netidee

PROJEKTE

EtherTrust

Zwischenbericht | Call 12 | Projekt ID 2158

Inhalt

1 Einleitung

In unserem Projekt EtherTrust beschäftigen wir uns mit der Entwicklung eines Analysetools für Smart Contracts, das Nutzern und Entwicklern von Smart Contracts schließlich mit Hilfe eine Online-Services verfügbar gemacht werden soll. Da das Ziel unseres Tools ist, belastbare Garantien für Ethereum Smart Contracts zu liefern, involviert das Projekt auch eine theoretische Modellierung der zugrunde liegenden Analyse und einen Beweis für deren Korrektheit.

2 Status der Arbeitspakete

2.1 Arbeitspaket 1 - *Bootstrapping*

Kurzbeschreibung der Haupttätigkeiten
Erkenntnisse zur Vorgangsweise
Kurzbeschreibung der erreichten Ergebnisse
Besondere Erfolge/ Probleme
Gab es große Abweichungen zum Plan? Warum?

Das Arbeitspaket 1 beschäftigt sich hauptsächlich mit der Literaturrecherche (1.1), der Auswertung existierender Ansätze zur Analyse von Ethereum Smart Contracts (1.2), dem Austausch mit der Community (1.3) und der Formulierung der Problemstellung (1.4). Das Vorgehen entsprach im Wesentlichen der üblichen Vorgehensweise, wie sie in der Wissenschaft praktiziert wird: Wir haben eine ausführliche Recherche existierender wissenschaftlicher Publikationen betrieben und uns auch andere Tools, die nicht in wissenschaftlichen Veröffentlichungen behandelt werden, angeschaut und ihre Funktionsweise analysiert. Des Weiteren haben wir uns intensiv über unsere Erkenntnisse mit anderen Wissenschaftlern (beispielsweise auf Konferenzen) ausgetauscht. Unsere Ergebnisse, eine Übersicht über existierende Ansätze haben wir schließlich in einer wissenschaftlichen Publikation (‚Foundations and Tools for the Static Analysis of Ethereum Smart Contracts', siehe Projektseite), die auch die allgemeine Problemstellung (nämlich die Eigenschaften, die wir von einem Analysetool für Smart Contracts erwarten) formuliert.
Bei der Bearbeitung dieses Arbeitspaketes haben wir festgestellt, dass leider viele der existierenden wissenschaftlichen Publikationen zu Smart Contract Analysetools, leider weder ihren Code noch genaue Details zur verwendeten Analyse bereitstellen. Dies macht es sehr schwierig, ihre Funktionsweise zu analysieren und mit anderen Tools zu vergleichen.
Ein besonderer Erfolg war es natürlich, dass wir unsere Ergebnisse publizieren konnten und auch ein im Rahmen eines Tutoriums auf einer großen Konferenz präsentieren durften (mehr dazu im Bereich Öffentlichkeitsarbeit).

Planabweichungen gab es im Wesentlichen nicht. Man sollte nur anmerken, dass es sich bei der Recherche in einem so schnelllebigen Bereich wie Kryptowährungen um einen kontinuierlichen Prozess handelt, so dass wir in den anderen Arbeitspaketen auch immer wieder etwas Zeit in die Recherche stecken müssen.

2.2 Arbeitspaket 2 – *Formale Semantik und Sicherheitseigenschaften*

Kurzbeschreibung der Haupttätigkeiten
Erkenntnisse zur Vorgangsweise
Kurzbeschreibung der erreichten Ergebnisse
Besondere Erfolge/ Probleme
Gab es große Abweichungen zum Plan? Warum?

