13 Die technologischen Ansätze und Herausforderungen des Web3 und Metaverse

Yvonne-Anne Pignolet & Stefan Schmid[1]

Dieser Artikel gibt eine Übersicht über die technologischen Ansätze und Herausforderungen des Web3 und des Metaverse. Das Web3 ist eine dezentralere und partizipativere Form des heutigen World Wide Webs, in dem digitale Güter "tokenisiert" werden können und die Benutzer die Kontrolle und Rechte über ihre Daten behalten: Sowohl Besitztum ("Ownership") als auch die Verwaltung und Steuerung ("Governance") sind verteilt. Das Web3 kann durch Blockchain-Technologien realisiert werden, auf dem dann Anwendungen wie ein Metaverse, eine von Computern erzeugte virtuelle Welt, mit Hilfe von Smart Contracts implementiert werden. Wir diskutieren Sicherheits- und Effizienzaspekte dieser Technologien, sowie spezifische Herausforderungen der Governance, Ownership und Tokenisierung.

13.1 Einführung

Web3 und Metaverse sind zur Zeit in aller Munde. Die beiden Schlagworte werden manchmal sogar als Synonyme benutzt, unterscheiden sich aber. Vereinfacht gesagt versteht man unter Web3 eine "dezentralere" und "partizipativere" Form des WWW. Während die Benutzer:innen im Web1 vor allem Inhalte "lesen" können, können sie im Web2 auch Inhalte "posten", zum Beispiel auf sozialen Netzwerken wie Facebook. Bei Web2 werden diese Inhalte

1 Mehr über die Autor:innen erfahren Sie im Autor:innenhinweis auf S. xxx.

durch große Firmen verarbeitet und verbreitet. Mit Web3 wird das Teilen von Inhalten (inklusive Rechten oder Programmcode) dezentral: die Benutzer:innen behalten die Kontrolle über die Daten selbst. Digitale Güter können "tokenisiert", das heißt in kleine Teile ("Tokens") segmentiert werden, die jeweils einen anderen Besitzer haben können.

Im Web3 werden somit sowohl Besitztum ("Ownership") als auch die Verwaltung und Steuerung ("Governance") verteilt, und Besitzer:innen der Tokens entscheiden zusammen, mit digitalen Abstimmungen, wie sich zum Beispiel eine Anwendung weiterentwickeln soll. Die entsprechenden Programme und Protokolle werden als "Smart Contracts" bezeichnet, da sie Vorgänge automatisch ausführen und dokumentieren, wenn die nötigen Bedingungen erfüllt sind, und somit traditionelle Verträge ersetzen können. Web3 kann durch dezentrale Blockchain-Technologien realisiert werden, wie es zum Beispiel beim Internet Computer, Algorand oder Avalanche der Fall ist. Der Handel mit Kryptowährungen kann als Teilbereich von Web3 angesehen werden. Weitere Anwendungen des Web3, welche schon heute Milliarden umsetzen, sind beispielsweise non-fungible tokens (NFTs, unteilbare und eindeutige Repräsentation von digitalen oder physikalischen Gegenständen), Marktplätze und Anwendungen basierend auf Daten die vom Benutzer selber kontrolliert werden (zum Beispiel von einer Autoblackbox), Stable Coins mit automatischen Preisbildungsmechanismen und weltweitem, schnellen und günstigen Zahlungsverkehr, und viele mehr.

Metaverse, also eine von Computern erzeugte virtuelle 3D Welt, in welcher sich die Benutzer:innen bewegen und interagieren, kann als Anwendung auf Web3 umgesetzt werden. Zugang zum Metaverse erfolgt zum Beispiel via Headset oder auch immer mehr über haptische ("fühlbare") Technologien.

Die technologischen Herausforderungen von Web3 und Metaverse sind vielfältig und betreffen verschiedene Aspekte. In diesem Artikel werden einige wichtige

Herausforderungen und Lösungsansätze genauer beleuchtet. Das Ziel des Artikels ist es, eine Einführung zu geben, und nicht eine umfassende oder wissenschaftliche Abhandlung zu sein. Er enthält deshalb auch keine wissenschaftlichen Literaturhinweise.

13.2 Sicherheit und Privatsphäre

Web3- und Metaverse-Anwendungen müssen sehr hohen Sicherheitsanforderungen genügen. Im Web3 betreffen diese Anforderungen beispielsweise die teuren digitalen Güter und Portfolios von Kryptowährungen, die dort verwaltet werden und eine sichere und korrekte Governance kritisch machen. Das Metaverse wiederum muss beispielsweise die Privatsphäre der Benutzer:innen schützen und, wo nötig, Anonymität bieten.

