Smart Contracts für Nutzung in einem WebShop Umfeld

Marko Alten, Christian Enderle, Yannik Laufer, Jona Ruthardt

Problemstellung

Die Anzahl der verfügbaren Computer Applikationen und Programmen ist in den letzten Jahren stetig gestiegen. Klassischer Weise werden diese Software Produkte mittels Softwarelizenzen für die Nutzung aktiviert. Zwar wird für die Softwareauslieferung mittlerweile vermehrt auf das Erstellen von Nutzerkonten gesetzt, denen die entsprechenden Lizenzen zugeschrieben werden, diese Herangehensweise hat aber jedoch auch ihre Nachteile (vgl. Kapitel „Vorteile gegenüber einer klassischen Lösung). Durch Smart Contracts und Blockchain-Technologien ist es möglich den Vorgang des Erwerbs von Softwarelizenzen sowohl für Konsumenten als auch für Anbieter einfacher, effizienter und sicherer zu gestalten.
Der in dem Project entwickelte Proof of Concept stellt eine prototypische Implementierung einer Online Shop Plattform dar, über die es möglich ist, Softwarelizenzen zu erwerben. Eine Besonderheit unserer Lösung ist dabei, dass die Zahlung der Lizenzkosten erst nach dem Kauf und dem Erhalt der Lizenzschlüssel getätigt werden muss. Dies erlaubt es das Produkt zunächst – mit einer Demovariante vergleichbar – zu testen und erst vollständig zu erwerben, wenn man mit den gebotenen Leistungen im Einen ist. Wird innerhalb eines definierten Zeitraums durch den Kunden keine Zahlung durchgeführt, so wird der Lizenzschlüssel automatisch deaktiviert und die Software ist nicht mehr nutzbar. Des Weiteren erlaubt dieser Verzögerte Zahlungsvorgang ein Zahlen auf Rechnung, was von Buchhaltungsabteilungen von Konzernen und Unternehmen unter Umständen eher befürwortet wird.

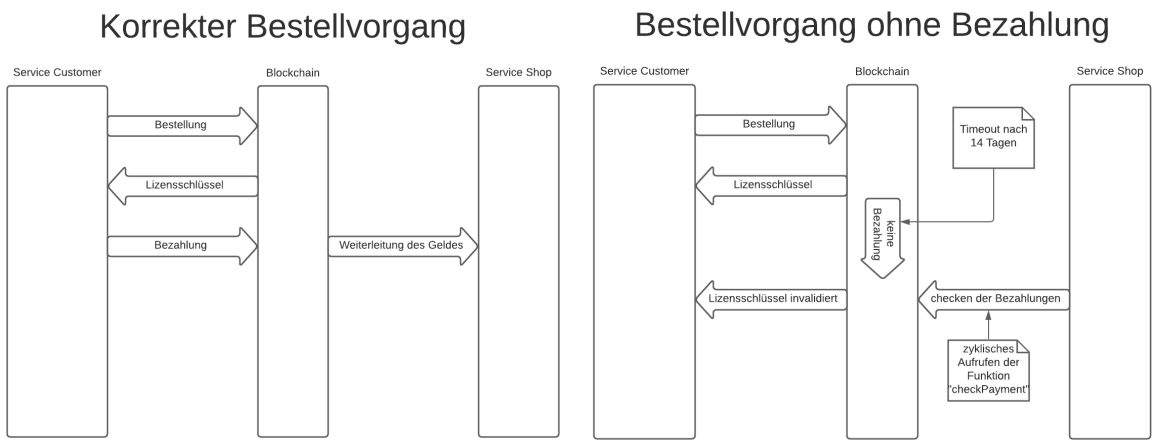
Lösungsansatz

Architekturentscheidungen

In der prototypischen Implementierung des Web Shops für Softwareprodukte gibt es drei verschiedene Parteien:

- **Service Customer** – Der Service Customer ist der Kunde, der eine Softwarelizenz erwerben will. Dieser ist in der Lage im Web Shop das entsprechende Produkt auszuwählen und einen Kaufvorgang zu initiieren.
- **Blockchain** – Über die Blockchain werden die Bestellungs- und Zahlungstransaktionen via Smart Contracts verwaltet, überwacht und erstellt.
- **Service Shop** – Der Service Shop ist der Anbieter der Software und verkauft Lizenzen für diese auf der Shop Platform zu einem gesetzten Preis.

