Blockchain: Realistischer Einsatz in der Softwarelizenzierung?

bei

Integrität und Nachvollziehbarkeit sind zwei der wesentlichen Anforderungen an Lösungen in dem Bereich des Softwareschutz- und Lizenzmanagement. Auf Basis von kryptographischen Hardware- und Softwarevertrauensankern sowie Algorithmen, die Änderungen von Systemzuständen bewerten können, sind Softwarehersteller in der Lage zu definieren wie ihre Software von Endkunden genutzt werden darf. In dem Bereich der Steuerung von industriellen Maschinen kann so zum Beispiel definiert werden, dass ein lizenziertes Design nur in einer bestimmten Anzahl produziert oder gedruckt werden darf [1].

Diese Schutzziele und betriebswirtschaftliche Anforderungen legen nahe, sich mit Thema „Blockchain" zu befassen, also einer verteilten Echtzeitdatenbank, welche folgende Merkmale bietet:

– Es gibt keine zentrale Instanz oder explizite, vertrauenswürdige Partei.

– Transaktionen sind (innerhalb einer definierten Gruppe) öffentlich und von jedem Teilnehmer einsehbar und nachvollziehbar.

– Transaktionen können nicht (ohne Einvernehmen aller Beteiligten) geändert werden.

– Das Transaktionskonto (der Ledger) kann ausführbaren Code enthalten (sogenannte Smart Contracts).

So könnten also Softwarelizenzierungsmodelle, die eine Art Zähler oder „unit counter" beinhalten, über Blockchaintechnologien abgebildet werden – eine Frage, der wir nun im Rahmen dieses Beitrags nachgehen werden.

Blockchain: Überzogene (technische) Erwartungen

Vereinfacht gesprochen versuchen Blockchaintechnologien, ein dezentralisiertes, digitales Transaktionskonto zu etablieren, in welchem Transaktionen nicht im Nachhinein geändert

werden können. Jedoch beschreibt dies ein ideales Modell, von dem die zu dem jetzigen Zeitpunkt verfügbaren, technischen Blockchainimplementierungen abweichen. Ein in der Vergangenheit oft zitiertes Beispiel sind die erheblichen Energie- und zeitlichen Aufwände, die für die Erstellung einer Bitcointransaktion benötigt werden [2].

Sehr viel umfassender wird der gegenwärtige Stand der Technik in dem Beitrag von Dinh et al. [3] auf der SIGMOD 2017 beschrieben. Es wird ein Rahmenwerk vorgestellt, auf dessen Basis 11 der zurzeit verfügbaren Blockchainplattformen verglichen werden, darunter Ethereum und Hyperledger. Diese sehr lesbare Analyse kommt fast zeitgleich zu einem ähnlichen Schluss wie der aktuelle Blockchain „Hype Cycle" von Gartner [4]: „[…] in its current state blockchains are not yet ready for mass usage […], their designs and codebases are still being refined constantly, and there are no other established applications beyond crypto-currency." [3].

Smart Contracts: Chaincode in Hyperledger

Smart Contracts sind Programme, die innerhalb einer Blockchain ausgeführt werden. Stark vereinfacht gesprochen sind es „wenn-dann"-Bedingungen, die auf Basis erfolgter Transaktionen ausgeführt werden. So ist diese Idee eines Smart Contracts, in dem Hyperledger Framework als sogenannter „Chaincode" instanziiert, also ein Go- oder Java-Programm mit einem eindeutigen Identifier, welches auf die an einer Hyperledger-basierten Bockchain beteiligten Instanzen (Peers) verteilt wird [5]. Sollte also die Steuerungssoftware einer Maschine ein lizenziertes Design drucken (unserem initialen Szenario folgend), so müsste dies als Transaktion festgehalten und gegebenenfalls ein assoziierter Chaincode ausgeführt werden.

Unabhängig von der genauen Semantik dieser Chaincodes stellt sich jedoch die wesentliche Frage, wie genau die Transaktion von der Maschine invokiert wird. Über ein spezielles Hyperledger SDK würde die Maschine melden, dass sie soeben einen Druckauftrag ausgeführt hat. Genau dieses Szenario zeigt aber auf, welche praktischen Probleme noch gelöst werden müssen – nämlich wie genau die Maschine nachvollziehbar ihre Werte als Transaktion an die Blockchain meldet. Da der Lizenzgeber dem Betreiber der Maschine unter Umständen nicht voll vertraut, müssen die bewährten Vertrauensanker der Hersteller von Softwareschutz- und Lizenzierungslösungen mit dem Transaktionsmodell von Blockchains wie Hyperledger in Verbindung gebracht werden.

Blockchain: Die eigentliche Arbeit beginnt erst

Blockchaintechnologien werden eindeutig langfristige (positive) Auswirkungen auf ein integres nachvollziehbares Transaktionsmanagement ohne zentrale Instanzen haben.

Jedoch zeigt das aufgeführte praktische Beispiel aus der Lizenzierung, dass neben der eigentlichen Arbeit an technischen Blockchainimplementierungen noch sehr viel Arbeit an der vertrauenswürdigen Anbindung von existierenden Infrastrukturen und den Datenquellen für Transaktionen erfolgen muss. Es gilt, die eigentliche kontrollierte lokale Ausführung von Programmcode sowie die damit entstehenden lokalen Daten nachvollziehbar mit dem Aufruf von Blockchain-APIs in Verbindung zu bringen.

Referenzen

[1] Wibu-Systems Website: „Schutz und Lizenzierung für Embedded-Geräte“ http://www.wibu.com/de/webinar-schutz-und-lizenzierung-fuer-embedded-geraete.html

[2] Becker et al., 2012: „Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency“ Workshop on the Economics of Information Security (WEIS 2012)

[3] Dinh et al., 2017: „Blockbench: a framework for analyzing private blockchains“. ACM SIGMOD 2017

[4] Gartner, 2017: „Hype Cycle for Blockchain Technologies“ 2017 https://www.gartner.com/doc/3775165/hype-cycle-blockchain-technologies–

[5] Hyperledger Fabric: „Chaincode for Developers“

http://hyperledger-fabric.readthedocs.io/en/latest/chaincode4ade.html

Der Autor: Vor seiner Funktion als Leiter der Stabsstelle Corporate Technology bei Wibu-Systems arbeite Dr. Andreas Schaad (CISSP) in verschiedenen technischen und Managementpositionen für Ernst & Young, SAP Research Security & Trust und HUAWEI Security Research. Er hält 13 internationale Patente und über 50 internationale Veröffentlichungen in dem Bereich der IT-Sicherheit.