

Langfristige Trends in der Produktion

Blockchain

Worum geht es?

Eine Blockchain ist eine Datenbank, die von einem Netzwerk von Computern gemeinsam genutzt wird.

Sobald ein Datensatz der Kette hinzugefügt wurde, ist es sehr schwierig, ihn zu ändern. Um sicherzustellen, dass alle Kopien der Datenbank gleich sind, führt das Netzwerk ständige Prüfungen durch. Blockchain ersetzt die zentrale Instanz mit einem sogenannten peer-to-peer Netzwerk. Jedes Mitglied des Netzwerks hat Einsicht auf dieselben Daten, und Transaktionen werden gegenseitig und gemeinsam bestätigt. Die Informationen werden ständig mit der Datenbank abgeglichen, die an mehreren Standorten gespeichert und sofort aktualisiert wird. Das bedeutet, dass die Aufzeichnungen öffentlich und nachprüfbar sind. Da es keinen zentralen Standort gibt und die Daten an Millionen von Stellen gleichzeitig existieren, ist es schwieriger sie zu manipulieren. Drei grundlegende informationstechnische Funktionen kommen bei einer Blockchain üblicherweise zum Einsatz: (i) eine Hashfunktion (d.h. ein mathematischer Fingerabdruck) über getätigte Transaktionen in einem Datensatz (=Block); dadurch können Dateneinträge im Nachhinein nicht unbemerkt verändert werden; (ii) eine asymmetrische Verschlüsselung (public – private Key) um die Authentizität eines Benutzers sicherzustellen; und (iii) ein sog. Konsensprotokoll welches die Abstimmung der Transaktionen zwischen mehreren Beteiligten (die sog. „Miner“) in einem Blockchainsystem technisch durchführt.

Warum ist dieser Trend wichtig?

- Der Dezentrale Ansatz der Blockchain-Technologie ermöglicht sichere und nachvollziehbare Transaktionen ohne zentrale Vertrauensinstanz
- Dezentrale Netzwerke reduzieren die potentiellen Transaktionskosten und erhöhen die Geschwindigkeit, vor allem in einem internationalen Umfeld. Transaktionen werden in Echtzeit und sofort durchgeführt
- Sicherstellung der Datenechtheit und -nachvollziehbarkeit bei Verfolgung von Teilen entlang der Lieferkette und Einhaltung von regulatorischen Auflagen
- Erleichterung der Führung von Aufzeichnungen und Transparenz innerhalb von Prozessen, an denen mehrere Parteien weltweit beteiligt sind
- Durch Integration der Blockchain mit dem Einsatz von IoT-Geräten kann jeder Teilnehmer der Lieferkette einen Echtzeitüberblick über die Lieferkette und deren Dokumentation erhalten

Das österreichische Ökosystem zu diesem Trend

- [AIT](#)
- [Universität Wien](#), [WU Wien](#), [TU Wien](#)
- [EY](#)
- [IBM](#)
- [Riddle and Code](#)
- [Blockchain Landscape Austria](#)

Wo finde ich weiterführende Information?

- [ABC: Austrian Blockchain Center](#)
- [AIT](#)
- [Wirtschaftskammer Österreich informiert](#)
- [Leopold H., Blockchain update - Post-Bitcoin Cryptocurrencies - Society has to shape technology \[1\]](#)