In Arbeitspaket 2 werden die Grundlagen für das Analysetool gelegt, indem zunächst die Semantik von Ethereum Smart Contracts als auch für uns interessante Sicherheitseigenschaften formal definiert werden. Zusätzlich implementieren wir die Semantik auch in einem Beweisassistenten, was uns erlaubt die Semantik zu testen und später auch maschinell verifizierte Beweise zu führen. Die Formalisierung der Semantik war als solche sehr herausfordernd, da die von Ethereum bereitgestellte Beschreibung an vielen Stellen ungenau und fehlerhaft ist und wir so auch konkrete Implementierungen für die Ausführung von Smart Contracts in Betracht ziehen mussten. Um generische Sicherheitseigenschaften zu formulieren, mussten wir viele existierende Probleme von Smart Contracts analysieren um die darunterliegende Problematik zu verstehen und dann formal auszudrücken. Die Ergebnisse, eine vollständige formale Semantik für Ethereum Smart contracts, eine Implementierung im Beweisassistenten F* und formale Sicherheitseigenschaften, die reale Schwachstellen in Smart Contracts ausschließen, haben wir in unserem wissenschaftlichen Papier ‚A Semantic Framework for the Security Analysis of Ethereum smart contracts' (siehe Projektseite) zusammen gefasst, das auf der Konferenz POST akzeptiert wurde. Ein besonderer Erfolg war, dass wir für dieses wissenschaftliche Papier sogar einen Best Paper-Award der Dachkonferenz ETAPS erhalten haben, was eine große wissenschaftliche Auszeichnung ist und zeigt welch großes Interesse an dem Thema unserer Forschung besteht.
Wesentliche Planabweichungen gab es bei der Bearbeitung des Arbeitspaketes nicht. Wir haben jedoch die Beobachtung gemacht, dass die Semantik von Smart Contracts in letzter Zeit häufiger von Ethereum angepasst wurde. Aus diesem Grund, stecken wir aktuell auch Energie darein, die Änderungen einzupflegen und unsere Implementierung zu verbessern, damit diese eine bestmögliche Grundlange für unsere Analyse darstellt.

2.3 Arbeitspaket 3 – *Statische Analyse*

Kurzbeschreibung der Haupttätigkeiten
Erkenntnisse zur Vorgangsweise
Kurzbeschreibung der erreichten Ergebnisse
Besondere Erfolge/ Probleme
Gab es große Abweichungen zum Plan? Warum?

Arbeitspaket 3 widmet sich der formalen Spezifikation der Analyse von Ethereum Smart Contracts. Zu diesem Zweck muss die oben beschriebene Semantik abstrahiert werden und ebenso müssen die Sicherheitseigenschaften abstrahiert werden, so dass sie mithilfe der abstrahierten Semantik ausdrückbar sind. Schließlich soll die definierte Analyse im Rahmen eines Analyse-Tools implementiert werden, so dass Smart Contracts automatisch auf die vordefinierten Sicherheitseigenschaften hin analysiert werden können.
Zu diesem Zweck haben wir die Analyse zunächst theoretisch skizziert und sie dann mithilfe eines Prototyps implementiert um zu evaluieren, ob die theoretische Analyse auch praktisch anwendbar ist. Das Problem liegt darin, dass wir zur automatischen Durchführung der Analyse einen sogenannten SMT-Solver nutzen. Da dieser sehr komplex ist, muss man in einem gewissen Rahmen experimentell evaluieren welche Formulierung und Enkodierung der Analyse zu effizienten Ergebnissen führt. Dies hat sich als komplizierter herausgestellt als wir anfangs dachten, insbesondere auch, weil die Komplexität des Codes des Analysetools über die unterschiedlichen Änderungen der Analyse immer weitergewachsen ist und damit auch immer unübersichtlicher wurde. Obwohl wir zwischenzeitlich einen funktionierenden Prototyp hatten, haben wir uns deshalb entschieden, das Tool noch einmal neu zu implementieren – diesmal auf eine allgemeinere Art und Weise. Das ist uns besonders wichtig, da wir ja am Ende belastbare Sicherheitsgarantien liefern wollen und somit auch eine Implementierung benötigen, der wir das nötige Vertrauen entgegenbringen. Außerdem ist uns bei der ersten Implementierung auch aufgefallen, dass es besserwäre das Tool so zu designen, dass es etwas fortgeschrittenen Nutzern und anderen Wissenschaftlern eine Schnittstelle liefert um neue oder maßgeschneiderte Eigenschaften zu enkodieren. Mit den Erkenntnissen, die wir während des Experimentierens gewonnen haben, hoffen wir jetzt ein sehr viel saubereres Tool programmieren zu können, dessen Verbindung zur formalen Analysedefinition klar ersichtlich ist und das leicht angepasst und um neue Eigenschaften erweitert werden kann.
Aus diesem Grund sind wir mit diesem Arbeitspaket noch nicht soweit fortgeschritten, wie wir wollten, auch wenn wir schon eine gute theoretische Grundlage gelegt haben (die Analyse und die entsprechenden abstrakten Eigenschaften sind bereits in einem Papier zusammengefasst: ‚EtherTrust: Sound Static Analysis of Ethereum bytecode', siehe Projektseite).