Einige Herausforderungen in diesem Bereich sind nicht neu, aber immer noch sehr aktuell, beispielsweise bezüglich der Verwendung von Passwörtern: Passwörter sind in der Praxis oft problematisch und während sich Technologien immer mehr in Richtung passwortfreier Identitäten hin entwickeln, oft mit Hardware-basierten Lösungen für Gesichtserkennung, Irisscan oder Fingerabdrücken, haben letztere Ansätze eigene Nachteile und sind unflexibel, was deren Einsatz im Alltag zum Teil schwierig macht.

Web3 und Metaverse werfen auch wichtige grundsätzliche Fragen auf, zum Beispiel wieviel und welche Informationen andere Benutzer:innen über meine Aktionen haben dürfen und welche die Plattformbetreiber. Kryptowährungen wie Bitcoin bieten eine sogenannte Pseudo-Anonymität: Benutzer:innen dürfen so viele Pseudonyme erstellen wie sie möchten, die Transaktionen zwischen den Pseudonymen sind dann aber öffentlich. Für gewisse Anwendungen kann aber eine volle Anonymität wünschenswert sein, zum Beispiel dass weder die Benutzer:innen noch die Plattformbetreiber wissen, wie groß eine Transaktion

war oder sogar ob sie überhaupt stattgefunden hat. Eine volle Anonymität birgt allerdings auch Gefahren und kann missbraucht werden (z.B. für Geldwäsche). Welche Art von Anonymität angeboten werden soll und wie sie umgesetzt wird, muss also von Fall zu Fall bestimmt werden.

Wichtige Sicherheitsfragen stellen sich auch bezüglich Cloud Computing: viele Web3- und Metaverse-Anwendungen werden in Rechenzentren laufen – aus Ressourcen- und Effizienzgründen. Die moderne Kryptographie bietet einige interessante Ansätze, Cloud Ressourcen sicher zu nutzen. Beispielsweise können mittels sogenannter homomorpher Verschlüsselung und sicherer Multiparty Computation, Berechnungen in der Cloud stattfinden, ohne dass ein Cloud Provider die Daten, auf denen er rechnet, einsehen kann.

Auch Hardware-basierte Trusted Execution Environments sind eine wichtige Technologie, um Interaktionen vor Plattformbetreibern geheim zu halten. Mit der sogenannten “Attestation” Technik kann verifiziert werden, dass diese vom Plattformbetreiber auch tatsächlich benutzt werden. Allerdings lässt sich ein Restrisiko nicht vermeiden: Side-Channel-Attacken (zum Beispiel mit Spannungsmessungen durch den Plattform Betreiber) können nicht ausgeschlossen werden. Außerdem müssen die Benutzer:innen auch dem Hardware-Hersteller vertrauen.

Spezielle Technologien werden auch für die besonderen Sicherheitsanforderungen von Smart Contracts benötigt. So kann es in gewissen Anwendungen wünschenswert sein, den Source Code von Smart Contracts geheim zu halten. Technologien wie Garbled Circuits oder Oblivious RAM unterstützen solche Anwendungen, sind aber immer noch Gegenstand aktiver Forschung. Eine grundsätzliche Frage ist, ob Smart Contracts veränderbar oder unveränderbar sein sollen: ein unveränderbarer Smart Contract ist einfacher zu verifizieren, ein veränderbarer flexibler in der Anwendung.

13.3 Effizienz und Skalierbarkeit

Viele Blockchain-basierte Technologien haben den Ruf, langsam und ineffizient zu sein. Grundsätzlich gilt: Um Dezentralität mit minimalem Vertrauen zu erreichen, muss Fehlertoleranz gewährleistet sein. Das erfordert Redundanz: Daten müssen verteilt gespeichert und berechnet und transportiert werden, was Overheads mit sich bringt. In Web2-Umgebungen liegt der Fokus der Fehlertoleranz auf technischen Ausfällen von Maschinen, welche aber grundsätzlich alle die Protokolle gemäß Spezifikation ausführen. Im Gegensatz dazu erfordert Web3 eine Fehlertoleranz gegen böswilliges Verhalten: eine kleine Anzahl von böswilligen Akteuren darf keine negativen Auswirkungen auf die Sicherheit und Erreichbarkeit haben. Dazu müssen stärkere Fehlermodelle beim Design und der Analyse der Protokolle und Softwareentwicklung berücksichtigt werden.

Ein besonderes Augenmerk fällt auf die sogenannten Consensus Protokolle, welche es ermöglichen, dass alle beteiligten Maschinen sich einigen, welche Operationen in welcher Reihenfolge als nächstes ausgeführt werden. Je nach Protokoll kann dieser Prozess riesige Energiemengen verschlingen und zum Flaschenhals werden.

Allerdings haben die neuen Generationen von Protokollen hier viele Fortschritte gemacht und erlauben es, tausende Operationen gleichzeitig in wenigen Sekunden unumkehrbar abzuwickeln, und dies ohne energie-aufwändige Verfahren wie zum Beispiel bei Bitcoin. Diese Protokolle noch effizienter zu machen, ist Gegenstand aktueller Forschung.

