The Blockchain. A Viable Choice for Software Licensing?

bei

In software protection and license management, solutions need to bring two qualities to the table: Integrity and traceability. Using cryptographic hardware and software anchors of trust as well as special algorithms with the power to track changes to system states, software developers can determine how their products are employed by the end user. With licensing capabilities in place, modern industrial machinery can, for instance, be told by its operating software that only so many units of a licensed product can be produced in any given production run. [1]

With protection requirements and commercial considerations of this nature to account for, it is no wonder that the industry is turning towards the concept of the blockchain as a possible solution, a distributed real-time database with the following desirable properties:

- there is no need for a central broker or named trusted party
- the blocks are public (within the peer group) and can be verified by any participant
- without peer consensus, the blocks are resistant to unwanted modification
- a ledger can contain executable code based on defined conditions (smart contracts)

Software licensing concepts using unit counters could be implemented by means of the blockchain technology. This article will look in more detail at the new opportunities.

Blockchain: Too high hopes in technology?

In a nutshell, a Blockchain tries to approximate a decentralized and distributed digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively. However, this model remains an unattainable ideal, as technical constraints force current implementations to compromise. One oft-quoted challenge is the exorbitant time and computing power needed for Bitcoin transactions. [2]

The current state of the technology was described in far more detail as part of SIGMOD 2017 by Dinh et. al. [3] who introduced a framework to compare eleven of the current blockchain platforms, including Ethereum and Hyperledger. They come to the same

conclusion as Garnter [4]: "[…] in its current state blockchains are not yet ready for mass usage […], and there are no other established applications beyond crypto-currency." [3]

Smart Contracts: Chaincode in Hyperledger

Smart contracts are applications executed in a blockchain. At the risk of oversimplification, they are "if-then" conditions executed on the basis of past transcations. A smart contract, implemented as a so-called "chaincode" in the Hyperledger framework, works as a Go or Java application with a unique identifier that is distributed across the entities (peers) along the Hyperledger blockchain. [5] For the control software of a printing machine to allow the production of a licensed design (to stay with our initial scenario), this would have to be recorded as a transaction and possible need a special chaincode to be executed.

Irrespective of the specific semantics of that chaincode, the key question is how the transaction is invoked by the machine. The machine would need a Hyperledger SDK to report that the it has printed the design. The practical problems are evident: how can the machine report its state as a properly traceable transaction in the blockchain? In our scenario, and in the real world, the owner of the licensed design and creator of the license does not trust the actual operator of the printing machine. This means that the established anchors of trust of software protection and licensing specialists need to be reconciled with the transaction-based concept of blockchains like Hyperledger.

Blockchains: There is work to be done

Few people would doubt that blockchain technology will have a lasting (positive) effect by enabling distributed transaction management with reliable integrity and traceability. However, this hypothetical example of real-world licensing scenarios already shows that much work still needs to be done not just on the blockchain technology itself. What is needed is a trusted link between the blockchain and established infrastructures and data sources engaged in the transactions. The challenge is to bring together the controlled local execution of software code and the data created by it with the blockchain APIs to record what has happened on the ground.

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

The Author: Before joining WIBU Systems as Head of Corporate Technology, Dr. Andreas Schaad (CISSP) started as a security auditor for Ernst & Young, London. He then worked for SAP Research Security & Trust, acting in various architectural and management roles for over 10 years in Germany and France. He was then responsible for setting up and implementing the HUAWEI Security Research Center in Darmstadt, Germany. He holds 13 international patents and authored over 50 publications in the domain of IT Security.