuchung der Sicherheit eines zugrunde liegenden Protokolls hängt klarerweise von der Vollständigkeit des Spiels ab, also davon, ob alle möglichen Interaktionen zwischen den Spieler*innen berücksichtigt wurden. Folglich sind vollständige Modelle oft recht große und komplexe Spiele. Zum Beispiel im von uns modellierten, sogenannten Closing Game, das die Abschlussphase im Bitcoin Lightning Netzwerk genau darstellt, gibt es Billionen möglicher Verhaltensweisen (Kombinationen von Spielstrategien). Die Größe von Modellen macht die manuelle Analyse spieltheoretischer Sicherheitsmodelle praktisch nicht durchführbar.

Im Rahmen meiner Dissertation stelle ich daher das CheckMate Framework vor, um das Schlussfolgern über die spieltheoretische Sicherheit von Blockchain Protokollen zu ermöglichen. Soweit uns bekannt ist, bietet CheckMate das erste automatisierte Framework zur Umsetzung spieltheoretischer Sicherheit, das zum Beispiel die Sicherheit realer Protokolle im Bitcoin Lightning Netzwerk beweisen oder widerlegen kann. Verwandte Ansätze zur Spielanalyse existieren, aber aktuelle Techniken sind auf die Verarbeitung von Spielen mit numerischen Werten beschränkt. In meiner Arbeit plädiere ich für die Verwendung symbolischer Werte, die Sicherheit für jeden möglichen numerischen Wert garantieren. Dadurch wird also zum Beispiel jeder mögliche Kontostand in decentralized Finance Anwendungen berücksichtigt.

Wir zeigen, dass die Formalisierung korrekt und vollständig ist: Unsere Sicherheitsbeweise implizieren spieltheoretische Sicherheit und umgekehrt. In diesem Zusammenhang führen wir neuartige Denkansätze auf Basis von SMT-Solvern ein, die skalieren und formale Verifikation nicht nur zur Umsetzung spieltheoretischer Sicherheit nutzen, sondern auch Gegenbeispiele und/oder Verfeinerungen der Voraussetzungen liefern, bei denen Sicherheitseigenschaften verletzt werden.

2 Allgemeines

Das zentrale Ziel meiner Arbeit besteht darin, die folgende Frage für ein gegebenes Blockchain Protokoll zu beantworten:

“Ist dieses Protokoll spieltheoretisch sicher?”

Konkret heißt das zweierlei Eigenschaften nachzuprüfen, nämlich: “Kann ehrlichen User*innen des Protokolls kein Schaden zugeführt werden, egal wie sich andere Teilnehmende verhalten?”, sowie “Bringt das ehrliche Verhalten den größtmöglichen Profit und ist somit die rationale Wahl?” Falls eine dieser beiden Fragen mit Nein beantwortet wird, ist das Protokoll spieltheoretisch *nicht sicher*. In diesem Fall möchten wir weiters folgende Frage beantworten: “Können Bedingungen hinzugefügt werden, um das Protokoll sicher zu machen, und welche sind das?”

Um die genannten Fragen zu beantworten, ergeben sich eine Reihe von Teilfragen: Was bedeutet es genau, dass die zuvor erwähnten Sicherheitseigenschaften erfüllt sind? Wie können wir Sicherheitseigenschaften im Sinne der Spieltheorie ausdrücken? Wie modellieren wir ein dezentrales Protokoll als Spiel? Können wir sicherstellen, dass keine möglichen Angriffspunkte übersehen werden? Gibt es eine allgemeine Methode, solche Protokolle zu modellieren, und wenn ja, können wir korrekte Modelle synthetisieren? Können wir den Denkprozess automatisieren?

Ziel meiner Arbeit ist es, ein Framework zu entwickeln, das die Spezifikation eines Blockchain Protokolls nimmt und der Benutzer*in sagt, ob es aus spieltheoretischer Sicht sicher ist. Wie oben erwähnt, existiert die Verifizierung der zugrunde liegenden Kryptografie bereits und fällt daher nicht in meinen Forschungsbereich. Durch meine Arbeit möchte ich Sicherheitsrisiken finden beziehungsweise ihre Abwesenheit beweisen. User*innen, die ausschließlich “sichere” Protokolle verwenden, haben die Garantie, dass ihnen - egal wie sich andere Teilnehmende verhalten – durch die Nutzung dieser kein Schaden entstehen kann. Darüberhinaus, werden sich rationale “Angreifer*innen” ehrlich verhalten, weil ihnen das schließlich den besten Profit bringt.

In meiner Arbeit möchte ich also

a) Sicherheit mithilfe von spieltheoretischen Konzepten definieren.
b) Richtlinen, Hilfsmittel und Automatisierung zur Modellierung von Protokollen als Spiele bereitstellen.
c) den SMT Solver Z3 verwenden, um spieltheoretische Modelle von Protokollen automatisch zu analysieren.
d) Sicherheitsergebnisse über Blockchain Technologie erhalten.

3 Ergebnisse

Während der Laufzeit des Stipendiums wurden drei wissenschaftliche Papers in Fachkonferenzen publiziert. Sie sind alle auf der Projekt Homepage downloadbar. Alle diese Publikationen beschäftigen sich mit unterschiedlichen Aspekten der spieltheoretischen Sicherheit von Blockchain Protokollen.

(1) Sophie Rain, Zeta Avarikioti, Laura Kovács, Matteo Maffei,
Towards Game-Theoretical Security Analysis of Off-Chain Protocols,
In *36th IEEE Computer Security Foundations Symposium* – CSF 2023, page 31–46.

(2) Lea Salome Brugger, Laura Kovács, Anja Petkovic Komel, Sophie Rain, Michael Rawson,
CheckMate: Automated Game-Theoretic Security Reasoning.
In *31th ACM Conference on Computer and Communications Security* - CCS 2023, page 1407–1421.