2.4 Arbeitspaket 4 – *Website*

Arbeitspaket 4 umfasst die Entwicklung der Website. Leider haben wir mit diesem Arbeitspaket noch nicht begonnen, weil wir aktuell unsere Energien in die Fertigstellung des Analysetools stecken und die konkrete Neugestaltung des Tools Auswirkungen auf die Funktionsweise der Website haben wird. Wir planen spätestens im Februar mit der Entwicklung der Website zu beginnen.

3 Zusammenfassung Planaktualisierung

Alle Anpassungen des Plan-Excels kurz zusammengefasst

Die größte Änderung in dem Plan besteht darin, dass wir die Projektlaufzeit gerne verlängern würden. Das hat verschiedene Gründe: Zum einen haben wir festgestellt, dass die Implementierung des Analysetools leider doch mehr Zeit in Anspruch nimmt, als gedacht. Das liegt vor allem daran, dass wir während der Entwicklung gemerkt haben, dass ein allgemeinerer Ansatz bei der Implementierung viele Vorteile bringen würde (siehe Diskussion zu Arbeitspaket 3) und deshalb sehr gerne jetzt lieber die Zeit investieren würden um ein stabileres Tool zu entwickeln, dass leichter erweitert werden kann. Wir denken, dass dies dem Open-Source-Gedanken am meisten entspricht, da wir gerne wollen, dass unser Tool als Basis für weitere Anwendungen dienen kann.
Ein weiterer Punkt, der unsere Projektplanung beeinflusst, ist dass sich kurzfristig ergeben hat, dass eine der Projektleiterinnen (Clara Schneidewind) Ende Januar für ein dreimonatiges Praktikum in die USA geht. Da somit eine Person fehlt, die sehr gut in das Projekt eingearbeitet ist, befürchten wir, dass wir den Zeitplan so nicht einhalten können.
Aus diesen Gründen würden wir das Projekt gerne um 3 Monate verlängern. Wir haben die Planung entsprechend angepasst. Insbesondere hat Arbeitspaket 3 nun eine sehr viel längere Laufzeit und die Implementierung (Arbeitspaket 4) haben wir entsprechend nach hinten geschoben. Da der prinzipielle Ablauf gleich bleibt, hat diese Änderung jedoch keine Auswirkung auf den Netzplan.
Eine weitere Anpassung, die wir vorgenommen haben, ist die Arbeitsteilung für das Arbeitspaket 4. Ursprünglich hatten wir geplant die Implementierung hauptsächlich von einem studentischen Mitarbeiter durchführen zu lassen. Da sich aber herausgestellt hat, dass es schwierig ist, einen Studenten zu finden, der über so lange Zeit sich mit so hohem Stundenaufwand der Implementierung widmen kann, haben wir uns entschieden den studentischen Mitarbeiter von Lehrstuhlseite weiter zu unterstützen, insbesondere mit einem PostDocs (Marco Squarcina) des Lehrstuhls, der eine große Expertise in Web-Entwicklung hat, und später auch mit unserem Teammitglied Clara Schneidewind, wenn sie aus den USA zurückkehrt.