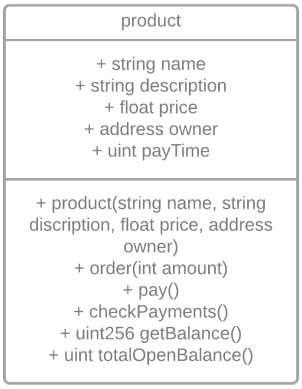
Dabei interagieren die Parteien wie im folgendem Ablaufdiagramm:



Im regulären Fall wird – getriggert durch einen Smart Contract – nach der Bestellung dem Nutzer ein Lizenzschlüssel für die Software zugestellt. Innerhalb einer definierten Zeitspanne bezahlt der Kunde die Software durch eine Transaktion auf der Blockchain. Wurde der korrekte Betrag überwiesen, so wird das Geld an den Service Shop, sprich den Softwareanbieter, weitergeleitet und der Kauf ist vollständig abgewickelt. Führt der Kunde die Bezahlung jedoch nicht fristgerecht durch, so wird der ausgestellte Lizenzschlüssel invalidiert und die Software ist nicht mehr nutzbar. Dieser Vorgang ist im rechten Teil der obenstehenden Abbildung aufgezeigt.
Hierbei werden die Transaktionen in die Blockchain geschrieben und via Smart Contracts überwacht. Dadurch ist gesichert, dass eine langfristige Nutzung nur bei erfolgreicher und vollständiger Zahlung ermöglich ist.

Implementierung

Für die Implementierung des Proof of Concepts für den Softwarelizenz Web Shop wird eine permissioned Etherium Blockchain eingesetzt. Der Smart Contract für den Softwarekauf wurde dabei mittels Solidity implementiert und durch Unit-Tests in JavaScript getestet. Durch die Klasse bzw. den Smart Contract *product* werden hierbei die angebotenen Softwareprodukte repräsentiert. Eine Instanz dieser Klasse enthält sowohl Informationen zu Name, Preis, Besitzer und Zahlungsdatum als auch Funktionen die durch die verschiedenen Akteure aufgerufen werden um das Produkt zu kaufen, zu bezahlen, oder zu überprüfen, ob die Zahlung bereits geleistet wurde. Die *product* Klasse ist somit wie folgt aufgebaut:



Das Nutzeroberfläche des Web Shops, über den der Kunde des Kaufvorgang vor nimmt wurde mittels eines einfachen HTML-Frontends erstellt und dient in der jetzigen Form in

erster Linie dem Vorführen der funktionalen Möglichkeiten die die Blockchain-basierte Lösung für den Kauf von Softwareprodukten bieten kann wobei eine intuitive Nutzung und ein attraktiven Aussehen zweitrangig sind.

