Digitalen Technologien Verbindung und Vernetzen – auf immer neuen Wegen

Martin Pirker; Institut für IT-Sicherheitsforschung, FH St.Pölten

Abstract. Die ständige Weiterentwicklung von digitalen Diensten und dem Internet hat Applikationen in die Cloud gebracht. Die vermehrte Arbeit im Homeoffice wiederum machte uns die Abhängigkeit von zentralisierten Diensten bewusst. Der Versuch der Transformation von zentralisierten Applikationen in ein dezentrales Modell, beispielweise auf Ideen von verteilten Data-Ledgers basierend, zeigt vielerlei Herausforderungen auf. Dieser kurze Beitrag bringt ein paar Aspekte zur weiteren Reflektion dieser Situation.

Keywords: Dezentralisierung, Distributed Data Ledger, Blockchain

Beitrag im Rahmen des 16. Forschungsforums der österreichischen Fachhochschulen von 19.-20. April 2023 an der FH St. Pölten.

1 EINLEITUNG

Im Laufe der Jahre – nein, der Jahrzehnte – entwickelten sich die digitalen Technologien, die digitalen Netze und ihre Möglichkeiten beständig weiter. Was heutzutage an Technologien selbstverständlich ist, musste erst einmal von Grund auf ausgedacht und praktisch entwickelt werden. So im Überblick betrachtet, könnte man diese Entwicklung in mehrere (Entwicklungs-)Phasen zusammenfassen.

Die ersten Rechner waren riesengroß, sehr teuer, und es gab nur ein paar Stück – weltweit. Im Folgenden waren Computer noch immer sehr teuer, aber es gab schon einzelne verstreut in den Universitäten – die diese Technologien ja dann auch weiterentwickelten – und bei finanzstarken Firmen, die passende, reale Problemstellungen für die neuartigen Rechenhelfer hatten. Der damalige Großrechner stand in der Zentrale, in einem Rechenzentrum, von außen konnte man sich via Telefonleitung und einfachen Text-basierenden Terminals verbinden und die Rechenleistung nutzen, ohne direkt vor Ort zu sein.

Die nächste Stufe der Weiterentwicklung war der günstige Mikrocomputer. Der persönliche Computer („PC“) für jeden Mitarbeiter, auf jedem Schreibtisch, wurde praktisch möglich – man war nicht mehr von der Zentrale abhängig. Die steigende Anzahl an Computern erforderte auch einem Datenaustausch zwischen diesen. Diese Vernetzung, um Daten immer effizienter austauschen, ermöglichte wiederum neuartige Anwendungen. Es ergab sich schließlich die weltweite Vernetzung in Form des Internets wie wir es heute kennen und nutzen.

Der Preisverfall von Rechenleistung, der effizientere Einsatz von (Hardware-) Ressourcen, und der wachsende dynamische Bedarf an Rechenleistung gebar schließlich die „Cloud“. Eine Cloud bietet Rechenleistung und Speicherplatz als Dienstleitung, anmietbar je nach Bedarf bei Cloud Providern. Die dazu nötige Internetverbindung zur Cloud war inzwischen schnell genug. Die weitere Entwicklung wurde von vielen vorhergesagt: alles geht in die und nur mehr mit der Cloud. Das bedeutet aber auch, die Ressourcen sammeln sich wieder bei wenigen großen, zentralen, internationalen Providern.

Die Covid-19 Pandemie verbannte schließlich einen großen Teil der Mitarbeiter ins Homeoffice. Die Qualität der Vernetzung und der zentralen Dienste – auch der Cloud-Dienste – offenbarte unsere Abhängigkeit von dem Funktionieren dieser. Oder, direkter formuliert, wenn beispielsweise die bekannten Office 365 Dienste einmal nicht (mehr) funktionieren [1], wo ist dann überall Stillstand?

Diese praktischen Erfahrungen und gegebenen Abhängigkeiten haben bei manchem wieder ein Nachdenken über zentralisierte Dienste bzw. gegenüber Cloud-Diensten motiviert. Das Pendel geht wieder in die Gegenrichtung – das Thema „local-first“ Software [2], also weg von zentralisierten (Cloud) Ressourcen, mehr zu lokalen laufenden Programmen, lokalen Daten und lokaler Datenverarbeitung, gewinnt wieder an Bedeutung.