Es gibt jedoch auch fundamentale Grenzen. Ein globaler Konsensus braucht mehrere sogenannte Round-Trip-Times (RTTs), welche selbst bei Lichtgeschwindigkeit in der Größenordnung von ca. 100 Millisekunden liegen. Außerdem steigt die minimale Anzahl ausgetauschter Nachrichten für

deterministische Entscheidungen quadratisch mit der Anzahl beteiligter Maschinen. Deshalb ist ein wichtiger Ansatz für eine höhere Geschwindigkeit Sharding: Wenn sich eine Teilmenge der involvierten Rechner untereinander einigen kann, kann sich die Laufzeit signifikant verbessern, vor allem auch, wenn sie sich geografisch in der Nähe befinden. Das steht allerdings im Konflikt zur Dezentralisierung. Wichtig ist es auch, zwischen Schreib- und Leseoperationen zu unterscheiden: Leseoperationen sind oft wesentlich schneller, da sie keinen Consensus benötigen; das Überprüfen der Authentizität und Integrität der gelesenen Daten erfordert jedoch kryptographische Protokolle, sowohl bei Schreibe- und Lese-Operationen.

Effizienz- und Skalierbarkeits-Fragen betreffen auch den Speicher: Alle Transaktionen für immer global zu speichern und zu verwalten kann teuer sein. Eine wichtige Frage ist, ob und wie eine “Auditability” auf effizientere Art sichergestellt werden kann: Wie können also Transaktionen später verifiziert werden, ohne dass alle Daten gespeichert werden? Oft sind hierzu spezifische Lösungen nötig, zugeschnitten auf den Use Case.

Sogenannte “2nd Layer Solutions”, wie Payment Channel Networks und Rollups, sind wichtige Technologien, um Blockchain-Technologien effizienter zu machen. Das Ziel dieser Technologien ist es, die Anzahl nötiger Consensus Operationen zu reduzieren und Transaktionen “lokal beweisbar” zu machen, mittels dezentraler "Peer-to-Peer-Technologien".

Hohe Performanz-Anforderungen können auch beim Zugang zum Metaverse entstehen: Virtual- und Augmented-Reality-Technologien, 360-Grad-Kameras oder 3D holographische Displays, können Bandbreiten in der Größenordnung von mehreren Terabit pro Sekunde erfordern – mehr als heutige 5G Netzwerke bieten. Aktuell wird sehr aktiv an 6G Kommunikationstechnologien geforscht, insbesondere auch in Deutschland.

13.4 Governance

Während im Web2 die Benutzer:innen noch abhängig von der Governance großer Firmen waren, sollen die Benutzer:innen des Web3 direkt involviert werden können. Welche Form diese Beteiligung haben wird, hängt von der Plattform ab und ist Gegenstand aktueller Debatten. Eine zu fein-granulare Beteiligung der Benutzer:innen, zum Beispiel zu technischen Detailfragen, kann diese überfordern und zu geringer Stimmbeteiligung führen.

Ein interessantes Konzept bietet dazu die "flüssige Demokratie", welche es erlaubt, die eigene Stimme entweder persönlich abzugeben, oder an eine andere Entität zu delegieren. Anders als bei einer traditionellen indirekten Demokratie, bei der Repräsentanten für alle Themen und für eine mehrjährige Periode gewählt werden, erlaubt eine flüssige Demokratie den Beteiligten die Stimmübertragung jederzeit zu widerrufen und auf bestimmte Themenfelder oder sogar individuelle Abstimmungen und Wahlen zu beschränken. Dies soll in einem evolutionären Prozess die Stimmen bei kompetenten Entscheidungsträger:innen anhäufen. Aktuell wird auch untersucht, mit welchen Anreizsystemen Benutzer:innen zum Abstimmen motiviert werden können.

Eine verwandte Frage ist, wieviel Stimmrecht ein Benutzer haben soll. Ein Ansatz könnte sein, die Stimme des Benutzers proportional zu seiner Anzahl Tokens zu zählen. Allerdings sind Tokens oft sehr ungleichmäßig über Benutzer:innen verteilt, was zu "rich getting richer" Phänomenen führen kann. Ein alternativer, "Per-Person-Ansatz" kann technisch schwierig umzusetzen sein und bedarf eines "Proof of Personhood": Es muss möglich sein, sogenannte Sybil Attacken zu verhindern, wo sich ein Benutzer als mehrere Personen ausgeben kann. Diese Anforderung kann auch in Konflikt stehen mit der Anforderung von Anonymität von Benutzer:innen. Existierende Technologien wie Computational Puzzles sind in der Praxis aber oft teuer und unpraktisch.

