1. 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 meiner Arbeit möchte ich also Sicherheit mithilfe von spieltheoretischen Konzepten definieren, Richtlinen, Hilfsmittel und Automatisierung zur Modellierung von Protokollen als Spiele bereitstellen, den SMT Solver Z3 verwenden, um spieltheoretische Modelle von Protokollen automatisch zu analysieren, und Sicherheitsergebnisse über Blockchain Technologie erhalten.
Dadurch finde ich Sicherheitsrisiken beziehungsweise beweise ich ihre Abwesenheit. 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.

2. Ergebnisse

Im Rahmen des Stipendiums habe ich drei Papers veröffentlicht. Sie sind alle auf der Projekt Homepage downloadbar. Alle diese Publikationen beschäftigen sich mit unterschiedlichen Aspekten der spieltheoretischen Sicherheit von Blockchain Protokollen.
In der Ersten haben wir definiert was spieltheoretische Sicherheit heißt und entsprechende spieltheoretische Formeln eingeführt. Darüberhinaus haben wir in ein Blockchan Protokoll als Spiel modelliert und dessen Sicherheit (manuell) analysiert. Das hat uns erlaubt erste Richtlinien zum Modellieren von Protokollen zu definieren. Die zweite Publikation beschäftigt sich hauptsächlich mit der Automatisierung der spieltheoretischen Sicherheitsanalyse. Die dritte Publikation, beinhaltet schließlich die für den tatsächlichen Gebrauch optimierte und skalierte Version von CheckMate, unserem Tool zur automatischen Sicherheitsanalyse. Wir haben dafür einige weitere Spiele modelliert und analysiert.
Abgesehen von den bereits veröffentlichten Ergebnissen, forsche ich zur Zeit an drei weiteren Projekten.
Das Erste hat die automatische Modellierung von Protokollen als Spiele (Spielsynthese) als Ziel.
Das zweite Thema ist die nächste Generation von CheckMate, die durch das innovative Konzept der Compositionality, CheckMate erweitern, es schneller und leichter anwendbar machen wird. Letztlich arbeite ich auch noch an einem Projekt zur Modellierung und Verifizierung einer Blockchain Brücke.

3. Geplante weiterführende Aktivitäten

In den nächsten Monaten möchte ich die oben erwähnten laufenden Projekte zu Compositionality, Spielsynthese und zur Modellierung der Blockchain Brücke abschließen und bestenfalls als Papers bei Konferenzen einreichen. Daüberhinaus werde ich Ende des Jahres meine Dissertation verfassen und anschließend verteidigen.

4. Anregungen für Weiterführung durch Dritte

Die automatische Analyse der spieltheoretischen Sicherheit halte ich für sehr abgerundet. Daher würde ich weitere Forschung vor allem in der Modellierung der Protokolle empfehlen. Bestenfalls in der Form einer weniger restriktiven automatischen Spielsynthese. Eine andere interessante Richtung wäre die Anwendung von spieltheoretischen Analysen in anderen Forschungsbereichen, sowie die Kombination von kryptographischer und spieltheoretischer Sicherheit in einem gemeinsamen Framework.