2 Dezentralisierung

Ein Einsatz von lokalen Programmen, also nicht die Nutzung von zentralisierten Servern, Services und Cloud-Ressourcen, bietet eine Reihe von interessanten Eigenschaften, die in unserer vernetzten Welt mitunter schon in Vergessenheit geraten sind.

Ein Paper [2] zählt sieben erstrebenswerte Eigenschaften von Software auf, die bewusst mit einem „local-first“ Gedanken entwickelt wird: 1) Lokale Software arbeitet schneller als eine nur über ein Netzwerk erreichbar (Cloud-)App. 2) Die Daten am lokalen Gerät können leicht auf ein weiteres (lokales) Gerät kopiert werden. 3) Eine lokale Applikation arbeitet immer, auch wenn gerade kein Internet verfügbar ist. 4) Der Datenaustausch und konfliktarme Datenabgleich mit anderen wird durch Fortschritte bei den Algorithmen immer leichter möglich. 5) Lokale Daten existieren quasi ewig und eine lokale Applikation ist somit potenziell auch ewig verwendbar – also unabhängig von einem (Cloud-)Provider. 6) Die Sicherheit und Privatheit der Daten ist unter lokaler Kontrolle – wie die Daten bei einem Provider gespeichert werden und wer auf diese Zugriff hat ist meist nicht klar. 7) Es ist klar, wer die lokalen Daten verarbeitet und wie – und man hat die Entscheidungshoheit, ob und wann man sie mit anderen teilen möchte.

Ein weiterer Ansatz zur Dezentralisierung von Applikationen ist über die Nutzung von Ideen von Blockchains. Blockchains sind eine mögliche Ausprägung von Distributed Ledger Technologies (DLT). DLTs sind vorstellbar als Datenbanken – Data-Ledger – zu denen nur Daten hinzugefügt werden können und wobei dann die Änderungen der Daten(-blöcke) über einen Verbund bzw. Netzwerk von Teilnehmern repliziert und synchronisiert werden. Eines der bekanntesten Blockchain Projekte ist Bitcoin, welches spezifische Designentscheidungen zu Kernproblemen in der Umsetzung eines Distributed Data Ledgers getroffen hat, mit dem Ergebnis, dass das Gesamtdesign von Bitcoin für genug Teilnehmer attraktiv war – und Bitcoin auch für bestimmte Anwendungen sehr erfolgreich machte. Allgemein betrachtet gibt es aber viele Varianten und Designmöglichkeiten [3][4] von DLTs bzw. Blockchains. Es besteht somit das Potential das DLTs für bestimmte Anwendungsfälle eine bessere Lösung bieten als bisherige. Allerdings, für welche dies theoretisch plausibel erscheint und wieviel sich dann auch praktisch umsetzen lässt, dafür ist noch viel an Forschung notwendig.

3 Forschung

Das Josef-Ressel Zentrum für Blockchain-Technologien und Sicherheitsmanagement an der FH St. Pölten untersucht unter anderem, wie man klassische zentralisiert angelegte (Server-) Anwendungen auf ein dezentraleres Modell umstellen könnte. Oder anders formuliert, wenn man eine ursprünglich zentralisiert angelegte Applikation lokal ausführen möchte, und nicht ständig per Netzwerk mit einer entfernten (Cloud-) Instanz interagieren möchte, was müsste sich dafür alles ändern für die Applikation – und was ändert sich implizit durch die geänderte Ausführungsumgebung? Was sind die

erwartbaren Vor- und Nachteile?

Eine theoretische Beleuchtung des Szenarios – siehe [5] für Details die hier leider nicht Platz finden – zeigt mehrere Herausforderungen auf. Beispielsweise Applikationen interagieren immer mit Daten, die dann aber nicht mehr zentral verwaltet sind, sondern lokal für eine Applikation verfügbar sein müssen. Dies erfordert die Replikation jeglicher Veränderungen (an Dateien, Datenbanken, etc.) über alle Applikationsnutzer, und insbesondere die Sicherstellung der Konsistenz der Daten. Weiters, wenn alle Daten dezentral vollständig repliziert sind, ist auch das Löschen von Daten ein Problem – dies muss auf allen Kopien von Daten passieren – auch im Hinblick auf die Anforderungen der Datengrundschutzverordnung.

