netidee Call12 | Stipendium-ID 2235

Kurzfassung

Die Cryptocurrency Bitcoin wurde im Jahre 2008 mit dem Erstellen des ersten Blocks, dem Genesis Block, gestartet. Seitdem hat sich die Rechenleistung des Netzwerkes, welches die Blockchain der digitalen Währung absichert, erheblich vervielfacht. Heute erweitern um die zwanzig professionelle Miner laufend die Blockchain, indem sie immer auf den jeweils neuesten, ihnen bekannten Block aufbauen. Die Miner belohnen sich dabei selbst, da sie mit jedem erstellten Block für sich neue Bitcoins schürfen.
Im Jahre 2014 zeigte Eyal und Gün Sirer erstmals, dass es neben diesem gewünschtem, ehrlichen Verhalten abweichende Miningmethoden gibt, welche den relativen Ertrag eines Miners gegenüber seiner Kontrahenten erhöht. Dieser sogenannte Selfish-Mining-Angriff und all seine Modifikationen werden in der vorliegenden Diplomarbeit in einem definierten Szenario mit zwanzig Miner untersucht und mit bisherigen Forschungsergebnissen verglichen. Im Gegensatz zu vorangegangen Untersuchungen, wurde hierfür eine neuartiges, deterministisches Simulationsframework basierend auf *Docker* entwickelt. Dieses Simulationsframework ermöglicht es einerseits die Netzwerklatenz auf natürliche Art und Weise zu berücksichtigen und andererseits die Referenzimplementierung von Bitcoin direkt wiederzuverwenden. Letzteres hat den Vorteil, dass keine zeitaufwendige und fehleranfällige Adaptierung oder Abstraktion der Referenzimplementierung notwendig ist und alle Eigenschaften des implementierten Bitcoinprotokolles automatisch in die Simulation miteinfließen. Um das Simulieren der verschiedenen Selfish-Mining-Strategien zu ermöglichen, wurde weiters ein Proxy implementiert, welcher einen Node im Netzwerk eclipsed und mithilfe dessen verschiedenste Selfish-Mining-Angriff ausführt.
Die Simulationen der verschiedenen Selfish-Mining-Strategien zeigen, dass ein dishonest Miner seinen relativen Ertrag gegenüber den Rest des Netzwerkes steigern kann und untermauern somit den momentanen Forschungsstand sowie die Relevanz des Selfish-Mining-Angriffs. Als effizienteste Selfish-Mining-Strategien unter dem verwendeten Simu-lationsszenario mit zwanzig Miner konnte Selfish-Mining und Equal-Fork-Stubbornness identifiziert werden.

Schlagwörter
Selfish-Mining, Selfish-Mining-Angriff, Bitcoin, Blockchain, Simulation, Simulationsframework, Netzwerklatenz, Referenzimplementierung, Docker