Langfristige Trends in der Produktion

Weiterführende Informationen

Blockchain kann als DAS Hype-Thema der letzten Zeit, mit überzogenen Erwartungshaltungen in weiten Bereichen, bezeichnet werden. Es gilt zwischen grundsätzlichen Themenbereichen zu unterscheiden: (1) Finanz- und Währungsaspekte bei virtuellen Währungen (es gibt über 2000 verschiedene, wobei Bitcoin global bei weitem den größten Anteil ausmacht [5]). Durch die Realisierung einer virtuellen Währung ohne übliche Finanzmarktstrukturen und Mechanismen sind Aspekte der Finanzwirtschaft betroffen, wie z.B. fehlende Regulierungen von Bankwesen, Einflüsse auf Kursentwicklungen, Vereinfachung von Finanztransaktionen in einem globalen Kontext – dies gilt aber auch für die Kriminalität [7]; z.B. geht Europol davon aus, dass 40% aller Finanztransaktionen in virtuellen Währungen durch kriminelle Handlungen motiviert sind [6]. Das AIT spezialisierte sich auf Forensik-Werkzeuge um Transaktionen in virtuellen Währungen im Kampf gegen die organisierte Kriminalität entsprechend nachvollziehen zu können und hat damit eine weltweit führende Kompetenz etabliert [2]. (2) Energieverbrauch. Bestimmte Konsensprotokolle sind derart konzipiert, dass sie durch die notwendigen Rechnerleistungen einen sehr großen Energieverbrauch mit sich bringen; z.B. benötigt die virtuelle Währung Bitcoin mittlerweile gleich viel Energie wie ein mittlerer Staat dieser Erde obwohl nur ein sehr geringer Anteil aller weltweiten Finanztransaktion damit abgewickelt wird! Bei geschlossenen Blockchainnetzen sind natürlich auch einfachere Konsensprotokolle in Verwendung. (3) Durch den großen Energieverbrauch für bestimmte Konsensprotokolle, wie für die virtuelle Währung Bitcoin, ist damit auch ein Markt im Zusammenhang mit dem Energiepreis entstanden. Wenn mit geringen Kosten Energie bezogen werden kann, rentiert sich die Durchführung der Berechnung für das Konsensprotokoll (d.h. Mining). Deshalb haben sich Miner in speziellen Gebieten angesiedelt wo Rechner mit geringen Energiekosten betrieben werden können. Es ist wichtig zu bemerken, dass z.B. für Bitcoin mittlerweile mehr als 50% der Miner-Kapazitäten (durch nur 4 Organisationen!) in China ansässig sind. Nun ist es wichtig zu erkennen, dass damit ein erhebliches Sicherheitsproblem verbunden ist. Wenn sich die Miner zu Kartellstrukturen zusammenschließen, kann sogar eines der Grundprinzipien der Unveränderlichkeit von Transaktionen in einer Blockchain aufgehoben werden [3]. Durch die weltweite einfache Handhabung von Finanztransaktionen sind Blockchains auch in der Realisierung von Crowd-Funding Prozessen, sog. ICOs, Initial Coin Offerings ein beliebtes Thema. Beim Einsatz für die Kontrolle von physikalischen Transaktionen wie Logistikprozesse, gilt es zu beachten, dass nur die virtuelle Welt der Transaktionen abgesichert werden kann. Manipulationen der physikalischen Abläufe können durch eine Blockchain nicht verhindert werden.

Videos:

- [Was ist eine Blockchain? – einfach und verständlich erklärt](#)

Referenzen:

- [1] Leopold H., Blockchain update - Post-Bitcoin Cryptocurrencies - Society has to shape technology, OSCE Asian contact group - Economic Connectivity – Financial Technology Innovations, AIT Austrian Institute of Technology Report, 15.6.2018; on Researchgate: https://www.researchgate.net/publication/327136420_Blockchain_update_-_Post-Bitcoin_Cryptocurrencies_-_Society_has_to_shape_technology
- [2] Blockchain Technologies am AIT, <https://www.ait.ac.at/themen/data-science/blockchain-technologies/>
- [3] Romiti, M., Judmayer, A., Zamyatin, A., & Haslhofer, B. (2019). A deep dive into bitcoin mining pools: An empirical analysis of mining shares. 18th annual workshop on the economics of information security (WEIS 2019); <https://arxiv.org/abs/1905.05999>
- [4] IKT der Zukunft Leitprojekt “Smart Contracts for data sharing“
- [5] <https://de.statista.com/statistik/daten/studie/296205/umfrage/marktkapitalisierung-digitaler-zahlungsmittel/>
- [6] Europol IOCTA report 2015 und 2018 <https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018>
- [7] Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. Journal of Cybersecurity, 5 (1). <https://doi.org/10.1093/cybsec/tyz003>