1. Projektziel

EtherTrust ist ein Analysetool für Ethereum Smart Contracts, welches von Forschern der ‚Security and Privacy Group' an der TU Wien entwickelt wird. Ethereum Smart Contracts sind dezentrale Programme, die Geldflüsse der Kryptowährung Ethereum steuern. Da diese Programme die Kontrolle darüber haben, wie Geld auf der Ethereum Plattform verteilt wird, sind solche Anwendungen besonders sicherheitskritisch und Programmierfehler oder schadhafte Programme können schwere finanziellen Schäden verursachen. Aus diesem Grund ist es wichtig, solche Programme, bevor sie unwiderruflich auf der Ethereum Blockchain veröffentlicht werden, auf ihre Sicherheit hin zu überprüfen. Leider sind Smart Contracts jedoch in einem für Menschen unleserlichen Maschinencode geschrieben, so dass es einer Computergestützten Analyse bedarf um verlässliche Garantien über das Verhalten eines Vertrages zu liefern. EtherTrust ist ein vollautomatisches Analyse-Tool, das beweist, ob ein Smart Contract eine gewisse Sicherheitseigenschaft erfüllt. Somit kann es Entwicklern dabei helfen herauszufinden, ob ein von ihnen geschriebener Smart Contracts fehlerhaft ist. Gleichzeitig bietet EtherTrust auch Nutzern von Smart Contracts die Möglichkeit zu überprüfen, ob die Smart Contracts mit denen sie interagieren potentiell sicherheitskritisches Verhalten aufweisen. EtherTrust erreicht dieses Ziel, indem es intern einen Smart Contract in eine logische Repräsentation seines Ausführungsverhaltens übersetzt, welche dann mit einem automatisierten Lösungsprogram für logische Probleme analysiert wird. Mithilfe eines mathematischen Beweises, dass diese Übersetzung wesentliche Charakteristika des Vertrages erhält, können wir sicherstellen, dass das Ergebnis des Lösungsprogramms einen sicheren Rückschluss auf das Verhalten des ursprünglichen Vertrages zulässt.

2. Projektendergebnisse

1	*Projektzwischenbericht*	*CC-BY-4.0 International*	*netidee.at/ethertrust*
2	*Projektendbericht*	*CC-BY-4.0 International*	*netidee.at/ethertrust*
3	*Entwickler-DOKUMENTATION*	*CC-BY-3.0 AT*	*netidee.at/ethertrust*
4	*Anwender-DOKUMENTATION*	*CC-BY-3.0 AT*	*netidee.at/ethertrust*
5	*Veröffentlichungsfähiger Einseiter*	*CC-BY-3.0 AT*	*netidee.at/ethertrust*
6	*Dokumentation Externkommunikation zur Erreichung Sichtbarkeit /Nachhaltigkeit*	*CC-BY-3.0 AT*	*netidee.at/ethertrust*
7	*Vollständige EVM Bytecode Semantik*	*CC-BY-4.0 International*	*netidee.at/ethertrust*
8	*Implementierung der EVM Bytecode Semantik in F**	*GNU-GPLv3*	*netidee.at/ethertrust*
9	*Abstrakte Semantik für EVM Bytecode*	*CC-BY-4.0 International*	*netidee.at/ethertrust*

10	*Formalisierung von Sicherheitseigenschaften für smart contracts*	*CC-BY-4.0 International*	*netidee.at/ethertrust*
11	*Formalisierung von abstrakten Sicherheitseigenschaften für smart contracts*	*CC-BY-4.0 International*	*netidee.at/ethertrust*
12	*Analyse-Framework für Ethereum smart contracts*	*GNU-GPLv3*	*netidee.at/ethertrust*
13	*Webservice zum automatisierten Analysieren von Ethereum smart contracts*		*netidee.at/ethertrust*

3. Geplante weiterführende Aktivitäten nach netidee-Projektende

Wir planen EtherTrust nach Projektende weiterzuentwickeln. Insbesondere ist es unser Ziel, Laufzeitverhalten und Präzision von EtherTrust zu verbessern und das Tool um weitere vordefinierte Sicherheitseigenschaften zu erweitern. Wir hoffen EtherTrust auf diese Weise anwendungsfreundlicher zu machen und durch die zusätzlichen Funktionalitäten eine größere Zahl an Nutzern zu erreichen.

4. Anregungen für Weiterentwicklungen durch Dritte

EtherTrust wurde bewusst modular gestaltet, so dass es leicht von anderen Wissenschaftlern und Entwicklern weiterentwickelt werden kann. Kern dieses modularen Aufbaus ist die Spezifikationssprache HoRSt, in welcher das logische Ausführungsverhalten und Sicherheitseigenschaften des Vertrages auf eine menschenlesbare Weise definiert werden. Diese Spezifikationen können leicht von Dritten modifiziert und ergänzt werden, ohne dass sich diese mit Implementierungsdetails des Tools befassen müssen.