schule verantworten
führungskultur_innovation_autonomie

begriffs-box

Michael Wagner
Drexel University, Philadelphia, USA

Web3

DOI: https://doi.org/10.53349/sv.2022.i1.a174

Web3, das. Substantiv, neutral.

Der Begriff „Web3“, früher auch als „Web 3.0“ bezeichnet, hat seinen Ursprung in den Gründerzeiten des World Wide Web. In den letzten Monaten wurde der Begriff allerdings zunehmend zum Synonym für Blockchain Technologie und Kryptowährungen. Warum ist dem so? Der folgende Text ist der Versuch einer einfach zugänglichen Erklärung einer extrem komplexen Fragestellung.

Die ursprüngliche Vision des Web3 drehte sich um das semantische Web, einem von Tim Berners-Lee um die Jahrtausendwende postulierten Konzept, welches, extrem vereinfacht gesagt, die uneingeschränkte Maschinenlesbarkeit aller im World Wide Web enthaltenen Informationen zum zentralen Ziel erklärt.

Diese an und für sich sehr einfache Idee hat überraschend weitreichende Konsequenzen.

Zunächst erfordert die Maschinenlesbarkeit aller Informationen, dass die Benutzer*innen des Web3 zu jedem Zeitpunkt in voller Kontrolle über ihre Daten sein müssen. Dies deshalb da diese Daten transparent zur Verfügung gestellt werden, um die Funktionsweise des Web3 gewährleisten zu können. Alles muss für alle einsichtig und überprüfbar sein.

Konsequenterweise kann es daher keine zentrale Einheit oder Institution geben, welche die alleinige Kontrolle über die dem Web3 zugrunde liegende Daten oder Technologien besitzt. Alle Nutzer*innen müssen uneingeschränkt gleichberechtigt am System teilhaben können. Daraus ergibt sich in weiterer Folge die Bedingung einer dezentralen Computerinfrastruktur als Basis des Web3.

Die Erforschung dezentraler Computernetzwerke hat in der Informatik eine lange Tradition. Ohne hier auf Details eingehen zu wollen, sind es zwei Forderungen für deren Realisierung,

welche uns schlussendlich in Richtung Blockchain Technologie und, für viele sehr überraschend, insbesondere auch in Richtung Kryptowährungen lenken.

Zum einen muss die zugrunde liegende Infrastruktur extrem resilient gegenüber jedweder Manipulation sein. Da es keine zentrale Einheit oder Organisation gibt, die unautorisierte Veränderungen der Daten erfassen, verhindern, oder sogar korrigieren kann, müssen diese Daten vollkommen unabänderlich (im Englischen „immutable“) im System existieren.

Hier kommt Blockchain Technologie ins Spiel. In einer Blockchain wird die „Immutability“ der Daten über die kryptographische Verlinkung einzelner Datenblöcke gewährleistet. Werden Daten in einem Datenblock der Blockchain manipuliert, so bricht die Datenkette an dieser Stelle und die manipulierten Daten werden in Folge vom dezentralen Netzwerk ignoriert.

An dieser Stelle darf nicht unerwähnt bleiben, dass die oft zitierten Hackerangriffe auf Blockchains ausschließlich auf deren programmiertechnische Implementierung abzielen. Blockchains als Datenstruktur sind, zumindest probabilistisch gesehen, nahezu hundertprozentig unangreifbar. Tatsächlich sind einige neu entwickelte Blockchains darüber hinaus quantenresistent. Das heißt, es lässt sich nachweisen, dass sie selbst mit Hilfe von Quantenrechnern nicht gezielt manipuliert werden können.

Dies alles stimmt allerdings nur, wenn eine zweite Forderung erfüllt ist. Dies ist die Bedingung, dass alle Netzwerkknoten zu jedem Zeitpunkt im Konsens über den Status der Blockchains sein müssen. Im Netzwerk muss ständige Einigkeit herrschen. Dies geschieht mit Hilfe sogenannter Konsens-Mechanismen oder Konsens-Algorithmen.

Die Suche nach dem optimalen Konsens-Mechanismus ist ein hartes Problem, welches theoretische Informatiker seit Jahrzehnten beschäftigt. Zwar ist man in den letzten Jahren einer Lösung deutlich näher gekommen. Es wäre allerdings naiv zu behaupten, dass die derzeit im Blockchain Umfeld verwendeten Konsens-Mechanismen („proof of work“, „proof of stake“, „asynchronous byzantine fault tolerance“, etc.) eine ideale Lösung bereitstellen können.