Ein Kernproblem eines dezentralisieren Ansatzes ist auch immer die Sicherheit und Integrität der Daten. Viele verteilte, dezentral laufende Kopien einer Applikation bedeuten auch viele einzelne Ausführungsumgebungen, die es abzusichern gilt. Eine naheliegende Lösung ist die vollständige Verschlüsselung der Applikationsdaten, wobei der lokale Nutzer immer nur die Daten entschlüsseln und verändern kann die für ihn freigegeben sind. Dies benötigt wiederum eine Verwaltung von Rechten und Privilegien pro Nutzer, die allen zur gleichen Zeit aktuell verfügbar sein muss – ein Distributed Data Ledger in Form einer Blockchain ist hierfür eine mögliche Lösung.

Die Absicherung der Ausführung einer Software auf einer bestimmten Plattform durch Verwendung von speziellen Hardwaretechnologien die auf modernen PCs verfügbar sind (Trusted Computing Technologien) ist bereits ein sehr fortgeschrittener Ansatz, macht aber für Teilnehmer mit Spezialaufgaben in einem dezentralen Ansatz Sinn.[6] Allgemein betrachtet, eine detailliertere Reflektion über Cybersecurity und verteilte (Blockchain-) Anwendungen reicht aus um alleine ein Buch zu füllen – auch hier sei auf die Literatur verwiesen. [7]

4 CONCLUSIO

Das Internet und die vielen digitalen Technologien und Applikationen dringen immer mehr in unser tägliches Leben ein – und verändern unserer aller Alltag und Interaktionen. Das Pendel schwingt über die Jahre mal mehr zur Zentralisierung, mal mehr zur Dezentralisierung. Aus den Homeoffice Erfahrungen heraus stellt sich derzeit die Frage, mit welchen Veränderungen und Technologien kann man dezentralere Applikationen und gleichzeitig eine einfache Zusammenarbeit ermöglichen?

Positiv betrachtet verbinden und vernetzen wir uns Menschen immer mehr. Negativ betrachtet muss es auch eine Gegenbewegung zu mehr Lokalität geben, damit wir nicht alle abhängig werden von zentralen Diensten und Cloud Providern. DLTs und Blockchains sind ein Ansatz zur Dezentralisierung von Applikationen – für welche Applikationen und Anwendungsszenarien diese sinnvoll ist, wird uns hoffentlich die Forschung einen guten Weg aufzeigen.

5 REFERENZEN

[1] Beispiele:
https://www.heise.de/news/Neuer-Ausfall-in-Microsofts-Cloud-Microsoft-365-betroffen-4292269.html
https://www.heise.de/news/Weltweiter-Ausfall-von-Microsoft-Cloud-Diensten-weitgehend-behoben-4914691.html

[2] M. Kleppmann, A. Wiggins, P. v. Hardenberg, M. McGranaghan; Local-first software: you own your data, in spite of the cloud; Proceedings of the 2019 ACM SIGPLAN International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software, 2019; https://doi.org/10.1145/3359591.3359737

[3] N. Kannengießer, S. Lins, T. Dehling, A. Sunyaev; Trade-offs between Distributed Ledger Technology Characteristics; ACM Computing Surveys, Volume 53, Issue 2, Article No.: 42; https://doi.org/10.1145/3379463

[4] J. Kolb, M. AbdelBaky, R. H. Katz, D. E. Culler; Core Concepts, Challenges, and Future Directions in Blockchain: A Centralized Tutorial; ACM Computing Surveys, Volume 53, Issue 1, Article No.: 9; https://doi.org/10.1145/3366370

[5] M. Pirker, E. Piller; Obstacles and Challenges in Transforming Applications for Distributed Data Ledger Integration; Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES) 2021; https://doi.org/10.1145/3465481.3469194

[6] M. Schüpany, M. Pirker; A Revisit of Attestable Nodes for Networked Applications; Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES) 2022; ACM; https://doi.org/10.1145/3538969.3544433

[7] Howard E. Poston; Blockchain Security from the Bottom Up: Securing and Preventing Attacks on Cryptocurrencies, Decentralized Applications, NFTs, and Smart Contracts; Wiley 2022; ISBN: 978-1-119-89629-6