Des Weiteren mussten wir eine Änderung in der Stundenberechnung durchführen. Leider waren wir das letzte Mal falsch informiert wurden inwiefern an unserer Universität Wochenstunden korrekt in effektive Arbeitsstunden umgerechnet werden. Das haben wir nun entsprechend angepasst, was zu einer allgemeinen Verringerung der Stundenlast geführt hat. Das kommt uns jedoch durchaus entgegen, da wir so nun dem sehr arbeitsaufwendigen Arbeitspaket 3 eine höhere Stundenzahl zukommen lassen können und gleichzeitig im Budget bleiben.
Eine weitere Anmerkung zu der Berechnung der Lohnkosten ist, dass wir festgestellt haben, dass sich Stundensätze leider monatlich ändern (da es Abgaben wie die U-Bahn-Steuer oder die FLAF-Abgabe gibt, die vom Arbeitgeber zu entrichten sind und monatlich variieren). Als Stundensatz haben wir deshalb jetzt den mittleren Stundensatz über den Berichtzeitraum veranschlagt. Es kann jedoch sein, dass der Stundensatz für den Endbericht entsprechend leicht variiert.
Erfreulicherweise haben wir auch festgestellt, dass Arbeitsplatzkosten nur für Mitarbeiter anfallen, die nicht ohnehin schon am Lehrstuhl angestellt sind und das außerdem anscheinend doch kein Overhead anfällt. Die Planung wurde entsprechend aktualisiert.

4 Öffentlichkeitsarbeit/ Vernetzung

Beschreibung der bereits erfolgten Öffentlichkeitsarbeit oder Vernetzung, bzw. Beschreibung des Plans künftiger Aktivitäten

Bisher haben wir es geschafft insbesondere durch Vorträge und Tutorien bei Konferenzen und Schools Aufmerksamkeit für unser Projekt zu erregen. So haben wir einen Vortrag zur Semantik und den Sicherheitseigenschaften im April 2018 bei der Konferenz POST (Teil der ETAPS Konferenz) in Thessaloniki gehalten. Da wir auf dieser Konferenz für unsere Publikation auch einen Best Paper Award erhalten haben, wurde dem Projekt dort eine besondere Aufmerksamkeit zuteil.
Ein 90-minütiges Tutorium (die Folien dazu sind auf unserer Projektseite veröffentlicht) zu EtherTrust haben wir auf der Verifikationskonferenz CAV gegeben, die dieses Jahr Teil der FLoC Konferenz in Oxford war, einer großen Logikkonferenz, die nur alle vier Jahre abgehalten wird. Als Teil von FLoC konnten wir mit diesem Tutorium viele Forscher im Bereich der Logik und Verifikation erreichen. Außerdem konnten wir die Konferenz nutzen um mit anderen Wissenschaftlern, die ebenfalls an der Analyse von Smart Contracts arbeiten, zu sprechen, beispielsweise mit den Entwicklern von KEVM oder Entwicklern der Ethereum Foundation.
Des Weiteren hat Professor Maffei einen Vortrag über EtherTrust bei der „Summer School on Security & Correctness in the IoT“ in Graz gegeben.

Über Präsentationen hinaus, bemühen sich unsere Teammitglieder sich auch in der Blockchain Community zu vernetzen, so hat Clara Schneidewindbeispielsweise im Juni 2018 den „Master Workshop: Off the chain“ besucht, bei dem sich viele Forscher und Enthusiasten der Blockchain-Community versammelt haben um über Lösungen für das Skalierbarkeitsproblem von Cryptocurrencies zu diskutieren. Ebenso hat Clara Schneidewind im Oktober das „Symposium on Post-Bitcoin Cryptocurrencies” in Wien besucht, bei dem die Chancen von Cryptocurrencies, wie Ethereum diskutiert wurden und bei dem sich viele nationale und internationale Wissenschaftler und Interessierte eingefunden hatten.

In der Zukunft wollen wir EtherTrust weiter in der akademischen und nicht-akademischen Welt vorstellen. Wir denken, dass die besonders effektiv möglich sein wird, sobald wir den ersten Prototypen unserer Website haben, da dies uns erlaubt, das Tool live zu demonstrieren und potentielle Nutzer zum Ausprobieren zu animieren.