Jeder heute verwendete Konsens-Mechanismus hat Schwachstellen und ist in letzter Konsequenz nicht unangreifbar oder problemlos umsetzbar. Diese Schwachstellen reichen von negativen Auswirkungen auf die Umwelt durch exzessiven Energiebedarf bei „proof of work“ Blockchains über mangelnde Dezentralisierung bei einzelnen „proof of stake“ Blockchains bis hin zu mangelnder Skalierbarkeit einer breiten Palette von Konsens-Mechanismen.

Es darf allerdings erwartet werden, dass es in den nächsten Jahren zur Etablierung eines „dominanten Designs“ für einen optimalen Konsens-Mechanismus kommen wird, welcher die Grundlage für eine Verwirklichung des Web3 darstellen kann. Dies erklärt auch die große Anzahl von Wissenschaftler*innen und Firmen, die sich mit diesem Thema derzeit beschäftigen. Es entscheidet sich heute, welche Technologien unsere Zukunft dominieren werden.

In Bezug auf die ursprüngliche Frage ergibt sich daher zunächst ein Zusammenhang zwischen Web 3 und Blockchain-Technologie. Kurz gesagt, werden Blockchains heute als wichtigste und vielversprechendste technologische Grundlage bei der Umsetzung eines semantischen Webs verstanden. Wo aber kommen nun Kryptowährungen ins Spiel und warum sind diese hier relevant?

Die Antwort dazu ist verblüffend einfach, erfordert beim Einzelnen in der Regel allerdings ein vollständiges Umdenken über Wert und Zweck von Kryptowährungen.

Im aktuellen kollektiven Verständnis der Gesellschaft sind Kryptowährungen eine Antwort auf die 2008 durch die Immobilienblase ausgelöste Finanzkrise. Dies wird insbesondere durch den Mythos rund um Bitcoin in nahezu religiöser Form propagiert. Die wissenschaftliche Realität sieht allerdings wesentlich differenzierter, und in letzter Konsequenz auch deutlich unspektakulärer, aus.

Kryptowährungen lösen ein zentrales Problem aller Konsens-Mechanismen. Sie stellen sicher, dass Netzwerkknoten ein nachhaltiges Interesse haben, sich aktiv am Konsens zu beteiligen. Wäre dieses Interesse nicht gewährleistet, so könnten bösartige Akteure im Netzwerk das Desinteresse der Netzwerkknoten ausnutzen, um den Konsens in eine bestimmte Richtung zu manipulieren.

Kryptowährungen sind daher nicht mehr und nicht weniger als Anreizsysteme zur Sicherstellung der Funktionsweisen von Blockchains zu verstehen.

Oder anders gesagt, es ist nicht die Blockchain, die die Kryptowährung ermöglicht, es ist vielmehr die Kryptowährung, die dies ermöglicht. Und wie bereits erwähnt, ist die Blockchain-Technologie der derzeit vielversprechendste Ansatz zur Verwirklichung des Web3. Web3, Blockchains und Kryptowährungen sind damit eng verknüpfte Konzepte und in der Diskussion über die Zukunft des Internet kaum voneinander zu trennen.

Es bleibt zu erwähnen, dass in diesem kurzen Text viele Sachverhalte aufgrund ihrer hohen Komplexität nahezu bis zur Unkenntlichkeit vereinfacht dargestellt werden mussten. Unerwähnt blieb insbesondere, wie aus einer Blockchain als Datenstruktur die Basis für eine dezentrale Softwareumgebung wird. Hier kommen so genannte „smart contracts“ und „decentralized Applications (dApps)“ zum Einsatz.

Interessierte Leser*innen sind daher eingeladen, sich mit dem Thema weiter zu beschäftigen, um auf zukünftige Entwicklungen im Schulbereich besser vorbereitet zu sein.

Literaturhinweis

Wattenhofer, R. (2019). *Blockchain science: Distributed ledger technology*. Inverted Forest Publishing.

Autor

Michael Wagner, Univ. Prof. Dr.,
ist seit 2012 Department Head des Department of Digital Media am Antoinette Westphal College of Media Arts and Design der Drexel University in Philadelphia, USA. Vor seinem Wechsel an die Drexel University war er unter anderem als Universitätsprofessor an der Donau-Universität Krems sowie als Rektor der KPH Wien/Krems tätig.
Kontakt: michael.g.wagner@drexel.edu