13.5 Tokenization und Ownership

Im Web3 können Benutzer:innen selber bestimmen respektive mitbestimmen, wie ihre Daten genutzt werden, und von deren Monetarisierung profitieren. Eine wichtige technologische Herausforderung hier betrifft die Verwaltung der Ownership: Während heute zum Beispiel Grundbucheinträge oft föderal organisiert sind (z.B. pro Gemeinde oder Land), sollen im Web3 Ownerships global und redundant gespeichert werden, selbst für kleine Tokens und potenziell für sehr lange Zeit. Dies führt nicht nur zu großen Datenmengen und somit Herausforderungen für die Skalierbarkeit wie oben diskutiert, sondern bringt auch Anforderungen an die Langlebigkeit von Speichermedien und die Verfügbarkeit von Geräten zu deren Verarbeitung. Wie eine sehr langfristige und "dichte" Speicherung von Information erfolgen kann, ist eine aktuelle Forschungsfrage.

Das Speichern von Keys ist besonders interessant: Aufgrund der dezentralen Natur des Web3 haben Benutzer:innen plötzlich eine große Eigenverantwortung, die Sicherheit ihrer Daten sicherzustellen – dies ist eine der Hauptherausforderungen dieser neuen Technologie. Einerseits müssen Schlüssel sicher gespeichert werden und sollten zum Beispiel nicht übers Internet gestohlen werden können. Andererseits soll es aber auch möglich sein, Schlüssel weiterzugeben, zum Beispiel soll es möglich sein, Tokens an Nachkommen zu vererben. Wichtige Technologien hier basieren auf Key Sharing und Threshold Kryptographie, welche es erlauben, Schlüssel auch redundant und somit fehlertolerant zu verwalten. Viele neuartige Dienste, wie Custody Solutions, bieten Lösungen zur Schlüsselverwaltung, allerdings zum Preis einer neuen Abhängigkeit von den Dienstanbietern, welche wiederum gegen die Idee des Web3 sprechen kann.

Die Regulierung solcher neuartiger Systeme erfordert ebenfalls neue Technologien. Insbesondere erfordert eine automatisierte Regulierung klare

formale Definitionen, die sich auf Smart Contracts abbilden lassen. Außerdem muss es möglich sein, steuerbare und rechtlich relevante Ereignisse automatisiert feststellen zu können.

Je nach Gebiet kann Web3 in Zukunft auch die Durchsetzung von Rechten unterstützen. Zum Beispiel wird erforscht, wie benutzerspezifische digitale Wasserzeichen erstellt und verwendet werden können, um Urheberrechtsverletzungen mit Authentizitäts- und Integritätsgarantien von Blockchain-Plattformen zu verfolgen.

Je dezentraler ein System jedoch ist, desto mehr wird es sich mit Herausforderungen mit Akteuren in unterschiedlichen Rechtsprechungen auseinandersetzen müssen. Es stellt sich zum Beispiel die Frage, wie der Zugang zu Material, welches in bestimmten Ländern verboten ist, eingeschränkt werden kann, wenn die Betreiber der Maschinen wegen der oben beschriebenen Verschlüsselungs- und Berechnungs-Technologien gar keine Kenntnis vom Inhalt haben.

13.6 Diskussion

Die meisten diskutierten Technologien haben das Ziel, die vom Web3 angestrebte Dezentralität zu erreichen. Es gibt allerdings viele praktische Aspekte, die in der Realität zu einer Zentralisierung führen können und dadurch beispielsweise eine Zensur ermöglichen. Wenn Infrastruktur nur auf einer kleinen Anzahl Betreiber läuft (z.B. nur auf einer Handvoll Cloud Providern) oder nur durch eine kleine Anzahl Internet Service Provider verbunden ist, wenn die Maschinen nur in wenigen Staaten betrieben werden oder an Abstimmungen nur “Power-User” teilnehmen oder die größten Token Holders überproportional viel Gewicht erreichen, kann das in der Praxis den Zielen des Web3 widersprechen.

Zusammenfassend haben Web3 und Metaverse das Potenzial, unsere Gesellschaft nachhaltig zu verändern. In vielen Bereichen sind die wissenschaftlichen Grundlagen für diese Veränderung bereits vorhanden, zum Beispiel dank moderner Kryptographie. Wichtige Fragen sind aber aktuell noch nicht zufriedenstellend beantwortet, insbesondere zu den "menschlichen Faktoren". Parallel zu den rechtlichen Grundlagen müssen effiziente Technologien entwickelt werden, die es den Benutzer:innen einfach machen, sich intuitiv und sicher in den neuen digitalen Welten zu bewegen. Eine weitere spannende Frage betrifft inwiefern verschiedene Metaverses und Blockchains zusammenarbeiten werden und sich ergänzen können – und gleichzeitig ihre Unabhängigkeit bewahren.