(3) Sophie Rain, Lea Salome Brugger, Anja Petkovic Komel, Laura Kovács, Michael Rawson,
Scaling CheckMate for Game-Theoretic Security,
In *Proceedings of the 25th Conference on Logic for Programming, Artificial Intelligence and Reasoning* – LPAR 2024, page 222-231.

In (1) haben wir definiert was spieltheoretische Sicherheit heißt und entsprechende spieltheoretische Formeln eingeführt. Damit habe ich Ziel a) von Kapitel 2 erfüllt. Die Eigenschaften um spieltheoretische Sicherheit festzustellen sind weak(er) immunity - zu garantieren, dass ehrlichen Teilnehmenden kein Schaden entsteht -, sowie collusion resilience und practicality -um sicherzustellen, dass sich rationale Teilnehmende ehrlich verhalten. Darüberhinaus haben wir in (1) die Abschlussphase des Lightning Protokolls als Spiel modelliert und dessen Sicherheit (manuell) analysiert. Das hat uns erlaubt erste Richtlinien zum Modellieren von Protokollen zu definieren (Ziele b und d).

In der Publikation (2), haben wir uns hauptsächlich mit der Automatisierung der spieltheoretischen Sicherheitsanalyse beschäftigt. Damit ist auch Ziel c) abgedeckt. Weiters haben wir in diesem Paper die Frage “Können Bedingungen hinzugefügt werden, um das Protokoll sicher zu machen, und welche sind das?” gelöst. Unser Tool CheckMate kann solche Bedingungen finden. Wir sind sogar einen Schritt

weiter gegangen und stellen, falls von der User*in gewünscht, alle möglichen “Angriffe” bereit.

Die dritte Publikation (3), beinhaltet schließlich die für den tatsächlichen Gebrauch optimierte und skalierende Version von CheckMate. Wir haben auch einige Benchmarks dafür definiert und analysiert (Ziel d).

Abgesehen von den bereits veröffentlichten Ergebnissen, habe ich weiters ein Projekt zur automatischen Modellierung von Protokollen als Spiele (Spielsynthese) in Zusammenarbeit mit der Ethereum Foundation. Das spielt ebenfalls in Ziel b) hinein. Details dazu habe ich in meinen Blogeinträgen “Was hat Synthese in der Informatik verloren” und “CheckMate trifft Ethereum” berichtet.

Ein anderes Thema das zur Zeit in Arbeit ist, ist die nächste Generation von CheckMate, durch das innovative Konzept der Compositionality in der Spieltheorie wollen wir CheckMate erweitern, es schneller und leichter anwendbar machen. Damit ist es für Ziele c) und d) relevant. Der Blogeintrag “Die nächste Generation von CheckMate”, erklärt die Idee. Letztlich arbeite ich auch noch an einem Projekt zur Modellierung und Verifizierung einer Blockchain Brücke, was ebenfalls für das Ziel b), sowie Ziel d) von Bedeutung ist. Über dieses Forschungsprojekt habe ich auch einen Blogeintrag versfasst, nämlich “Von der Theorie in die Praxis”.

4 Geplante weiterführende Aktivitäten

Wie im Planungsdokument festgehalten, habe ich folgende weiterführende Aktivitäten geplant. Zuerst möchte ich die Arbeit zu Compositionality zu einem Ende führen, die Ergebnisse in einem Paper zusammenfassen und bei der prestigeträchtigen Konferenz Principles of Programming Languages (POPL) im Juli einreichen.

Danach möchte ich meine Forschung zur Spielsynthese abschließen, den Prototypen implementieren und die Resultate ebenfalls in einem Paper sammeln. Ich habe dafür noch keine konkrete Veranstaltung im Blick, sollten die Ergebnisse sehr erfolgreich sein, könnte ich mir vorstellen sie bei der renommierten Konferenz über Programming Language Design and Implementation (PLDI) einzureichen.

Das dritte Forschungsprojekt in Bearbeitung ist die Modellierung der Blockchain Brücke. Ich hoffe die Modellierungsphase bis zum Herbst erfolgreich zu beenden und werde die Erkenntnisse nach Ablauf der Geheimhaltungsklausel öffentlich bekannt machen. Im Rahmen meines Doktorates wird sich realistischerweise keine Publikation dazu ausgehen. Ich schließe aber nicht aus, das nach Abschluss meines Studiums nachzuholen.

Abschließend, werde ich gegen Dezember diesen Jahres beginnen meine Dissertation zu schreiben und diese im Frühjahr 2025 verteidigen.

5 Anregungen für Weiterführung durch Dritte

Nach Abschluss des Compositionality Projekts halte ich die Automatische Analyse von Spielmodellen durch CheckMate für sehr abgerundet. Notwendig wäre meiner Meinung nach weitere Forschung in der Modellierung von Protokollen um auch diejenigen, die nicht von meinem Syntheseprojekt profitieren (also all jene die nicht vollständig in Solidity definiert sind), automatisch erstellen zu können. Das ist nämlich immer noch die größte Lücke in diesem Forschungsgebiet.

Es wäre außerdem interessant zu betrachten inwiefern sich unsere Ergebnisse auf andere Bereiche anwenden lassen. Das heißt, zu überlegen ob spieltheoretische Analysen auch in anderen Forschungsgebieten sinnvoll und gewinnbringend sind.

Allgemeiner betrachtet wäre es spannend herauszufinden ob man die Verifizierung der kryptographischen mit der Verifizierung der spieltheoretischen Sicherheit symbiotisch in einem System vereinen kann. Dadurch müssten User*innen ihr System nur einmal formal modellieren.