Ein Proof-of-Publication Service

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Dr. Kai Brünnler
Experte: Daniel Voisard (Bundesamt für Kommunikation BAKOM)

Mit Proof-of-Publication kann man, ähnlich wie beim Timestamping, die Existenz gewisser Daten im Nachhinein beweisen. Darüber hinaus bietet es die Möglichkeit sogenannte alternative Timestamps auszuschliessen. In dieser Arbeit wurde ein Dienst entwickelt der für Clients Proof-of-Publication anbietet und die Daten mithilfe von Bitcoin unveränderbar absichert. Mehrere Clients können sich dabei die Gebühren teilen.

Ausgangslage

Es existieren bereits Timestamping-Dienste, welche die Echtheit von Daten verifizieren. Das Problem dabei ist allerdings, dass ein unabhängiger Prüfer diesen Diensten glauben muss, korrekt gearbeitet zu haben. Des Weiteren gibt es einige Dienste die ihre Daten bereits heute in der Blockchain von Bitcoin speichern. Jedoch bieten diese kein Proof-of-Publication, also die alternativlose Veröffentlichung von Daten, an. Proof-of-Publication ist ein viel stärkerer Begriff als Timestamping. Konkret bedeutet Proof-of-Publication, dass zu einem gewissen Zeitpunkt alle Veröffentlichungen der beweisenden Partei bekannt sind.
Mit einem Proof-of-Publication-Dienst, der seine Daten in der Blockchain von Bitcoin speichert, könnte man diese Anforderungen erfüllen. Dabei würde er für seine Clients die Aufgabe der Veröffentlichung der Daten übernehmen. Die korrekte Funktionsweise dieses Dienstes kann dann von einem unabhängigen Kontrolleur überprüft werden.

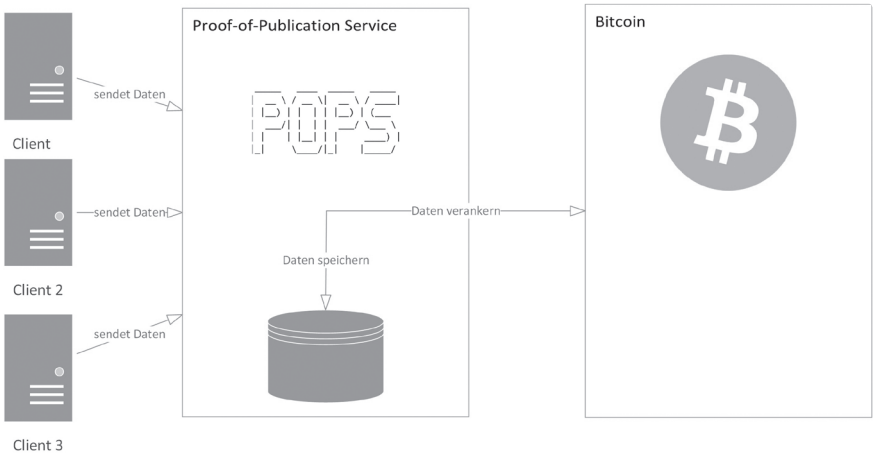
Ziele

Das Hauptziel dieser Arbeit war es, einen Prototyp eines solchen Dienstes zu entwickeln, der die entstandenen Gebühren für die Bitcoin-Transaktionen an seine Clients weiterverrechnet. Wenn mehrere Clients im selben Zeitraum Daten veröffentlichen wollen, sollen diese Daten ausserdem aggregiert und die anfallenden Gebühren auf die Clients aufgeteilt werden. Als Plattform für die Bezahlung soll dabei der Micropayments-Dients 21.co benutzt werden.

Ergebnis

Mithilfe der Python Bibliothek von 21.co wurde ein Prototyp entwickelt der Daten in der Blockchain von Bitcoin veröffentlicht. Clients können per Internet Daten an den Dienst schicken und diese veröffentlichen lassen. Der Prototyp funktioniert dabei so, dass die Clients mit den mitgeschickten Daten ein Timeout spezifizieren können, bis wann die Daten in das Bitcoin-Netzwerk verschickt werden müssen und wenn sich weitere Clients in dieser Zeit melden, werden die Transaktionsgebühren aufgeteilt. Nach Ablauf des Timeouts erstellt die Software eine Bitcoin-Transaktion an sich selbst, die zusätzlich einen Hash der erhaltenen Daten enthält. Ein unabhängiger Verifizierer muss nun bloss die Daten des Dienstes und die Daten in der Blockchain von Bitcoin vergleichen um die korrekte Funktionsweise zu überprüfen. Dieser Prototyp kann ausserdem dank der Container-Technologie Docker auf sehr einfache Art und Weise installiert werden.

Jonas Liechti



Schematischer Aufbau des Proof-of-Publication Services