Vorteile gegenüber einer klassischen Lösung

Gegenüber einer klassischen Lösung bei der Lizenzschlüssen für Softwareprodukte vergeben werden hat unsere Blockchain-basierte Lösung den Vorteil, dass die Gültigkeit des Lizenzschlüssels über eine Blockchain verwaltet werden kann. So kann eine Lizenz wieder entzogen werden, sollte keine Bezahlung erfolgt sein und eine unrechtmäßige Weitergabe bzw. ein Weiterverkauf (Schwarzmarkt) oder Diebstahl der Lizenz ist verhindert. Der Verkäufer hat stets Transparenz darüber, wer Besitzer der Lizenz ist. Dadurch wäre es auch möglich besser zu überwachen und verhindern, dass eine Lizenz von unterschiedlichen Nutzern auf verschiedenen Geräten genutzt wird.
Im Vergleich zu Konzepten bei denen man zu herstellerspezifischen Nutzerkonten Softwarenutzungsrechte kauft hat die von uns vorgeschlagene Lösung den Charme, dass diese es nicht erfordert sich ein separates Nutzerkonto anzulegen, sondern es ausreichend ist, wenn der Käufer eine Etherium-ID hat. Dies vereinfacht den Kaufprozess und macht es überflüssig jede Menge verschiedene Nutzerkonten zu erstellen. Außerdem werden so keine personenbezogenen Daten an den Web Shop übertragen, da die eigentlichen Transaktionen pseudonymisiert über die Blockchain abgearbeitet werden.
Die vorgestellte Lösung hat für die Softwarehersteller den weiteren Vorteil, dass einiges an Aufwendungen für die Koordinierung, Durchführung und die Überprüfung der Transaktionen entfällt, was eine Blockchain-basierte Lösung kosteneffektiver macht.
Durch die Garantie, dass ein Käufer der Software diese auch bezahlt haben muss um diese zu Nutzen und die Gewährleistung, dass ein Konsument auch die versprochene Softwarelizenz zugestellt bekommt, wenn er diese Bestellt und Bezahlt hat kann das Vertrauen in den Web Shop auf beiden Seiten gesteigert werden. Betrug kann verhindert bzw. ausgeschlossen werden.

Fazit

Das Konzept, welches im Zuge des Projektes prototypisch implementiert werden konnte zeigt, dass es möglich und aus ökonomischen und privatsphäretechnischen Gründen nützlich sein kann, traditionelle Modelle zum Verkaufen von Softwarelizenzen durch Blockchain-basierte Systeme zu ersetzten. Es bestehen bereits heute die technischen Voraussetzungen um ein solches System einzusetzen und erfolgreich zu nutzen. Jedoch wird es mittelfristig noch schwer sein Endanwender von Blockchain-basierten Lösungen zu überzeugen, da die generelle Akzeptanz dieser Technologie noch gering ist. Es wird vermutlich erst erforderlich sein, dass Kryptowährungen und Blockchains sich am Markt durchsetzen, bevor auch die von uns vorgeschlagene Lösung sich etablieren lässt. Dennoch hat der PoC ein Potential gezeigt und hat gegenüber klassischen Ansätzen einige Vorteile.
Es sind aktuell aber noch einige, zum Teil erstrebenswerte, Funktionen nicht verfügbar. So ist es beispielsweise nicht möglich, die Softwarelizenz auf offizielle Weise von einem Nutzer zu einem anderen zu übertragen. Auch ist es in dem PoC noch nicht möglich, dass sich der Softwareanbieter das transferierte Geld auszahlen lässt. Diese Funktionen wären jedoch in einem Produktivsystem ohne größere Schwierigkeiten implementierbar.

Ausblick

Der aktuell implementierte PoC ist lediglich auf den Vertrieb einer einzigen Softwarelösung ausgelegt. Es wäre jedoch denkbar ein vergleichbares Konzept für vielerlei Softwareprodukte unterschiedlicher Entwickler anzubieten und so eine Art zentralen Software Store zu entwickeln. In diesem könnte es möglich sein, verschiedene Produkte unterschiedlicher Hersteller mittels einer zentralen Lizenzierungslösung ohne die Notwendigkeit vieler Nutzeraccounts bei den einzelnen Herstellern zu erwerben. Dies resultiert in einem einfacheren und sichereren Softwarebeschaffungsprozess und größerem Cross Selling Potential.

Durch den Aufbau und die Struktur unserer Blockchain-basierten Lösung wäre auch die Implementierung von Abomodellen in Zukunft möglich. Hierbei würden monatliche Kosten für die Nutzung der Softwareprodukte anfallen und sollten diese nicht innerhalb eines gewissen Zeitraums beglichen werden so wird auch hier der Lizenzschlüssel invalidiert.